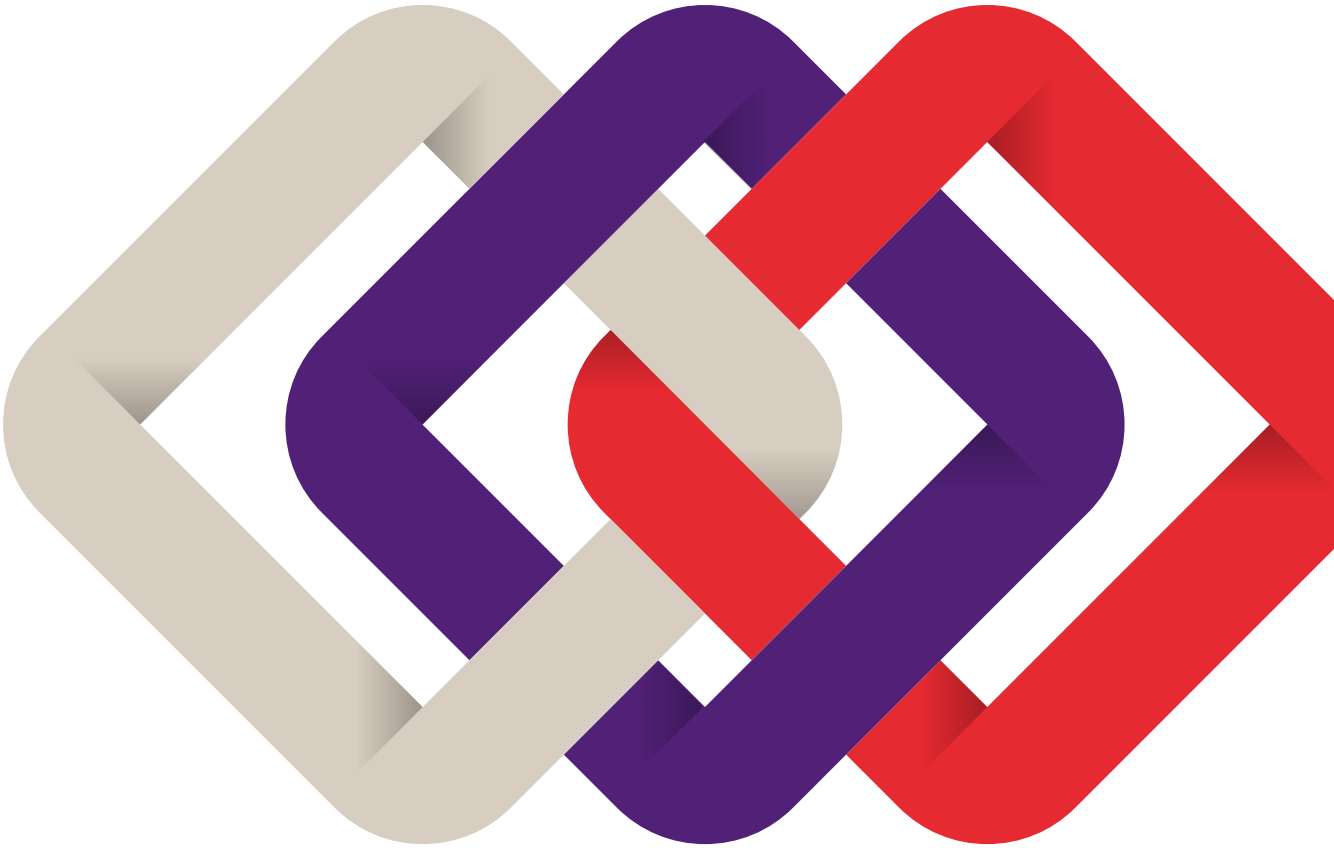
Grant Thornton

An instinct for growth™

Managing operational risk

Understanding the sources and minimising the impacts



Operational risk

Operational risk impacts all of your organisation all of the time and is unavoidable.

It does not depend on the size or nature of the business, but it can bring even the biggest organisations to their knees.

Understanding the causes of operational risk is a real challenge since these causes can be complex and subtle – or blunt and brutal. There are internal sources of operational risk and these can be understood in detail and managed. But there are external sources of risks too – as we have seen many times in the headlines. These external risks are uncontrollable and often unpredictable.

History has shown us that the impacts arising when operational risks materialise will always exceed the bare cost of the operational loss event itself – often very substantially.

If you can't avoid the risks, you can limit their impact on your business. To do that requires the classic elements of risk measurement and management. But it needs more. You must have the right tools and talent to fully understand the risks, to allocate your control resources, and to prepare for the worst.

And that's where we can help…

Operational risk — **everywhere, always**

We have the tools and the talent to help you manage and mitigate operational risks and avoid the losses they lead to. We have a market-leading breadth of experience in all aspects of operational risk management that allows us to provide our clients with true insight and innovation.

Our ability to deliver the current best in risk management advice and support, together with a far-reaching view of the road ahead has proven itself invaluable to all corners of the financial services industry.

Operational losses cause reputational losses.

Avoiding losses

Organisations underestimate the importance of operational risk management, and poor operational risk management can lead to three types of damage to a business:

1. **Outright loss** – the complete direct cost of a loss event, such as from loss of assets or processing errors
2. **Regulatory overhead** – operational losses are a critical consideration when regulators and external assessors take a view of an organisation. Operational risk events may lead to greater scrutiny and expensive mandated investigations (such as Section 166 reviews)
3. **Reputational damage** – this is a risk of a risk. It arises from operational risks and its impact can be unquantifiable making it potentially fatal for your organisation

Such losses are a result of a failure to embed an effective operational risk management framework in the business. For operational risk management to be effective there must be focus from all levels of management. But operational risk management – and accountability – can often be compartmentalised and assessed differently across business functions, which in turn leads to critical inconsistencies of treatment.

To combat this, an organisation must have a risk framework that translates the organisation's strategy into tactical and operational objectives, assigning responsibility throughout the organisation with each manager and employee fully accountable for the identification and control of risk as part of their job description.

It is essential for such a framework to fully reflect the organisation's risk culture – the tone from the top – and to be comprehensive enough to ensure consistency in measurement and management. So, as operational risks arise from such a wide variety of sources, risk management must be aligned and fully embedded within all parts of the business in order to be effective, including:

- business strategy
- business plan
- risk appetite
- procedures and policies
- organisational culture.

Check your account

Operational events that make the headlines are hard to miss. But the breadth of causes and consequences is telling.

A major UK retail banking organisation suffered a major computer meltdown that led to a failure in its network of cash machines, online and phone services. A string of operational risks had crystallised and interacted and ended up locking millions of their customers out of their bank accounts. On its own this was unacceptable, but it was the second major outage in 12 months, making it catastrophic.

Following the crashes in its systems, the bank's management were obliged to make an apology to their customers – and settle £70 million of compensation claims, followed by a £56 million fine levied by the Bank of England.

Software upgrades were cited as a cause – which is true – but the failures led from a combination of operational risks including a lack of alignment between operational risk management and the group's change, information technology and customer conduct strategies. The risk functions had not gauged the risk and impact of the network failures and no-one joined the dots to be able to anticipate the outcome.

Why do we need operational risk management?

- Credit ratings are built on a keen analysis of an organisation's risk management capabilities and demonstrating high quality operational risk governance provides for often substantially more favourable credit ratings and corresponding reductions in overall financing costs
- Operating costs can be significantly reduced by systematically identifying and mitigating potential risks before they can lead to a loss
- Operational risk management is necessary to prevent large and unexpected spikes in costs and profits and is essential for avoiding major hurdles to meeting revenue targets
- Sophistication in measuring operational risk is vital to ensure accurate and optimum capital is held
- Good operational risk management supports the overall risk culture which is a critical feature of modern and efficient organisations. Furthermore, a strong sense of ownership of risk management fostered throughout your staff has been shown to promote staff engagement and retention. The benefits extend further to the customer base who prefer safely controlled businesses
- Certain operational risks can be insured and a careful identification and quantification of these risks can help to provide additional guards against the cost of operational events, as well as generating savings in insurance premiums
- The extent and pace of regulatory change is itself presenting risks, not least from overloading all staff with changing processes and control objectives. A sound risk framework is critical to absorbing the impacts of major regulatory and other change projects throughout the organisation.

"When it comes to operational risk, many firms only see the tip of the iceberg."

Building the framework

Enabling better decisions comes from having a two-way view.

Forward

To the type of control framework that properly fits an organisation's risk appetite and risk culture, and to the types of scenarios that the organisation may face tomorrow.

Backward

To ensure the lessons from the organisation's past have been digested and controlled for. To fail once is perhaps unfortunate and your shareholders might have some tolerance; to fail twice is unforgiveable. Similarly, risk managers should look not only to the loss event history from their own organisation, but must consider the events that have affected their peers both near and far. To fail to learn from the mistakes of others might also be considered unforgiveable when it comes to operational losses.

One of the functions of a well-embedded risk management framework is to ensure the right information is delivered to the right people at the right time so managers are in a better position to make educated decisions.

To support this, the risk manager must have a range of tools and data sources at their disposal, including:

A comprehensive risk register

- The foundation of the risk control environment is the risk register. Here we can build a picture of the challenges facing the organisation and ensure that the right managers are accountable for the controls set against them. It also forms the basis for the self-assessment of the effectiveness of the operational control structures.

Loss data

- To build a true cost of operational losses and to anticipate the likely impact of current risks to the organisation requires a well-structured and complete record of the organisation's loss events. But beyond internal losses, the organisation must cast a wide net across the sector it operates in to collect and digest loss data from other organisations. Only with a view of internal and external event data can we begin to build meaningful risk assessment models and tailor a control framework around them.

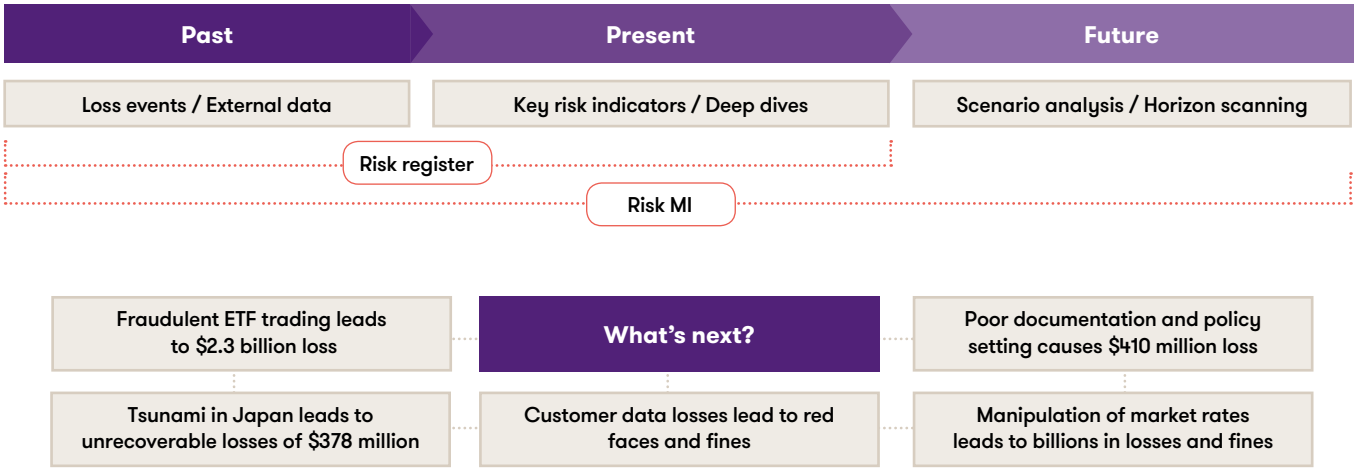
Management information

- The management information (MI) must work for the organisation. It must have sufficient breadth to capture all the risks of interest and this requires sophisticated analysis of correlations and dependencies to describe emergent risks arising from staff behaviours. A well-planned data analytics approach is critical to ensure the subtleties of complex operational risks are not overlooked. For instance, a fraud may be detected only by linking hordes of correlated data points. And for a data-analytics approach to surveillance to work, there must be a full consideration of the pros and cons of delegated and retained authority models. Do we opt for centralised support teams to collate data, operate controls, and pass exceptions to accountable supervisors, or is a distributed model more appropriate where control and monitoring functions are performed by supervisors themselves?

Building the framework

continued

Finally, all of the organisation's risk management functions must have an eye to the future. What is the next challenge facing a function or process, the organisation as a whole, the sector it operates in, or beyond?



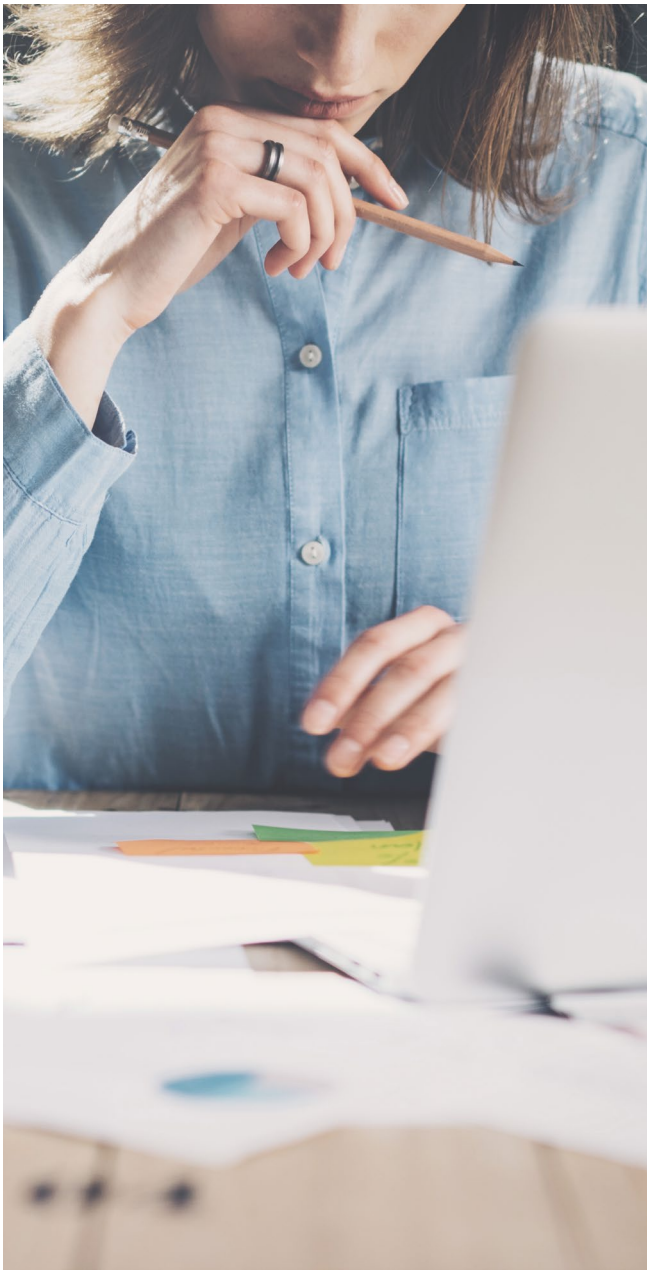
How do you grasp a cloud?

The scope of operational risk is enormous and as the risk management framework evolves, the volume of information that the organisation can provide becomes ever more immense.

There is a real danger that those tasked with identifying and preventing the next risk event are swamped and begin to lose sight of real risk events. The board will always want to know what is important, what is next, and what are we doing about it. So one of the priorities for risk management framework is to have a careful definition of what operational risk is for the organisation and how to filter all of the data it can collect that describes those risks and the controls against them.

There are many ways to classify operational risks and this might be the first step in understanding the sources for your organisation. One of the most straightforward and hence consistently used classifications of operational risk has been provided by the Basel Committee on Banking Supervision (BCBS). The committee defines operational risk as 'resulting from inadequate or failed internal processes, people and systems, or from external events.' This includes legal risks, which greatly expand the scope of an operational risk management framework, but importantly they exclude reputational and franchise risks, which has led to gaps in quantifying operational risk impacts.

BCBS goes on to present seven categories of operational risks and for each one there are a number of contributory factors. This approach leads to a common pitfall encountered by operational risk managers across the financial services sector which is the tendency to 'box up' operational risk and ignore the individual risk components. This can leave an organisation exposed to unforeseen risks and furthermore can introduce a sense of blinkered complacency throughout the organisation: 'all the KPIs are green – we're doing fine!'



Risk types

Internal fraud

Events intended to defraud, misappropriate property, or circumvent regulations or company policy, involving at least one internal party, categorised into unauthorized activity and internal theft and fraud.

External fraud

Events intended to defraud, misappropriate property, or circumvent the law, by a third party, categorised into theft, fraud, and breach of system security.

Employment practices and workplace safety

Acts inconsistent with employment, health and safety laws or agreements, categorised into employee relations, safety of the environment, and diversity and discrimination.

Clients, products, and business practices

Events due to failures to comply with a professional obligation to clients, or arising from the nature or design of a product, which include disclosure and fiduciary rules, improper business and market practices, product laws, and advisory activities.

Execution, delivery, and process management

Events due to failed transaction processing or process management that occur from relations with trade counterparties and vendors, classified into categories such as transaction execution and maintenance, customer intake and documentation and account management.

Damage to physical assets

Events leading to loss or damage to physical assets from natural disasters or other events such as terrorism.

Business disruption and system failures

Events causing disruption of business or system failures.

Sources and causes

	Internal fraud	
Sources	Credit fraud	Insider trading
	Theft, embezzlement, robbery	Misappropriation of assets
	Unauthorised transactions	Intentional mismarking of position
	Bribery and corruption	
Causes	Lack of control	Omissions (eg failure to supervise employees, inadequate due diligence efforts)
	Employee action/inaction	Organisational structure - excessive concentration of power
	Management action/inaction	Changes in market conditions
	Poor corporate governance, flawed corporate strategy	

	External fraud	
Sources	Theft, forgery, and robbery	Cyber crime - system security and hacking
Causes	Lax security	Employee inaction/inaction
	Lack of internal control	Changes in market conditions
	Management action/inaction	

	Employment practices and workplace safety	
Sources	Employment discrimination	Safety of environment
	Compensation, benefit, termination issues	Organised labor activity
Causes	Management action/inaction	Staff selection and compensation
	Lack of control, insufficient policy and guidance, weak compliance oversight, etc	Corporate governance
	Employee action/inaction	Other or unspecified

	Clients, products and business practices	
Sources	Suitability, disclosure, and fiduciary (eg disclosure issues, lender liability, fiduciary breaches)	Improper business and market practices (eg unlicensed activity, money laundering, market manipulation, improper trade, antitrust)
	Other (eg misuse of confidential information, advisory activities)	
Causes	Omissions (eg lack of proper training procedures, inadequate due diligence efforts, failure to supervise employees)	Changes in market conditions
	Management (or employee) action/inaction	Employee action/inaction
	Organisation structure, excessive concentration of power	Failure to correctly respond to new technology

Sources and causes

continued

	Damage to physical assets	
Sources	Terrorism, vandalism	Natural disasters
Causes	Changes in market conditions	Strategy flaws
	Employment action/inaction	

	Business disruptions and system failures	
Sources	Software failures	Telecommunications
	Hardware failures	Utility outage/disruptions
Causes	Poor management oversight including inadequate technology planning	Lack of internal control
	Employee inaction/inaction	Changes in market conditions
	Management action/inaction	

	Execution, delivery and process management	
Sources	Transaction execution and maintenance (eg accounting error, data entry error)	Customer/client account mismanagement
	Failed or inaccurate mandatory reporting	Other (eg losses due to new market regulations, strategy failures, mergers and acquisitions)
Causes	Lack of control (eg poor documentation, lax security, insufficient compliance measures, failure to test for data accuracy)	Changes in market conditions
	Omissions (eg failure to supervise employees, inadequate due diligence efforts)	Strategy flaws
	Management action/inaction, poor execution	Lack of control
	Employee action/inaction, misdeeds, errors	Management action/inaction
	Change in market conditions (eg mergers and acquisitions, regulatory pressure, financial reporting)	

What we do

We have expertise that extends right across all aspects of operational risk management. Our team have market-leading experience gained from leading roles throughout the financial services sector.

We can help with all stages of the operational risk lifecycle from building and developing frameworks from first principals, to helping optimise the business as usual management of operational risks, and facilitating your business to interpret and respond to the many changes in the market and the rules that govern it. We have helped some of the largest and most complex organisations in the world understand and deal with the operational risks they face and we have consistently helped our clients to avoid the costs of risk. Our credentials extend across three broad categories:

Advisory and consultation

Helping firms to decode new legislation and the causes of their operational risks, then developing and embedding commercially effective risk control structures.

Comprehensive assurance

Work to fully describe the effectiveness of existing risk management structures and provide an organisation's various stakeholders with the confidence that operational risk is understood and managed.

Resource support

Bringing our staff to support organisations during periods of peak demand or in the wake of risk events. Our team consists of industry experts who have worked in risk management roles so can begin adding value right from the start.

"We have helped some of the largest and most complex organisations in the world understand and deal with the operational risks they face and we have consistently helped our clients to avoid the costs of risk."

Contact us

Sandy Kumar
Chair of Financial Services Group
Head of Business Risk Services UK
T +44 (0)20 7865 2193
E sandy.kumar@uk.gt.com

Paul Young
Managing Director
Business Risk Services
T +44 (0)20 7865 2781
E paul.l.young@uk.gt.com

Anthony Ma
Senior Manager
Business Risk Services
T +44 (0)20 7184 4796
E anthony.k.ma@uk.gt.com

Grant Thornton

An instinct for growth™

grantthornton.co.uk

GRT106816