Executive Guide:
The Business Value of Operational Risk Management
Can you afford to manage a business without knowing the risks? Of course not. But suppose you decide – for whatever reason – to not take risk management very seriously. What could happen? Naturally, your business could fail; that’s probably the worst case. Your business could be acquired by someone else who extracts the worthwhile parts and employees and scraps the rest.

The business could simply float along in the river, doing very little but still surviving. Could your business also magically become successful without risk management? Anything is possible, of course, and it would probably be the stuff of MBA team projects or business books.

Now that we’ve established that risk management could play a role in your organization’s present and future, let’s identify the activities that you should follow if you want to do it right. First, it’s essential to have senior management buy-in and support. Next, you’ll want to be sure you understand how your business functions at an operational level. This means examining things like supply chains, business processes, staffing, finances, and competition. In other words, you must really understand the ins and outs of your organization and how it operates. This way you can better identify where risks and vulnerabilities may exist.

Next step is to conduct an operational risk assessment, which means you identify internal and external risks, threats, and vulnerabilities; evaluate their likelihood of occurring and their potential impact to the firm; and then identify how you’ll deal with them. Once you’ve identified risks and threats and their impact on the organization, decide how you’ll deal with them. You can accept them, mitigate them, or avoid them. This is where things like insurance can be used to accept and/or mitigate risks.

More importantly, use the model developed by the U.S. Department of Defense, which defines operational risk management (ORM) as the following principles:
Management

Business Without It

- accept risk when benefits outweigh the cost
- accept no unnecessary risk
- anticipate and manage risk by planning
- make risk decisions at the right level

If you can clearly see, through analysis, that the potential outcomes (e.g., increased revenue) of a specific risk or threat are more significant than the cost needed to manage the risk, then the decision should be to assume the risk. And if you have performed a sufficiently robust risk analysis, you should be able to identify most operational risks and vulnerabilities, further be able to identify those situations that clearly will not benefit your organization, and then manage through those risks. Risk data can and should be used to enhance planning activities. After all, if you know where risks exist, you ought to be able to design business plans that address the risks, avoid them, or leverage them to your advantage. Finally, it’s essential to know at what level business decisions need to be made in an organization. Results of the risk analysis may indicate that some decisions won’t need to be escalated to the highest levels in the company, while others clearly must have top-level management approval.

In summary, a successful business should regularly assess its risks, no matter how well the company is performing. In fact, probably the best time to take a closer look is when things are going well. This way you may be able to identify a situation that – at the moment – is under the radar and would otherwise be considered of little consequence. And ignorance of such a situation could lay the groundwork for a business-ending catastrophe. Don’t wait until operations are going under. Schedule and conduct regular risk assessments to keep your business running at its best.

By Paul Kirvan, CISA, FBCI

Paul Kirvan, CISA, FBCI, is an independent BC/DR/IT audit consultant with more than 25 years of experience. He is a founding member and secretary of the Business Continuity Institute’s USA Chapter and a former director of the BCI’s international board.
The Business Value of Operational Risk Management

Operational risk management (ORM) is more than knowing how to evaluate risk. It is a continuously-repeated process which includes risk assessment, risk decision-making, and implementation of risk controls that result in risk acceptance, mitigation, or avoidance.

ORM is more complicated than a basic definition. According to the Global Association of Risk Professionals (GARP), operational risk management takes on many meanings depending on the industry or framework. A few examples of the different definitions are listed below.

In its international standard for banking regulators, the Basel Committee on Banking Supervision defined operational risk as the risk of loss resulting from inadequate or failed processes, people, and systems or from external events. Known as Basel II, this definition includes legal risk but does not address strategic and reputational risk.

The U.S. Navy summarizes the principles of ORM as:
- accept risk when benefits outweigh the cost
- accept no unnecessary risk
- anticipate and manage risk by planning
- make risk decisions at the right level

The international standard on risk management, ISO 31000, takes a broader, more generic definition:
- risk management: coordinated activities to direct and control an organization with regard to risk
- risk management process: systematic application of management policies, procedures, and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring, and reviewing risk

No matter how it is defined, operational risk management plays a vital role in all of an organization’s processes and must be part of the overall enterprise business improvement strategy. The International Organization on Standardization (ISO) has recognized the importance risk plays and is re-working many of its management system standards to encourage “risk-based thinking,” replacing the need for “preventive action” with “actions to address risks and opportunities.”

ORM is not a standalone activity carried out by a company’s risk experts; it is part of the responsibilities of management and a concern to all of the organization’s stakeholders. Risk identification and management are vital to strategic planning, project development, and change management. Correctly instituted, ORM is a cross-functional and dynamic process that is critical in helping decision-makers reach informed choices based on facts and data, not opinions. It helps management prioritize actions and distinguish the best route amid alternative courses of action.

The benefits are many, but ORM, once implemented, facilitates reducing operational and compliance costs and provides a detection system that will help reduce future exposure to risk.

Reduction of Operational Cost/Loss

Only through understanding and taking certain risks can an organization grow, and growth requires capital. However, capital can be a rare resource. Each risk taken requires a corresponding level of capital. Less capital, therefore, equals less growth capacity. The more organized a company can be from an operational risk perspective, the more capital it has available to invest in profitable growth activities.

Lower Compliance and Auditing Costs

Regulatory compliance is a basic part of doing business. Non-compliance can be an expensive proposition; it diverts the organization’s attention from normal operations, attract-
ing scrutiny from regulators which can result in additional fines, repetitive audits, potential legal action, and bad press. Compliance can be a source of competitive advantage, but non-compliance can be an advantage for competitors. Operational risk management plays a critical role in helping to assure regulatory compliance by identifying all applicable regulatory areas of concern, status, and associated risk levels.

**Early Detection of Unlawful Activities**

With the plethora of security breaches recently, both internal and external, instances of unlawful activities and misconduct remain a constant threat to public trust.

As part of an organization’s governance structure, fraud is one of the critical areas that should be addressed during development of an ORM process. Senior management and even the board of directors should be involved in conveying expectations regarding the risk of fraud and security violations.

In order to ensure early detection, specific continuous monitoring policies and procedures should be considered. Prevention procedures need to be established to reduce the impact on the organization, and detection techniques should be established to uncover events when preventive measures fail or unmitigated risks are realized.

Tahir Abbas, an expert in financial internal audits and risk management from the University of Lahore and a member of the Association of Certified Fraud Examiners, provided some guidance during a fraud risk assessment workshop regarding some strong anti-fraud controls that should be considered, including:
- proper separation of duties
- use of authorizations
- physical safeguards
- job rotations

**Reduced Exposure to Future Risks**

Of course, once an organization has assessed its current status and addressed, prioritized, and taken action on the current risk profile, the ultimate goal is to reduce or even eliminate exposure to future risks. This requires the real-time process of continually assessing the inputs and outputs of an organization, improving and applying lessons learned, and building an intelligent knowledge database. As illustrated below, the more an organization learns and applies ORM, the stronger and more resilient the organization will be.

The ongoing integrated process of identifying, assessing, and responding to risk is effective operational risk management. Successfully managing risk involves evaluating the likelihood that an event will occur and the resulting impact. With this information, organizations can determine the acceptable level of risk for delivery of products/services and express it as their risk tolerance.

There is no one-size-fits-all approach to managing operational risk, but we do know that it is important to leverage the proper balance of training, standards, and tools and incorporating all the key people, processes, and technology in order to have the best chance of success. Organizations will continue to have unique risks, threats, vulnerabilities, risk tolerances, and how they implement ORM practices will vary. The key is to determine activities that are important to critical service delivery and prioritize investments to maximize the impact of each dollar spent. Ultimately, operational risk management is aimed at reducing and better managing risks while increasing efficiency and profits.

**John DiMaria** is a BSI certification portfolio expert, HISP, MHISP, Six Sigma Black Belt, and a certified Associate Member of the Business Continuity Institute with more than 30 years of experience in management systems and international standards.
Certificate of the Business Continuity Institute (CBCI)

BCI Certification is an internationally recognised stand-alone credential leading to the post nominal designation of CBCI – Certificate of the Business Continuity Institute. Certification is gained through taking the Certificate of the BCI Examination which tests the candidate’s knowledge of the prescribed Body of Knowledge, the BCI’s Good Practice Guidelines – a guide to global good practice in Business Continuity.

Diploma of the Business Continuity Institute (DBCI)

The BCI Diploma is an academic qualification leading to the post nominal designation DBCI – Diploma of the Business Continuity Institute. The Diploma is delivered via distance learning in partnership with Bucks New University.

For more information on BCI CERTIFICATION go to www.thebci.org
www.bucks.ac.uk
Email or call on education@thebci.org.
703 891 6780

For all information on BCI TRAINING go to www.thebci.org
Email or call on education@thebci.org
703 891 6780

Business Continuity Institute Training

The BCI offers world-class, high-quality training, delivered by BCI licensed training partners located around the globe. All our training partners are experienced and respected Business Continuity professionals, bringing a wealth of real-life experience to the classroom.

Four days plus optional exam

The official Good Practice Guidelines (GPG) course is the most comprehensive, complete review of Business Continuity concepts and industry good practice from around the world and serves as the foundation for the Certificate of the BCI examination. The Good Practice Guidelines Course covers the six Professional Practices, taking students through each stage of the BCM Lifecycle.

Introduction to Business Continuity

This course is delivered over 1.5 days and is a basic introduction to the world of Business Continuity. It is designed as a first step for newcomers who need to have a good understanding of the subject.

**Business Continuity Institute Membership**

Statutory membership of the BCI provides BC professionals worldwide with:

- International recognition and status through accreditation.
- Assurance of technical and professional competency in business continuity

BCI members enjoy benefits including:

- Networking opportunities, face to face and online.
- A wide range of tools and resources
- Member-only offerings such as the Mentoring Programme, Consultancy Register and CPD system
- Free downloadable GPG and discounts to training and events

Use your CBCI or DBCI to apply. Or did you know that you can apply through our Alternative Route to Membership using the ABCP, CBCP or MBCP credentials? For more information on either route, please contact us, or come to visit our booth.

---

**About BCI Corporate Partnership**

The BCI Corporate Partnership enables organizations to work more closely with the BCI to help raise the profile of Business Continuity management as a discipline within their organization and to promote the highest standards of professional competence in BC in organizations working in any sector worldwide.

---

**Annual North American Awards**

Don’t miss the forth Annual North American Awards – exclusively at DRJ Spring 2015!

See [www.thebci.org](http://www.thebci.org) for more information
Senior Practitioners Invited to Take Part in the Senior Advanced Track at DRJ Spring World 2015

The extremely popular Senior Advanced Track is back this Spring in Orlando. This year, we are building an even better experience for business continuity planners at DRJ Spring World 2015.

The theme of this special report was designed to coincide with the same topic, The Business Value of Operational Risk Management. Senior practitioners are invited to attend the one-day track on Monday, March 23, 2015, as part of your regular conference experience. Look for further details at www.drj.com/spring. If you are interested in attending, contact senior-track@drj.com to learn about the requirements.

The Senior Advanced Track will feature a general session panel discussion in the morning and three breakout sessions in the afternoon, separate from our general offerings to attendees. This one-day track will conclude with an exclusive “Meet the Experts” reception in the evening. There is no additional cost for this specialized track.

Topics will reinforce the Senior Advanced Track theme – The Business Value of Operational Risk Management – and will include industry leaders, C-level executives, their top clients, and much more. Past attendees rave about the in-depth training they received during the Senior Advanced Track. Don’t miss your chance to attend this excellent track. Be sure to e-mail your qualifications now so you can be at the front of the line when qualified attendees are confirmed.

See the complete brochure for DRJ Spring World 2015 at www.drj.com/spring