Information risk management and compliance — expect the unexpected

M Drew

This paper sets out to demonstrate how establishing an effective information risk management programme is a key element in an enterprise's overall operational risk and governance programme. Establishing such a programme provides a golden opportunity to rationalise and align a number of processes and disciplines into an overall effective risk and compliance programme. This paper provides the opening steps for establishing such a programme to open up the possibility of such an opportunity. The business need has been created through legislation and regulation, accounting standards, best practice or contractual commitments for effective governance and appropriate risk management while meeting the need to generate profit and be cost effective. Aspects of financial risk, e.g. credit risk, are supported through mature processes and there is wide commercial experience in many of these finance related areas; however, other aspects of risk may be of such low frequency that little or no experience has been accumulated. For some risks the processes have not been developed to manage the risk — or where a risk management process is present, they are either immature or ineffective.

1. Introduction

The accelerated rate of global regulation change and security pressures has raised the awareness in all levels of management about risk, related controls, and their appetite for risk taking. Many organisations, at all management levels, struggle with risk management in general, together with experiencing difficulty in implementing meaningful processes, measurement, reporting and business risk strategies with regard to risk appetite. Few rational businesses have a risk appetite as such — they manage or accept risk, and some may seek risk through ventures, or may even buy risk (through financial derivatives).

The risk management methodology is not laid out, but sufficient detail is included to provide a framework by which an enterprise[1] can take the necessary steps to implement enterprise risk management (ERM) [1].

More specifically, additional detail is provided for a sub-component related to information and communications technology (ICT), which in this paper is termed information risk management. The HM Treasury's *The Orange Book — Management of Risk — Principles and Concepts* [2] (and associated framework [3]) states that risk is uncertainty of outcome, and good risk management allows an enterprise to:

- have increased confidence in achieving desired outcomes,
- effectively constrain threats to acceptable levels,
- take informed decisions about exploiting opportunities.

Observed results from an effective risk management capability are:

- a better understanding by all levels of management of the business processes,
- risk cockpit measurement and reporting empowers management to plan, do, check and act not only in the area of risk management but also of unexpected and crisis management events,
- better governance in many enterprises has resulted in improved effectiveness of operations leading to greater customer confidence and satisfaction,
- stakeholders have increased confidence in the enterprise's corporate governance and its ability to deliver.

2. The business issue

Regulation, together with the associated reporting, has reached a point where it has become a necessity and potential burden even for smaller enterprises. How it is approached can be seen as either a necessary evil and

[1] The term enterprise is used throughout this paper to encompass all forms and sizes of organisation (government, voluntary sector, private sector, and public organisations and associations/groups).

expense, or as an opportunity and differentiator. What are the drivers that have created this state of affairs?

Running any business represents a whole set of risks — some expected and well controlled, others unexpected near-misses or costly events. Good management is about taking risks and managing risk effectively. On the other side is the requirement created through legislation and regulation, accounting standards or contractual commitments for effective governance and appropriate risk management. These requirements and standards have been 'forced' on enterprises by successive governments because enterprises have failed to meet their obligations or reach acceptable standards. Aspects of financial risk, e.g. credit risk, are supported through mature processes and there is wide commercial experience in many of these finance-related areas. However, other aspects of peril (hazard) may be technology-induced or of such low frequency that little or no experience has been accumulated to manage them — nor in many cases have the necessary processes been developed to identify and manage these types of peril, and if processes are in place, they are likely to be limited in their deployment or effectiveness.

Additionally, there are a range of business risks beyond those related to regulatory compliance, reputation and customer ire. Each line of business in every enterprise has a number of perils (risks) some of which are beyond their control, e.g. market-place fluctuations. These external risks are known and often catered for within the business strategy, or with compensating processes, and are managed accordingly. Well-managed enterprises will have an inventory of risks within each line of the business. Each risk should have an owner and be periodically reassessed. However, there are broad ranges of risk that relate to information ICT that cross the lines of business. These have in the past been seen as the exclusive domain of the information or computer security function when they really belong to business as a whole. This will be developed further in section 4.

Mature enterprises have widened the remit of the information or computer security function to cover risk and compliance into a function known as information risk management (IRM). It acts in a compliance role to ensure the business functions own and manage risks related to both their own business processes and ICT-induced risks. Having this 'compliance' capability is an important distinction from each line of business managing its own risks, and accepting a particular ICT security risk within one part of the business that may not be acceptable in another line of business. Hence there is a need for a cross-functional compliance capability. A fragmented approach is often inconsistent and can be expensive, so rationalisation and aligning for effective compliance can offer cost savings and potentially unlock competitive advantage.

2.1 Expect the unexpected

The absence of evidence is not necessarily the evidence of absence, however. Donald Rumsfeld, former US Secretary of Defense, on 12th February 2002 at a Department of Defense news briefing [4], uttered what has now become a widely reported saying:

> As we know, there are known knowns. There are things we know we know. We also know there are known unknowns. That is to say we know there are some things we do not know. But there are also unknown unknowns, the ones we don't know we don't know. And if one looks throughout the history of our country and other free countries, it is the latter category that tends to be the difficult one.

While not eloquently stated, Rumsfeld's statement highlights that we should expect the unexpected and where risks affect life-safety or the survival of an enterprise, preparations should be made to remove or substantially mitigate the risk or to provide contingencies. Regimes should also be established that limit or compartmentalise operations, so that if they fail the whole enterprise does not fail as well. The vigilance employed in managing recognised operational risks inside an enterprise should not stop there, and consideration should be given to high-impact probable risks coming to fruition. The best public examples are Enron accounting practices, and Baring's rogue trader — each was a low frequency event that had a high impact on the business (causing it to cease trading) and no measures were in place to mitigate or limit the effect of the event.

Where do you start in expecting the unexpected?

An inventory of risks will provide the basis of the known risks, and ownership will focus management's attention on managing risk, and sensitise them to assessing for the unknown or emerging threats. This sensitising is, in effect, changing the culture and structure of the enterprise to risk. With experience of managing risk, managers will develop a risk appetite as to how they approach the treatment of the risk, and this will ultimately affect the approach and reporting of risk. In the following sections we will explore these aspects — inventory, ownership, organisation, culture, appetite, approach, reporting, and the results of this approach.

2.2 Developing an inventory of risks

COSO's ERM Integrated Framework[2] [5] talks about 'event identification' — where internal and external events affecting the achievement of an entity's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channelled back into management's

[2] COSO stands for Committee of Sponsoring Organisations of the Treadway Commission — a private organisation dedicated to improving the quality of financial reporting through business ethics, effective controls and corporate governance.

strategy or objective-setting processes. Within this paper this 'event identification' process should be used to develop an inventory of risks and classify them in terms of:

- opportunities,
- killer risks,
- other perils (hazards) that are requiring some level of control or management.

The risks each enterprise is likely to encounter fall into one of four categories:

- financial,
- strategic,
- operational,
- external perils (hazards).

Each category can be sub-divided with aspects appropriate to the type of enterprise.

The development of the inventory is not a one-off exercise but will require periodic reassessments across the business by the business process owners or their delegates against a set of criteria.

The options available to create the initial inventory of risks are:

- to engage a consultant/consultancy to, through a series of executive interviews, identify critical processes and their associated risks,
- for management to perform a self-assessment [6] within each line of business of the risks they face across all their processes,
- for the executive management to engage with the internal audit function in identifying risks within each line of business.

The first is a top-down approach, and provides a high level of sponsorship and focus to manage identified risks. However, it is likely to misdirect efforts away from significant risks known to, and managed by, middle and lower management. A bottom-up approach of self-assessment to identify and report risks requires significantly more effort. This approach relies on trust by staff that there will not be a 'blame culture' that will punish them in some way for declaring a weakness or failure (see section 2.5).

Using consultants or self-assessment or internal audit (or a combination thereof) are all potentially successful approaches to establishing an inventory of risks. The passage of time and performance of repeated assessments will refine and improve the inventory, and at least the reviewer of such assessments will know the boundaries of the risks.

2.3 Classifying risks

Risks can be classified as:

- opportunities — an event or a possibility due to a favourable combination of circumstances that gives rise to the chance for benefit,
- killer risks — an event or a possibility due to an unfavourable combination of circumstances that gives rise to the chance/hazard of a major loss or damage resulting in permanent cessation of operations,
- other perils — an event or a possibility due to an unfavourable combination of circumstances that gives rise to the chance/hazard of a loss or damage resulting in disruption of operations and possible financial losses.

They can be further segmented and grouped as:

- cross functional risks — those risks that are common to one or more lines of business, e.g. loss of reputation,
- business process unique risks — those risks only occurring within a specific operation/process within that line of business, e.g. withdrawal of a single product line for quality reasons.

Experience shows the relationship of opportunity to killer, to other risks, is of the order of 1: 15: 200. While these ratios are not empirically derived and will vary by business sector, they have been repeatedly observed in mature operations within the financial sector in the UK. That is to say, for large enterprises for each opportunity (e.g. competitive risk), there would be of the order of fifteen risks that threaten the survival of the enterprise (say, loss of a key building or staff), against the order of hundreds of other perils (such as an extended outage of an ICT service).

Opportunities should be channelled back into the management's strategy or objective-setting processes so that they can be capitalised upon where appropriate. Even if an identified opportunity is not adopted, management will be aware that the opportunity may be capitalised on by a competitor, thus creating a threat and risk to the enterprise. The enterprise strategy could then be modified to manage this particular situation.

Killer risks that threaten the survival of the enterprise require a focus of attention such that they will be fully treated to a level acceptable to executive management and stake/stockholders. These killer risks require continuous risk treatment, monitoring and reporting, so that when the level of risk changes (increases or decreases), the risk treatment can be modified to meet it.

The other perils require appropriate segmentation and evaluation to decide on the ownership, risk treatment, residual risk, measurement and, if required, reporting. This should represent the bulk of the risks. There will be common risks for each line of business. For example, the risk that the product line strategy proves ineffective within that line of business is owned and managed within that business. Similar risk may apply in each line of business, but they are independent of each other, and each would have a varying impact on the enterprise as a whole.

Some of the other perils are identical in each line of business, e.g. common processes or services such as loss of telephony. The ownership of these risks should be assigned to a service provider or central function who will be responsible to each line of business for the management of the risk.

2.4 Risk culture

Successful operational risk management relies heavily on an enterprise's attitude to governance. Some may see it as a necessary evil and expense, others may see it as an opportunity and differentiator. If it is seen as an opportunity and a differentiator, then almost certainly an effective risk and governance programme will result in a competitive advantage, and should yield savings (both through prevention of losses and improvement in processes).

It is therefore essential that the enterprise has the appropriate culture for risk management and governance. If senior and line management promote it as an opportunity and a differentiator, and encourage an open approach to risk identification and treatment, then staff will respond. If, however, the enterprise sees governance as a necessary evil, then almost certainly resistance will be encountered and a blame culture adopted for failure or weaknesses. Therefore the key factor is that senior management should positively promote and practice risk management and governance as a critical success factor for the enterprise.

2.5 Organisation (structure)

The necessary starting points to achieve a successful risk management programme are establishing the risk management organisation and risk ownership, supported by clear and simple processes. Far easier said than done, but an approach is described in section 4.

The risk management process organisation (see Fig 1) will rely on the culture of the enterprise for its success, so a critical success factor (CSF) will be changing or maintaining the enterprise's attitude to operational risk and risk management in general (including project management and management of change). This maintenance of the enterprise's culture must be an element in the processes adopted.

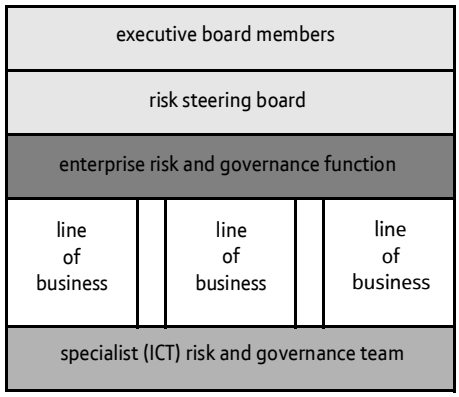

Fig 1 Risk management process organisation.

The structure adopted should be simple, and be accountable to the executive either directly or through a steering group formed from senior executives across each line of business within the enterprise. This steering group, or the executive, must assign ownership into the lines of business for risks and compliance. A policy of 'open reporting' of risks[3] is critical to the success of any risk management programme and governance. A steering group can perform an oversight function for the executive by challenging the reporting and assessments made by the business as appropriate. This oversight function will improve visibility, awareness and shared experience across the enterprise.

3. A twist to treating risks

Most practitioners in the risk management community are well versed in avoidance, reduction and the transfer of risk, and see risk acceptance as the weak choice [8]. Far better are the more assertive enterprises — while looking to treat risks in the classical manner, they are also more likely to set an appetite for risk that introduces a twist to the treatment of risk through multiple approaches, including accepting risk as part of the business environment.

- Risk avoidance

  This normally entails not performing an activity that could carry a potential risk. An example would be not installing an application on the system in order to avoid the vulnerabilities that are known to exist in it. While avoidance of all risks means that there is no exposure, avoiding all risks also means the limiting of the functionality of the system or additional expense that accepting them may have avoided.

- Risk reduction

  This encompasses methods that reduce the severity of an incident or the likelihood of it happening. Examples

[3] By open reporting, the author means a blame free culture for reporting weakness and failures at the earliest opportunity. Some organisations call this a 'whistle blower' charter [7].

include the patching of systems and the use effective access control mechanisms — firewalls and intruder detection systems designed to reduce the likelihood of a threat agent exploiting vulnerability. The balance must be drawn between the cost and the level of restriction on the functionality of the system, and the proportion of attacks that are detected or prevented. Other approaches such as simplifying the business process or reducing the elements of a process can also reduce risk as well as reducing cost. For complex processes, controls could be included at appropriate stages within the process to detect failure early so as to permit remediation or early treatment.

- Risk acceptance

  This is the approach where the impact that results from an incident is accepted when it occurs. Self-insurance is one aspect of risk acceptance. Risk acceptance can be a viable strategy for risks where the impact or the likelihood is small and where the cost of insuring against them or reducing them would be greater over time than the total potential losses sustained. All risks that are not avoided, reduced or transferred are accepted by default. This includes risks that are catastrophic and either cannot be insured against or, if they can, where the premiums would be unacceptably high. It should be noted that any potential losses over the amount that has been insured is an accepted risk. The residual risk that remains after actions to reduce the level of risk must be either accepted or transferred.

- Risk transfer

  This means transferring the risk to another party, typically by either contract or insurance. Liability among suppliers or other contractors is often transferred this way. In many cases, the treatment of risk will be a combination of the groups defined above, possibly with some of the risk transferred, or some partially mitigated with the residual risk being accepted. Avoidance is a rare exception and often undesirable. Suprisingly the minority of enterprises set out with a risk acceptance strategy whereby they balance their risk appetite [5] with effective management and acceptance of risk by line management.

- Appetite

  Effective management and acceptance of risk breeds a healthy attitude and culture for risk. An enterprise's risk appetite will tune and self-regulate line management's sensitivity to managing risks — it helps them select the risk treatment approach and balances the cost against value. A culture that avoids risks 'at all costs' is less cost-effective and probably less efficient and nimble at changes to processes. The 'gamblers' are those enterprises that refuse to pay the costs of treating risks that are not guaranteed (even if the probability is high) and they are unlikely to refine or maximise processes and are likely to succumb to failure. So the middle ground of balanced risk appetite with effective management (control) and acceptance of risk is an obvious choice to make.

  Risk appetite, while widely coined and used in the risk management community, does not have clear definitions that are commonly accepted and understood outside the financial services sector. The practitioners, as a result, have converted other risks into financial terms to provide a common measure enabling them to convey a risk in financial terms. Risk appetite is the amount of risk exposure, or potential adverse impact from an event, that the enterprise is willing to accept or retain. This risk appetite provides a threshold beyond which the enterprise will apply risk treatments and controls to reduce the risk exposure level to within the appetite of the enterprise.

  So the twist is not slavishly and prudently avoiding, reducing, transferring or accepting risk, but to consciously balance the value the enterprise is prepared to actively put at risk in order to obtain the benefits of the opportunity. In addition, they actively assess the scale of exposure that is tolerable and justifiable should the risk be realised.

  Some possible benefits of defining the risk appetite within an enterprise are that it will permit management:

  — to make informed business decisions,

  — to focus on the risks that exceed a defined threshold or appetite for risk,

  — to strengthen a culture with an awareness of risk and openness to report new risk,

  — to qualify a range between daring and prudence.

Putting a value on risk is a topic for consideration elsewhere, but there are a number of established methodologies available. An individual enterprise's line of business and market-place will dictate the appropriate level of complexity necessary for valuing risks. Typically the level of a risk will be measured by the likelihood of an incident occurring and the financial impact if it does. This is best done by capturing experts' opinions of loss severities and frequencies (using both internal and external expertise) and discussing with responsible management in each line of business individual loss scenarios and the total losses an enterprise could sustain as a result. The output of this business impact analysis will result in the benefits listed above.

4. An approach to effective risk management

The disappointing aspect is that there is no 'silver bullet' to permit establishment of an effective risk management

programme in an enterprise. Establishing such a programme is not a one-time activity but is a long-term set of inter-linked programmes of activity complemented by a compliance programme where the key drivers in deciding the initial and ongoing approach to managing risk are:

- to expect the unexpected,
- to establish an inventory of risks for each line of business,
- to create a risk management organisation and then establish enterprise-wide:
  - — risk culture,
  - — risk ownership,
  - — risk management processes,
- to decide with the lines of business their 'risk appetite' and thresholds beyond which the enterprise will apply risk management treatments and controls,
- to define risk strategy,
- to establish measurement and reporting processes (to executive, to staff, to stake/stockholders).

There are a number of additional sub-processes required to complete the picture that will become obvious as the programme is established. Before starting, it is essential that there is the appropriate sponsorship agreed and resources made available. Like the quality programmes of the 1980s the savings made will yield the resource to implement and manage the programme, although in the short term there may be a bubble of extra resources required before the resulting efficient, agile processes and better management decision making yields the savings.

The earlier references to 'expect the unexpected' is intended to make the point that no process is foolproof. Establishing the programme will significantly reduce the risks and improve awareness, but it cannot be expected to identify every eventuality (without prohibitive cost and probably detracting from the business operation), so expect and prepare for failure. This means having contingencies and a crisis management capability that, at a bare minimum, has mock rehearsals of crisis management or recovery exercises. This capability could and should be linked into a business continuity/disaster recovery programme.

4.1 Line of business inventory of risks

The operations of each line of business expose the enterprise to unique as well as common risks. The appropriate line management should be involved in the risk assessment process throughout and accept ownership directly of unique risks or be assigned ownership of common or joint risks. The risks each line of business encounters falls into one of four families:

- financial,
- strategic,
- operational,
- external perils (hazards).

Senior management should recognise and accept that the lines of business may require specialised support in certain areas, e.g. ICT. As stated earlier in section 2.2, risk identification requires business management to assess where internal and external events will affect achievement of an enterprise's objectives, distinguishing between risks and opportunities. This has to consider both abnormal events (expect the unexpected) as well as the known likely events that could disrupt operations, e.g. mergers and acquisitions.

There is a strong likelihood that similar risks will be found in each line of business. Where they need a unique treatment for that particular business then they should be retained within each line of business. However, some process or technology risks are common to several or all lines of business and can be treated centrally, e.g. PC software defects that result in security exposures. The inventory of risks should record each business line that has the exposure so that an overall assessment of the total value of the risk can be made.

4.2 Risk management organisation

The risk management organisation discussed in section 2.5 has to be based on the existing enterprise's structure and established corporate operations, with some central point owning the risk management process. The process owner should be responsible for enterprise-wide awareness of both the risk policy and processes. It is this central point that will cultivate the enterprise's risk culture, ensure continuous ownership and management of risks, and refine and assure the quality of the risk processes and reporting. For the cross-functional risks like ICT, the central point should ensure consistency of approach but not of implementation. For example, an ICT risk acceptable to the research and development or marketing function may be entirely unacceptable to the finance function of the enterprise.

Key to the success of the risk management organisation is that ownership of risk and risk management responsibility ultimately rests with management in the lines of business. The central function is there in an advisory and compliance capacity, not a 'performing' role. The exception being where common risks have been assigned to a specialist function such as treasury operations or the ICT security team.

4.2.1 Culture

A highly developed state of the knowledge and values shared by members of an enterprise can be termed the culture of the enterprise — the most important aspect of

which is the shared values. However, few managers and even fewer members of their staff are likely to have experience, or a working knowledge, of risk management — to the silent majority it is an 'unknown' entity with no shared value. Human nature being what it is, the unknown represents a possible fear in many ways — personal embarrassment, exposing personal credibility, weakening authority and so on. Lacking a shared value can increase the perceived risk. Therefore there is a critical need to raise the awareness and confidence of managers and staff as to both what risk management is about, and their individual roles and responsibilities. How readily the enterprise assimilates risk management depends on the underlying knowledge and shared value of risk management.

Earlier in section 2.2, the need for openness in declaring risks and issues was stressed. Endemic in some enterprises is a tendency to blame individuals when they highlight an issue. This must be strongly discouraged with respect to declaring weaknesses or potential risks. Identifying and declaring risks must be seen by all as a positive act when done at the earliest opportunity, and as a failure when deliberately covered up or ignored. When this is recognised throughout the enterprise, then a positive risk culture emerges. A process weakness or risk to a process should be seen as an opportunity to improve a process or to exploit a change for the better.

Instrumental in establishing and maintaining the required culture is the need for effective communications and awareness across the enterprise. A model example is provided in the 'Communicating Risk Tool-kit' [9].

4.2.2 Ownership

The many previous references to ownership hopefully convey the importance of ownership of risks and accountability for risk management. This ownership and accountability lies with management and their staff within the lines of business. Some risks may be centrally supported with specific expertise or skills, but that does not relinquish the ownership from within the lines of business. The manager closest to the operation can best assess the risks and controls appropriate within their operation for the majority of operational risks, with the exception of technology-related risks and some external process risks.

Ownership and accountability empowers line managers to decide whether to accept a risk or treat it in some way and accept the residual risk if any. Having identified operational risks, recording and reporting each risk with its 'total value' and its treatment to the central function discharges the main accountabilities, but ownership remains with the management in that line of business.

4.2.3 Processes

In section 2.2, the processes related to identifying, classifying and treating risks were introduced. For a model approach, refer to *A Risk Management Standard* [10] that lists examples both of risk identification techniques and of risk analysis methods and techniques.

The overall model risk management process in the standard is shown in Fig 2.

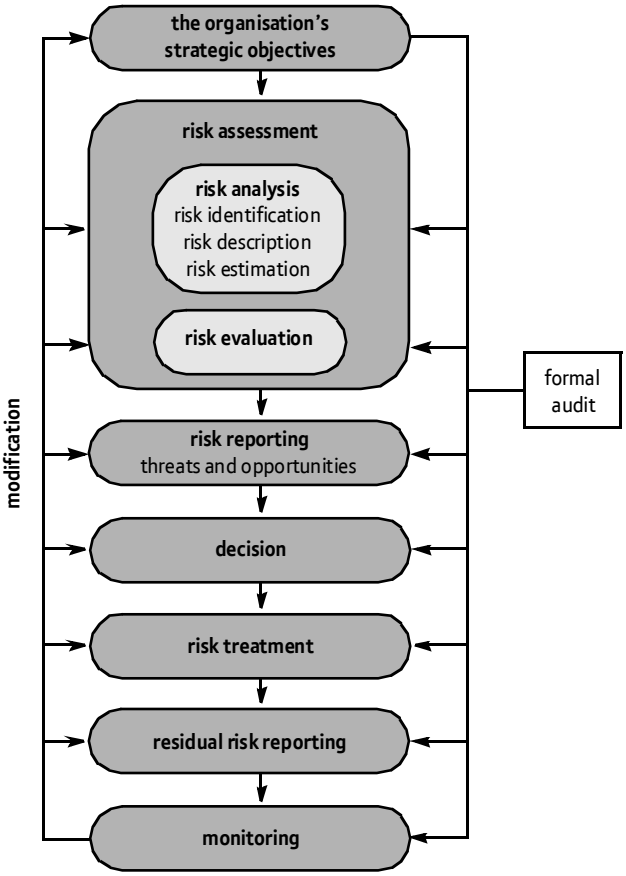

Fig 2 Extract from *A Risk Management Standard* [10].

While identifying, classifying and treating risks is problematic, there are a number of other processes that are key in ensuring success in managing a risk programme. Assessing the value of the risks identified within the enterprise comes a close second in difficulty to measurement and reporting.

As the risk programme matures in the enterprise, the role of automation in both data collection and managing workflow to prioritise and address the treatment of risks, will increase in value. Similarly the issue of timeliness and quality of information associated with risk management processes cannot be over-emphasised, particularly for 'near-miss events' and repeated failure incidents, e.g. timely action on fraud can substantially reduce losses by orders of magnitude in excess of 100:1.

Automation is required to ensure that the key professionals spend their time on value-add tasks and not on

administrative tedium. Automation has the added benefit of often reducing the complexity of a process and provides a basis for a better understanding of process for re-engineering at some time in the future.

4.3 Risk appetite

An enterprise's culture, business strategy, and sectorial competitive position all influence the enterprise's risk appetite. Furthermore, each business sector (government, public, private, voluntary or institutional) displays a unique tolerance of various risk categories — hence there is no uniform set of risk categories applicable to all enterprises.

However, 'risk appetite' is core to achieving effective risk management and should be a fundamental part of every enterprise's risk management strategy before considering how risks can be treated. If an organisation has not considered its risk appetite, it probably will not have addressed risk effectively at all. Risk appetite may be assessed in different ways depending on whether the risks being considered are opportunities, killer risks, or simply perils to be considered when doing business:

- for risks seen as opportunities, the enterprise should consider the value they are prepared to actively put at risk in order to obtain the benefits of the opportunity, i.e. compare the value (financial or otherwise) of potential benefits with the losses which might be incurred,
- for killer risks and other perils, the enterprise's risk appetite should include scale of exposure that is tolerable and justifiable should the risk be realised, i.e. cost of treatment versus the cost of the exposure should the exposure become a reality, and finding an appropriate balance.

Some risk is unavoidable and not within the ability of the enterprise to completely manage and should be treated with contingency plans should the risk be realised. The contingency could be to cease trading in the sector, or transfer the risk via insurance, or diversify into other sectors without that risk.

For each segment of the enterprise, the risk appetite provides guidance on the limits of risk they may take as authorised by senior management. The limit of risk may either be based on the cost of control versus exposure, or cost of exploiting an opportunity versus potential rewards. Risk appetite is dynamic and will vary in time for the enterprise, and executive management will vary their guidance on the limits they give to each segment of the enterprise accordingly. Therefore it can be seen that there is a corporate risk appetite (a summation across the enterprise) and a risk appetite delegated into the lines of business, which in turn may be further segmented within that line of business. The delegated risk appetite will require effective reporting and escalation processes so that the inventory (portfolio) of risks continuously reflects the cumulative effect.

When executive management has a clear comprehension of its risk appetite, together with core competence in risk management, it is very likely to deliver superior returns to its stakeholders by comparison to risk-adverse operations.

4.4 Risk strategy

Risk strategy defines the broad outlines for coping with risk, and defines the approach to be adopted across the enterprise. The strategy does not necessarily have to be in written form as long as the intended executive directives are clearly laid out either in a policy document or in the standard processes implemented. The risk strategy in effect is the overall organisational approach and direction specified by the appropriate executive officers or the board, that are embedded into common methods and uniform processes adopted within the enterprise. A risk strategy (documented or otherwise) should have addressed many of the following elements:

- risk organisation and responsibilities,
- the enterprise's attitudes to risk,
- the ownership both of the risk and of the management of situations in which control failure leads to material realisation of risks,
- the methodology that risk issues are to be considered at each level of business planning,
- highlighting risk as an opportunity as well as a threat,
- promoting peer review and benchmarking risks where appropriate,
- encouraging proactive reporting of risk through the line,
- identifying new activities that should be assessed for risk and incorporated into risk management operations,
- defining the need for monitoring, review and gaining assurance about the management of risk,
- specifying the need for common criteria that will inform assessment of risk and the definition of specific risks as critical,
- promoting the balancing of the risk portfolio and establishing a risk appetite,
- supporting effective innovation and encouraging well-managed risk-taking to generate improved delivery of the enterprise's aims and objectives,
- driving the integration of risk management into established procedures and arrangements,

- encouraging effective communication about risk with staff and all stakeholders, inside and outside the enterprise.

4.5 Reporting and measurement

The author has always believed that within the world of information risk management, if you cannot measure it, then you should not be doing it. The real problem is that effective measurement and reporting is difficult, and requires innovative approaches with attention to detail. The detail should show anomalies without becoming simply a blizzard of all available information. The detailed measurements need to be there but the reporting should be selective, with the ability to drill down for the detail if necessary. In Formula One (F1) motor racing, the volume of detailed telemetry provided from the car lapping at an average speed of over 100 mph is amazing. The engineer back in the pits is looking at less than 5% of that data, but this is the critical information that will show anomalies that will then allow a more detailed selective analysis of the other 95% of the data — all happening in real time with only seconds to spare from measurement, then reporting, to deciding the action that should be taken to resolve the anomaly.

Taking the F1 analogy, how should an enterprise organise its reporting? For enterprises with critical real-time risks and also for large enterprises with high volumes of measurement data, automated real-time reporting techniques are the only rational approach. The answer is to use technology to bring together measurements into an executive dashboard or a risk cockpit [11, 12] with selected data that highlights anomalies. For other types of enterprise without the need for real-time reporting or with lower volumes of measurement data, then traditional manual reporting mechanisms may suffice. These enterprises should recognise that there is a risk of failure in non-mechanised processes, and the probable consequence of such a failure to report and take action. Those enterprises with a balanced risk appetite and effective management will recognise the value in mechanisation of the process and adopt a 'dash-board/cockpit' reporting system.

5. Specialised risk management areas — IRM

In specialised technical areas it may be necessary to centralise some competencies that can provide support across the lines of business. More specifically for ICT, there is a strong case for the establishment of an IRM capability as part of the overall enterprise's risk management organisation. In this particular area there is a requirement for technical expertise to understand the ICT risks by establishing a specific inventory of ICT operational risks based on the technology and architecture of the ICT operation. With pervasive use of ICT to automate processes and hold information, this has become critical to every size and type of enterprise.

Section 2.2 called for sector-specific standards, codes of practice, etc, to be used to develop self-assessment checklists to assist in risk identification. ICT is a sector in its own right and the appropriate sources that should be used in the development of checklists are:

- ISF Standard of Good Practice [13],
- COSO [5],
- Control Objectives for Information and Related Technology (COBIT®) [14],
- IT Infrastructure Library (ITIL) for IT operations [15],
- ISO-IEC 27000 Series for specific security standards [16].

For more exhaustive information related to ICT, the IT Compliance Institute (ITCi) [17] have a unified compliance project (UCP) with a number of comprehensive matrices. These provide sufficient detail in topic areas to be considered and cross-reference to the regulations to which they relate. An auditor or information security specialist could use these to develop self-assessments for use by staff and management. There are a number of others covering:

- leadership and high-level objectives,
- audit and risk management,
- monitoring, measuring and reporting,
- design and implementation,
- technology acquisition,
- operational management,
- IT staff management and outsourcing,
- records management,
- physical security,
- systems continuity,
- privacy.

The information risk management organisation should operate across the enterprise to ensure consistent management of risks and the appropriate governance. The IT Governance Institute [18, 19] says, '... ICT is essential to manage transactions, information and knowledge necessary to initiate and sustain economic and social activities. These activities increasingly rely on globally co-operating entities to be successful. In many organisations, ICT is fundamental to support, sustain and grow the business. Effective and timely measures aimed at addressing these top management concerns need to be promoted by the governance layer of an enterprise. Hence, boards and executive management need to extend governance, already exercised over the enterprise, to IT by way of an effective IT governance framework that

addresses strategic alignment, performance measurement, risk management, value delivery and resource management. IT governance is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives'. To review an IT governance framework, see COBIT [14], the DTI Web site [20], or ISACA [21].

6. Expected outcome

Where risk management is maturely implemented there is a better understanding by all levels of management of the business processes, and where and how change can be affected. Through risk dashboards or risk cockpits, measurement and reporting is easier and more effective at empowering management to plan and perform[4], not only in the management of risks but also for unexpected (the unknown unknowns) and crisis management events. Establishing a risk appetite permits focused strategic planning by the executive that in turn promotes greater business opportunities and potential improved risk/reward ratios. The resulting improved governance through more effective and confident risk management in many enterprises has resulted in improved effectiveness of operations leading to greater customer confidence and satisfaction. Hence a key differentiator and market advantage to the enterprise.

6.1 Next steps

For those enterprises with existing risk management processes, a health check to assess the appropriateness and effectiveness of their risk management system should be undertaken periodically to ensure that it is not over- or under-'engineered'.

For those enterprises either without, or with immature risk management processes there is a need to decide an approach and strategy towards operational and enterprise risk management. A process to iteratively approach the tasks is to use Boyd's OODA loop [23] that is used by the military. It systematically calls for processes to observe, orient, decide and then act. Using that technique with the approach stated above should allow any enterprise to develop and implement a risk management system even without the help of experts; although expert assistance can significantly accelerate implementation.

7. Conclusions

Risk management is an effective and appropriate process for all types and sizes of enterprise that helps manage expected risks and also helps management to be better prepared for the unexpected. The benefits include improved effectiveness of operations, reduced incidents or unexpected events, leading to improved customer satisfaction. The risk management programme is a long-term strategic initiative, requiring all levels of management to commit to a 'no blame culture' if weaknesses or failures are to be promptly identified and managed.

[4] The 'plan do check act' (PDCA) cycle was in fact originally developed by Walter A Shewhart, a Bell Laboratories scientist who was a friend and mentor of Deming [22], and the developer of statistical process control (SPC) in the late 1920s. There are also several recent variations on this concept such as the Boyd OODA loop [23].

References

1 A publicly available sample proposal to assist a company with the development and implementation of a global enterprise risk management (ERM) strategy can be found at — http://www.delcreo.com/delcreo/about_delcreo/ERM%20Implementation%20Narrative.doc

2 'The Orange Book', — http://194.128.65.69/sdtoolkit/reference/org_library/related/orange-book.pdf

3 HM Treasury Risk Management Assessment Framework — http://www.hm-treasury.gov.uk./media/17A/81/17A8166B-BCDC-D4B3-16668DC702198931.pdf

4 US DoD briefing — http://www.defenselink.mil/transcripts/2002/t02122002_t212sdv 22.html

5 COSO Enterprise Risk Management, Integrated Framework — http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf

6 Typical commercial self-assessment tool — http://www.gocsi.com/membership/securcompass.jhtml

7 Open reporting example — http://www.trinitymirror.com/governance/terms/tm_objectid=14107357&method=full&siteid=111046&headline=whistleblowers-charter-disclosure-policy-name_page.html — this applies to the reporting of any breaches of agreed processes or systems.

8 Jones A: 'Risk framework for ICT security management version 1-0' (EX013506-TR-004_D16-CSM3-Risk_Framework_for_ICT_Complete_Security_ Management_V1-0 Final.doc), internal BT document.

9 UK Resilience and Emergency Preparedness — http://www.ukresilience.info/preparedness/risk/communicatingrisk.pdf

10 'A Risk Management Standard', AIRMIC (2002) — http://airmic.com/Downloads/Pubs/AIRMIC_Risk-Management-Standard.pdf

11 BT Risk Cockpit — http://www.btglobalservices.com/business/global/en/news/2005/edition_4g17_orm.html (this is a BT 'point of view' paper, which examines how to unlock the business value of your operational risk management initiatives).

12 Evans G and Benton S: 'The BT Risk Cockpit — the visual approach to ORM', BT Technol J, 25, No 1, pp 88—100 (January 2007).

13 Information Security Forum (ISF), Standards — http://www.isfsecuritystandard.com/index_ie.htm

14 COBIT Framework — http://www.isaca.ch/files/CobitFramework.pdf

15 ITIL — http://www.itil.co.uk/

16 ISO-IEC27000 Series (security standards) — http://www.iso27001security.com/index.html

17 IT Compliance Institute (ITCi) — http://www.itcinstitute.com/

18 The IT Governance Institute — http://www.itgi.org/

19 A Management Briefing from the IT Governance Institute and the Office of Government Commerce — http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=22493&TEMPLATE=ContentManagement/Content Display.cfm

20 Aligning COBIT, ITIL and ISO 17799: Guidance from the IT Governance Institute and UK Office of Government Commerce — http://www.isaca.org/Template.cfm?Section=Whats_New1&Template=/ContentManagement/ContentDisplay.cfm&ContentID=22487

21 'Information security: Protecting Your Business Assets', (Information Protection Framework includes classification) — http://www.dti.gov.uk/bestpractice/assets/security/ispyba.pdf

22 Deming W E: 'Out of the Crisis', Cambridge, Mass, MIT Centre for Advanced Engineering Study (1986).

23 Boyd J: 'OODA loop', — http://www.d-n-i.net/fcs/ppt/boyds_ooda_loop.ptt

Mark Drew joined BT in 2004 as a Principal Researcher within BT's Security Research Centre at Adastral Park. He has been actively involved in risk management, compliance, information security and business continuity since 1984. He commenced his career as an IBM computer engineer for 13 years. Following his engineering experience he developed specialist skills in a wide variety of management positions including engineering research, application development, project and service management, asset and all the systems management control disciplines. He is now recognised as a highly information and data protection, and related subjects.

Since leaving IBM in 1995, he has worked in the UK financial services sector prior to joining BT.