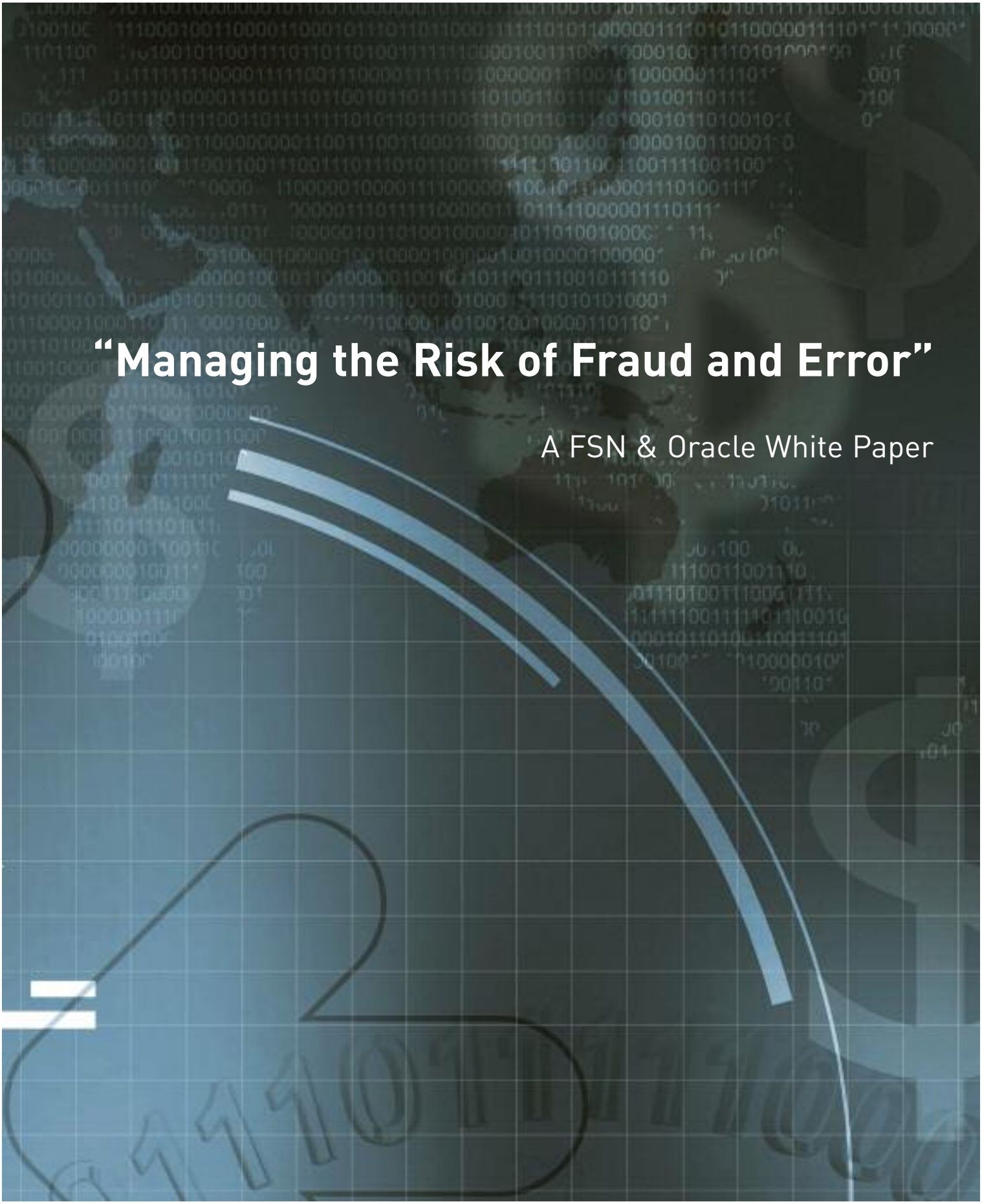


"Managing the Risk of Fraud and Error"

A FSN & Oracle White Paper

FSN
Professional & Technical Publications

ORACLE®

Contents

Introduction

Fraud and error are two sides of the same coin. Lax procedures coupled with organizational inertia, poor systems and processes are the 'Petri dish culture' on which fraud and error thrive.

Despite the seriousness of the problem both fraud and error are romanticized. Films and television dramas glamorize fraud and mistakes are frequently portrayed as a necessary staging post on the way to accumulating knowledge and wisdom. Colorful language such as "Ponzi" and "Pyramid" help to reinforce the impression that fraud is a harmless crime, yet these schemes amount to nothing less than premeditated deceit – often on an enormous scale.

In fact the scale of fraud is truly breathtaking. The amount of money lost annually to governments, private sector institutions and individuals in the United States alone is estimated to be equivalent to the Gross Domestic Product of a country the size of Brazil. Neither is this a 'victimless' crime. Occupational fraud flows straight through to the bottom line, robbing businesses and their employees of profit and investment while driving up costs for government agencies, NGO's and not-for-profit organizations. Errors too can be just as costly and devastating to organizational effectiveness and reputation.

So what is driving the growth of fraud and error and what can be done to reverse the tide?

The economy

A challenging economy is a key factor fuelling the growth of fraud at an organizational and a personal level. Businesses are tempted to bend the rules or embark on scams to show results in a more flattering light while previously exemplary employees are tempted to commit fraud on their organizations because of severe financial pressures.

"The swindler is not, as a rule, a thug. He will not blackmail. He will not murder. Your daughter is reasonably safe with him."

Justice Gerald Sparrow, A History of Scams, Fraud and Swindles, by James Morton.

Automation and volume of transactions

The inexorable growth in automation renders organizations more vulnerable to error and presents would be fraudsters with novel and greater opportunities to exploit loopholes in systems safe in the knowledge that massive transaction volumes will mask their activity.

Increased globalization

Increases in cross-border trading coupled with the lengthening of global supply chains has introduced greater risk of error and fraud as companies struggle to maintain visibility of business processes and trading partners especially in countries that have gained a reputation for a more relaxed regulatory environment.

Reported crime

The financial crisis and individuals' experience of say identity and credit card fraud has created much greater awareness of fraud. Some would even argue that greater automation has made it easier to detect and measure fraud. Given the scale of economic damage to government and corporate balance sheets, regulators around the world are taking a much greater interest in developing legislative and regulatory frameworks to contain the problem. So there is much greater reporting of fraud and much greater prominence is given to the relevant legislation and the financial penalties meted out to offenders.

"In the United States there has been a significant increase in prosecutions under the Foreign Corrupt Practices Act (FCPA) and with fines potentially amounting to more than $100m per incident it has elevated FCPA risk from a piece of 30 year old legislation gathering dust onto the corporate front burner."

Toby Bishop, director of the Deloitte Forensic Center for Deloitte Financial Advisory Services LLP.

The passage of the Dodd Frank Act 2010 which introduced whistle-blower awards to be paid by the Securities and Exchange Commission (SEC) to people that provide information about securities law violations (and that lead to the recovery of more than $1m) is also concentrating minds on the breadth and scale of fraudulent activity.

What next?

Despite the enormity of the problem the causes of fraud and error are not rocket science and neither are the steps that can be taken to abate it beyond the grasp of most organizations. This white paper seeks to illustrate that with appropriate technology, processes and organizational behaviour, fraud and error can be drastically reduced leading to immediate and enduring improvements in corporate performance, profitability and organizational effectiveness.

"You will discover that while fraud may outwardly seem complex it rarely is. You don't need a degree – just an understanding of fundamental business procedures and terminology."

Corporate Fraud Handbook, Prevention and Detection, by Joseph. T. Wells.

Why does fraud and error happen?

There are very many factors which affect the incidence of fraud and error. Organizational culture and business change, size and complexity of its operations, and industry all have a significant bearing on the ease with which fraud and error can arise. Fraud, for example, is rife within financial services and the soft under-belly of the public sector makes it an easy target as well. But the networked economy, greater automation, new methods of systems deployment and the stretching of global supply chains and increasingly outsourced business processes all play a part in the risk profile.

Recent research illustrate that systems upgrades exacerbate the risk of fraud and error. Transitioning from one environment to another may require controls to be reconstituted or the addition of new controls to take account of changed processes and functionality. Furthermore, processes involving payments to third parties, such as 'purchase to pay' and 'order to cash' are particularly susceptible to fraud, waste and error.

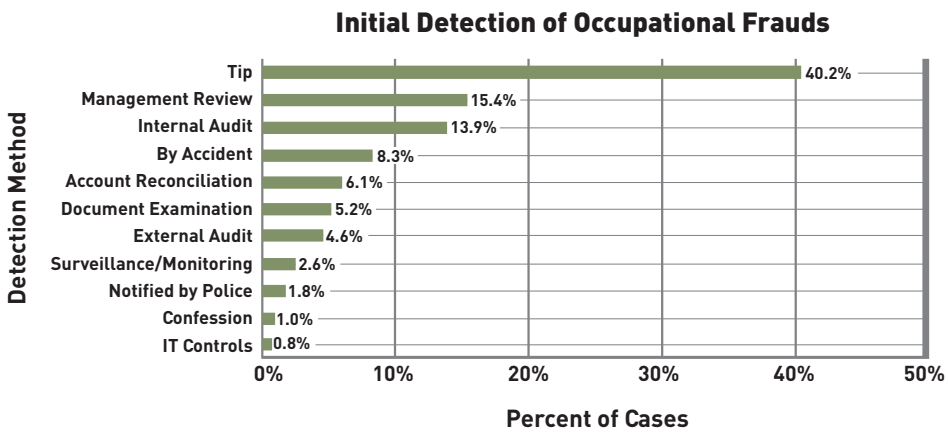
The sheer complexity of the business landscape and the scale of transaction volumes can be truly overwhelming.

Organizational factors

The notion that fraudsters are criminals from birth is seriously misplaced. Most frauds are committed by first time offenders (of the thousand or so cases included in The Association of Certified Fraud Examiners' 2010 Report to the Nations on Occupational Fraud and Abuse, 85% of perpetrators had not previously been criminally charged or convicted). However, academics in the field such as Professor Timothy Pearson, Executive Director - Institute for Fraud Prevention, cite the growing menace of the predator and organized crime as opposed to the occasional 'bad apple'.

When it comes to detecting fraud and error our collective record is modest and presently relies heavily on the vigilance of people rather than automated controls. Astonishingly, around 40 percent of fraud is discovered via tips rather than management controls, see figure 1.

***Fig 1:** Organizations rely heavily on tips to uncover fraud*



Source: The Association of Certified Fraud Examiners' 2010 Report to the Nations on Occupational Fraud and Abuse

The popular view that the lowly employee is the main culprit is a myth. 'Management override' of established systems of control represents a significant risk. New acquisitions in remote areas of an organization, perhaps in emerging or developing economies represent the most severe risk as lack of regulatory safeguards, poor enforcement and cultural differences can give rise to business practices that would not be tolerated elsewhere or are simply illegal. Lengthening supply chains with multiple suppliers who may not be closely supervised magnify the risk of offences under the FCPA or the newly introduced 2010 Bribery Act in the UK. The risk is succinctly summed up by Professor Tim Pearson, "Ask yourself who am I doing business with?"

The networked economy

Rampant growth in volumes, technical complexity and an ever increasing variety of deployment options all play a part in laying organizations open to fraud and error. The growth in volumes makes it hugely difficult to identify errant transactions. Manual controls and the traditional operations of internal audit are blunt instruments in the face of terabytes of corporate data.

It is a problem often exacerbated by the fractured nature of operational and management information systems frequently reliant on multi-vendor platforms. Add the current vogue for cloud based applications, outsourced operations and an over-dependency on spreadsheet-based processing and it becomes obvious that data is not only scattered throughout an organization but the risk of error and fraud is simply hard baked into the systems architecture.

Inadequate resources

In the face of such apparently insurmountable odds many organizations respond weakly to the challenge. They neither have a coherent strategy for combating error and fraud or the skilled resources that are vital for an effective response.

"It is very rare to find someone responsible for fraud. It takes certain experience and skills to discover fraud otherwise it is like looking for a needle in a haystack. If you haven't seen a fraud you are unlikely to recognize one."

Professor Timothy Pearson, Executive Director - Institute for Fraud Prevention

Others refer to the 'Black Swan' effect, i.e. the management response that "it is so rare it couldn't happen here". Yet this is severely at odds with government and industry-specific reports estimating fraud losses at many billions of dollars annually in the U.S. Add in losses through error (about which little is reported) and it becomes clear that fraud and error require a robust response if profitability and performance are not to be severely dented.

As Timothy Pearson puts it acerbically, "there is no line for fraud losses [or losses through error] in the financial statements."

Responding to the challenge

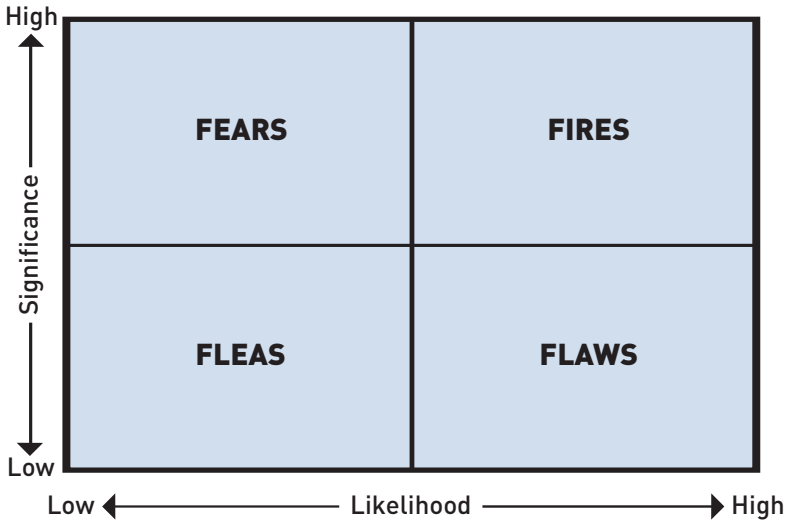
A risk based approach

The challenge of tackling fraud and error is formidable yet it is possible to stack the odds in favor of the organization by adopting best practice methodologies, tools and techniques and by leveraging an appropriate blend of organizational structure, process and technology. Underlying the whole response is the need for a methodical risk-based approach which allocates resources according to need and encourages a rapid return on investment (ROI).

One such technique is that described by Toby J.F. Bishop and Frank E. Hydoski in their book Corporate Resiliency – Managing the Growing Risk of Fraud and Corruption. While this clearly focuses on managing fraud the underlying principles of the risk based approach are equally applicable to managing error since the methodology concentrates the organization's efforts according to the "likelihood" of an incident and its "significance". The authors choose their words wisely since the "significance" of both fraud and error is not purely financial. An incident of error or fraud can be extremely damaging to corporate image, reputation and share price. Indeed, there is evidence that an organization's control environment (about which more later) now forms part of the assessment of corporate strength by ratings agencies.

Bishop and Hydoski's risks based methodology suggest a response according to four quadrants. See Figure 2 below.

***Fig 2:** Four types of Fraud and Corruption Risks*



Source: Toby J.F. Bishop and Frank E. Hydoski Corporate Resiliency – Managing the Growing Risk of Fraud and Corruption Wiley 2009

For example, the "Fires" quadrant (High Likelihood/High Significance) is particularly relevant to certain industry operations for which fraud is a significant operating cost that must be controlled aggressively on a day-to-day basis to avoid intolerably high losses. Such operations include insurance, telecom, retail, public sector procurement, and the credit card arms of retail banks. These operations typically receive significant investment in technology to contain fraud and error while other divisions of the same organization may receive little attention. For other enterprises the risk of fraud and error may thought to be so infrequent that investment is difficult to justify, but this can lead to organizations being vulnerable to potentially catastrophic losses.

The "Flaws" quadrant (High Likelihood/Low Significance) includes risks such as fraudulent travel and expense claims. Traditionally this area receives considerable attention, with operating personnel sometimes going 'treasure hunting'. This is the term Toby Bishop uses to describe an excessive focus on 'victories', i.e. catching a large number of people cheating on expenses. While a certain amount of effort is appropriate for this area, the outcomes can be disruptive to the organization and may be of modest value in risk management terms.

Once the risk of error or fraud is understood it can then drive the type of response. For example, the high likelihood/ low significance type of error may justify investment in automated controls monitoring, while a potential fraud that is highly significant but rarely crops up may be better managed though the provision of a whistleblower hotline and automated transaction monitoring, to try to prevent or detect individual transactions that might expose the organization to excessive risk. In extreme cases, the appropriate response may be to withdraw from a particular line of business or geography altogether, for example, because of the high probability of violating the FCPA.

What should the control environment look like?

The historic approach

Traditionally, the control environment is a collection of interrelated manual and automated controls (financial and otherwise) designed to ensure that authorized business transactions are processed completely and accurately. In broad terms this comprises;

General computer controls – what may be regarded as IT governance which ensures that, for example, applications are technically robust; databases are sound, secure and backed up.

Application controls – that is manual and automated controls deeply embedded within and across business processes, which ensure that authorized transactions are processed completely and accurately and the integrity of the underlying data and policies are preserved.

Organizational controls – for example, management oversight, audit committees, internal and external audit functions which ensure the integrity of all controls.

But this definition of the control environment has not withstood the test of time. In today's more challenging and highly regulated environment, the controls environment is expected to cover more ground (risks), for example, ensure that business is ethical, environmentally sound, complies with anti-corruption legislation and prevents fraud to name but a few. This goes well beyond traditional financial compliance and Sarbanes-Oxley. So what has changed?

General controls have given way to the need for much broader IT governance to reflect the need to manage closely the heady mixture of, say, development offshore, outsourcing, cloud computing, multi-vendor platforms, virtualization and to ensure that the organizations have the skills, resources and methodologies to meet these escalating demands.

Secondly, organizations no longer view their operations from an applications perspective but take a process view of the way they do business supported by workflow technology. By extension, the control environment needs to follow processes rather than isolated applications, for example, 'purchase to pay' rather than purchase order processing, payables and general ledger. Indeed, a recent survey conducted by the OAUG (Oracle Applications User Group) highlighted the importance of the process perspective, with cash oriented processes heading the list of processes most vulnerable to fraud, waste and error, for example,

Procure to pay:	**76%**
Order to cash:	**65%**
Hire to retire:	**43%**
Record to report:	**39%**
Acquire to retire:	**24%**
Prospect to order:	**21%**
Concept to market:	**13%**
Don't know/not sure:	**13%**
Other:	**1%**

Finally, traditional organizational structures, built around financial management may no longer be 'fit for purpose'. Today's management structures need to address a much broader range of risks, a more changeable operating environment and a more complex legislative environment.

Governance, Risk and Compliance (GRC)

On an enterprise basis all of the above is swept up in GRC – a holistic term, popularized over the last decade as new software tools have become available to manage governance structures, the risks that organizations face and the ever growing list of compliance demands. Every organization and every software vendor has its own take on the definition of GRC. Gartner, for example, defines GRC as "the automation of the management, measurement, remediation, and reporting of controls and risks against objectives, in accordance with rules, regulations, standards and policies."

But GRC is more than a clever definition. It brings all of the control strands together providing an integrated repository in which (i) enterprise risks, can be documented, quantified, prioritized and managed (ii) governance procedures, such as, board and management activities, oversight structures, strategy setting, performance monitoring and reporting can be recorded and (iii) that there is a documented controls environment for the evaluation, monitoring, and reporting of the controls that facilitate compliance with regulatory requirements as well as corporate policies and procedures.

But in parallel with this new definition of the control environment there has been a step-change in technology which has enabled the rapid development of potent GRC platforms in which constant surveillance of the controls environment is technically, operationally and economically feasible.

So what does the ideal GRC architecture look like?

Integration

Integration is a key requirement that weaves its way both across the GRC landscape and between the GRC environment and the underlying process controls. It is important that there is an explicit link between the strategic performance and risk objectives expounded in the GRC layer and the controls embedded in underlying business processes and infrastructure which ensure their delivery.

Controls automation

In the face of massively growing data volumes it is vitally important that greater emphasis is placed on automated controls. Automated controls are not a complete substitute for manual controls which still have an important place in the controls environment. For example, there is no real substitute for the manual review of intricate group adjustments in a financial consolidation by an experienced group controller. Imbued with years of knowledge of the enterprise he/she can sniff out the unexpected or unusual journal entry. But manual controls have their limitations; most notably that the volume of such transactions may make it impractical or unreasonably costly monitor this way. Also, people may become less effective when they get tired or distracted by seemingly more urgent priorities. Our group controller, perhaps working late one night could miss an important journal or overlook its significance. On the other hand automated controls (provided they are correctly constructed) can be relied upon to work effectively time after time.

Continuous Controls Monitoring (CCM)

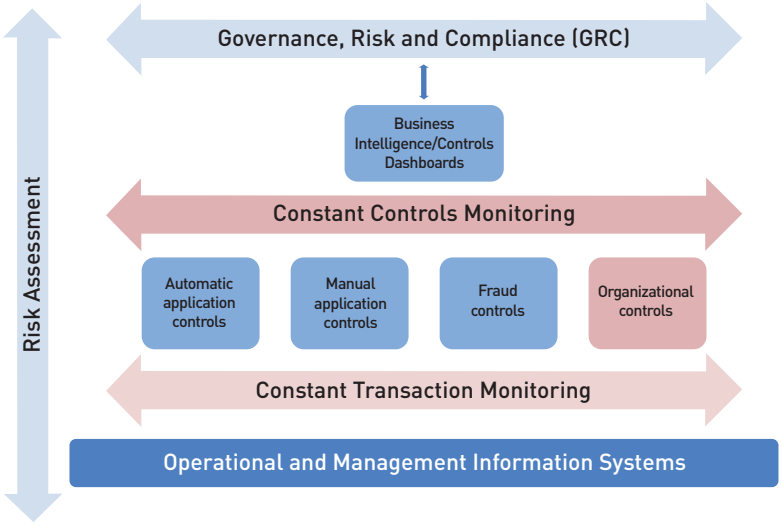
CCM is a powerful component of the new age controls environment which allows key controls to be monitored for unexpected changes. For example, a change to supplier details, in the purchase to pay cycle, an amendment to pricing in the vendor catalogue, the authorization of a new vendor account and so on. Supported by workflow and email alerts CCM technology allows inadvertent or malicious changes to be detected quickly – something that would be practically impossible based on manual review of change requests or manual scrutiny of master file change reports.

Continuous Fraud Monitoring (CFM)

Although fraud controls designed specifically to prevent or detect fraud share much in common with application controls (and indeed may be identical in many instances) they deserve special mention since they often go beyond the boundaries of process controls which are designed principally with financial integrity in mind.

These controls, driven by fraud risks catalogued in a GRC repository often require intricate set-up and monitoring. Fraud prevention controls relevant to the 'Purchase to Pay' cycle could include comparison of vendor details with employee details for items such as tax codes, common addresses and names. Or perhaps differences between 'delivery' and 'bill to' addresses between purchase orders and vendor invoices and so on. Once again unexpected changes to these deeply embedded controls, designed to prevent and detect fraud can be automatically reported in real time leveraging a predetermined work flow for investigation and remediation.

***Fig 3:** A modern GRC based controls environment*



Source: FSN Publishing Limited 2011

Transaction monitoring

In addition to monitoring controls a GRC system can enable transaction monitoring for unusual conditions such as transaction values outside of expected ranges, prices which deviate from agreed catalogue prices, multiple identical purchases and duplicate payments. Transaction surveillance may not be feasible for all organizations and indeed, depending on the risk based approach advocated by Bishop and Hydoski, might be limited to selected higher-risk transaction streams only or may not be necessary. But the facility to review transactions is essential to reducing the risk of fraud and error in many organizations.

Analysis and reporting

Business intelligence capability incorporated within the GRC environment can provide the reporting and analysis that gives insights into trends across the controls environment. Dashboards can highlight control issues pending, percentage remediated, which applications are affected, error rates and workload in different areas of the business. Summary information presented in an accessible way can elevate controls reporting beyond operations and internal audit to other stakeholders on the board and audit committee that need assurance that the control environment is performing effectively.

Efficient and comprehensive analysis tools and techniques are key to delivering the ROI promised from continuous monitoring of controls and transactions – not only detecting incidents faster, but ensuring that identified (potential) problems that could do the most harm to the organization are automatically flagged for a response and remediation.

The organizational implications

Technology, though vital, cannot solve all risks of fraud and error on its own. While 'softer' issues such as culture elude precise definition or quantification there is no doubt that culture plays a vital role in many aspects of GRC, for example, the reporting of fraud, the accuracy of business forecasts and the integrity of financial statements. Modern systems can provide the framework for effective GRC but there is still no substitute for the human touch.

But there are significant human barriers to implementation as well. Despite plenty of compelling business cases illustrating rapid ROI from better fraud prevention and rapid remediation of problems before they become crises, some boards of management prefer to 'bury their heads in the sand'. A company with a 10 percent profit margin which experiences an average loss of $160,000 would need to generate $1.6m in revenue to make up for the shortfall – no easy task in a competitive environment. But even this simple case ignores the impact of lost management time, legal and other related audit and recovery costs that accompany a single fraud incident. Not to mention collateral damages like a loss is public trust or erosion of brand value and reputation.

There are also well founded concerns about management simply overriding the control structures that have been put in place.

"Management override is the Achilles heel. It is a bulldozer that pushes aside processes and controls when fraud is committed either individually or collaboratively."

Toby Bishop, director of the Deloitte Forensic Center for Deloitte Financial Advisory Services LLP.

In these circumstances process controls might be totally ineffective, so what is left? The answer seems to lie in "entity level" controls such as high-level transaction monitoring, together with empowering the organization and its employees to recognize malpractice and to report wrongdoing. Whistle-blower systems, hotlines, anonymous mailboxes, education, codes of conduct and conflict of interest disclosures are just some of the techniques that can be deployed. Emboldening external stakeholders, such as audit committees and remuneration committees that have personal reputations and wealth at stake is another check and balance on management excesses.

Summary

Fraud and error is on the increase, fuelled by economic difficulties, increased globalization and a more aggressive regulatory regime which expands the realms of what is unacceptable corporate behavior.

Although some sectors of the economy are more susceptible to fraud and error than others, no organization is immune to the risks and it is a risk-based approach that holds the key to the efficient allocation of resources when it comes to tackling the problem.

Historic approaches to managing controls which were designed principally to ensure the integrity of financial statements have proved to be sorely lacking in the face of a much more extensive risk landscape underscored by burgeoning compliance requirements, massive growth in transaction volumes, increased complexity and the constant threat of fraud.

Systems of Governance, Risk and Compliance offer a much more holistic and integrated approach rather than the scatter gun approach adopted by many organizations. New capabilities such as automated controls monitoring and surveillance of transactions coupled with advanced analytics and reporting offers the best prospects of protection against inadvertent mistakes and organized fraud.

But despite significant progress there are many human barriers to mounting an effective response. Chief among these are lingering doubts about the financial effectiveness of investing in better controls, a natural reluctance to accept change and deliberate management override of the control environment. Others are in 'denial' – unwilling to face up to the risk of fraud – until of course it directly affects their organization.

However, for organizations that 'grasp the nettle' the rewards can be high, in terms of reduced risk, superior financial performance and enhanced market reputation.

Leading author Gary Simon, Group Publisher of FSN and Managing Editor of FSN Newswire

Contributing authors Toby Bishop, director of the Deloitte Forensic Center for Deloitte Financial Advisory Services LLP

David Krauss, Sr. Director, Oracle Governance, Risk, and Compliance Applications, Oracle

About Oracle Fusion GRC Applications for Fraud and Error Reduction

Oracle Fusion GRC Applications for Fraud and Error Reduction improve bottom-line performance by continuously monitoring transactions and applying advanced forensic analysis and embedded application controls across business processes – so you can detect more incidents and respond faster, preventing problems before they escalate or even occur.

About FSN

FSN Publishing Limited is an independent research, news and publishing organization catering for the needs of the finance function. This white paper is written by Gary Simon, Group Publisher of FSN and Managing Editor of FSN Newswire. He is a graduate of London University, a Chartered Accountant and a Fellow of the British Computer Society with more than 27 years experience of implementing management and financial reporting systems. Formerly a partner in Deloitte for more than 16 years, he has led some of the most complex information management assignments for global enterprises in the private and public sector.

Gary.simon@fsn.co,.uk

www.fsn.co.uk

FSN Publishing Limited
Clarendon House
125, Shenley Road
Borehamwood
Herts
WD6 1AG
United Kingdom

Worldwide Enquiries
Phone: + 44 (0)20 8445 2688
Email: gary.simon@fsn.co.uk

www.fsn.co.uk

Oracle Corporation
Worldwide Headquarters
500 Oracle Parkway
Redwood Shores, CA
94065
U.S.A.

Worldwide Enquiries
Phone: +1.650.506.7000
+1.800.ORACLE1
Fax: +1.650.506.7200

www.oracle.com