

Prodigy Newsbyte

BROUGHT TO YOU BY THE PRODIGY GROUP
SINGAPORE | HONG KONG | MALAYSIA | INDONESIA

Recommendation For An Effective Continuous Audit Process

By David Coderre

An evolving regulatory environment, increased globalisation of businesses, market pressure to improve operations, and rapidly changing business conditions are creating the need for more timely and ongoing assurance that controls are working effectively and risk is mitigated properly. To meet this need, many internal auditors are using continuous auditing to maximise the effectiveness of their work. Learning what continuous auditing does and how it works can help auditors make better use of this process, while maintaining internal audit's independence and objectivity in evaluating the effectiveness of controls, risk management, and governance processes.

What Is Continuous Auditing?

To understand the benefits of continuous auditing, it is important to know the differences between continuous auditing and continuous monitoring. Continuous auditing is the use of audit methods, ranging from ongoing control evaluations to continuous risk assessments on a more frequent or ongoing basis. Technology plays a key role in the continuous audit process by automating the pattern analysis of key numeric fields and the examination of trends. Technology also enables the comparison of detailed transaction analysis against specific thresholds, the identification of exceptions and anomalies, the testing of controls, and the comparison of processes or systems over time.

On the other hand, continuous monitoring is a process that management puts in place to ensure that its policies, procedures, and business processes are operating effectively. It typically addresses management's responsibility to assess the adequacy and effectiveness of internal controls. For instance, management may identify critical control points and implement automated tests to determine if these controls are working properly.

The continuous monitoring process usually involves the automated testing of all transactions and system activities within a given business process area against control rules. Monitoring may occur on a daily, weekly, or monthly basis based on the nature of the underlying business cycle.



For example, depending on the specific control rule, related test, and threshold parameters, certain transactions are flagged as control exceptions after which management is notified. The continuous monitoring function also may be tied to key performance indicators (KPIs) and other performance measurement activities.

Many of the continuous monitoring techniques used by management are similar to those performed by internal auditors during continuous audit activities. However, continuous auditing usually enables auditors to evaluate the adequacy of management's monitoring function and identify and assess risk areas

[The Prodigy Group]

Singapore – (65) 6221 2810
 Hong Kong – (852) 2815 5606
 Malaysia – (60) (3) 2283 5050
 Indonesia – (62) (21) 4288 3120

[Email: enquiry@prodigy-group.com]

Find us on the Web:
[\[www.prodigy-group.com\]](http://www.prodigy-group.com)

Continued from page 1

By using data-driven indicators of risk and electronic testing of controls, IT auditors can provide audit committees and senior management with independent assurance that control systems are working effectively and risk is being managed. Furthermore, continuous auditing helps IT-savvy auditors to:

- Develop a dynamic risk-based plan by assessing changing levels of risk on an ongoing basis
- Support the scope and objectives of individual audits by providing the audit team with a better understanding of the materiality and nature of the transactions being performed
- Assess levels of compliance by performing detailed testing of controls
- Identify potential fraud, waste, and abuse by brainstorming fraud risks and the development of data-support audit tests

Continuous auditing consists of two main components — continuous risk assessment and continuous control assessment. Below is a description of each. Continuous risk assessments refer to audit activities that identify and evaluate companywide risk levels by examining trends and comparisons within a single process or system. These processes are then compared to their past performance and other business systems. For example, product line performance is compared to previous-year results and also is assessed within the context of one plant's performance versus the others.

While management is responsible for developing and maintaining a system that identifies and mitigates risk, The Institute of Internal Auditors' (The IIA's) states that auditors should assist the organisation by identifying and evaluating significant exposures to risk and by contributing to the improvement of risk management and control systems.

The organisation encourages auditors to establish risk-based plans to determine the priorities of internal audit activities that are consistent with the organisation's goals. Throughout the continuous audit process, auditors are responsible for evaluating the state of risk and control systems and providing this information to the audit committee and senior management. In the case of legislation such as the U.S. Sarbanes-Oxley Act of 2002, auditors also evaluate management's assessments of their internal controls. Ideally, internal auditors are not part of the controls monitoring process and do not design or maintain the controls, thereby retaining their independence. Auditors can use continuous risk assessments to identify and evaluate risk levels on an ongoing basis. This allows auditors to assess management's risk mitigation activities and support the development of objectives for individual audits and the annual audit plan. Continuous risk assessments can include the evaluation of detailed transactions against a cut-off point and a comparative analysis on a summary of the transactions. This type of comparison enables auditors to examine a process' consistency by measuring its variability in a number of dimensions. In operations, for instance, measuring the variability in the number of defects is a method for testing the consistency of a production line. The more variability in the number of defects, the more concerns about the proper and consistent functioning of the production line.

The second component of continuous auditing is continuous control assessment. Continuous control assessment refers to audit activities that identify whether selected controls are working properly. Traditionally, control testing is performed on a retrospective and cyclical basis after business activities occur. The testing procedures often are based on a sampling approach and include activities such as reviews of policies, procedures, approvals, and reconciliations.

Continued in page 3

JUST FOR LAUGH

WORKING DAZE JOHN ZAKOUR
KYLE MILLER



Prodigy

Data Solution

[The Prodigy Group]

Singapore – (65) 6221 2810
 Hong Kong – (852) 2815 5606
 Malaysia – (60) (3) 2283 5050
 Indonesia – (62) (21) 4288 3120

[Email: enquiry@prodigy-group.com]

Find us on the Web:
[\[www.prodigy-group.com\]](http://www.prodigy-group.com)

Prodigy

Data Solution

Continued from page 2

Today, organisations recognise that this approach gives internal auditors a narrow scope of evaluation and is used too late to be of real value to business performance or regulatory compliance activities. Through continuous control assessments, individual transactions are monitored against a set of control rules that determine if internal controls are functioning as designed and that highlight exceptions. A well-defined set of control rules warns organizations when process or system controls are not working as intended or are compromised. By identifying control weaknesses and violations, auditors can let audit committees and senior management know whether controls are working properly.

Continuous control assessments don't need to occur in real-time. The frequency depends on the control's risk level and the degree to which management is monitoring the controls. For example, management may perform ongoing monitoring of purchase cards on a transaction basis, while auditors run the purchase card analytics once a month after receiving the card transactions from the credit card company. And, in some cases, auditors may perform the initial control testing, after which management will monitor the control on an ongoing basis.

Starting The Continuous Audit Process

Many organisations have been evaluating the introduction of continuous auditing to support regulatory control assessment requirements. While having an adequate automated system for testing controls contributes to the assessment of internal controls and the overall mandate for a higher standard of corporate governance, additional benefits in the form of improved business performance can be equally significant. Therefore, it is important for the chief audit executives (CAEs) to consider the short- and long-term objectives of continuous auditing. The effort involved in gaining access to and knowledge of key business systems and processes has the potential to reduce the burden of compliance and eliminate impediments to business performance.

To start the continuous audit process, auditors first need to understand continuous audit objectives and requirements. Continuous auditing can be approached on an incremental basis (i.e., starting small and building on each success). When developing an approach to continuous auditing, IT auditors should make sure they have considered the short- and long-term objectives to address management-set goals adequately. The continuous audit process can be started in two ways. The first requires the use of the organisation's continuous monitoring or enterprise risk management (ERM) function. The extent to which management is performing continuous monitoring will affect the continuous audit effort, as well as internal audit's assessment of management's continuous monitoring.

In areas where management has not implemented continuous monitoring, auditors should apply detailed testing by employing continuous audit techniques such as testing detailed transactions from an ERP system to determine segregation of duties were not violated. The same is true for management's ERM function. In some cases, auditors may play a proactive role establishing risk management and control processes. In companies where management is performing continuous monitoring or ERM, auditors only need to perform procedures to determine if they can rely on these processes, such as:

- Reviewing the continuous monitoring and ERM framework.
- Determining whether there is a systematic process to identify and assess risks and controls
- Verifying that the organisation responds properly to identify risks and control deficiencies.

A second starting place is the organisation's current risk-based audit plan. Simply by including data-driven indicators of risk, auditors easily can bring continuous auditing to bear on the selection of audit activities. A key point to remember is that auditors can start small. The IT auditor or audit team leader can increase the use of data analysis to support individual audits, then run the same analysis six months later to see if the audit recommendations have been implemented and if they had the desired effect.

The key to making effective use of continuous auditing is to develop a good understanding of the main business processes and the associated information systems and infrastructure (i.e., their controls and the data contained therein). However, the adoption of continuous auditing will not only require auditors to have knowledge of information systems, but also enable them to analyse the data. This means that IT auditors need to have the necessary data analysis skills.

Furthermore, auditors must realise that continuous auditing will change the way audits are conducted, including the procedures and level of effort required by auditors. This will place demands on the audit department and possibly the work performed by IT auditors. In particular, auditors will have to obtain the support of the audit committee and senior management to move forward with the implementation of continuous auditing.

Continuous auditing also will allow auditors to identify the organisation's key controls and risk areas any time during the year. The results will not be linked to a specific audit necessarily, nor will the level of assurance be as high as if a full audit was conducted. In addition, a formal audit report may not even be issued. The audit committee, management function, and internal auditors will have to realise the implications this may

Continued in page 4

[The Prodigy Group]

Singapore – (65) 6221 2810
 Hong Kong – (852) 2815 5606
 Malaysia – (60) (3) 2283 5050
 Indonesia – (62) (21) 4288 3120

[Email: enquiry@prodigy-group.com]

Find us on the Web:
[\[www.prodigy-group.com\]](http://www.prodigy-group.com)

Continued from page 3

have on future audit reports and findings. Finally, auditors must be prepared to manage and report the results obtained. For instance, auditors need to consider:

- How often will continuous audit tests be run?
- How will the company deal with anomalies?
- What reporting mechanisms will be developed?
- What will be audit's and management's response?

Other Considerations

While technology has made data easier to access than before, and computing power makes real-time analysis increasingly feasible, technical hurdles remain. In particular, information to be audited must be generated by reliable systems, the continuous audit process must be highly automated, and an effective link between the auditor's system and that of the audited entity must exist. The CAE must ensure that continuous auditing is adopted as an integrated, consistent approach to a controls-based, risk-oriented audit plan.

In addition, the audit department will have to document, develop, and maintain the technical competencies and technology necessary to access, manipulate, and analyze the data contained in disparate information systems. To overcome these challenges, IT auditors must understand the business process sufficiently well before defining the appropriate analytical techniques and identifying potential risk and key control points. IT auditors also should have the ability to gain access to relevant data in a timely manner and be capable of normalising data from disparate systems across the organization.

In addition, the audit department will have to document, develop, and maintain the technical competencies and technology necessary to access, manipulate, and analyze the data contained in disparate information systems.

To overcome these challenges, IT auditors must understand the business process sufficiently well before defining the appropriate analytical techniques and identifying potential risk and key control points. IT auditors also should have the ability to gain access to relevant data in a timely manner and be capable of normalising data from disparate systems across the organization. The aim is to identify the most accurate and effective data source and control points to perform continuous audit tests and analyses. This also will enable auditors to perform a comprehensive set of tests and analyses that address key control points and risk areas, as well as report results in a timely manner. Doing this will require auditors to understand the nature of the tests or analyses used to:

- Investigate exceptions, processes, and systems identified as being at risk.
- Accumulate and quantify total risk exposures.
- Monitor and modify continuous audit variables, tuning the system to produce manageable results.

Finally, IT auditors will have to manage and respond to continuous audit results and determine their appropriate use, follow-up, and reporting mechanisms. For instance, auditors will have to identify whether appropriate action is taken on the findings reported to management and if continuous audit results are considered by management when assessing activities.

Moving Forward

Management's use of continuous audit procedures will help determine if controls are effective and the information produced for decision-making is relevant and reliable. An important benefit of continuous auditing is that instances of error and fraud are reduced significantly, operational efficiency is increased, and bottom-line results are improved through a combination of cost savings and a reduction in overpayments. Additionally, organisations that use continuous auditing often find that they achieve a rapid return on investment. When using continuous auditing, internal auditors need to address the end-to-end business process and IT controls present in business activities. The reliability of business systems and transactional data is paramount not only to the internal control framework and the integrity of financial reporting, but also to the efficiency of business operations. Thus, ensuring the reliability, integrity, and availability of business systems and data should be a key objective for IT auditors and senior managers.

Finally, continuous auditing can help internal auditors and senior management identify and assess risk at many levels throughout the organisation. At a higher level, continuous auditing should take place as part of the annual planning process. Continuous audit results should be used when determining the risk-based audit plan and be made available to the audit team leader as a starting point for the audit. During the conduct of individual audits, continuous auditing can be used to further examine risks. As part of the planning and implementation phases, specific key controls can be tested, such as separation of duties, while comparisons can be used to identify operation improvement areas. After the audit, data-driven indicators can be used to determine if improvements were realised and whether audit recommendations were implemented and had the desired effect.

Prodigy

Data Solution

[The Prodigy Group]

Singapore – (65) 6221 2810
 Hong Kong – (852) 2815 5606
 Malaysia – (60) (3) 2283 5050
 Indonesia] – (62) (21) 4288 3120

[Email: enquiry@prodigy-group.com]

Find us on the Web:
[\[www.prodigy-group.com\]](http://www.prodigy-group.com)



ACL TIPS

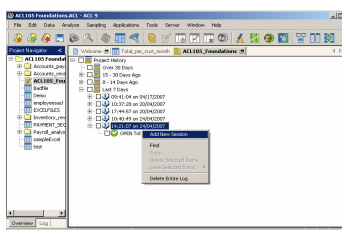
Building New and Different Sessions in Your Log File Now

ACL automatically creates a command log when you create an ACL project. The command log records and displays the commands issued and the results obtained during your data analysis project. The command log acts as valuable documentation that you can use to retrace your steps and repeat earlier results.

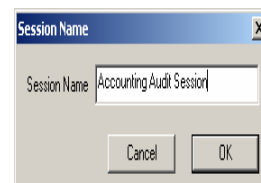
But do you know in the context of the command log, sessions give you the ability to label a series of commands for historical purposes? When you start a session, you can give it a descriptive name. When you later review your log, you can easily see the commands in the session, and the descriptive name reminds you why you performed the commands.

Steps in Adding New Session

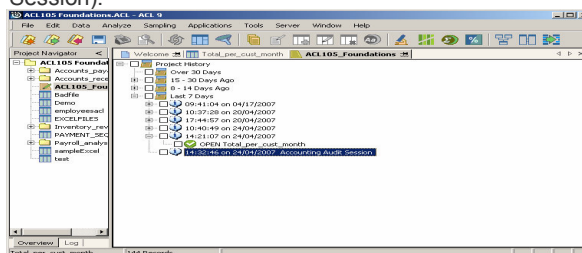
Go to log file then Right Click choose "Add New Session"



Named your session



Any commands that you performed from now on will be recorded onto the new session log file (in the example above, the new activities will be log onto Accounting Audit Session).



Planning For The Best

Source: CFO

A new study by the American Productivity and Quality Centre (APQC) finds that finance organisations that focus on planning, budgeting, and forecasting as key elements of their business strategy are higher performers in all areas than those that focus on cost accounting, controls, and cost management. In general, high-performing companies spend a higher percentage of their resources on budgeting and planning (B&P), but when compared with poor performers, they spend less overall on finance.

The top 20% of participants in the study spent 29 US cents for each US\$1,000 of revenue on budgeting, planning, and forecasting, making it their highest cost. They spent just 25 US cents on cost accounting, controls, and cost management, and 24 US cents on evaluating and managing financial performance. The worst performers spent the most on controls and cost management (US\$2.47) and still spent US\$1.81 on planning and US\$2.08 on managing financial performance.

"High cost does not equal effectiveness," says Lisa Higgins, chief operating officer of APQC and co-author of the report. She says companies that spend a higher percentage up front on B&P have lower overall costs across the board in finance and faster cycle times.

For example, the top performers complete the budget cycle in 30 days, while the bottom 20% take 90 days. High performers are also more likely to use rolling forecasts and link the budgeting process to strategy and compensation. Of course, higher spending on controls and cost management is often a symptom of deeper problems rather than a cause of them. Companies that spend more on planning probably have the luxury of doing so because their financial house is already in order.

Prodigy

Data Solution

[The Prodigy Group]

Singapore – (65) 6221 2810
 Hong Kong – (852) 2815 5606
 Malaysia – (60) (3) 2283 5050
 Indonesia – (62) (21) 4288 3120

[Email: enquiry@prodigy-group.com]

Find us on the Web:
www.prodigy-group.com



Risk Management In Practice: Fraud & Corruption

Source: Martin Samociuk

Despite significant investment in governance frameworks, fraud and corruption management rarely gets beyond compliance requirements. Martin Samociuk explains how employees can be harnessed in the ongoing fraud fight.

Over the past few years, most large organisations have expended a great deal of effort in complying with new legislation that has been introduced in response to a spate of corporate collapses resulting from fraudulent and corrupt behaviour. This has included significant investment in corporate governance, operational risk management and corporate responsibility frameworks.

The result is that there is a greater understanding of the processes and controls that mitigate fraud and corruption. However, once the regulatory requirements have been satisfied, that has usually been the extent of the fraud and corruption prevention strategy, particularly if the organisation has not suffered any prior large frauds. As a number of banks have recently discovered, focusing purely on processes and controls is not enough to prevent fraud. Even after expending all the effort to comply with the legislation, fraudsters have still been able to work undetected over long periods of time. Those organisations have found that there are other elements of a strategy that need to be in place if they are to avoid the unpleasant effects of fraud and corruption.

They have realised that they have not invested enough time and effort in developing one of the most potent anti-fraud and corruption weapons – their own employees. To implement an effective strategy, the organisation needs to empower employees to prevent fraud and corruption. The first step in this process is to make senior management aware that investing in an anti-fraud and corruption culture can help to avoid the unpleasant after effects.

The effects of fraud and corruption

Discovery of fraud and corruption in an organisation has a number of unpleasant effects. The first is the dramatic and damaging effect on innocent employees and third parties – loss of morale and shattered confidence, high stress from investigations and being under suspicion. There is also an unpleasant realisation by senior management that because fraud and corruption losses eventually come off the bottom line, every dollar lost reduces net income by the same amount. If the profit margin of the organisation is, say, 10 per cent, then to recover the lost income requires 10 times the revenue to be generated. Hence, to recover a \$10 million loss requires \$100 million dollars of extra revenue. Additionally, in most cases, the hidden indirect cost such as constraints on expansion and development, damage to reputation and employee morale greatly outweigh the direct costs. Senior managers quickly realise that the costs of investigation are not to be taken lightly. If a case is complicated and involves the international movement of funds, then the investigation costs can be very complex. It is not unusual to spend \$1 million or more on investigating a \$10 million fraud. When cross border money transfers and offshore tax havens are involved, this can cost more than the amount lost.

Prodigy

Data Solution

[The Prodigy Group]

Singapore – (65) 6221 2810
 Hong Kong – (852) 2815 5606
 Malaysia – (60) (3) 2283 5050
 Indonesia – (62) (21) 4288 3120

[Email: enquiry@prodigy-group.com]

Find us on the Web:
[\[www.prodigy-group.com\]](http://www.prodigy-group.com)

Continued from page 6



Probably the single most important (and often the most ignored) realisation by senior management is that the organisation may be carrying other ongoing frauds. There is a wealth of evidence to support this message. For example, research by the Association of Certified Fraud Examiners in the US across a wide range of industries has repeatedly indicated that the typical organisation loses around 5 per cent of its annual revenues to fraud and corruption.

Clearly, investing in preventing fraud and corruption, and hence removing hidden costs, is far better than investigating and cleaning up post event. Once this is acknowledged, then there are a number of steps that can be taken to enhance a fraud and corruption risk management strategy.

Tone at the top

The first step is to set the correct tone at the top. A healthy and ethical organisational culture from the top down is a cornerstone of effective fraud and corruption prevention. However, there is a big difference in aboard of directors simply issuing a code of conduct and fraud and corruption policy and then only paying lip service to it, and in empowering employees to prevent dishonest or corrupt business practices.

For example, some chief executive officers are hired because they achieve results by being ruthless, decisive, aggressive risk-takers who are totally fixated on the bottom line profit. There is nothing intrinsically wrong with this because improved profit is still what the shareholders and stock markets want to see.

However, when these CEOs are surrounded by weak fellow directors and managers, they may begin to treat the company and its assets as their own. They run up large personal expenses which the company pays for, or have work done on their homes by company contractors, or treat their employees as personal servants.

They also pressure employees to indulge in business practices that may be fraudulent and corrupt, but are acceptable, as long as they are making large profits for the company. At the extreme end of the scale, and the most difficult for employees to deal with, is the personality type known as the 'corporate psychopath'. Corporate psychopaths have an overwhelming urge to obtain power and the status that having a lot of money brings.

They desire influence and power over their colleagues and make plans over long periods of time and lie, deceive and manipulate as necessary to commit their frauds without feeling any remorse to commit their fraud. They enjoy humiliating staff without making it obvious that they are behind it and can change their stories so skillfully that it can leave employees confused and wondering if they have stumbled onto a room full of smoke and mirrors.

There is very little to distinguish this type of person from those in the upper echelons of organised crime. Very few people actually see the real persona. Only those few who are on the receiving end of the psychopath's attention catch a glimpse of what is lurking below the surface. The pressure exerted by such a dishonest CEO, director or senior manager can motivate other managers and employees to participate in a major fraud. Such frauds can have catastrophic effects and, once started, are hard to stop. Management-initiated frauds can spread rapidly through an organisation.

This leads to a lack of interest in controlling the business and an increasing temptation to join in with similar, albeit smaller frauds. Honest employees may be powerless because they have not been provided with any awareness training as to what constitutes fraudulent or corrupt behaviour, nor a practical means of reporting concerns. Employees need to see that dishonest or corrupt business practices are not tolerated anywhere in the organisation, even at the top.

Fraud and corruption awareness training

Practical awareness training is essential to assist employees to identify when they may be dealing with fraudulent or corrupt individuals, particularly those who may be senior to them, and to train them how to respond. It is common to find that very few employees have previously received any form of practical instructions.

However, after training, all employees, whatever their position or level, have found the subject engaging, interesting and as a result have been much more prepared to do something about the problem of fraud and corruption. The most effective programs are those that are realistic, enjoyable, and interactive where feedback from the participants is an integral part of the program. Practical, engaging training scenarios and case examples should be used as a mandatory part of training for all employees. The content and examples used should be regularly reviewed and updated. It is very important, before developing and launching a fraud and corruption awareness program, to identify a sponsor that will support it and ensure that it has received sufficient management attention. Sponsors can include corporate security, human

Continued in page 8

Prodigy

Data Solution

[The Prodigy Group]

Singapore – (65) 6221 2810
 Hong Kong – (852) 2815 5606
 Malaysia – (60) (3) 2283 5050
 Indonesia – (62) (21) 4288 3120

[Email: enquiry@prodigy-group.com]

Find us on the Web:
[\[www.prodigy-group.com\]](http://www.prodigy-group.com)

Continued from page 7

Not having a sponsor can lead to the program not being taken seriously and people being too scared to report potential problems for fear of retribution. Often a joint sponsorship team involving one or more executive board members is the preferred and stronger solution. The training program should demystify fraud and corruption for the participants, help their understanding of the methods used against the company by different opponents, as well as teach them how to defend against fraud and how to spot and deal with the red flags. Participants should be encouraged to recognise the loopholes from the perspective of a potential criminal, and the way that psychology may be used to fool an honest person.

Example

An employee with a severe gambling problem used a ballpoint pen containing erasable ink to make out a spurious cheque to a genuine payee. He waited until his manager had an office full of people before knocking on the door and requesting an 'urgent' signature. The manager, whose mind was on other urgent issues, verified that the cheque was made out to the expected payee and signed it without querying the supporting documentation. After this, the employee rubbed out the payee name, inserted his own name and cashed the cheque. He used this technique to raise dozens of cheques over a number of years and obtained more than \$5 million. The fraud only came to light when he went on holiday and a colleague discovered how he had been hiding discrepancies in the books. Equally important is to train managers to detect when employees may have problems that could potentially lead to fraud. For example, several recent frauds have involved employees who had developed gambling addictions as a result of depression. To feed their addictions, they had resorted to stealing from their employer. In each case, the employees had displayed changes to their behaviour and other red flags, which colleagues had either ignored, or not recognised the significance of. Specific training should be provided on how to identify and deal with employees who may be suffering from depression.

Empowering employees

Having trained employees to spot the red flags or fraud and corruption, it is then essential to empower employees to report concerns. Usually, the first reporting line is to their direct line manager. If that is not feasible – for example, when they have suspicions about their line manager – the organisation should implement a whistle blowing procedure to provide a confidential and anonymous route for employees. There is a legal requirement in some countries that have adopted whistle blowing legislation for the whistleblower to be protected from any adverse reaction by the company or directors following their disclosure, providing that the disclosure was not malicious. However, in spite of improvements in legislation, it is still a brave employee who raises issues involving the CEO or other executive director.

Employees working for an executive who is a corporate psychopath may find it very difficult to come up with solid proof even if suspicions are raised about behaviour or lifestyle, or if there is evidence in transactions or documents. The corporate psychopath is an expert at manipulating situations, evidence and people and will have built up a powerful network of supporters, both executive and non-executive. The employee who raises concerns can be sidelined, but not in a manner where they could successfully argue that they had been unfairly discriminated against as a result of them blowing the whistle. Designing and implementing a whistle blowing reporting line, the sponsors together with independent executives – for example, on the audit committee – should include a procedure for dealing with those extreme cases where an employee or external party may raise issues implicating the CEO or other director. Employees are then empowered to report concerns at every level of the organisation without the fear of retribution.

Measuring fraud and corruption resistance

An increasing number of organisations are realising that even though they may be able to certify that they comply with relevant legislation, they still do not have any effective way of measuring how resistant they are to fraudsters or corrupt individuals, or of benchmarking against other organisations, nor of testing the level of understanding by employees about fraud and corruption. Recognizing this need, one of the world's largest independent third party certification and assessment agencies, Det Norske Veritas (DNV), has developed a prototype Fraud and Corruption Resistance Assessment protocol which comprises 12 main elements. The objective is to test in practical terms how effective has been the implementation of the fraud and corruption strategy. The result is a unique fraud and corruption resistance profile of the particular organisation and the gaps represent where there is room for improvement. Behind the assessment model, a detailed protocol consisting of over 500 questions has been developed in an attempt to ensure consistency and avoid ambiguity. Also a weighting and scoring system for each of the 12 elements is applied.

For example, element 1 (Tone at the Top) explores the role of senior management in setting the 'tone at the top' and how the message that fraud and corruption will not be tolerated is communicated throughout the organisation. It is then further divided into eight sub-elements: policy; quality of policy; fraud and corruption resistance management strategy; stakeholder engagement; management representative; operational risk management; existence of relevant standards and procedures; and senior management participation.

[The Prodigy Group]

Singapore – (65) 6221 2810
 Hong Kong – (852) 2815 5606
 Malaysia – (60) (3) 2283 5050
 Indonesia – (62) (21) 4288 3120

[Email: enquiry@prodigy-group.com]

Find us on the Web:
www.prodigy-group.com

Continued from page 8

This is with a total of 46 key questions which carry a weighting equivalent to 12.5 per cent of the total. The end result is a rating that measures resistance. A regular fraud and corruption resistance assessment would typically be requested by either a non-executive board member or the audit committee, but it could equally be initiated from within the company, provided there was some degree of independent assessment. It is unlikely that any organisation is ever going to be 100 per cent fraud and corruption proof. Just being in business carries an inherent risk of fraud and corruption, and fraudsters are very adept at identifying and exploiting new opportunities. However, executives who empower their employees can build an organisation with a much higher resistance to fraud and corruption, thereby adding significant value for shareholders and stakeholders alike.



The following statistics about fraud and white-collar crime are featured in the Association of Certified Fraud Examiners' Report to the Nation. The Report contains a wealth of information about the causes of fraud, the direct and indirect costs of occupational fraud and abuse, and the methods by which employees and other insiders commit fraud. Fraud and abuse costs U.S. organizations more than \$400 billion annually.

- The average organization loses more than \$9 per day per employee to fraud and abuse.
- The average organization loses about 6% of its total annual revenue to fraud and abuse committed by its own employees.
- The typical perpetrator is a college-educated white male.
- Men commit nearly 75% of the offenses.
- Losses caused by managers are four times those caused by employees.
- Median losses caused by executives are 16 times those of their employees.
- The most costly abuses occur in organizations with less than 100 employees.

Communicating With The CEO

Source: CFO

What can the board of directors do to make sure that their CEO has moved to a place focused on mitigating operational risks to enhance opportunities and long term strategy? Fundamentally, the first task is to make sure that the CEO has a management system in place for operational risk. What is needed is a process approach for establishing, implementing, operating, monitoring, maintaining and improving the effectiveness of an organisation's operational risk enterprise architecture (OREA).

Let's break OREA down this a little further to get a better view of some of the specific operational attributes:

Plan

Establish policy, objectives, targets, processes and procedures for managing operational risks to deliver results in accordance with the organisations business objectives.

Do

Implement and operate the policy, controls, processes and procedures.

Check

Assess and measure in applicable areas while reporting results to management for review.

Act

Take corrective and preventive actions based on results to continually improve the OREA framework.

Operational risk management is getting the attention of organizations outside of the major banks at a rapid pace. Board of directors in any industry will soon realize that the successful CEO of the future will be a master of building a culture with effective operational risk management systems at its core.

Prodigy

Data Solution

[The Prodigy Group]

Singapore – (65) 6221 2810
 Hong Kong – (852) 2815 5606
 Malaysia – (60) (3) 2283 5050
 Indonesia – (62) (21) 4288 3120

[Email: enquiry@prodigy-group.com]

Find us on the Web:
www.prodigy-group.com

ISACA International Conference

ACL Services Ltd is proud to be one of the sponsors for the ISACA International Conference which will be held in Swissotel, The Stamford – Singapore on the 11th July 2007.

Audit Risk Management Kuala Lumpur, 12-13 Aug 2007

The Prodigy Group is holding a 2 days conference targeting on the issues and challenges on Audit & Risk Management. We cordially invite you to join us in this fruitful event.

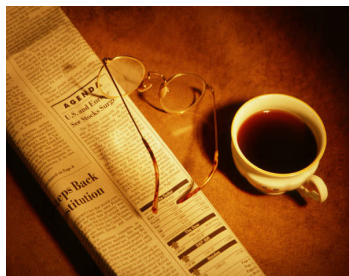
For information of the seminar or becoming as one of our prominent speakers, please email us at conference@prodigy-group.com

IIA Malaysia National Conference 2007

The Prodigy Group is proud to be one of the sponsors for the IIA Malaysia National Conference to be held at the Kuala Lumpur Convention Centre from 20 to 21 August 2007. We would like to invite our valued customers to our booth at the conference for a lucky draw. Simply drop your business card to qualify for the draw. For more information on our participation at the IIAM conference 2007, kindly contact conference@prodigy-group.com.

Prodigy

Data Solution



NEWS FLASH

Fraud Risk Management Consulting

Huge costs are associated with a fraud occurring. Beyond losses directly from the fraud, there are significant costs associated with investigation, litigation, legal, regulatory issues, public relations, staff issues and management time.

Working closely with our partner – Insight Risk Consulting, we are able to help your organisation to strengthen your business and maintain good corporate governance. With our extensive experience servicing the needs of financial services and multi-national clients in Asia, Australia, the United States and Europe, we are sure in providing a proven approach to identify fraud exposures and avoiding the catastrophic consequences of fraud.

Let us begin stress test your control environment and identify loopholes that lead to fraud succeeding. Contact us at enquiry@prodigy-group.com for more information.

www.prodigy-group.com

We are pleased to invite you to our NEW WEBSITE at www.prodigy-group.com.

In this newly design website, we have included more information with regards to our products and services, as well as industries resources for areas such as risk management, audit & compliance, financial planning and management and security management.

Also, visit our newly launched PDS Career Center (*under the Community Tab*) for recruitment help! If you have ever used Monster, CareerBuilder or hundreds of other job boards, you'll know that they can be an extremely effective means to post and search for jobs.

We understand that highly-skilled field like risk management, audit and compliance require something more targeted. As our website is frequently visited by professionals in the field of risk management, audit, compliance and finance, it provides you a targeted platform to receive quality candidates instead of dozens of unqualified ones.

ACL Certification Exam

We are pleased to launch the ACL Certification which participants will earn the ACDA (ACL Certified Data Analyst) designation. For more than 16 years, ACL's proven solutions have enabled auditors and financial decision makers to assure control compliance, reduce risk, detect fraud, minimise loss, enhance profitability, and achieve fast pay back.

The ACL Certification Program sets the industry benchmark for technical proficiency and professional expertise in using ACL software. You will gain greater confidence, broader recognition of your competence and experience using ACL technology, and a competitive advantage in today's job market.

To find out more about the ACL Certification Exam, please contact us at training@prodigy-group.com

Success To Our First Maiden Seminar In Hong Kong

The very first maiden Hong Kong seminar was held at the Renaissance Harbour View Hotel – Hong Kong on the 25th April 2007 in conjunction with ACL Services Ltd. We had received overwhelming response in this half day seminar and we would like to express our sincere thanks to all delegates and our prominent speakers for their continuous support and participation.

Interested to be on our mailing list for our next Hong Kong seminar? Email us at conference@prodigy-group.com

[The Prodigy Group]

Singapore – (65) 6221 2810
 Hong Kong – (852) 2815 5606
 Malaysia – (60) (3) 2283 5050
 Indonesia – (62) (21) 4288 3120

[Email: enquiry@prodigy-group.com]

Find us on the Web:
[\[www.prodigy-group.com\]](http://www.prodigy-group.com)

In our next issue,

- ◆ Corporate Governance
- ◆ Operational Risk
- ◆ Sarbanes Oxley
- ◆ ACL Tips
- ◆ Just For Laugh etc.....

Open Enrolment ACL Training Schedule

Singapore ♦ Hong Kong ♦ Malaysia ♦ Indonesia ♦ Thailand ♦ Philippines
 May – June 2007

Prodigy Data Solution is the ONLY ACL certified trainer in Asia South. As certified training provider, we can ensure that your classes will use the latest version of the software, the most up-to-date training materials, and techniques distilled from ACL's experience in delivering training worldwide to over 30,000 ACL users for over a decade.

VENUE	COURSE NAME	May-07	Jun-07	Jul-07
SINGAPORE	ACL 105 - Foundation of ACL : Concepts & Practice	07-08	11-13	08-11
	ACL 111 - Foundation of ACL: Banking & Finance (NEW ONLY O.S.)	-	-	-
	ACL 201 - Data Analysis Techniques	10-11	07-08, 14-15	12-13
	ACL 301 - Advanced ACL Concepts & Techniques: Functions	21	18	25
	ACL 302 - Advanced ACL Concepts & Techniques: Scripts	22-23	19-20	26-27
	ACL 303 - Advanced ACL Concepts & Techniques: Functions & Scripts	21-23	18-20	25-27
	Fraud Detection Techniques Using ACL	24-25	25-26	30-31
	ACL Data Access	28	21	18
	Introduction to Data Forensic Techniques (NEW)	29	22	16
ACL Version 9: Refresher	30	29	20	
JAKARTA, INDONESIA	ACL 105 - Foundation of ACL : Concepts & Practice	02-04	04-06	02-04
	ACL 111 - Foundation of ACL: Banking & Finance (NEW ONLY O.S.)	-	-	-
	ACL 201 - Data Analysis Techniques	10-11	07-08	16-17
	ACL 301 - Advanced ACL Concepts & Techniques: Functions	23	13	18
	ACL 302 - Advanced ACL Concepts & Techniques: Scripts	24-25	14-15	19-20
	ACL 303 - Advanced ACL Concepts & Techniques: Functions & Scripts	23-25	13-15	18-20
	Fraud Detection Techniques Using ACL	28-29	18-19	23-24
	ACL Data Access	07	22	26
	Introduction to Data Forensic Techniques (NEW)	08	27	25
ACL Version 9: Refresher	30	29	27	
KUALA LUMPUR, MALAYSIA	ACL 105 - Foundation of ACL : Concepts & Practice	14-16	18-20	04-06
	ACL 111 - Foundation of ACL: Banking & Finance (NEW ONLY O.S.)	-	-	-
	ACL 201 - Data Analysis Techniques	17-18	21-22	09-10
	ACL 301 - Advanced ACL Concepts & Techniques: Functions	28	27	11
	ACL 302 - Advanced ACL Concepts & Techniques: Scripts	29-30	28-29	12-13
	ACL 303 - Advanced ACL Concepts & Techniques: Functions & Scripts	28-30	27-29	11-13
	Fraud Detection Techniques Using ACL	24-25	21-22	23-24
	ACL Data Access	21	04	26
	Introduction to Data Forensic Techniques (NEW)	31	05	30
ACL Version 9: Refresher	04	06	27	
HONG KONG	ACL 105 - Foundation of ACL : Concepts & Practice	14-16	11-13	02-04
	ACL 111 - Foundation of ACL: Banking & Finance (NEW ONLY O.S.)	-	-	-
	ACL 201 - Data Analysis Techniques	21-22	14-15	05-06
	ACL 301 - Advanced ACL Concepts & Techniques: Functions	17	20	23
	ACL 302 - Advanced ACL Concepts & Techniques: Scripts	18-19	21-22	24-25
	ACL 303 - Advanced ACL Concepts & Techniques: Functions & Scripts	17-19	20-22	23-25
	Fraud Detection Techniques Using ACL	-	25-26	26-27
	ACL Data Access	-	27	-
	Introduction to Data Forensic Techniques (NEW)	-	28	30
ACL Version 9: Refresher	-	29	-	
MANILA, PHILIPPINES	ACL 105 - Foundation of ACL : Concepts & Practice	-	20-22	-
	ACL 111 - Foundation of ACL: Banking & Finance (NEW ONLY O.S.)	-	-	-
	ACL 201 - Data Analysis Techniques	-	-	-
	ACL 301 - Advanced ACL Concepts & Techniques: Functions	-	25	-
	ACL 302 - Advanced ACL Concepts & Techniques: Scripts	-	26-27	-
	ACL 303 - Advanced ACL Concepts & Techniques: Functions & Scripts	-	25-27	-
	Fraud Detection Techniques Using ACL	-	28-29	-
	ACL Data Access	-	-	-
	Introduction to Data Forensic Techniques (NEW)	-	-	-
ACL Version 9: Refresher	-	-	-	

Onsite specialised workshops are also available. Kindly contact training@prodigy-group.com for more information

The Prodigy Group is a total solution provider offering extensive solutions on Audit & Compliance, Risk Management, Financial Management and Security Management to financial executives, audit professionals, fraud investigators, risk managers, business analysts, IT professionals and senior executives. Through the experiences and expertise of our consultants, our solutions developed have been proven and tested in many established organisations, giving our clients confidence in the reliability, accuracy, and integrity of the data underlying the increasingly complex business operations.

Integrating market-leading software, Prodigy facilitates our clients in managing commitments and obligations better and hence improved their internal business processes. Transformed around the themes of simplicity and usability, our solution can be applied extensively throughout the organisation, be it for financial management, anti-money laundering, data forensics, performance analysis, management reporting and so forth, providing organisations with the in-depth analysis and foresight needed to overcome the complex challenges ahead and to Prodigy's overarching goal of performance with integrity.

Authorised Distributor for ACL, KnowRisk, INCA Planning & Arbutus

Prodigy
Data Solution