



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

Prodigy Newsbyte

The Insider Threat: 16 Tips to Protect Critical Data

By: Linda McGlasson, 9th March 2009.

Is 2009 the Year of the Insider Threat?

Last August's arrest of a Countrywide employee in California illustrates the potential impact of a single insider with access to sensitive information. The FBI charged the former employee with taking 2 million names and personal information from the mortgage bank and selling them for a profit.

Another example: **Last month's indictment in federal court** of an ex-consultant at Fannie Mae for allegedly placing a logic timebomb on the mortgage giant's computer systems last October. If not discovered, this trap would have wiped out all the company's 4,000 computer servers.

These illustrate the need to have monitoring and controls in place, along with an education program to help employees learn about the insider threat as part of an information security awareness program.

Heightened Risk

The increased number of employers handing out pink slips doesn't help quell the threat, with a record number of people on the unemployment lines and others at work worried about their own positions. "We're going to see some insider events where insiders are tempted enough by money to enable these compromises to take place from outsiders, allowing access to payment data and account information," says Mike Urban, Senior Director of Fraud Solutions at Fair Isaac, predicts,

Urban, with more than 14 years of electronic fund transfer experience and fraud resolution in the industry, says all institutions should review their strength against an insider threat. "When should institutions be concerned about insider threat," he says. "During times before, during and after a merger takes place, or during uncertain times such as the times we're in now."

The areas once thought separate -- financial fraud and information security -- are converging, he notes. "People are laid off, you've got fewer people doing work -- a lot of things that would be normally picked up, or watched or noticed will not be because the person that used to do that isn't there anymore," Urban says. Even employees who are still at the institution and think they may be laid off begin thinking what they could take to protect their own financial future wellbeing," he says.

Senior management needs to consider the risks when system mergers take place. "There's a lot of chances for information to be in places it shouldn't be," Urban says, so a high level of awareness needs to be encouraged.

Tips for Fighting the Threat

Organisations also should take a close look at the "Insider Threat Study" by Carnegie Mellon's CERT Program. Randy Trzeciak of Carnegie Mellon's CERT insider threat research program was recently interviewed by Information Security Media Group on 100 insider cases that the study compiled since 2001 and some highlights from its findings.

The study shows the "big picture" analysis of insider IT sabotage and has seven general observations about the cases. Another excellent source for institutions to follow that Trzeciak recommends is the CERT "Common Sense Guide to the Prevention and Detection of the Insider Threat."

Here are 16 practices that CERT says will help provide an institution with defensive measures that could help prevent or detect insider incidents:

1. Consider threats from insiders and business partners in your enterprise-wide risk assessments. This is especially difficult for institutions, as the scope of the "insider" stretches out to service providers and vendors.

2. Clearly document and consistently enforce policies and controls. CERT sees that clear documentation and communication of technical and organisational policies and controls "could have mitigated some of the insider incidents, theft, modification and IT sabotage" it has in its case library.

3. Institute periodic security awareness training for all employees. Developing a culture of security awareness is only the first step, CERT says employees "also need to be aware that individuals, either inside or outside may try to co-opt them into activities counter to the organisation's mission."

4. Monitor and respond to suspicious or disruptive behavior, beginning with the hiring process. This should begin even before an employee is hired, CERT says. Things to look out for include repeated policy violations "that may indicate or escalate into more serious criminal activity."

5. Anticipate and manage negative workplace issues. Institutions should carefully review their processes, beginning with pre-employment, employment and termination. Of special note, CERT notes, "Contentious employee terminations must be handled with utmost care, as most insider IT sabotage attacks occur following termination."

6. Track and secure the physical environment. Most institutions are already on top of this issue, though CERT's reminder about access attempts is clear. "Access attempts should be logged and regularly audited to identify violations or attempted violations of the physical space and equipment access policies."

7. Implement strict password and account management policies and practices. This is important, CERT says, and "password and account management policies and practices should apply to employees, contractors and business partners."

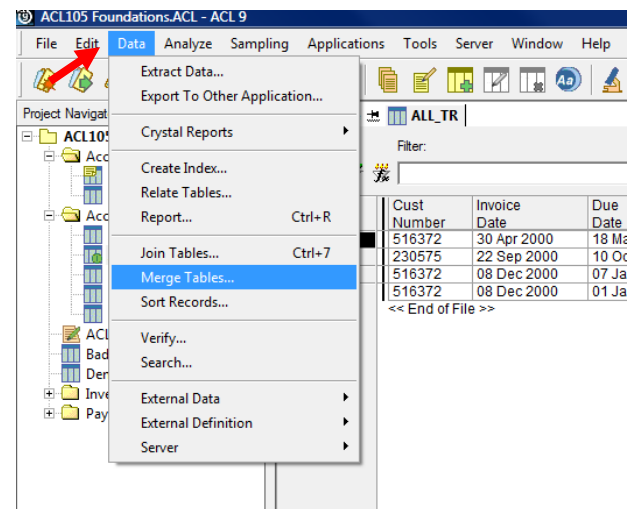
8. Enforce separation of duties and least privilege. By giving employees only the resources they need to do their jobs, "the possibility that one individual could commit fraud or sabotage without cooperation of another individual within the organisation is limited."



Merging Files

When performing our audit work, sometimes we need to combine the records from more than 1 file before we can perform the analysis. To accomplish this, we can use the MERGE command.

Unlike JOIN and RELATE which add columns (fields), MERGE adds rows (records). The MERGE command can be found under Data (as shown below)



There are some rules that must be followed:

1. Ensure that all tables that are to be combined have exactly same structure. The fields must also be ordered similarly.
2. All of the tables must be in the same project.

Sometimes when ACL keeps prompting you with an error even though it looks like you have followed the rules closely, don't get frustrated – the trick here is that you need to Extract all the harmonized fields to the new table before you can merge it. Once you have combined all the files, the temporary table can be deleted.

Key points to note when using this command:

1. Choose one of the tables as your reference for the structure and ensure that the rest follow this table structure and field sequence.
2. If you make any changes to the field length or type, this field must be extracted to the new table while ensuring that the sequence of the field same as that of the reference table.

HAPPY MERGING!

9. Consider insider threats in the software development life cycle. While this one won't apply to many of the institutions that operate systems but don't develop them, consideration should be made to look into the software development from vendors and core service providers.

10. Use extra caution with system administrators and technical or privileged users. Many institutions already follow CERT's recommendations on this by separation of duties or employing the two-man rule for critical system administrator functions. CERT's insight on this, "Technically adept individuals are more likely to resort to technical means to exact revenge for perceived wrongs."

11. Implement system change controls. In CERT's study of 100 insider incidents, there are a wide variety that relied on unauthorised modifications to the organisation's system -- a strong argument for change controls as a mitigation strategy.

12. Log, monitor and audit employee online actions. CERT's study shows new findings in this area that can help institutions to refine data leakage prevention strategy. One example CERT gives is to monitor an employee's online actions around the time the employee is terminated.

13. Use layered defense against remote attacks. CERT's recommendation is based on the premise that should employees know they are being monitored, a disgruntled insider will try to use remote access to gain access. Especially important is disabling remote access and retrieval of company equipment from terminated employees.

14. Deactivate computer access following termination. This should happen quickly, including all physical locations, networks, systems, applications and data.

15. Implement secure backup and recovery processes. CERT admits that no institution can completely eliminate the risk of insider attack. Preparation and implementation of a secure backup and recovery process is critical.

16. Develop an insider incident response plan. CERT says this could prove challenging, "because the same people assigned to a response team may be among the most likely to think about using their technical skills against the organisation." CERT recommends that only those responsible for carrying out the plan need to understand and be trained on its execution.

Six Steps to an Effective Continuous Audit Process

Source: Internal Auditor Online

Establishing priority areas and determining the process' frequency are two of the six steps that internal auditors and senior managers need to take into consideration before making the switch to continuous auditing.

The need to improve and accelerate audit activities has led in part to the increased adoption of continuous auditing as a vital monitoring tool. Initially recorded at AT&T Corp. by its Bell Laboratories research center during the late 1980s and early 1990s, continuous audit efforts are now under way in organisations including Siemens, HCA Inc., Unibanco, the New York Federal Reserve, and IBM. Additionally, legislation such as Section 404 of the U.S. Sarbanes-Oxley Act of 2002 and audit software vendors, including ACL, IDEA, Approva, and Oversight, are molding and giving large momentum to the continuous audit field. Consequently, as continuous auditing continues to grow around the world, internal auditors and senior managers need to understand the necessary actions required to support an effective continuous audit process, including establishing audit priority areas and determining the process' frequency.

BEFORE PITCHING THE IDEA

When organisations begin evaluating the adoption of continuous auditing, three common issues usually arise that if expected can be managed effectively. First, is the confusion among auditors and senior management regarding the differences between continuous auditing and continuous monitoring. Second, is the need for auditors to understand the role of continuous auditing as a meta control (i.e., a control of controls). And third, is the concern that implementing continuous auditing will lead to a loss of independence and objectivity as audit professionals become operationally involved in the process. While the way in which companies address these challenges will be unique to their organisation, the following best practices can help them prepare for these issues.

Continuous Monitoring Vs. Continuous Auditing

Typically, continuous monitoring is a management function to ensure that company policies, procedures, and business processes are operating effectively and addresses management's responsibility to assess the adequacy and effectiveness of internal controls. In addition, continuous monitoring 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.

Although many of the continuous monitoring techniques used by management are similar to those performed by internal auditors during continuous audit activities, continuous auditing usually enables auditors to evaluate the adequacy of management's monitoring function and identify and assess risk areas. In addition, clearly communicating the differences between the two will aid in avoiding confusion or resistance to continuous auditing as a redundant effort.

Meta Control

Continuous auditing also tends to be dynamic in nature (i.e., the auditor can turn continuous audit processes on and off based on current system loads by reconfiguring these activities according to the internal audit plan). Therefore, by monitoring particular configurable items, continuous auditing provides an additional level of controls and acts as a meta control.

For example, a bank can issue an alarm under pre-specified circumstances to the bank manager's supervisor whenever loans reach a pre-authorised level. This activity then increases the level of controls that can be configured, such as by including the choice to have an alarm issued and under which circumstances.

Independence and Objectivity

Finally, because continuous audit activities are different from those taking place during a more traditional audit, audit principles need to be re-conceptualised. This is because continuous auditing often places the auditor in the middle of the transaction flow. For instance, at a major US-based electronic brokerage firm that monitors its client's electronic transactions, auditors are notified when a transaction is blocked after certain analytical parameters are met. The auditor then deals directly with the client. As this example illustrates, it is important for internal auditors to make sure that the continuous audit process has a system of checks and balances to maintain the independence and objectivity of their work throughout the audit.

KEY STEPS TO IMPLEMENTING CONTINUOUS AUDITING

Once the issues above are understood by managers and auditors

continuous auditing. Generally, the implementation of continuous auditing consists of six procedural steps, which are usually administered by a continuous audit manager. Knowing about these steps will enable auditors to better monitor the continuous audit process and provide recommendations for its improvement, if needed. These steps include:

1. Establishing priority areas.
2. Identifying monitoring and continuous audit rules.
3. Determining the process' frequency.
4. Configuring continuous audit parameters.
5. Following up.
6. Communicating results.

Figure 2. Continuous audit implementation steps

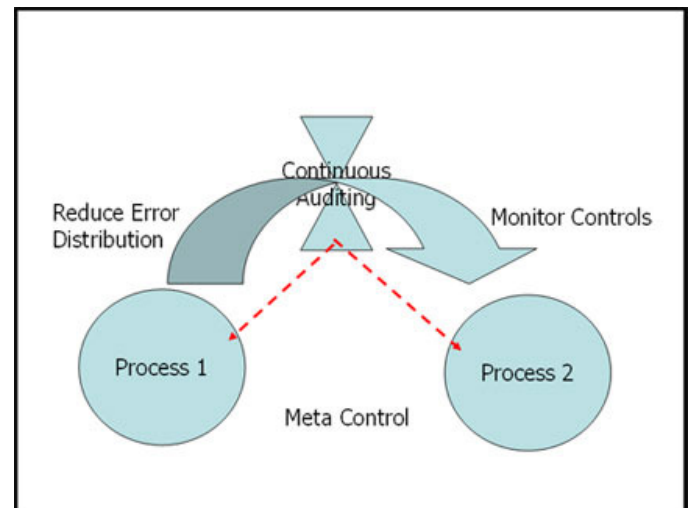
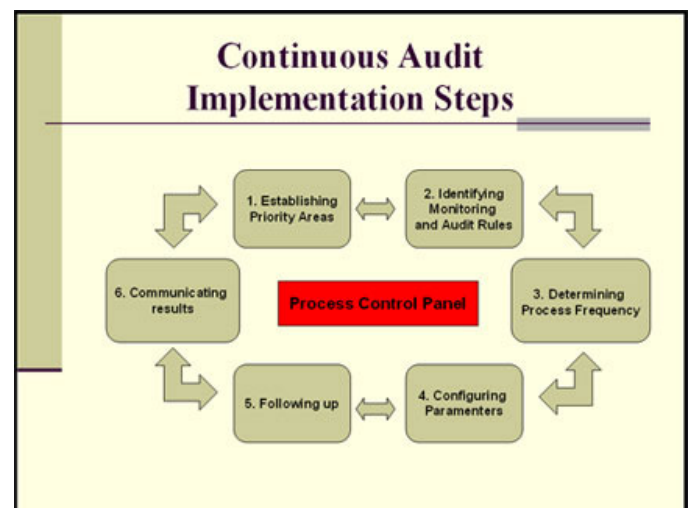


Figure 1. Illustration of the continuous audit process' dynamic nature



Below is a description of each:

1. Establishing Priority Areas

The activity of choosing which organisational areas to audit should be integrated as part of the internal audit annual plan and the company's risk management program. Many internal audit departments also integrate and coordinate with other compliance plans and activities, if applicable. (Steps 2-6 below are applicable to all of the priority areas and processes being monitoring as part of the continuous audit program.)

Typically, when deciding priority areas to continuously audit, internal auditors and managers should:

- Identify the critical business processes that need to be audited by breaking down and rating risk areas.
- Understand the availability of continuous audit data for those risk areas.
- Evaluate the costs and benefits of implementing a continuous audit process for a particular risk area.
- Consider the corporate ramifications of continuously auditing the particular area or function.
- Choose early applications to audit where rapid demonstration of results might be of great value to the organisation. Long extended efforts tend to decrease support for continuous auditing.
- Once a demonstration project is successfully completed, negotiate with different auditees and internal audit areas, if needed, so that a longer term implementation plan is implemented.

When performing the actions listed above, auditors need to consider the key objectives from each audit procedure. Objectives can be classified as one of four types: detective, deterrent (also known as preventive), financial, and compliance. A particular audit priority area may satisfy any one of these four objectives. For instance, it is not uncommon for an audit procedure that is put in place for preventive purposes to be reconfigured as a detective control once the audited activity's incidence of compliance failure decreases.

2. Monitoring and Continuous Audit Rules

The second step consists of determining the rules or analytics that will guide the continuous audit activity, which need to be programmed, repeated frequently, and reconfigured when needed. For example, banks can monitor all checking accounts nightly by extracting files that meet the criterion of having a debt balance that is 20 percent larger than the loan threshold and in which the balance is more than US \$1,000.

In addition, monitoring and audit rules must take into consideration legal and environmental issues, as well as the objectives of the particular process. For instance, how quickly a management response is provided once an activity is flagged may depend on the speed of the clearance process (i.e., the environment) while the activity's overall monitoring approach may depend on the enforceability of legal actions and existing compliance requirements.

3. Determining the Process' Frequency

Although the process is called continuous auditing, the word continuous is in the eye of the beholder. Auditors need to consider the natural rhythm of the process being audited, including the timing of computer and business processes as well as the timing and availability of auditors trained or with experience in continuous auditing. For instance, although increased testing frequency has substantial benefits, extracting, processing, and following up on testing results might increase the costs of the continuous audit activity. Therefore, the cost-benefit ratio of continuously auditing a particular area must be considered prior to its monitoring.

Furthermore, other tools used by the manager of the continuous audit function include an audit control panel in which frequency and parameter variations can be activated. Hence, the nature of other continuous audit objectives, such as deterrence or prevention, may determine their frequency and variation.

4. Continuing Continuous Audit Parameters

Rules used in each audit area need to be configured before the continuous audit procedure (CAP) is implemented. In addition, the frequency of each parameter might need to be changed after its initial setup based on changes stemming from the activity being audited. Hence, rules, initial parameters, and the activity's frequency — also a special type of parameter — should be defined before the continuous audit process begins and reconfigured based on the activity's monitoring results.

When defining a CAP, auditors should consider the cost benefits of error detection and audit and management follow-up activities. For instance, in the example of the bank described earlier, the excess threshold of US \$1,000 could lead to a number of false negatives (e.g., values that were ignored when the balance was smaller than US \$1,000 but were identified as representing a problem) and a number of false positives (e.g., values with balances above US \$1,000 that were flagged but were accurate).

If the threshold is increased to US \$2,000, there will be an increase in false negatives and a decrease in false positives. Because follow up costs would go up as the number of false positives increases and the presence of false negatives may lead to high operational costs for the organisation, internal auditors should regularly reevaluate if error detection and follow-up activities need to be continued, reconfigured, temporarily halted, or used on an ad hoc basis.

Furthermore, the stratification of audited data into sub-groups allows organisations to better monitor the activity and reconfigure any parameters (e.g., auditors will be notified when balances larger than 20 percent of the debt remain that are also larger than US \$5,000). However, the more complex the rule and its conditional components, the more parameters that must be examined, monitored, and sometimes reconfigured.

5. Following Up

Another type of parameter relates to the treatment of alarms and detected errors. Questions such as who will receive the alarm (e.g., line managers, internal auditors, or both — usually the alarm is sent to the process manager, the manager's immediate supervisor, or the auditor in charge of that CAP) and when the follow-up activity must be completed, need to be addressed when establishing the continuous audit process.

Additional follow-up procedures that should be performed as part of the continuous audit activity include reconciling the alarm prior to following up by looking at alternate sources of data and waiting for similar alarms to occur before following up or performing established escalation guidelines. For instance, the person receiving the alarm might wait to follow up on the issue if the alarm is purely educational (i.e., the alarm verifies compliance but has no adverse economic implications), there are no resources available for evaluation, or the area identified is a low benefit area that is mainly targeted for deterrence.

6. Communicating Results

A final item to be considered is how to communicate with auditees. When informing auditees of continuous audit activity results, it is important for the exchange to be independent and consistent. For instance, if multiple system alarms are issued and distributed to several auditees, it is crucial that steps 1-5 take place prior to the communication exchange and that detailed guidelines for individual factor considerations exist. In addition, the development and implementation of communication guidelines and follow-up procedures must consider the risk of collusion. Much of the work on fraud indicates that the majority of fraud is collusive and can be performed by an internal or external party. For example, in the case of dormant accounts, both the clerk that moves money and the manager that receives the follow-up money may be in collusion since the manager's key may have to be used for certain transactions.

ADDITIONAL CONSIDERATIONS

Besides the six steps described in the previous section, two additional issues that emerge when implementing continuous auditing are the infrastructure needed for the process to work and its impact on the workplace.

Organisational Infrastructure

Because continuous auditing is a part of the company's audit function, it must be kept independent of management. Therefore, during the planning stages, auditors need to keep in mind the process' independence when designing its structure. For instance, a typical internal audit department is structured so that areas of the department focus on different cycles or business activities. In addition, the department may be divided into financial and IT audit functions.

Sometimes, however, IT audit activities are incorporated as part of existing IT operations. In organisations such as these, the development of continuous auditing is usually delayed because the activity may not get the necessary development priority. Regardless of whether IT audit activities are part of the organisation's IT or internal audit department, the organisation must maintain the process' independence as well as allocate resources in support of continuous audit activities.

Impact on Personnel

In addition, the audit manager in charge of the continuous audit process should have a more technical understanding of IT as well as extensive experience on the activities being audited. However, hiring, training, and retaining auditors who can implement and monitor continuous audit activities might be challenging due to the scarcity of internal auditors with knowledge in the area. Furthermore, the continuous audit process might create a daily stream of issues that need to be resolved, which might prove stressful given current personnel resources, and might require the continuous audit manager to exert adequate authority in moments of exceptions.

FINAL THOUGHTS

While more organisations are progressively implementing continuous auditing — and, along the way, improving the quality of the data gathered during each audit — auditors and managers that are looking to implement a continuous audit approach need to be willing to move beyond their traditional yearly audit activities. Although not a lot of guidance exists today about the best ways to implement a continuous audit process, as with any major change, the evolution toward continuous auditing will take time and substantial attention from senior management.



Top 10 trends in Information Security for 2009

By: Rana Gupta, 24 December 2008

Advances in security technology simply have not kept pace with the Internet's growth. Security is getting better, but complexity is getting worse faster. It is expected that this trend will continue in 2009 as well

1) Data Breaches

There is an increase in the deployment of encryption technologies in order to protect sensitive data. In fact, there is a decreased security breaches via encryption solutions and this trend will continue in 2009 as well.

The economic melt down will lead to increasing incidents of data breaches though corporate will be clueless of this happening in most cases even so they will be reluctant to admit this in public even if they do detect/find such data breaches due to lack of any strong compliance acts in India.

2) Increasing web threats

As the number of available web services increases and as browsers continue to converge on a uniform interpretation standard for scripting languages, such as JavaScript, it is expected that the number of new Web-based threats to continue to increase.

3) Bot can be a threat

In the near future bots will further diversify and evolve in their behaviour. This might lead to increase in the hosting of more phishing sites. Bots can perpetrate a wide variety of malicious activity.

4) Protection of mainframe environment

With the continued growth of security threats and increase in government regulations and industry standards, such as PCI, it is more important than ever for enterprises to safeguard critical data that sits in mainframe environments to protect themselves against security breaches and hefty non-compliance fines.

5) Information is critical

Off late people have realised that information is more valuable than ever. Companies and institutions will be taking concrete majors to protect the information. So, it is expected that the industry will witness the increase in the user of single sign-on and authentication for users.

6) Hacking becomes profession

Hacking has become a criminal profession. It is no more a hobby. More and more attacks are undertaken in an organised manner and led by criminals with bad motives. Extortion related to denial-of-service attacks and phishing are two examples of criminal attacks. It is very important to address this issue.

7) Stronger mobile platforms

With the increase in mobile workforce and availability of more complex handsets (with lot of applications on it), the interest in mobile security will be higher. In the days to come anti-virus software for Mobile Phones will become a necessity and the industry will start to seek solutions to do away with spam through SMS.

8) Virtualisation a gateway to threat

From a security perspective, the spread of virtualisation is causing serious threats and the impact of the same in the enterprise space is quite evident. But one cannot live without virtualisation. That's why it will be observed that more and more enterprises will be opting for stringent security majors as far as virtualisation is concerned.

9) More complex less secured

As systems are getting more complex, they are getting less secure. And more and more use of Internet is making the infrastructure more complex. Advances in security technology simply have not kept pace with the Internet's growth. Security is getting better, but complexity is getting worse faster. It is expected that this trend will continue in 2009 as well. CIO/CSOs will continue to seek ways to protect data through out their lifecycle but will find that nothing fits their complex needs and at the end of the day their data will continue to remain as vulnerable as ever

10) Role of encryption

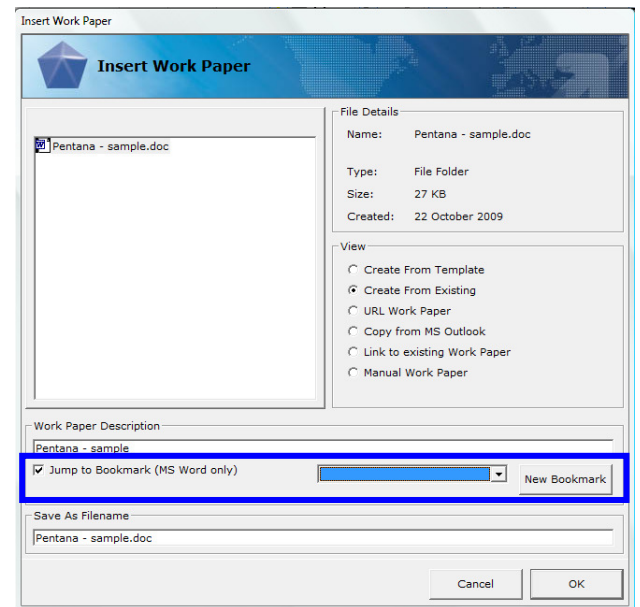
The more practical CIOs will be quick to realise that there is no silver bullet to take care of all their data-protection needs and deploy Disk Encryption solutions along with Pre-Boot Authentication to secure the data in the wake of physical theft of laptops or hard-disks.

Tips for PAWS

Using Bookmarks in Work papers

Bookmarks are useful for pointing to specific areas of a large document.

When adding a work paper based in MS Word or Excel or Visio, optionally click the 'Jump to Bookmark' checkbox if you want to jump to a specific bookmark within the resulting document.

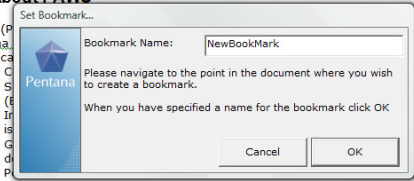


You can then select from existing bookmarks within the source document.

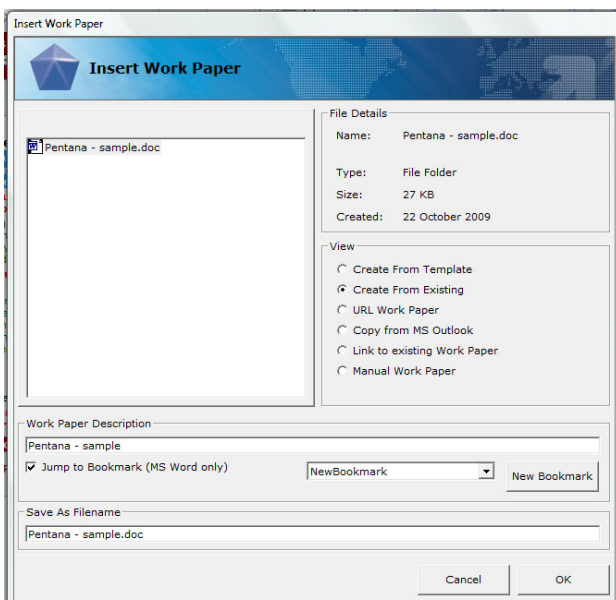
To create a new bookmark, click 'New Bookmark'. The following will appear:

Introduction

1.1 About PAWS



PAWS (Pentana) comprises the following product modules:
PAWS Universe – for the definition of business units or processes, the management, and analysis of an integrated Risks & Controls Register, assignment scheduling and management, and action tracking. PAWS Universe comes with:



Place the cursor in the document where you want the bookmark to be inserted, and type in the name for the bookmark. Then Click OK.

You will then come to the screen on the left. Click OK.

Voila! You have added a bookmark to your document. When you open your document, you will be brought to the location of the bookmark.

About the Survey: The Institute of Internal Auditors research foundation released their Global Audit Information Network (GAIN) 2009 IT Audit Benchmarking Survey and report in March 2009. The report provides a summary of key findings and recommendations from IIA members to help those looking to establish an effective IT audit process and acquire technology-based audit tools to maximize their internal audit efforts.

SURVEY

INTERNAL AUDIT BENCHMARKING 2009

“ACL training, consulting and the AuditExchange platform are helping us move toward a continuous monitoring environment. We’re increasing the perceived value of internal audit throughout the enterprise.”

Bob Walker, Internal Audit Manager
American Automobile Association of Northern California, Nevada & Utah

The 2009 IT Audit Benchmarking Survey found that ACL technology is the audit analytics solution of choice. ACL is significantly preferred in the areas of data extraction and analysis, fraud detection and continuous auditing. Reasons given for use of ACL by study participants include its ability to look at control weaknesses, the ease and breadth with which users can evaluate data, and its ability to provide exception reports.

There is increasing pressure on audit to do more with less. Internal audit’s role in business assurance is at the forefront as the profession looks to provide more confidence and transparency to the audit committee and CFOs around everyday business activities. To accomplish this, the current focus of many audit teams is to enhance the quality of their work and effectiveness of the department using technology. They need to be more productive, and better focused on emerging risks. Audit teams are also seeking to deliver timely value to the enterprise by distributing, tracking and escalating potential issues for better business insight and control.

In establishing a baseline for the report, auditors were asked ‘Do you have the skills to address the issues that will impact IT audits the most within the next 24 months?’ and, surprisingly, nearly one in three said no. Reasons given include:

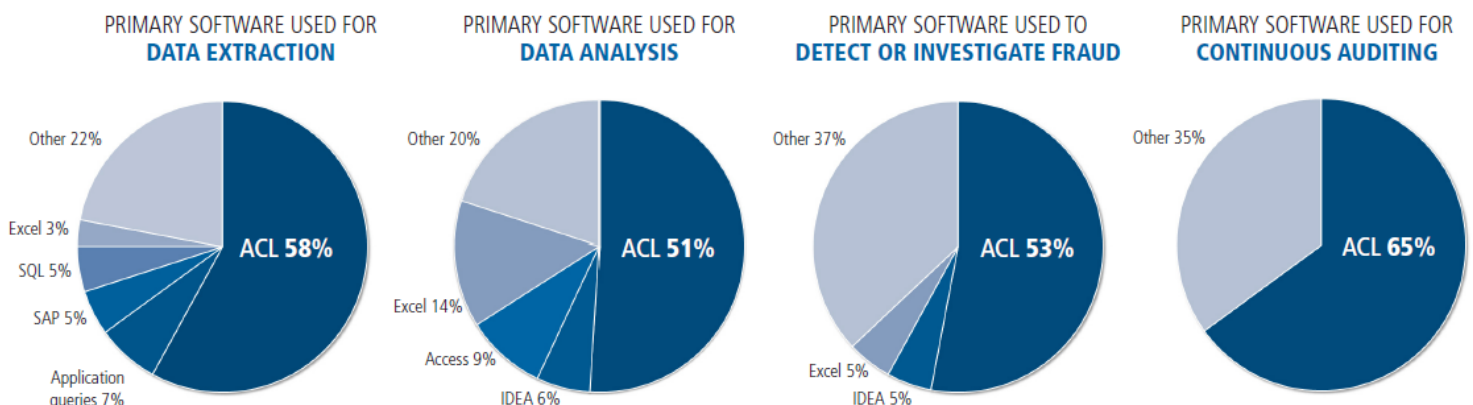
“The internal audit activity does not include IT auditors, auditors with the necessary IT training or knowledge.”

“The internal audit department does not have the financial resources or time to allow auditors to obtain the necessary skills, and there are not enough IT auditors.”

This is clearly an issue that needs to be addressed as more audit teams look to develop strategies to increase technology proficiently and usage throughout their departments. The benefits cited by survey participants of a robust audit technology program included increased productivity, ability to analyse an entire data population, and identifying financial savings to the organisation.

View the full report by searching “audit benchmark” on The IIA’s website: www.theiia.org

Summary of key findings among survey participants that use audit software for each function:





PRODIGY NEWS & EVENTS

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.

User Group Meetings Philippines and Singapore

We would like to thank all customers who had attended the recent Prodigy User Group Meeting in Philippines and ACL User Group Meeting in Singapore on 17 September 2009 and 8 October 2009 respectively.

At the same time, we would like to take this opportunity to thank Bank of Commerce for hosting the meeting at Intercontinental Manila, Philippines, as well as the Public Utilities Board (PUB) for hosting the meeting at Marina Barrage, Singapore.

We hope you have found the sessions to be useful and hope to see you at future events!

Contribute an Article & Get Rewarded!

Calling out to all Newsbyte readers! Simply submit an article and if it gets published in the next issue of Newsbyte, you receive a prize! Articles can revolve around the topics of Continuous Control Monitoring, Fraud Detection & Prevention, Business Assurance, Compliance or any topic of interests.

Hurry send in your article now!

Upcoming Conferences

The Prodigy Group is proud to be one of the sponsors for the following upcoming events:

IIA Indonesia 2009 National Conference

Date: 2-3 November 2009

Venue: Bandung, West Java

Theme: Current Issues in Internal Auditing Profession and Activities

TACS 2009

Date: 5-6 November 2009

Venue: Orchard Parade Hotel, Singapore

Theme: A Brave New World: Governance, Security and Assurance

We look forward to meeting you at the conferences!

NEW! Business Assurance Product

The **FulcrumWay GRCMonitor** is the latest addition to Prodigy's group of Business Assurance products. FulcrumWay **Segregation of Duties (SOD)** Software Services segregates access privileges within your ERP system and restricts sensitive data access to privileged users by employing a violations management engine, GRCMonitor, to scan user access using the security structure of your ERP system. GRCMonitor identifies users and their role assignments that violate one or more SOD policies. It enables your compliance, risk and IT teams to automate SOD risk assessments and changes, monitor role assignments and responsibilities, as well as detect, correct and prevent access violations.

For more information, please email us at enquiry@prodigy-group.com

ACL Certification Exam

Prodigy will be hosting the Intermediate level of ACL Certification Exam this coming November 2009 in the following countries: Singapore, Malaysia and Hong Kong.

The ACL Certification Program sets the industry benchmark for technical proficiency and professional expertise in using ACL software. ACL Certification evaluates and recognises your ability to integrate ACL technology into financial analyses and business processes. Earning the ACL Certified Data Analyst (ACDA) designation also enhances your professional development, validating your technical skills and the performance standards you bring to address key business challenges.

This closed-book, day-long exam is based on the most current version of ACL, and is divided into two components: a **Knowledge Inventory** and a comprehensive **Case Study**. The Intermediate level of ACL Certification is based on the ACL 100 and ACL 200 level courses. It is strongly recommended that you complete these courses prior to testing for the exam.

For more information, please email us at enquiry@prodigy-group.com

Thank You for Visiting Us

We would like to thank all customers and visitors who had visited our booth during the following events:

● **ACIIA Conference 2009** held at Kuala Lumpur Convention Centre, Malaysia from 19-20 October 2009.

● **IIA Philippines 62nd National Convention 2009** held at Puerto Princesa, Palawan from 26-27 October 2009.

To view photos taken during the events, please visit our **Event Gallery** at www.prodigy-group.com/community.php.



PRODIGY NEWS & EVENTS

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.

Latest Release of KnowRisk - V2.11

KnowRisk V2.11 is now released for general availability! Here is a summary of the new features and improvements in V2.11.

New Features

- Trend reports
- Historical reports
- Colours and filters in reports
- Risk Grid / Heat Map reporting
- Audit Log Browser
- KnowRisk Forms Expressions

Improvements

- Enhanced lists in KnowRisk Forms
- Amending KnowledgeBase data in KnowRisk Forms
- Editing Item Link fields in KnowRisk Forms
- Closing KnowRisk Forms
- Customising searches in KnowRisk Forms
- KnowRisk API improvements

For more information on KnowRisk V2.11, contact our Business Consultants at enquiry@prodigy-group.com.

NEW Training Courses!

Prodigy will be offering the following new ACL training courses. These courses will be conducted on-site.

ACL 252 – Using ACL to Detect Fraud

ACL 255 – Using ACL to Test Internal Controls Supporting SOX 404 Compliance

ACL 260 – Using ACL to Test Internal Controls: Supporting Controls & Regulatory Compliance

ACL 291 – Developing Your ACL Procedures: A Custom Workshop

ACL 292 – A Custom Workshop for AuditExchange

ACL 401 – Informatica PowerCenter 8 Level 1 Developer

ACL 501 – Understanding ACL: A Manager's Perspective

For more information, contact us at enquiry@prodigy-group.com.

DIG DEEP WITH ACL AX 2.0

Perform 100% audit with the latest release of AuditExchange!

Lack of resources in terms of manpower and budget is a problem commonly faced by internal auditors when planning the audit cycle. Confidence in the integrity of the data is often compromised as a result.

To solve the frustrations of both auditors and business stakeholders, ACL has released the **AX2.0** and it offers a lot more than just analytics. This latest release contains several enhancements to provide a deeper level of insight into the integrity of your business!

4 Key Capabilities of AX2:

- Centrally manage all audit content regardless of file type
- Make data analysis easier and more accessible to all team members
- Implement continuous auditing and monitoring more easily
- Close the loop – distribute, track and escalate exceptions

Highlights of AX2:

- Enhanced security allows you to better restrict repository content, even in the library
- Any user can now also perform basic analysis using a simple web-based interface
- Store all types of file in the repository, allowing you to centrally manage all audit content anywhere, anytime
- Open from and save to the repository directly from MS Word, Excel, and PowerPoint documents
- Create powerful interactive server-based scripts using a new set of analytic declarations created just for AX2
- Easily schedule analytics to run on the server, and monitor the status of scheduled jobs
- Supports the 3 phases of continuous auditing / continuous monitoring: automated data extraction, automated analysis and exception management
- Push exceptions out to the business area through a web-based system, and set workflow over those exceptions to ensure follow-up occurs quickly

AX 2.0 takes your audit to a higher level and promotes efficiency throughout the audit cycle. Auditing has never been so easy! Find out more about AX 2.0 by visiting acl.com/ax2demo or email us at enquiry@prodigy-group.com today!



ACL Open Enrolment Training Schedule

Prodigy Data Solution is the ONLY ACL certified trainer in Asia South. As a 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.

Location	Course Name	Nov-09	Dec-09	Jan-10
SINGAPORE	ACL 105 - Foundation of ACL: Concepts & Practice	09-11	07-09	
	ACL 201 - Data Analysis Techniques (workshop)	12-13	01-02	
	ACL 260 - Using ACL to Test Internal Controls (workshop)			07-08
	ACL 303 - Advanced ACL Concepts & Techniques: Functions & Scripts		21-23	13-15
JAKARTA, INDONESIA	ACL 105 - Foundation of ACL: Concepts & Practice	09-11	14-16	
	ACL 201 - Data Analysis Techniques (workshop)	12-13	17-18	
	ACL 303 - Advanced ACL Concepts & Techniques: Functions & Scripts	23-25		
KUALA LUMPUR, MALAYSIA	ACL 105 - Foundation of ACL: Concepts & Practice	02-04	07-09	
	ACL 201 - Data Analysis Techniques (workshop)	12-13	10-11	
	ACL 260 - Using ACL to Test Internal Controls (workshop)			14-15
	ACL 303 - Advanced ACL Concepts & Techniques: Functions & Scripts	23-25		11-13
	ACL 501 - Understanding ACL: A Manager's Perspective			07
HONG KONG	ACL 105 - Foundation of ACL: Concepts & Practice	09-11	14-16	11-13
	ACL 201 - Data Analysis Techniques (workshop)	16-17	17-18	14-15
	ACL 303 - Advanced ACL Concepts & Techniques: Functions & Scripts	18-20		18-20
MANILA, PHILIPPINES	ACL 105 - Foundation of ACL: Concepts & Practice	23-25	14-16	11-13
	ACL 201 - Data Analysis Techniques (workshop)	26-27		14-15
	ACL 303 - Advanced ACL Concepts & Techniques: Functions & Scripts		09-11	18-20

ACL Specialised Workshops are also available for users who want to attain higher levels of proficiency:

- PDS 601 ACL Data Access
- PDS 602 ACL Version 9 Refresher
- PDS 701 Introduction to Data Forensics Techniques
- PDS 801 Audit Techniques & Approach using ACL as the CAATTs Tool
- PDS 802 Quality Assurance & Compliance Using ACL
- PDS 803 Anti-Money Laundering (AML) Using ACL

For more information about the individual ACL Specialised Workshops, email us at training@prodigy-group.com.



Next Issue Topics:-

- Anti-Money Laundering
- Financial Fraud
- Continuous Control Monitoring

Our Regulars:-

- Just For Laughs
- ACL Tips
- PAWS Tips
- ACL Open Enrolment Training Schedule



The Prodigy Group is a premium total solution provider offering extensive IT solutions on Audit & Compliance, Risk Management, Internal Control Management and Business Assurance to audit & compliance professionals, fraud investigators, risk managers, business analysts, IT professionals, system security and senior executives. Prodigy's extensive expertise and experiences brings about the development of holistic GRC solutions that facilitate customers in managing their commitments and obligations better, improving internal business processes.

Transformed around the themes of simplicity and usability, our solutions have been proven and tested in many established organisations, giving clients confidence in the reliability, accuracy, and integrity of the data underlying the increasingly complex business operations.

Authorised Distributor for **ACL, KnowRisk, Arbutus, Pentana, Intellinx** and **GRCMonitor**