

Prodigy Newsbyte

Issue 11

May to Jul 2005

Special points of interest:

- Technology Critical to Sarbanes-Oxley Efforts
- IT Controls Impact Sarbanes-Oxley Compliance Efforts
- Newly Join Business Partnership
- Risk Metrics Needed for IT Security
- ACL Tips

Inside this issue:

ACL Tips	2
On A Lighter Side	3
IT Controls Impact Sarbanes-Oxley Com-	4
Prodigy News & Events	5
Risk Metrics Needed For IT Security	6
Risk Management Workshop	8
ACL Open Enrolment Training Schedule	9

Technology Critical to Sarbanes-Oxley Efforts

By Steve Stanek and Jeff Barrett, KnowledgeLeader Management Community

The Sarbanes-Oxley Act (SOA) raises the stakes for Chief Information Officers and information technology departments by requiring certification on the performance of systemic internal controls that contribute to the accuracy and integrity of financial reporting. The proverbial 'IT curtain' is now being pulled back to drive executives' accountability toward their ongoing design and operation.

Henceforth, CIOs must consider the evolution of the control environment as it pertains to the IT infrastructure and the systems that impact the financial reporting process.

"Technology executives need to ensure that business processes are honed and well-controlled before launching IT initiatives. They must make sure that controls are built into applications and that ownership of controls is assigned," says Jon Rydberg, a Protiviti Associate Director. Now, cooperation with business process owners is critical since many controls are technology driven.

Ownership of controls existed to some extent at most companies, but Sarbanes-Oxley formalizes verification of effective controls operation.

The first step is to identify key processes and assign explicit ownership of related controls and monitoring. Once this baseline is established, then the components and sub-processes of the internal controls structure, including IT application and systems infrastructure, are delineated.

Accountability for the proper operation of controls should be extended down into the organization to the individuals who operate underlying processes and manage the associated IT components. Coordination is essential to ensure the correct operation of internal controls elements that roll up into the more comprehensive compliance verifications.

Sarbanes-Oxley requires any significant changes or deficiencies in the control environment to be reported in SEC filings. Therefore, IT management and process owners should

work together to integrate compliance efforts not only as a best business practice but as a collaboration critical to ongoing SEC compliance efforts.

Application and Infrastructure Considerations

"The increase in the implementation of large-scale ERP platforms such as SAP and PeopleSoft increases the number of automated processes and the reliance on controls, "according to Rydberg." Although having sound processes irrespective of technology is important, having controls built into systems can be even important. Without integrity, a broken process can go wrong even faster."

Financial reporting and internal control compliance considerations should include the financial applications being supported and the underlying IT change and maintenance processes such as:

- Application & network access
- Application & reporting interfaces/integration
- Physical & logical system security, Database integrity
- Contingency planning & safeguarding IT assets

"Making sure that controls are built in prior automation and further technological advancements should be a priority. Information Technology management becomes even more significant when you consider its impact on data and process integrity," Rydberg concludes.

One approach to evaluating the IT controls related to financial reporting processes is to applying the standard methodology for assessing overall enterprise-wide internal controls. The COSO framework for internal control reporting is based on a set of financial statement assertions that form the objectives for the controls evaluation.

COSO, adopted by most industry organizations, supports control evaluations at the entity level and at the activity (or process) level.

Continued in Page 2



ACL Useful Tips

I ran a random record sample on a table. When I ran the sample again to double-check the results, I got different sample records. What happened?

You will get different sample records because you did not specify a seed value parameter in the Sample dialog box. When you select Record and Random in the Sample dialog box, the Seed box becomes available under Sample Parameters. If you leave this box blank, ACL generates a seed value for you that "pick" the records for your sample. That is, ACL randomises the output, which is often the effect you want.

The next time you run the Sample command, ACL will generate a different seed value, resulting in different records being selected. However, there may be times, as in your case, when you want to duplicate the output of the Sample command. To do so, you must enter a value in the Seed box the first time you run the sample. Then, when you run the sample again, use the same seed value. The same sample records will be selected as long as you are using the same table with the same number of records (population), and all other parameters are the same.

Issue 11

Continued in from Page 1 ...

The entity level IT controls should focus on the COSO elements of the overall control environment, risk assessment, information (data integrity) and communications (financial reporting tools/networks/interfaces) and monitoring (management reports/control reports).

The process level involves IT control considerations related to applications and access control that again assure financial reporting health within identified business processes.

According to Ed Hau, a recognition that this will be a bigger chore than most people first thought.

IT and Governance

Convincing CIOs of this has not been easy, according to Hau. "I'm finding that CIOs have been late to the game," he says. It's getting tough to engage them in a conversation. Every day they are bombarded by vendors trying to pitch things to them. It's not going to be easy for internal audit or outside consultants to suggest things."

In Hau's view deadline recently was pushed back 10 months or more, depending on a company's year-end date.

"Why not decompose processes, look at the IT infrastructure, and leverage corporate governance into IT arena?" Hau suggests. "Put in risk-management and performance tools so that they're ready once the auditors come around. Go to the root of the issue and deploy solutions around risk management and control management."

Hau says companies that certify compliance later in the game will probably have more expected of them than companies that certify early, which should serve as a further incentive for companies to set to work now.

"Getting involved early is the best prescription," he says. "Corporate governance applies to IT. It entails more uniformity, things like business process automation and management - workflow automation, metrics, control mechanisms, business rule engines to know what standards are and are not. What better way to leverage that than to suggest this is part of a corporate compliance and governance program?"

Software Tools

He gets no argument from Rich Lanza, authority on the use of data extraction/analysis technology and a frequent speaker and author on data analysis and project management.

Lanza says he believes companies will find the documentation and validation of internal controls to be an entirely new experience that will take many months to complete. And he warns against the temptation to put off action just because the deadline for compliance has been pushed back.

"I think it's become less of a focal point because the deadline's been pushed off a year," Lanza says. "I'm afraid there will be a flurry of activity later, and I think that's a mistake."

Lanza says the process could be speeded up by using transaction analysis audit software to assist in validating any documented controls. A leader in this arena is ACL Services Ltd. Such software enables a company to look at 100 percent of the data in less time than taking a sample.

Management should consider adopting these transaction analysis tools that can query data on transactions compiled in financial reports. Although tools such as ACL and other data manipulation tools are traditionally used by auditors, these programs can contribute to management's compliance efforts to:

- 1) substantiate management's assertions that controls are operating effectively,
- 2) identify control issues and operational improvements, and
- 3) establish an integrated test of controls for future certification efforts.

Lanza recommends stand-alone products rather than ones built into ERP systems, which he says are good transaction-based processors but weak in business analytics. Their strength lies in helping companies manage important parts of their business, including product planning, parts purchasing, inventory maintenance and order tracking.

However, most ERP applications such as SAP, Oracle, Peoplesoft, and JD Edwards all come with specific audit tools that can be utilized to maintain or evaluate internal controls.

"Much can be done through inquiry and observation, just talking it through," Lanza says. "But you have to download data and analyze it to validate controls. SAS 94 requires that if data sets or process flows are big enough, you need to do parallel simulations," he says.

Current validation methods are usually based on manual and automated procedures working in tandem. This has an inherent risk of human error, a risk that compounds as data volumes and regulatory requirements increase, Lanza says.

Continued in Page 3

Continued in from Page 3 ...

The more automation that can be built into the system the better, because it reduces the chances of human error and increases the amount of data that gets reviewed.

Lanza suggests companies establish a baseline of internal control gaps, key risk areas and issues within the information channels for use in future monitoring. Business process owners need to be asked several questions to better understand application processing controls and potential concerns, including:

- What are the highest risk areas within the process?
- What process will be in place to continue an appropriate level of evaluation of internal control, especially control gaps?
- How is the quality and timeliness of critical information validated?
- How are you notified of control issues in your process?
- Should you be notified of process issues more quickly than you are now?
- How will monitoring processes be made more efficient?

By answering similar questions, business process owners will be able to identify opportunities to improve internal controls, Lanza says.

Lanza is a strong supporter of continuous monitoring of controls, but he acknowledges that many people see this as "pie in the sky. It's seen as nice to have versus something we need now." He disputes that view, pointing out that

continuous monitoring quickly catches errors, as well as frauds, so that money is saved.

"Though all these control reviews, you find a lot of money," Lanza says. "You find reconciliations not being done, customers not being charged enough, overpayments to vendors, all kinds of things."

He gave the example of a company with a high risk in its revenue recognition. With automated monitoring, process owners could receive daily or even hourly transaction flow information, making the reports themselves a control activity.

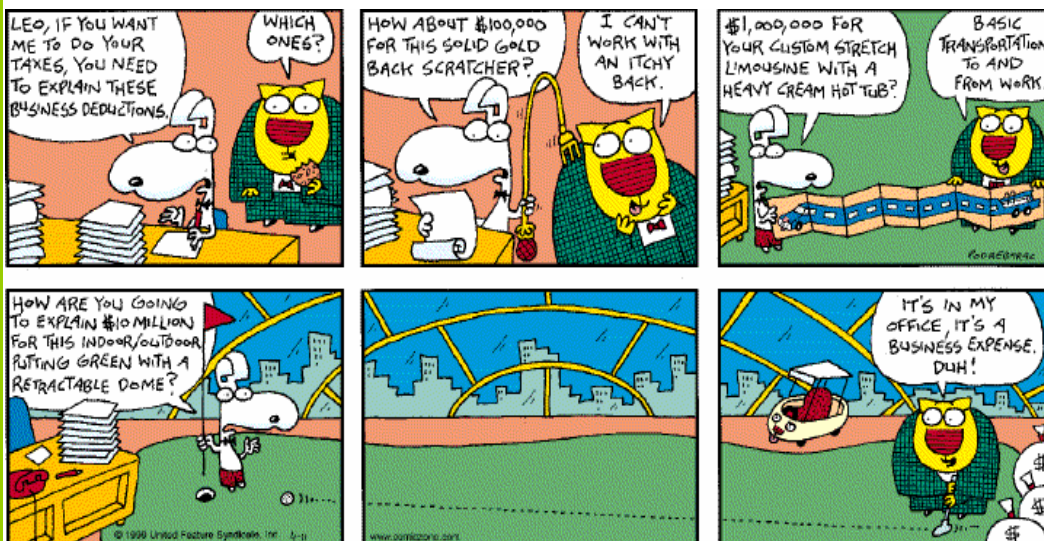
ACL products, which are used by most of the Fortune 100 companies and other firms around the world, feature controls compliance technologies capable of continuous monitoring as they run alongside operational application systems.

Companies do have to spend money for this kind of control and monitoring.

"Security, privacy, controls in the system . . . these things are not cheap to do," Lanza says. "When you build the requirements for your system, security and controls and reports and exception reports are the last things that get implemented because they are viewed as less important. I'm trying to push financial management people to focus more in the early stages of the IT project so such requirements are built in rather than bolted on later. You can also build in continuous monitoring capabilities such as reports to assist manage controls or through creating data streams into other tools like ACL for later analysis."



On A Lighter Side



visit us at
www.prodigy.com.sg

IT Controls Impact Sarbanes-Oxley Compliance Efforts

By Nancy Hala, KnowledgeLeader

Information technology (IT) is, incontrovertibly, a central business process element in most organizations today. To illustrate this point, consider that, as many organizations make the decision to outsource non core business functions (such as human resources), a trend has emerged to include IT in these outsourcing initiatives so that the function will be viewed and treated in an integrated, comprehensive way.

In other words, leaving IT out of the picture is no longer an option.

The same can be said of the widespread initiatives businesses are undertaking related to Sarbanes-Oxley Act (SOA) compliance. The financial reporting process, as well as processes that accept, record, accumulate, summarize and report the transactions underlying financial reporting, are accomplished with computers, programs and other technology-related equipment and software. Therefore, the effectiveness of the controls around these applications and systems will directly impact the integrity of the financial reporting, including the data that is input into the process, as well as the information that ultimately becomes the output.

With this in mind, many organizations have come to understand the significant impact IT carries in SOA compliance, and they recognize that IT must be carefully considered when documenting, evaluating and attesting to the effectiveness of internal controls surrounding financial reporting.

With this in mind, many organizations have come to understand the significant impact IT carries in SOA compliance, and they recognize that IT must be carefully considered when documenting, evaluating and attesting to the effectiveness of internal controls surrounding financial reporting.

In the realm of SOA testing and compliance, this basic structure can help organizations establish an effective, standardized methodology for reviewing and understanding the impact IT has on internal controls.

The scope of the IT environment that should be included in SOA compliance efforts includes:

- Security administration
- Application-change control
- Data management and disaster recovery
- Data centre operations and problem management
- Asset management

Mike Lynn is the senior vice president in charge of audit risk management at AXA Technology Services, a subsidiary of AXA Group Worldwide, the global financial

services organization. As a foreign subsidiary, AXA will not be required to comply with Sarbanes-Oxley provisions until 2005. However, the organization is striving to achieve compliance within the current year by partnering with an external public accounting firm. "We have a working model of what Sarbanes-Oxley will look like from an IT operations standpoint," he says. "We are using that model to roll out to the rest of the group. We believe this is a more efficient way of approaching Sarbanes-Oxley compliance, rather than beginning from scratch."

Lynn believes that using a Sarbanes-Oxley approach based on an IT perspective is beneficial in many ways. "The range of IT process-related risks is not as broad as general operational risks," he says "Therefore, IT standards are often approached in a more uniform manner. This helps us when it comes to rolling out risk and control standards."

According to Lynn, to establish Sarbanes-Oxley compliance forces an organization to conduct a widespread, cross-function risk assessment. This helps the audit team truly understand its business operating environment and develop effective controls. "Sarbanes is essentially an audit, but one that is focused on financial reporting, not operational efficiencies," he says. "So by looking at the activities that are required by Sarbanes from an IT perspective, we will better understand the status of general controls in the IT services environment and how they impact the organization's financial viability. For example, if a particular IT system is the foundation for a financial application but is not properly controlled, the data in that application may be inaccessible or unreliable, and that has significant compliance implications."

Key areas to be considered

The three key areas to consider when evaluating IT controls are corporate governance, IT governance (the CIO organization) and application and data owner governance.

Corporate governance is a critical area to examine first simply because it sets the "tone at the top" as defined by leadership. With respect to IT governance, there are two areas that must be addressed: IT operations and the overall governance of processes impacting IT. This involves the CIO organization and examines the impact on general or pervasive controls.

Finally, the application and data owners are the business groups interfacing with business-process owners.

The effectiveness of the application and data-process controls will ultimately affect the controls at the activity or process level, and therefore must be included in key areas to be considered in SOA compliance.

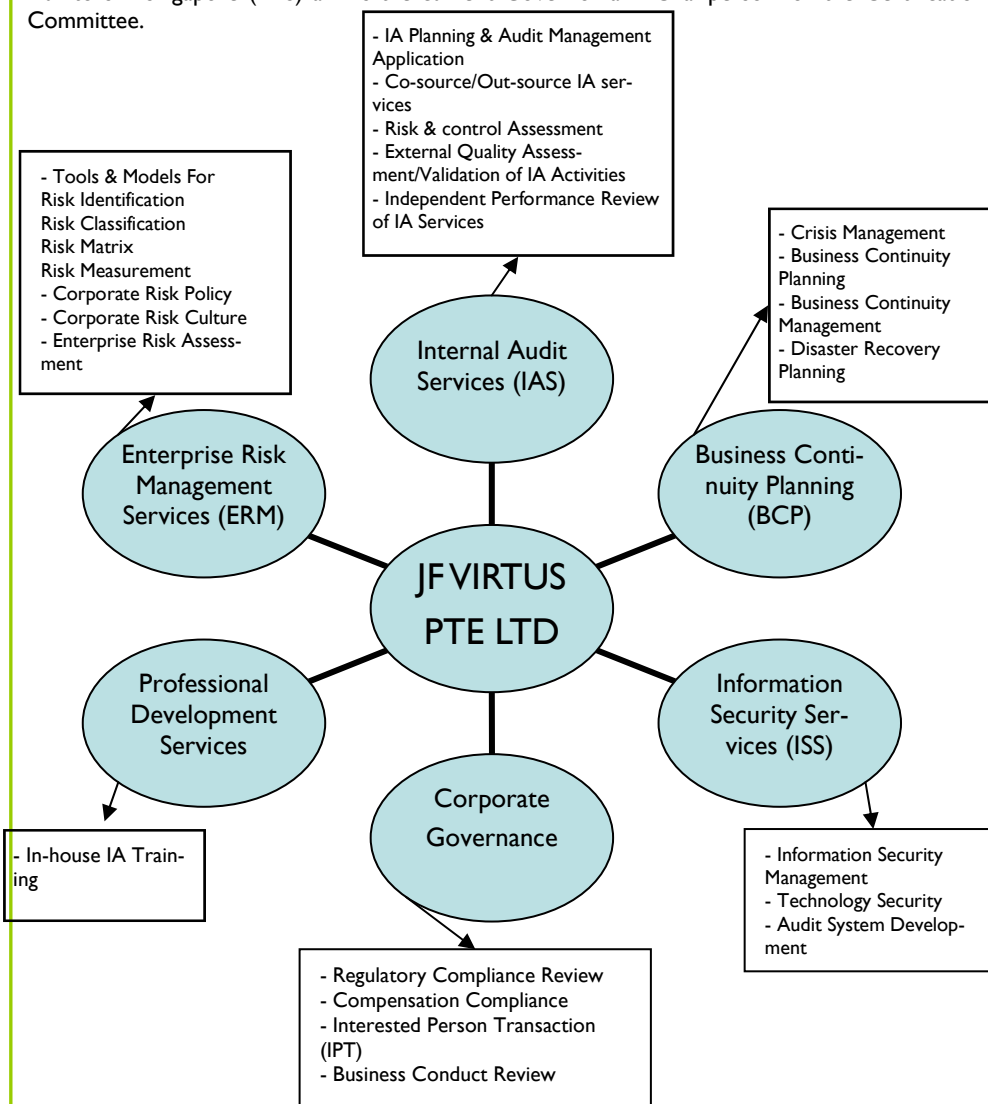


PRODIGY NEWS & EVENTS

Prodigy is pleased to announce the Newly Business Partnership with JF Virtus Pte Ltd

With this partnership, Prodigy Data Solution is pleased to extend the services in Risk Management, Internal Control Assessment, Corporate Governance, Unit Fund Management, Mortgage and Leasing Operations, Corporate Policy, Business Appraisal, Corporate Development, Technology Development, Business Process Re-engineering and Business Continuity Planning.

JF Virtus is headed by the Managing Director, CK Siow, whom has more than 25 years of Audit and Management experience in Operations, Business Systems, Information Technology, Finance, and Accounting with organisations in Canada, USA, England and Singapore. He is an active member of The Institute of Internal Auditors Inc since 1979 and served as a Governor in the Edmonton and Vancouver Chapters in Canada. He was the Vice-President of The Institute of Internal Auditors – Singapore (IIAS) and is the current Governor and Chairperson for the Certification Committee.



For more information, please write in to ck@cksiew.com

EXTERNAL CONSULTANT OPPORTUNITIES

Prodigy is currently seeking interest parties as our external consultants in Indonesia, Thailand and Philippines.

- He / She must possess:
- Experience in ACL
 - Audit experience
 - Strong analytics / Good in presentation skills
 - Willing to travel

For more information, please write in to info@prodigy.com.sg



EVENTS

Prodigy Seminar Series Jakarta Hilton International 27 April 2005

Prodigy Data Solution is organising a half-day seminar in Jakarta on 27 April 2005. This half-day seminar provides an excellent platform for users to gain valuable knowledge on latest trends and issues relating to Risk Management, Information System Security, Business Continuity Plan and Audit Professionalism.

Don't miss this rare opportunity to learn from the experts and gain further insights on the available technologies! Also, Prodigy will be launching new series of products and services at the seminar.

For further information, please contact

Mr Yazid
yazid@prodigy.com.sg

Ms Shock Hui
shock.hui@prodigy.com.sg

Mr Yoharto
yoharto@prodigy.com.sg

79B PAGODA STREET
SINGAPORE 059238
TEL: (65) 6221 2810
FAX: (65) 6221 2813
INFO@PRODIGY.COM.SG

Risk Metrics Needed for IT Security

By Will Ozier, President OPA Inc

Business leaders worldwide are becoming more aware of the importance of assuring the security of information assets. Information-security issues are among the hottest topics being addressed in trade media for organizational governance, executive, financial, audit and IT leaders. Conferences covering the latest information-security issues, tools and problems abound in both the public and private sectors.

Government efforts have helped increase security awareness, as well. In the United States, the President's Commission on Critical Infrastructure Protection (PCCIP) issued recommendations and launched information-security initiatives in both the government and private-sector arenas. The PCCIP has also established public-private cooperation and information sharing through the Partnership for Critical Infrastructure Security (PCIS) and Critical Infrastructure (CI) Information Sharing and Advisory Centres (ISAC), which are coordinated by the Critical Infrastructure Assurance Office (CIAO). These efforts address the emerging threats associated with the rapid growth of global Internet connectivity, as well as the disruptive potential of cyber and physical attacks, accidents, and natural disasters.

Despite this increased awareness and the persistent recommendations for improvement, key areas of information-security risk management and associated risk metrics continue to receive precious little attention. Although many guidance documents advocate taking a managed approach to risk — including risk analysis and assessment — none of them clearly and consistently define what constitutes a proper risk analysis and assessment. Even the well-known ISO 17799 standard falls well short of providing the kind of nuts-and-bolts “how-to” guidance that is needed, in my opinion.

The lack of formalized qualitative and quantitative risk metrics impairs the ability of risk managers and security professionals to effectively and consistently measure risk and points to the absence of a sound framework against which to record quantitative threat-experience data. Establishing a risk-management framework and risk metrics would greatly improve risk management by giving organizations a basis for risk analysis and assessment that would enable them to make business decisions about managing security risks.

Some Progress Made

As early as the mid-1970s, the basic metrics of risk were established, but they were not formalized or widely disseminated. In these early years, a variety of risk-assessment methodologies and techniques emerged to help organizations identify and manage non-classified

information-security risks on a cost-benefit basis.

Some of the manual methodologies and automated approaches that were developed during the 1980s were well-conceived and are still used today. Other approaches fell by the wayside. Highly subjective qualitative methodologies provided no real support for the standard business decision-making model, which is based on return on investment (ROI).

Conducting quantitative risk assessments without supporting automated tools proved to be almost impossibly time-consuming, complex, and inflexible. Also, they were completely incapable of supporting the “what-if” analysis that is essential to sound business decision-making. The inconsistent use of risk metrics and misinformation about risk further clouded the issues.

There has been progress in developing information - security risk metrics over the past two decades, but there is still a way to go before standard metrics are established, adopted, and practiced. To start with, the need to identify, measure, and manage information-security risk has been established and subsequently reinforced, albeit tentatively. The U.S. National Institute of Standards and Technology identified key qualitative and quantitative risk metrics and established a high-level framework of the risk-analysis and assessment process related to the broader function of information-security risk management, but this work was never formalized. Many organizations have published information-security risk-management guidance, including:

- The International Information Security Foundation (IISF) [Generally Accepted Systems Security Principles](#) (GASSP).
- The International Standards Organization (ISO) [ISO 17799](#).
- The Organization for Economic Cooperation and Development (OECD) [Information Security Principles](#).
- The European Information Security Forum (ISF) [Standard of Good Practice](#).
- The Institute of Internal Auditors (IIA) [Systems Assurance and Control](#) (SAC).
- The Information Security Audit and Control Association (ISACA) Control Objectives for Information and Related Technology (CobiT)

However, in most of the above documents and other guidance, the essential distinctions between *control objectives* and *controls* is either not clearly established or is not established at all.

...Continued in Page 7

Continued in from Page 6 ...

If the managed risk approach to information security were not recognized as the best way to achieve good information security, this would not be a big deal. But it is. It is virtually impossible to measure risk against “objectives,” but it is not difficult to measure risk against the lack or ineffective implementation of controls.

In addition to the above guidance publications, the [Information Systems Security Association \(ISSA\) Guidance for Information Valuation](#) has established methods and metrics for valuing an organization’s information assets. Critics who are unaware of this guidance have asserted that the lack of such metrics is an obstacle to executing quantitative risk analysis and assessment, because organizations don’t know how to establish the monetary value of their information assets.

Additionally, a variety of automated disaster-recovery planning, logical access-control, anti-virus, authentication, encryption, and firewall technologies have helped organizations manage information security. But, that said, without applying quantitative risk-analysis and assessment techniques to the issues, there is no reliable basis — specifically ROI — for determining how much money to spend to acquire and administer these risk-management tools.

Qualitative VS. Quantitative Approaches

Despite the general progress that has been made in recognizing the need for good information security, standard, well-defined metrics for analyzing and assessing information-security risks have not been established and formalized. Many guidance documents advocate a risk-based approach to managing information security, and they often suggest a quantitative methodology, in the loosest possible terms, as a solution. The time has come to establish and formalize the framework of metrics and measurement methods necessary to support this now-proven approach.

Qualitative approaches are characterized by subjective risk measures such as ordinal ranking (low risk or value, medium risk or value, and high risk or value) in a risk-to-value matrix. The qualitative methods emerged in part from a persistent belief that it was simply too difficult to get the real numbers. Also, qualitative approaches appealed to management, which was looking for the “least-effort” way to prove they had “assessed their risks.” After all, little attention has been paid to the results of risk analysis and assessment — until recently. In my experience, qualitative approaches, however otherwise encouraged, provide little basis for illustrating the scale of risk in monetary terms or for making informed risk-management decisions. The metrics of a qualitative risk analysis do not reflect independently objective values

such as the monetary value of an asset, the annualized rate of occurrence (frequency), the single loss exposure (impact), or the probability of loss. Although these qualitative metrics can be useful to establish for management that a problem exists, they can only address problems known by the user to exist, and they cannot support information-security investment decisions with ROI data.

Quantitative approaches are characterized by the use of independently objective measures for all risk metrics, including qualitative risk-metric descriptors such as “information asset,” “threat,” “vulnerability,” and “safeguard/control” nomenclatures. Asset values are expressed in monetary terms and threat frequency in annualized expressions that represent actual expected frequency (e.g., 1/10 for once in 10 years, or 50/1 for 50 times per year).

Quantitative risk metrics can be readily applied in basic risk-modelling algorithms. The best automated quantitative risk-analysis and assessment tools discuss risk in the familiar, numbers-oriented language of business (monetary value, probability, ROI). They readily support “what-if” analyses, and they facilitate risk-mitigation cost-benefit and ROI analyses.

Threat Data Lacking

Establishing metrics for quantifying risks in monetary terms isn’t the only challenge. Another serious problem is that there presently is no central repository of threat-experience (actuarial) data on which to base information-security risk analysis and assessment, nor are organizations required to collect that data, except for threats involving natural disasters, crime, and fires.

Such an actuarial database could provide a key element to a risk-metrics and measurement framework in which threat-experience data can be accumulated, “cleansed” of source-identifying attributes (where necessary), and made available for quantitative, probabilistic risk analysis and assessment. This framework would also give organizations a basis for measuring and cost-efficiently managing their compliance with qualitatively sound information-security principles such as those mentioned above. Historically, organizations have been reluctant to report information-security threat-experience information to government agencies and law enforcement for competitive, liability, and legal reasons. That fact has made it difficult to gather current and accurate information about security threat experiences.

...Continued in Page 8

visit us at
www.prodigy.com.sg

Continued in from Page 7 ...

Solution: Establish Metrics

There are signs that public- and private-sector enterprises — the consumers of technology products — are beginning to make information security a top priority. The time may be ripe to raise the information-security bar globally by establishing standard metrics for measuring security risks and a repository for collecting and analyzing the accumulated actuarial data.

The first step is to establish, formalize, and maintain both qualitative and quantitative risk metrics. These would include:

- . Detailed, level-set qualitative risk metrics and “how-to” guidance that sets forth good information-security risk-management practices and principles.
- . A “standard” qualitative risk-metrics population of threats that is maintained at a central repository such as an information threat-experience centre.
- . Quantitative threat-experience frequency data that will support quantitative approaches to information-security risk analysis and assessment. This collected threat-experience data could be made broadly available on a “not-for-attribution” basis and organized in a variety of analytic profiles.

In addition to these metrics, others are needed to support quantitative risk-analysis and assessment approaches, including the:

- . Credible monetary value of assets.
- . “Impact” as a percentage of asset value.
- . Annualized probability of loss.
- . Annualized expected loss.
- . Annualized safeguard and control costs.
- . Uncertainty.

Such risk metrics have been the foundation of the insurance industry for centuries.

Time For A Security Risk Framework

Many areas of risk — such as hazard loss, health, market, credit, project, and product development — are now routinely and effectively managed with often highly complex techniques and methodologies based on extensive experience-driven databases. It is time for the information-security industry and profession to establish its own risk metrics, measurement, and management framework. This framework would give business managers the tools they need to identify, measure, and manage the risks to their information assets and manage their information-security investments based on sound and reliable ROI data.

Risk Management for Manager Workshop

Date: 14th - 15th June 2005

Venue: Jakarta, Indonesia

Date: 16th - 17th June 2005

Venue: Hotel Rendezvous, Singapore



Early Bird Discount
Valid till 15th May 2005
Register Now!!

COURSE OVERVIEW

This two day course provides participants with a comprehensive background to risk management concept and focuses on providing tools and proven methodologies for providing guidance to staff for identification and management of risk, evaluation of risk management applications, evaluation of risk management documentation and the development of risk reports for senior management. Each participant will receive a certificate and training resource pack from Global Risk Alliance.

TRAINER – Mark Wheatley, Risk Advisor, Global Risk Alliance (GRA)

Mark Wheatley has worked extensively for Australian Government agencies at a high level, providing oversight for policy development and implementation, as well as provision of evaluation and auditing support for high level government projects over a period of 28 years. During this time he has been instrumental in the introduction and facilitation of risk management profiling for many major events of National importance, government facilities and departmental activities.

GRA is a leading provider of risk management training in Australia. Over the past three years, GRA has trained over 2000 people in a variety of courses including risk management, corporate government, business continuity planning, safety management systems and executive risk management training.

For more information, please contact Shock Hui at (65) 6221 2810 or shock.hui@prodigy.com.sg

ACL Open Enrolment Training Schedule

VENUE	COURSE NAME	MAY-05	JUN-05	JUL-05
Singapore	ACL 105 - Foundation of ACL: Concepts and Practice	04-06	01-03	04-06
	ACL 201 - Data Analysis Techniques and ACL Workshop	09-10	06-07	14-15
	ACL 301 - Advanced ACL Concepts and Techniques: Functions	18	15	11
	ACL 302 - Advanced ACL Concepts and Techniques: Scripts	19-20	16-17	12-13
	ACL 303 - Advanced ACL Concepts and Techniques: Functions and Scripts	18-20	15-17	11-13
	Fraud Detection Techniques Using ACL	26-27	23-24	28-29
	ACL v8 - Data Access	12	20	22
	ACL v8 - Refresher	16	21	08
Malaysia	ACL 105 - Foundation of ACL: Concepts and Practice	04-06	01-03	04-06
	ACL 201 - Data Analysis Techniques and ACL Workshop	10-11	13-14	12-13
	ACL 301 - Advanced ACL Concepts and Techniques: Functions	16	20	18
	ACL 302 - Advanced ACL Concepts and Techniques: Scripts	17-18	21-22	19-20
	ACL 303 - Advanced ACL Concepts and Techniques: Functions and Scripts	16-18	20-22	18-20
	Fraud Detection Techniques Using ACL	30-31	29-30	27-28
	ACL v8 - Data Access	-	-	-
	ACL v8 - Refresher	25	27	25
Indonesia	ACL 105 - Foundation of ACL: Concepts and Practice	09-11	01-03	04-06
	ACL 201 - Data Analysis Techniques and ACL Workshop	16-17	09-10	18-19
	ACL 301 - Advanced ACL Concepts and Techniques: Functions	18	15	11
	ACL 302 - Advanced ACL Concepts and Techniques: Scripts	19-20	16-17	12-13
	ACL 303 - Advanced ACL Concepts and Techniques: Functions and Scripts	18-20	15-17	11-13
	Fraud Detection Techniques Using ACL	25-26	20-21	25-26
	ACL v8 - Data Access	13	06	28
	ACL v8 - Refresher	30	24	21
Philippines	ACL 105 - Foundation of ACL: Concepts and Practice	-	06-08	-
	ACL 201 - Data Analysis Techniques and ACL Workshop	-	09-10	-
	ACL 301 - Advanced ACL Concepts and Techniques: Functions	-	15	-
	ACL 302 - Advanced ACL Concepts and Techniques: Scripts	-	16-17	-
	ACL 303 - Advanced ACL Concepts and Techniques: Functions and Scripts	-	15-17	-
	Fraud Detection Techniques Using ACL	-	23-24	-
	ACL v8 - Data Access	-	20	-
	ACL v8 - Refresher	-	21	-
Thailand	ACL 105 - Foundation of ACL: Concepts and Practice	04-06	-	06-08
	ACL 201 - Data Analysis Techniques and ACL Workshop	09-10	-	11-12
	ACL 301 - Advanced ACL Concepts and Techniques: Functions	25	-	18
	ACL 302 - Advanced ACL Concepts and Techniques: Scripts	26-27	-	19-20
	ACL 303 - Advanced ACL Concepts and Techniques: Functions and Scripts	25-27	-	18-20
	Fraud Detection Techniques Using ACL	19-20	-	25-26
	ACL v8 - Data Access	16	-	14
	ACL v8 - Refresher	13	-	15

79B PAGODA STREET
SINGAPORE 059238
TEL: (65) 6221 2810
FAX: (65) 6221 2813
INFO@PRODIGY.COM.SG

Coming Up in the
Next Issue of Prodigy
Newsbyte

- ◆ More Useful ACL Tips
- ◆ More Articles on Continuous Monitoring, Business Continuity Planning and Enterprise Risk Management
- ◆ And many other useful industries information

Feel free to write us any questions, comments or feedbacks on Prodigy Newsbyte via email at info@prodigy.com.sg