

Issue 28    Aug 2009 – Oct 2009

- ▶ SETTING THE STANDARD FOR COMBATING FRAUD.....1
- ▶ FIVE COMMON MYTHS DEBUNKED.....3
- ▶ MANAGING CORPORATE RISK THROUGH CONSISTENT, EFFECTIVE RISK ASSESSMENT .....4

# Prodigy Newsbyte

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

## Setting the Standard for Combating Fraud

**By: David Divitt, 9<sup>th</sup> December 2008.**

*Point of detection is a way to measure fraud that, if implemented across the board, could reduce fraudulent payments and reassure corporates and consumers.*

United we stand and divided we fall. This is an ancient and oft-quoted phrase that the payment industry would do well to heed if it is to take the next step in the long, expensive and damaging war that is being fought against fraudsters. Put simply, the industry needs to not only find more ways to share information and experiences on fraud but to actually design new standards that will deliver a more cohesive frontline in the war against fraud.

Clearly, the design and implementation of standards for fighting fraud, even at a national level, is quite complex. This is regardless of whether the standards in question are self-regulated, run by one of the card schemes or driven through an industry body. If standards are contemplated at an international level, which many would argue to be a sensible course of action when dealing with payment fraud, then this complexity grows by several magnitudes. As such, small but significant steps should be considered, the first being around the point of detection (PoD).

At the moment there is little industry-wide agreement on what defines fraud levels and the cost to a country or industry. Levels of fraud are typically reported in purely financial terms and then broken down into the various sub-categories making up that fraud - i.e. card, cheque, online and identity fraud. However the data, which comes from the banks' fraud departments, is purely numerical and does not take into account more sophisticated ways of measuring the true performance of a fraud prevention strategy, such as false-positives and detection rates. PoD, for example, could provide a more cohesive approach to an industry-wide anti-fraud strategy.

### Fraud Measurement with PoD

PoD measures how many missed fraudulent transactions occur prior to a bank's system generating its first alert on an account. As such, PoD is the metric that is most closely tied to fraud losses as it directly describes the number of lost transactions that occur before an analyst, or system, has the chance to stop a fraud. In practice this means that a PoD of 'five' means that, upon the fifth suspect transaction, the system raised an alert within the bank. This, of course, means that the four transactions prior to the PoD are all losses and potentially the fifth depending on whether the detection system has real-time prevention capabilities. By then multiplying the average loss per transaction by the PoD, there will be an accurate and transparent view of the real cost of fraud.

Ignoring the issue of whether to use PoD as an industry standard for a moment, it should be clear that even within individual banks, the argument for its use for fraud analysis is persuasive as it can play a central role in direct loss avoidance. This is because the sooner banks can detect fraud on an account, the sooner they can take action on it and stem their losses. Based on an average loss per fraudulent transaction, it is easy to see the potential savings if detection was targeted at earlier transactions in the fraud cycle. Even a small drop in the average PoD of half a transaction per account can make more difference than increasing detection rates by a large percentage.

## Implementing PoD

Despite all the benefits, PoD is yet to become a staple in fraud managers' repertoires. It is for this reason that an industry-wide view needs to be taken where, preferably, one of the card schemes should take the lead and introduce an industry standard for PoD. For example, if the industry-wide PoD rate was set at 'three', then it would become unacceptable for any fraud department to operate at a higher rate. It would also provide a coherent and unified level of response to fraud attacks.

Some consideration may need to be taken into account depending on the type of fraud, as some fraud types take longer to become apparent, however the systems and technology are already in place to enable the adoption of such an industry measurement. It would also contribute significantly to tackling the continually growing consumer fear on fraud, which is, in many ways, more damaging to financial institutions than the fiscal value of the fraud itself. The anecdotal and statistical evidence all points to consumers being either rationally or nonsensically afraid to undertake certain types of transactions due to the fear of being a victim of fraud. Given that the education programmes undertaken by banks and APACS, combined with the fear stoked up by the media, has made payment fraud prominent within the social psyche, there is an opportunity to build on this level of awareness.

By introducing a standard, in words that consumers can understand, and then they could appreciate to a far greater extent what is happening when fraudulent transactions start occurring on their account and be prepared to participate in the fraud prevention process. This is crucial as consumers currently find it hard to legitimise why a fraudster might be able to make ten or so fraudulent transactions before their bank puts a stop to their card or account. However, if PoD is used as a key measure of banks' anti-fraud systems, then consumers can be engaged with the process in the same way, for example, that they have historically understood other banking processes such as the time it takes for cheques to clear.

By creating a standard that consumers can relate to, new processes can be introduced that rely on customer input. One example is interactive SMS alerts that are sent to individual's mobile phones whenever a transaction occurs that is outside their pre-set trigger points such as when it is over a certain amount or outside their usual spending habits. The customer receives an SMS alerting them to the transaction and giving them the opportunity to immediately reply to block their card if it is fraudulent. Alerts can also be sent for any transaction that the bank thinks is suspicious, even if it is within the customer's usual limits. This has the potential to stop fraud after the first transaction and in so doing bring the PoD down to one, thereby dramatically reducing the amount of fraud undertaken against an individual account.

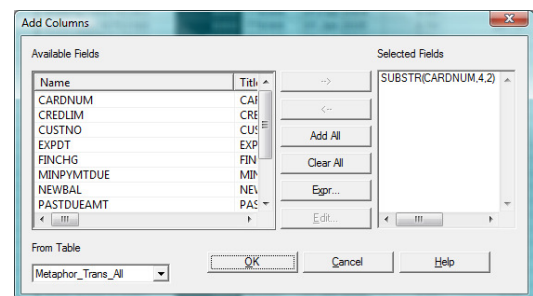
## Conclusion

For the industry to get behind PoD as a standard measure of fraud analysis would, as mentioned, require a significant industry ambassador to spearhead the initiative. However, the benefits to consumers and the banks individually are dwarfed in comparison to the overall effect such a unified response would have on the fraudsters. Where they are currently able to probe and exploit individual weaknesses, so they would find a coherent and singular response that will in turn lower the amount of fraudulent transactions that take place. It is this sort of strategy, combined with other anti-fraud standards that could subsequently emerge, that will ultimately reduce fraud levels and in so doing limit the attractiveness of payment fraud to the criminal community.

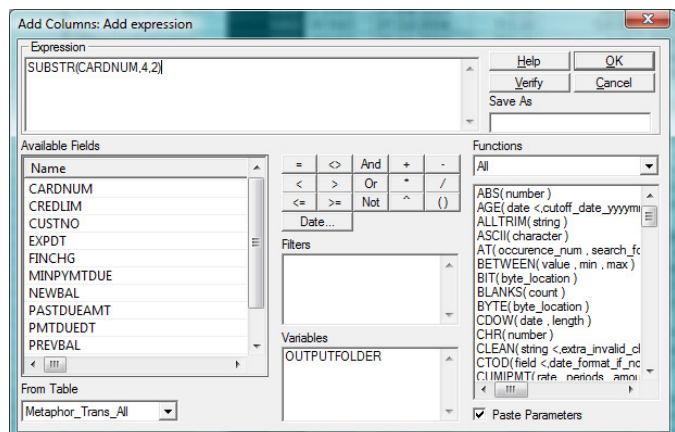


## Forgot to give a name to your expression?

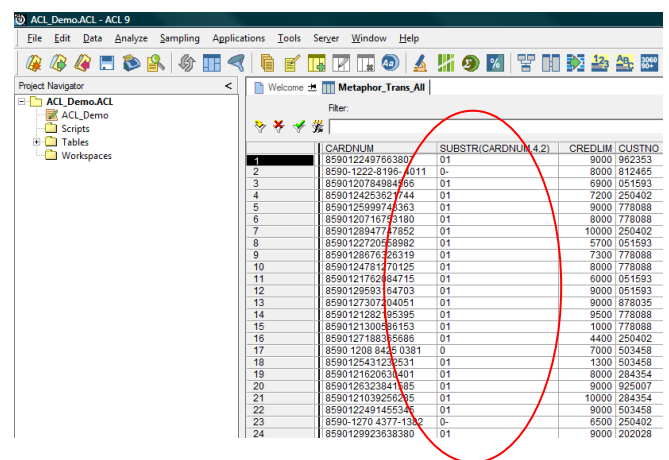
Sometimes, when you're rushing to create an expression, you may press the "OK" button accidentally without naming it (inside "SAVE AS"). Although the results may appear on the page, you will not be able to use the result for the next expression or operation. Command.



Pic.1



Pic.2



Pic.3

To solve the problem, you can give a name to the existing expression without recreating it. There are 2 ways to do this.

# Five Common Myths Debunked

By: Joan Herbig, 17 September 2008

There is a vast need for better information about PCI compliance in the marketplace. It is a relatively new standard and there is a lack of good information available. In this article I will outline a few of the most commonly held myths that we hear day in and day out from merchants, acquirers and service providers – along with the hard truths.

## Myth #1

*Breaches only happen to big-box retailers.*

**Fact:** Small- to medium-sized merchants are highly vulnerable and a frequent target. Based on most of the news coverage, security breaches may seem to happen only to huge corporations – such as the TJX security breach that compromised more than 94 million T.J. Maxx and Marshall's accounts. But, in reality, cardholder data compromises affect small online store owners far more frequently. Why? Because, the sheer number of them (according to Visa more than 6 million) makes them a more frequent target. Also, they are typically the least sophisticated technologically making them an easier target for hackers and carders.

## Myth #2

*PCI compliant merchants cannot be breached.*

**Fact:** While it is a critical step, PCI DSS compliance is only a periodic measurement at a point in time – not a guarantee. Just ask Hannaford Brothers groceries if PCI compliant merchants can't be breached. They were thought to be PCI compliant, but were still affected by a very public breach. There's a danger that organisations can develop tunnel vision dealing with PCI at the expense of building a sound security program. We recommend that companies develop a consistently high security posture, and in doing so, they will achieve PCI compliance. Any system involving people is vulnerable, either from accidental error or intentional acts of theft.

## Myth #3

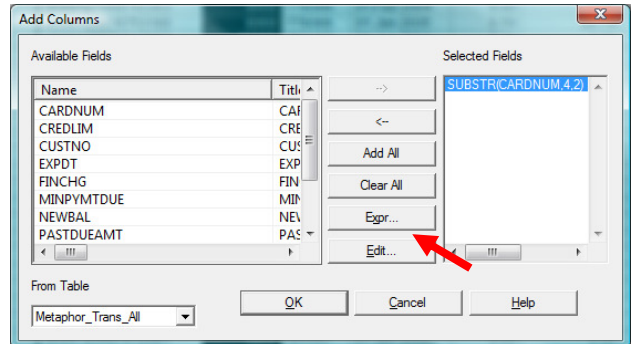
*E-commerce merchants that use PCI compliant shopping carts or payment gateways are by default PCI compliant.*

**Fact:** This may be the case, but PCI guidelines cover not only data security but also the physical security and the existence of written security policies. Once a year, regardless of how the merchant handles card data, every merchant is required to complete an SAQ, to complete the relevant Attestation of Compliance and, in most case, to submit the SAQ and the Attestation of Compliance to their acquirer. While it is important that terminals, gateways and shopping carts are compliant, that doesn't guarantee that merchants are secure from a physical standpoint or that they have employee training programs or security policies in place. SAQ A was specifically developed for merchants who outsource to a secure terminal.

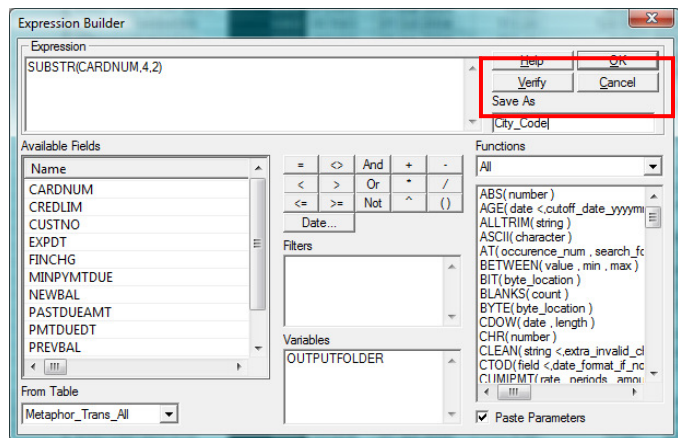
## Method 1

If you are in a stage as shown in Pic 2, follow these steps:

- Click on the expression on the right hand side
- Click Edit Button
- Put the field name on the Save as Column then click OK



Pic.4

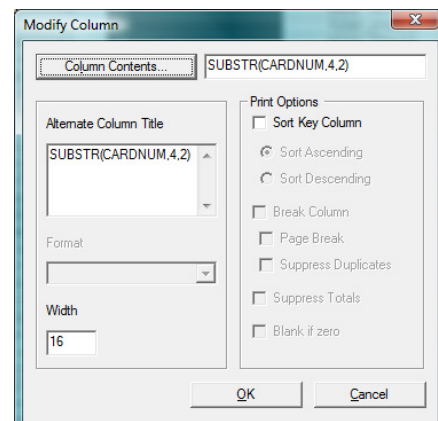


Pic.5

## Method 2

If you are in a stage as shown in Pic 3, follow these steps:

- Double click on the Header name for the field that you want to rename
- Click On the "Column Contents..." Button
- Put your field name on the "Save As" Column then click OK
- Rename the Alternate Column Title then Click OK



Pic.6

### Myth #4

*PCI compliance is too expensive.*

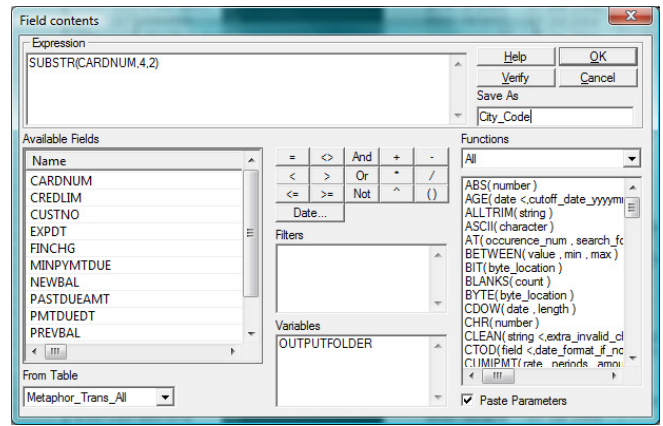
**Fact:** Non-compliance can be very expensive if not catastrophic. Non-compliance doesn't just result in costs associated with fines, credit card replacement and audit fees, but also from loss of business reputation and revenue. In fact a recent study stated that 70 percent of the cost of non-compliance was loss of revenue. This is significant for big companies that are crucified in the press, but may be catastrophic for small vendors, putting them out of business.

### Myth #5

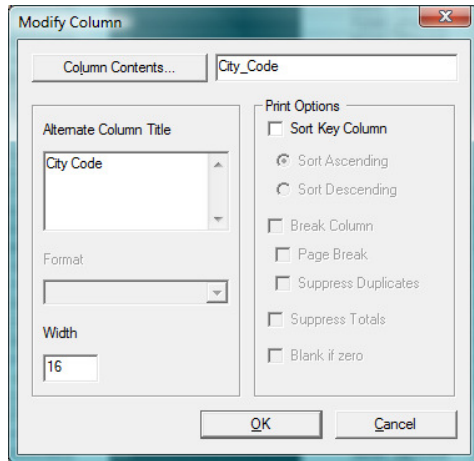
*PCI compliance is getting easier.*

**Fact:** The PCI Security Standards Council is working hard to clarify and simplify the standard. For example, in early 2008, the Council released version 1.1 of the Self-Assessment Questionnaire (SAQ), which now consists of four versions of the SAQ instead of the previous one-size-fits-all approach. While the attempt to segment merchants by validation type is a big step forward, it still presents confusion among many small merchants who are unclear on which SAQ they should complete. For small merchants in particular, protecting card holder data and maintaining a secure environment remains a complex endeavor.

Debunking these five common myths only scratches the surface. As PCI compliance and its guidelines continue to evolve, there will continue to be many lessons that still need to be learned.



Pic.7



Pic.8

# Managing Corporate Risk Through Consistent, Effective Risk Assessment

By: Denny Beran, 29 April 2009

## Managing Corporate Risk

In today's business environment, there are several ways an organisation can help to ensure they are setting the right tone and imbedding processes into their day to day operations to help manage corporate risks. Some of these include:

- Completing an **Enterprise-wide Risk Assessment** to help ensure the organisation has identified the major risks for its business and compensating controls are in place to manage these risks.
- Maintaining a strong Internal Audit function that is risk-based and focusing on the major strategic risks of the organisation.
- Conducting a **Fraud Risk Assessment** and establishing fraud awareness programs.
- Establishing an effective ethics hotline reporting process.

### How do you conduct an Enterprise-wide Risk Assessment?

First, you need to define who are the key stakeholders in the organisation both at the senior management and operating management levels. Once you have identified the key players, meetings should be conducted to brainstorm:

	CARDNUM	City Code	CREDLIM	CUSTNO	EXPDT	FINCHG	MINPYMTDUE	NEWBAL	PASTDUEAMT	PMTDUEDT
1	8500122497663807	01	8000	962353	01 Aug 2005	0.00	10.00	37.23	0.00	28 Apr '07
2	850012224781964011	01	8000	912486	01 Mar 2004	14.98	30.00	629.79	10.00	01 Mar '07
3	8500120784484456	01	6900	051930	01 Oct 2004	113.20	129.00	6408.12	0.00	04 May '07
4	8500124242421744	01	7200	250402	01 Apr 2004	101.41	0.00	5881.59	0.00	14 May '07
5	8500125999743363	01	5000	776088	01 Feb 2004	0.00	0.00	384.95	0.00	12 Mar '07
6	8500120716751380	01	8000	776088	01 Jan 2005	0.00	20.79	85.20	10.79	07 May '07
7	8500120847747652	01	10000	250402	01 Jan 2004	0.00	1.51	4.31	0.00	17 May '07
8	8500122720508862	01	8700	051930	01 Jan 2005	0.00	10.00	32.35	0.00	14 May '07
9	85001208161526139	01	7400	776088	01 Sep 2005	0.00	0.00	0.00	0.00	30 Apr '07
10	8500124781270125	01	8000	776088	01 Mar 2004	14.46	0.00	1280.69	0.00	04 May '07
11	8500124762684745	01	5000	051930	01 Jan 2005	0.00	0.00	-0.02	0.00	21 May '07
12	8500129593184763	01	8000	051930	01 Sep 2005	0.00	10.00	19.95	0.00	21 May '07
13	8500121707504951	01	1000	678035	01 Oct 2004	0.00	10.00	405.12	0.00	03 May '07
14	85001211082195395	01	9500	776088	01 Oct 2005	0.00	10.00	48.87	0.00	10 May '07
15	8500121305881653	01	7000	776088	01 Nov 2004	0.00	0.00	0.00	0.00	14 May '07
16	8500127188385666	01	4400	250402	01 Jan 2004	84.91	65.00	3009.93	0.00	04 May '07
17	85001208184510861	01	7000	503456	01 Jul 2004	0.00	0.00	-0.17	0.00	29 Apr '07
18	8500125431232631	01	1300	503456	01 Jul 2004	34.76	225.00	1988.63	183.00	30 Apr '07
19	8500121020530401	01	8000	284354	01 Mar 2005	0.00	10.00	101.82	0.00	12 May '07
20	8500120103849585	01	8000	925007	01 Apr 2005	0.00	10.00	24.24	0.00	03 May '07
21	8500121039256285	01	10000	284354	01 Nov 2005	0.00	0.00	0.00	0.00	20 May '07
22	8500122481465485	01	8000	503456	01 Jul 2004	0.00	10.00	378.65	0.00	18 May '07
23	850012701437711382	01	8500	250402	01 Jan 2005	87.52	102.00	5080.82	0.00	07 May '07
24	85001280291938380	01	8000	250402	01 Nov 2004	73.00	181.00	3871.38	0.00	17 May '07
25	85001235076129811	01	8800	925007	01 Jun 2005	0.00	0.00	0.00	0.00	26 Apr '07
26	850012810391602795	01	7000	962353	01 Nov 2004	64.51	0.00	488.92	0.00	17 May '07
27	8500122895563862	01	3800	284354	01 Mar 2005	84.26	0.00	3659.55	0.00	18 May '07
28	850012810391602795	01	7000	962353	01 Nov 2004	64.51	0.00	488.92	0.00	17 May '07
29	850012932000796	01	4900	503456	01 Jun 2005	77.36	90.00	4644.63	0.00	26 Apr '07
30	85001280291938380	01	5500	962353	01 Feb 2005	0.00	17.00	3792.57	598.00	05 May '07
31	8500128009071653	01	2400	776088	01 Sep 2004	0.00	50.00	1792.05	0.00	20 May '07
32	8500128742624780	01	8500	284354	01 Mar 2004	15.3	20.00	89.19	10.00	29 Apr '07
33	8500123888727712	01	8000	612465	01 Sep 2004	36.43	33.00	3550.59	0.00	13 May '07
34	8500127628113925	01	8000	925007	01 Nov 2005	0.00	0.00	-0.27	0.00	20 May '07
35	850012810391602795	01	8000	250402	01 Nov 2005	61.99	0.00	4887.82	0.00	26 Apr '07
36	8500124265629251	01	7000	962353	01 Mar 2004	0.00	0.00	-0.98	0.00	28 Apr '07
37	8500124265629251	01	2000	250402	01 Oct 2004	20.38	0.00	1804.42	0.00	11 May '07

Pic.9

## How do you conduct an Enterprise-wide Risk Assessment?

First, you need to define who are the key stakeholders in the organisation both at the senior management and operating management levels. Once you have identified the key players, meetings should be conducted to brainstorm:

- What are the major risks for the organisation in meeting their stated goals and objectives?
- What are the key risks that keep management up at night?
- What could go wrong that would cause the organisation to miss its stated performance targets and stated objectives?
- What are the key controls management has in place to mitigate these risks?
- How are these key controls being monitored for effectiveness and by whom?

These brainstorming discussions should be conducted using a control self assessment format, where the discussions are open and candid dialogue of both downside and upside risks.

From these meetings, you can begin to summarize the top 7 to 10 key business risks for the organisation and begin developing a risk matrix that would include:

- Defining the business owner(s) for the risks.
- Linking the key controls in place to mitigate each risk.
- Identifying the monitoring processes in place to help ensure the key controls are operating as stated.

As an example, a key strategy may be to attract and retain new customers as you enter a new market. What are some of the major risks with this strategy? One risk could be an ineffective marketing program that does not resonate with new customers. Once all the risks have been identified, you need to begin linking the key controls your organisation has in place to mitigate these risks. In this example, controls could include processes the organisation has in place to track advertising effectiveness including post advertising event analysis, market basket analysis and tracking of coupon redemption rates. Also, you should define what monitoring processes you have in place to ensure the controls are operating as intended. This could include trending analysis of performance over a stated period of time. A major benefit of this exercise is the ability to perform a gap analysis to identify where controls are ineffective or may need enhanced to mitigate a stated risk.

This risk matrix can serve many purposes in managing corporate risk but one that has worked very well in our organisation is in engaging the Audit Committee in discussing risks. To enhance corporate governance and to keep the process vibrant, we require a different business owner to attend each Audit Committee meeting to discuss risks for their areas and what controls they have in place to mitigate these risks. These discussions include probability of occurrence, likelihood and financial impact. This process keeps the discussion of enterprise risks front and center at every Audit Committee meeting. It also makes the business owner think about risks for their business area and helps to imbed risk management into the day to day decision-making processes.

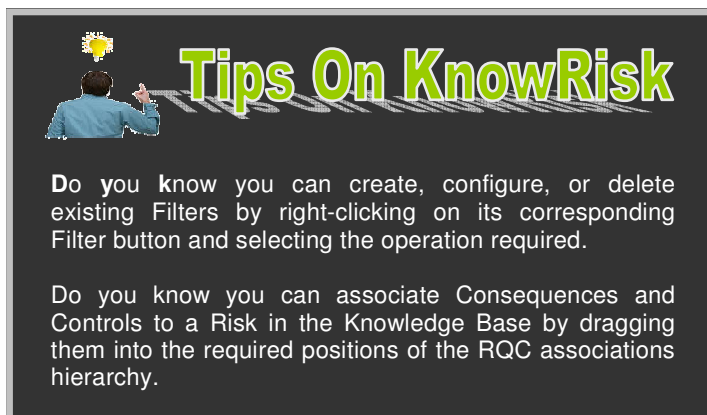
As you would expect, the risk matrix will need to be updated on a regular basis. Depending on the nature and type of business, it would not be unusual for this to be an annual process.

## What is the role of Internal Audit in enhancing Corporate Governance?

Internal Audit should be considered by management to be a valued partner and resource to enhance corporate governance. Internal Auditors have the ability to play a greater role than just testing SOX controls and compliance. As an example, Internal Audit should play a major role in completing the above Enterprise-wide Risk Assessment. Internal Audit can serve as an agent of change by getting involved in the key drivers/strategic initiatives of the organisation and by identifying emerging risks.

Active involvement from the Internal Audit group can help an organisation identify risks and establish the necessary controls to effectively mitigate those risks. They can also assess these controls in conjunction with management to ensure they are functioning as designed. Lastly, Internal Audit can perform a gap analysis to identify where controls do not exist to mitigate select risks.

To ensure Internal Audit has a good understanding of the major risks facing a organisation and that auditing is performing risk-based reviews that support an organisation's key strategic initiatives, the following should be completed on an annual basis:



**Tips On KnowRisk**

Do you know you can create, configure, or delete existing Filters by right-clicking on its corresponding Filter button and selecting the operation required.

Do you know you can associate Consequences and Controls to a Risk in the Knowledge Base by dragging them into the required positions of the RQC associations hierarchy.

- Developing/updating the inventory of auditable areas (e.g., key functions within the organisation that could be considered for a review).
- Ranking each function based on key risk factors including their financial, regulatory, operational, people, IT and reputational risks.
- Analysing where the organisation's risks and exposures are in conjunction with management to ensure the audit plan is risk-based and focused on the key initiatives of the long range business plan.
- Allocating resources based on where the organisation's key risks are and where Internal Audit is required to complete reviews (e.g. required by law).

Performing this assessment will help to ensure that Internal Audit is focused on the most important risks, is linked to the business and is completing audits that have an impact in the success of the organisation.

### Completing a Fraud Risk Assessment

In addition to completing an Enterprise-wide Risk Assessment, it is important to have additional processes and programs in place to combat fraud risk by increasing the level of fraud awareness within the organisation.

As a start, consider completing a **Fraud Risk Assessment**. Similar to an **Enterprise-wide Risk Assessment**, this can be accomplished through conducting brainstorming sessions with management to discuss potential fraud schemes and scenarios. A Fraud Risk Matrix should be developed which includes the owner of each process, a list of possible fraud schemes and scenarios impacting the process, and a detailed account of all controls in place to prevent or detect fraudulent activity.

Once the Fraud Risk Matrix is developed, reviews can be performed of select processes to evaluate the effectiveness of the stated controls to mitigate the fraud risks. This matrix provides you the ability to perform a gap analysis to identify areas where additional anti-fraud control enhancements should be implemented.

Completing a **Fraud Risk Assessment** will increase the overall level of fraud awareness throughout the enterprise. As a by-product of this exercise, implementing fraud awareness and training programs can help to keep the message fresh and alive in your organisation. As with any informational campaign, there are many ways to get the message out. Some of the more common methods are administering fraud and ethics training to your employees, conducting awareness and ethics presentations in departments within the organisation, and creating a "Red Flags" of fraud poster and distributing it throughout the organisation.

### Effective Ethics Hotline Reporting Process

One can never do enough to increase employee and vendor awareness of the ethics hotline. Required as part of SOX, this open line of communication to confidentially report situations of potential wrongdoing or unethical behavior cannot be overly promoted. All organisations should develop programs to increase awareness of the hotline and its purpose, including posting hotline numbers on internal and external websites; conducting awareness meetings with employees; and developing graphics communicating its purpose and when it should be used. In addition, you must ensure you communicate your no-retaliation policy and promote this in all your hotline awareness communications.

On a semi-annual basis, you should consider requesting that the Chief Audit Executive provide the Audit Committee with a summary of all hotline calls including their final disposition. This not only gives the Audit Committee an idea of the nature of the calls received but the assurance that the caller concerns were addressed.

Establishing an investigative protocol and guidelines to ensure that reported issues and concerns are reviewed with a high degree of consistency throughout the organisation is extremely important. The guidelines should define which department(s) will perform the investigation, the standards to follow in completing and documenting the work performed, and the communication process for advising relevant parties concerning the investigation and the results of the investigation.

In summary, taking the following steps will help to create good corporate governance and maintain a strong ethical climate within your organisation:

- Completing an Enterprise-wide Risk Assessment that includes engaging the Audit Committee and the business owners on the key risks facing the organisation and the key controls in place to mitigate these risks.
- Maintaining a highly qualified Internal Audit Department that is linked to the business and performing audits in high-risk areas.
- Completing a Fraud Risk Assessment that identifies the major fraud risks facing the organisation and the key controls in place to mitigate these risks.
- Communicating what is expected of your employees by clearly and convincingly stating your organisation's values and ethics and the kind of behavior that is expected from each employee.
- Providing a safe mechanism for reporting concerns so that those who know about, or are suspicious of fraudulent or other unethical violations, will come forward and report misdeeds without the fear of retaliation.
- Maintaining a zero tolerance for fraud by clearly stating your organisation's position on fraud.



# IT Security Series Part 1: Information Security Best Practices

By: Matthew Putvinski, 9 June 2009

## Information Security Best Practices: *How Strong is Your Information Security Program?*

Traditionally, documented security policies have been viewed as nothing more than a regulatory requirement. While this may have been true in the past, building a strong information security program (ISP) is a business imperative as you fight to keep the customers you have and work to attract new ones. Your information security policies can either work to help you grow your business or signal a red flag that security is not a top priority.

No matter how strong your security posture is now, if you don't document it, it won't last. You must assume that people instrumental in building your security environment will eventually move on. In that respect, training the replacement is a lot less painful and much more effective with a written guide. Without a policy manual, the new employee would eventually learn what to do but would you really want to risk a security incident while they are trying to figure it out?

It's important to understand that there is no procedure, policy, or technology that will ever be 100% secure. It just doesn't exist. You can, however, endeavor to get as close to perfect as possible.

Lack of a documented security policy is a huge red flag when determining liability in the event of an incident. You do not know when the next attack will happen and if someone is aggressively targeting you, they will cause pain. When it comes time to defend yourself, no matter the strength of your security environment, the lack of a documented information security program is a message that management has not taken data security seriously. This perception becomes increasingly dangerous when we're talking about a court of law and an untold number of potential customers in the court of public opinion.

Whether you are currently without a policy or want to ascertain where yours fits along the continuum, here are key components that should be in a best practices ISP.

### **Information Security Best Practices: *The Information Security Officer***

The first thing that any security program must do is establish the presence of the Information Security Officer. Depending on the size of your security environment, this could be a full-time position or a current employee who has the availability to take on further duties.

Besides the time element, the organisation must clearly define the expectations of the Information Security Officer and determine if an individual is capable to fill the role. During a later post I will describe the attributes that ascertain "capability", but the complete lack of someone in this role means that information security is not a priority in your organisation.

### **Information Security Best Practices: *End User Acceptable Use Guidelines***

Your policy should contain specific language detailing what employees can do with "your" workstations. While we hope that all company property is used for company purposes, this just isn't the case in real life. Instruct employees as to what is considered business use and explain the risks of downloading games or using tools like instant messaging.

### **Information Security Best Practices: *Software Updates and Patches***

What's your stance when it comes to patch management? Do you require patches and upgrades to be implemented immediately? Are you sure you're actually doing what your policy says?

Random checks to confirm you are following your own rules is the best way to monitor the activity.

If you're scratching your head at my use of the phrase "patch management", understand that if you don't keep up to date on your system patches and upgrades, you leave yourself wide open for the most basic of hacks. If you never update, your vulnerabilities are exponentially increased. Your best practices Information Security Program should clearly document your patch management procedures and frequency of the updates.

### **Information Security Best Practices: *Vendor Management***

You're only as strong as your weakest link, and when you work with third-party providers their information security downfall can become your issue. Make sure you document which vendors receive confidential information and how this information is treated when in the custody of the vendor. The lack of strict vendor guidelines could increase the risk of releasing your customers' private information.

### **Information Security Best Practices: *Physical Security***

Documents don't walk out of the office on their own. Having strict rules about who can physically access your offices and how they gain entry can decrease the likelihood that an unauthorized individual is present to steal information. The next step is to ensure that your policy documents how physical information is stored and destroyed.

### **Information Security Best Practices: *Data Classification and Retention***

Lessen your liability by classifying exactly what type of data you need and how long you need it. A breach is bad enough, what's worse is if data is stolen that you didn't need to keep or shouldn't have had to begin with. In the case of TJX, many of the credit card numbers affected had no business purpose in being kept.

### **Information Security Best Practices: *Password Requirements and Guidelines***

Your employees dread having another password to remember. The more complicated the requirements you make to ensure security, the more they decide to write them down and expose them to others. Establish a strong password policy but stay within reason for your employees. Sometimes, a little additional training as to why the policy is the way it is can be all you need to gain acceptance.

### **Information Security Best Practices: *Wireless Networking***

There is no doubt that the implementation of wireless networks has saved many organisations both time and money in comparison with traditional cabling. As you decide what type of network connectivity to adopt, understand that with increased flexibility allowed by wireless, a stronger encryption standard is required to ensure there is no abuse.

### **Information Security Best Practices: *Employee Awareness Training***

How well informed are your employees to identify or prevent a security incident? Each and every one of your employees can act as a member of your own security army with some simple training. The first step in recruiting them for the cause is to set the expectations appropriately and communicate those expectations in your policy.

### **Information Security Best Practices: *Incident Response***

Hands down, the worst time to create an incident response program is when you are actually having an incident. You can't undo what has happened and you're in crisis mode dealing with the after effects of the breach.

Not the time to be putting policy to paper.

Your reputation is severely at risk, and if you respond inadequately you risk making it worse with law enforcement as well as your customers. Act as if a breach is inevitable and take the time to develop the language and procedures you will use in the event of an incident to ensure you're prepared when the time comes.

### **Information Security Best Practices: *Annual Updates and Reporting***

Don't let all your hard work go to waste. The worst thing to do after investing time and resources into your information security program is to allow it to sit on the shelf and become obsolete. Threats and risks are changing daily and it is imperative that your policies stay up to date. Requiring an annual review, with results are reported to the Board of Directors and senior management, will help to ensure that your program remains current and can handle any future incidents.

Feel free to use this list in either building your program or as a checklist to determine your current status. Additionally, other good resources include the National Institute of Standards and Technology and the SANS Institute. The most successful policy will be one that blends in with the culture of your organisation rather than just existing to fill a regulatory requirement. In doing so, you increase the security posture of your organisation with as little effort as possible and help ensure you don't become another statistic in the evening news.



# 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.

TELL US WHY  
you  ACL

and you could win a trip to  
The IIA All Star Conference  
In Las Vegas,  
October 19-21, 2009!



Visit [www.acl.com/iheartacl](http://www.acl.com/iheartacl) NOW!

## User Group Meetings Philippines and Singapore

### Prodigy User Group Meeting Philippines

**Date:** 17<sup>th</sup> September 2009

**Venue:** Hotel Intercontinental, Makati City, Philippines

**Time:** 9.00am to 12.30pm

**Host:** Bank of Commerce Manila

### ACL User Group Meeting Singapore

**Date:** 25<sup>th</sup> September 2009

**Venue:** TBA

**Time:** 9.00am to 12.30pm

We are pleased to have our veteran users sharing their experiences at the meeting. This event also serves as a platform for users to network within the industry. For more information on the upcoming user group meeting, please email us at [conference@prodigy-group.com](mailto:conference@prodigy-group.com)

## Upcoming Conferences

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

### ACIIA Conference 2009

**Date:** 19-21 October 2009

**Venue:** Kuala Lumpur Convention Centre, Malaysia

**Theme:** Towering Experience: Towards Sustainable Success

### IIA Philippines 62<sup>nd</sup> National Convention 2009

**Date:** 26-27 October 2009

**Venue:** Puerto Princesa, Palawan

**Theme:** Running the Race to Excellence

### TACS 2009

**Date:** 1<sup>st</sup> week November 2009

**Venue:** Singapore

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](mailto: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](mailto: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:

- **IT Governance Conference** held at Sheraton Subang Hotel & Towers, Malaysia from 26<sup>th</sup>-27<sup>th</sup> May 2009.
- **5<sup>th</sup> Asia Pacific Audit & Governance Summit** held at JW Marriot Hotel, Malaysia from 2-3 June 2009.
- **National Conference on Internal Audit (SNIA 2009)** held at Sanur Beach Hotel, Denpasar, Bali from 16-18 June 2009.
- **2<sup>nd</sup> IT Summit** held at Hotel Intercon, Makati City, Philippines on 8<sup>th</sup> July 2009.

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

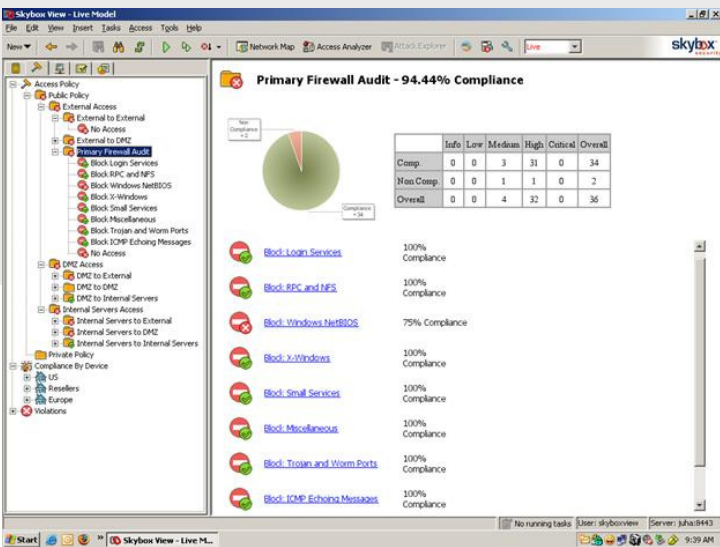
## NEW! IT & IS Audit Solutions

**Prodigy is pleased to deliver a complete solution suite for all your IT & IS Audit needs.**

**SenSage:** A log management solution that provides automated collection, storage, correlation and reporting to allow organisations to effectively monitor, report and investigate activity and events from thousands of different log sources throughout the enterprise.

**IMPERVA:** IMPERVA provides auditors with audit trails of user activities without the need to turn on the native logs of the databases. This will remove the load on the application server and therefore database auditing can be done without any impact on performance.

**Skybox Security:** Skybox security provides application and database scanners that will result in a single, centralised and normalised view of all vulnerabilities. These test are done periodic and automated therefore vulnerabilities can be established and the gaps can be patched.

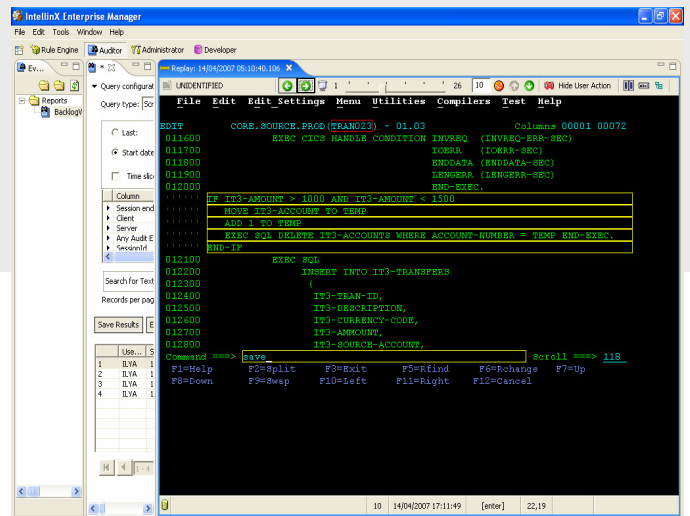


Contact our Business Consultants today for more information on our new IT & IS Security solutions!

**Websense:** A Data Loss Prevention (DLP) solution designed to protect customer information, intellectual property, and enforce and report on regulatory compliance. Websense automatically discovers confidential data, monitors its use, and enables administrators to create and implement content enforcement policies.



**Intellinx:** Intellinx software provides first-of-its kind cross-platform insider threat intelligences system for auditing and data leakage detection. Armed with the capabilities to track and zoom-in on all end-user activities with all the central applications, the system identifies exceptions and triggers instant alerts on suspicious events in real time, thereby reducing potential operational risk and fraud losses.





# 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.*

VENUE	COURSE NAME	Aug-09	Sep-09	Oct-09
SINGAPORE	ACL 105 - Foundation of ACL: Concepts & Practice	03-05	09-11	05-07
	ACL 201 - Data Analysis Techniques	06-07	17-18	08-09
	ACL 301 - Advanced ACL Concepts & Techniques: Functions	26	-	14
	ACL 302 - Advanced ACL Concepts & Techniques: Scripts	27-28	-	15-16
	ACL 303 - Advanced ACL Concepts & Techniques: Functions & Scripts	26-28	-	14-16
	Fraud Detection Techniques Using ACL	-	-	19-20
JAKARTA, INDONESIA	ACL 105 - Foundation of ACL: Concepts & Practice	03-05	07-09	12-14
	ACL 201 - Data Analysis Techniques	13-14	10-11	15-16
	ACL 301 - Advanced ACL Concepts & Techniques: Functions	24	-	-
	ACL 302 - Advanced ACL Concepts & Techniques: Scripts	25-26	-	-
	ACL 303 - Advanced ACL Concepts & Techniques: Functions & Scripts	24-26	-	-
	Fraud Detection Techniques Using ACL	-	-	-
KUALA LUMPUR, MALAYSIA	ACL 105 - Foundation of ACL: Concepts & Practice	04-06	02-04	05-07
	ACL 201 - Data Analysis Techniques	10-11	14-15	08-09
	ACL 301 - Advanced ACL Concepts & Techniques: Functions	-	28	-
	ACL 302 - Advanced ACL Concepts & Techniques: Scripts	-	29-30	-
	ACL 303 - Advanced ACL Concepts & Techniques: Functions & Scripts	-	28-30	-
	Fraud Detection Techniques Using ACL	-	-	26-27
HONG KONG	ACL 105 - Foundation of ACL: Concepts & Practice	17-19	21-23	12-14
	ACL 201 - Data Analysis Techniques	20-21	24-25	15-16
	ACL 301 - Advanced ACL Concepts & Techniques: Functions	-	28	-
	ACL 302 - Advanced ACL Concepts & Techniques: Scripts	-	29-30	-
	ACL 303 - Advanced ACL Concepts & Techniques: Functions & Scripts	-	28-30	-
	Fraud Detection Techniques Using ACL	-	-	-
MANILA, PHILIPPINES	ACL 105 - Foundation of ACL: Concepts & Practice	-	-	19-21
	ACL 201 - Data Analysis Techniques	-	-	22-23
	ACL 303 - Advanced ACL Concepts & Techniques: Functions & Scripts	-	-	26-28
	Fraud Detection Techniques Using ACL	-	-	-
BANGKOK, THAILAND	ACL 105 - Foundation of ACL: Concepts & Practice	-	-	-
	ACL 201 - Data Analysis Techniques	-	-	-
	ACL 303 - Advanced ACL Concepts & Techniques: Functions & Scripts	-	-	-
	Fraud Detection Techniques Using ACL	-	-	-



## Next Issue Topics:-

- Continuous Auditing
- Financial Fraud
- Information Security

## Our Regulars:-

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



Onsite specialised workshops are also available. Kindly contact [training@prodigy-group.com](mailto:training@prodigy-group.com) for more information.

The Prodigy Group is a premium total solution provider offering extensive IT solutions on Audit & Compliance, Risk Management, Internal Control Management, IT Security Management, and IT Risk & Governance 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, SymSure Monitor, Pentana, Intellinx** and **GRCMonitor**