Merger and Acquisition:

Effective Information Security Depends on Strategic Security Metrics

By Urs E. Gattiker, Ph.D.

When people talk about acquiring another firm, the term "due diligence" comes up sooner or later. Usually, legal definitions of due diligence say something such as:

> *Due diligence is a measure of prudence, activity or assiduity, as is properly to be expected from, and ordinarily exercised by, a reasonable and prudent person under the particular circumstances. It is not measured by any absolute standard but, nonetheless, depends on the relative facts of the special case.*

In plain language, this definition means that due diligence helps in making sure that the acquirer of the goods gets what he/she paid for. Nonetheless, before information security can protect the new entity it has to understand the component parts. Hence, including information security and legal compliance issues in the due diligence process can give the new enterprise a head start. An information security and compliance survey of combined assets is required as a first step in devising security for the joined organizations.

This article tries to advance knowledge about due diligence regarding information security and regulatory compliance. The objectives of this paper are to integrate research insights into decision making regarding a due diligence framework, and to explore whether such a tailored and targeted approach can help in the merging of two potentially diverse organizations.

There is an ever-growing number of standards, guidelines, checklists and assessment instruments with which organizations are expected to demonstrate some level of compliance. Organizations must also demonstrate that they exercise due diligence and are able to reach an acceptable standard of due care in how they manage their computing infrastructures and the information that such networks and systems create, transmit and store, particularly when connected to the Internet.

Conducting an audit of IT security and risk management as part of the due diligence process provides assurance to senior management that the terms and conditions of the takeover are fair and realistic. There are few remedies for the organization that fails to exercise due diligence. Being negligent in thoroughly assessing IT security and risk management before the firm agrees to a merger with, or takeover by, another firm may cause active investors to hold management liable for the lack of due care.

Why are IT security and risk management sometimes overlooked during due diligence? One answer is that top management and the board of directors begin the due diligence process with clear and explicit expectations of the benefits they hope to gain by making the acquisition. An example could be being able to enter a new market more quickly by acquiring a firm that is already successful in this lucrative market segment or country. While the board wants to minimize the firm's exposure to the many problems and pitfalls that can arise when making an acquisition, it might be willing to live with certain security and risk matters that are discovered during the due diligence exercise. If these problems and pitfalls can be identified, they may still be costly to fix down the line. Nonetheless, knowing and clearly understanding the cost implications of these IT security-related risks and challenges when making the decision to go ahead or refrain from acquiring the target can be extremely helpful during the negotiation process.

The due diligence process often results in shortcomings being discovered regarding legal compliance and due care of how data and information assets are being managed and protected. While such audit findings may not stop a merger or takeover from proceeding, they may affect negotiations between the parties. As important, audit findings may result in specific budget allocations being authorized to remedy discovered shortcomings after the merger or takeover has gone ahead. In fact, due diligence may reveal that it could be too costly to merge two systems and, instead, it would be more advantageous to run both in parallel for some time to assure a smooth operation. Eventually, transition may occur whereby data from one system may be moved over to the other. Thereafter, the less optimal IT infrastructure will get shut down. Knowing about such an approach before signing on the dotted line will help prevent a wringer affecting postmerger streamlining of activities and will help realize the synergy effects faster than otherwise possible.

At this stage, what is most important to understand is that to succeed in due diligence, the time to start thinking about due diligence is early in the process. Preparing for due diligence takes time and once due diligence is called for, it is too late to implement changes. Instead, every decision that one makes should be tested against the questions raised throughout this article (noted in italics). Answering these questions will help streamline operations, and the enterprise will benefit regardless of whether a possible merger looms around the corner.

How will the organization look when someone asks hard questions?

Most companies will have to go through due diligence someday. This might be due to being acquired by a friendly suitor, seeking outside investment (e.g., issuing a bond or getting a bank loan), going public or trying to secure more capital by issuing additional stock.

In the due diligence process, IT security rarely, if ever, takes center stage. In most cases, top management and the board of directors are considering a possible merger or takeover for strategic reasons, such as to accelerate the enterprise's efforts in entering a new market or gaining market share. As well, most firms do not seem to follow a structured framework in IT due diligence.[1]

Unfortunately, processes, functions or applications of information technology and data can have serious implications on a smooth transition after the merger or takeover has taken place. In fact, regulatory concerns regarding security for personal data, archiving technology and procedures, disaster recovery systems, and authentication of user access and privileges could dwarf future efforts for streamlining operations.

What if IT has been outsourced in the takeover organization?

The objective of due diligence is straightforward and simple. The acquirer is interested in minimizing its exposure to the many problems and pitfalls that can arise when making an acquisition. This requires not only that the IT resources and compliance level are investigated at the takeover target, but also that an audit of IT security and risk management is conducted at the outsourcer's location.

Generally, this is evaluated in terms of staff vetting, physical access security, database security, communications security, etc. But another vital consideration should be the effectiveness of each candidate location's legal preventive measures and remedies for data theft or misuse—and the complexity and cost of securing those protections. Such analysis regarding the state of data security and the level of legal protections in the country in which the outsourcer is located is no simple matter.

In spite of any impressive preventive measures that the targeted firm may have required its outsourcers to take, one must still investigate what kind of remedies and procedures were put into place in the event of a data security breach occurring offshore. In addition, the due diligence team must investigate what rules concerning control processes and procedures were invoked between the takeover target and the outsourcer. Without auditing these, adequate integrity, security and confidentiality of electronic records and rules cannot be ascertained. In fact, these may be vastly different from what it says on paper. How service level agreements (SLAs) between the targeted firm and its outsourcers work in practice must be addressed.

Unfortunately, many companies may be trying to parade their facilities to current clients, potential customers and journalists in the hopes of gaining free advertising. Conducting due diligence and risk assessments of service providers that are being used by the target firm is a must. Analysis of the contractual measures designed to meet various objectives and of how the service provider's compliance was monitored by the client has to be undertaken. This may also suggest adjustments that must be implemented after the takeover, reflecting necessary adjustments to respond to modified risks. A combination of all these measures should go a long way toward minimizing both the incidence and consequences of data theft and misuse incidents due to a merger.

Success of this exercise regarding outsourcing services will in large part depend upon the SLA and:

- If and how it allows the client to get out of a contract
- How much access the outsourcer is willing to provide to the due diligence team

In fact, an uncooperative outsourcer may leave the due diligence team no choice but to tell management that there is no way they can provide assurance that the outsourcer's terms and conditions of data and information handling are compliant and that they meet the best practice standards of the firm looking for a takeover target.

In reality, however, management may simply be willing to live with these unknown consequences to pursue the set corporate strategy by taking over the acquisition target.

What about the data room where all documents of the due diligence team will be held?

Due diligence typically takes the form of the acquirer's list of several hundred questions and/or requests for copies of documents. In turn, the potential seller must respond to the potential buyer on or before a specified date. While this goes beyond the scope of this article, a data room must be made ready for the due diligence team to provide a place for work and the studying and storing of confidential documents that cannot be taken off the premises.

Decision and Choices

As the previous information indicates, due diligence is an important process that is often not built on a well-established framework, and IT due diligence is not necessarily at the center of merger and acquisition negotiations. However, to improve risk management and increase the likelihood of a smooth transition after a merger or acquisition, it is important to address what information will be used by members of top management to support their decision-making process. It is also important to discuss how an IT framework for due diligence might support these efforts.

Usually, management will have access to data regarding financial and information assets of the acquisition target, as they are provided by the auditors. Responses to the due diligence questionnaire may also be helpful. However, such information will rarely, if ever, give decision makers a full picture about the complete rank of possible outcomes, let alone their probabilities.[2]

Decisions from experience (in this case, limited experience about mergers or takeovers) and decisions from description can lead to dramatically different behavior choices.[3]

Hence, as **figure 1** suggests, the way managers, board members and IT users are being cued about a possible information security event, such as data confidentiality being violated, will influence the person's assessment of this risk. Additionally, how they assess due diligence information regarding security and compliance will affect their opinion about a prospective acquisition target.

Figure 1 shows that information provided by internal control systems grounded on the COSO and *Control Objectives for Information and related Technology* (COBIT) frameworks[4] must be used carefully, thereby limiting the likelihood of management underestimating critical but rare events (e.g., possible failure), as research suggests.[5] Providing decision makers with easy-to-understand examples to which they can relate is, most certainly, critical. This approach will more likely convey information that is critical in the due diligence phase. In fact, such information must be available before a final decision is made to either go ahead or refrain

Figure 1—Considering Decision-making Moderators During Due Diligence

Event	Decisions based on	
	Experience	Description
Rare events	Underweighting of rare events	Overweighting of rare events
Example or information provided to management is easy to relate to	——	Information given more weight
Consider a proposition (e.g., it might be costly)	Enhances its subjective truth (e.g., could the merger fail)	

from going through with an acquisition, merger or takeover. *How will this look in practice when the takeover target has outsourced IT functions?*

As previously noted, due diligence efforts encompass collecting data about information security and legal compliance issues as well as technology processes, functions and applications. It is likely that such information is not at the top of the agenda for management, since strategic issues might be more paramount. Hence, as **figure 1** shows, it is critical to provide examples that get top management's attention (e.g., the competitor was slapped with a major fine because information security concerns were not addressed properly).[6] Such examples are easy to follow and help eliminate the risk for underestimating the severity of rare events in conjunction with security oversights and compliance issues that could cause problems after a merger or takeover is completed.

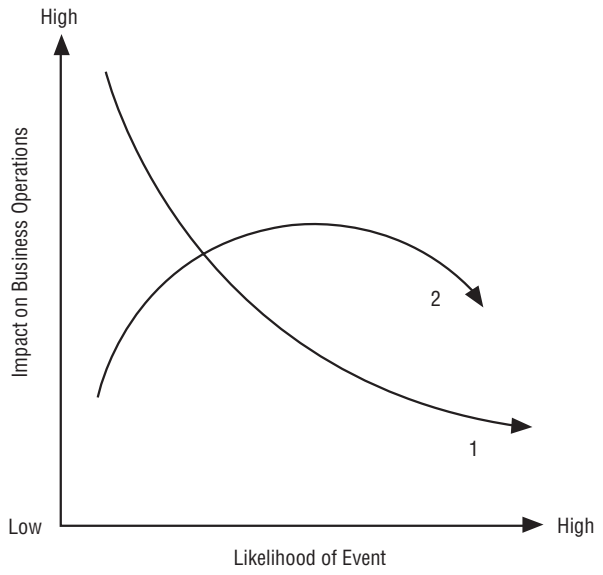
As mentioned previously, outsourcing brings a greater degree of complexity and uncertainty into the due diligence process. Accordingly, it becomes very important to make sure that management receives information that is highly relevant regarding security, data protection and risks. In particular, it is important to determine what the findings may mean in costs and time delays for the postmerger phase. The decision to be made may be as simple as where to locate the postmerger organization's IT operations. *Will it be located with the outsourcer of the firm launching the takeover or the one that does the IT work for the firm being acquired*?

Whatever decision is made, it is important to make sure that the risks are not forgotten. For instance, the severity of security concerns raised during the due diligence exercise can be underestimated by some decision makers. As well, nobody envisions ending up in front of a judge, but top management may be extremely cautious about this rare event, especially considering the growing number of executives who are being held accountable by regulators and prosecutors.

Information Security and Compliance

In an ideal world, people care about how information security regarding compliance issues might affect a due diligence process. But besides the challenge regarding information that allows management to make the best decisions for shareholders, employees and customers (see **figure 1**), management is worried about how a takeover or merger could affect operations. In particular, two IT systems need to be brought together that might not fit at all.

Figure 2—Likelihood of Merger or Acquisition Impacting Operations



In **figure 2**, curve 1 indicates that a few events may happen very rarely, but their impact on business operations could be severe, if not disastrous. Besides great financial consequences, such an event could trigger reduced customer satisfaction and trust and could damage the value of the brand.

Curve 2 describes a situation in which a rare event may have limited cost and operational consequences. For instance, thanks to redundancy services, a power failure may not cause much damage to the business.

To illustrate curve 2 in **figure 2**, a region may experience a power failure that affects one of the firm's call centers (A). This is most likely a relatively rare event in an industrialized country. But, if it does occur, customers who are trying to reach the call center are rerouted and served by another call center (B), due to well-working redundancy services. However, role-based access management may limit customer agents in call center B with access to client records from the region or country of call center A. Role-based access management must be designed and implemented in such a fashion that it will be easy to give call center B's customer service agents the authority to access customer records from call center A's country, at least during an emergency. It sounds obvious, but it is important to determine how fast this temporary change can be implemented to limit possible inconveniences customers might experience if they call the service hotline and are told that it is out of service.

As **figure 1** pointed out, managers may, based on experience, underestimate the likelihood of a critical event or overestimate the rare event based on descriptions. This means that the due diligence team will have to find a careful balance between the underestimating and overestimating of rare events that might create postmerger havoc or disaster due to IT infrastructure and security-related factors.

Figure 3 lists a set of considerations that will help in preparing for the due diligence process and in creating

procedures, guidelines and business continuity processes to help the firm cope with situations such as those discussed previously. It is important for each of the items to be considered and for focus to be placed on potentially critical risks regarding business operations, such as the customer hotline or cash management databases.

Regarding information assets and regulatory compliance in the due diligence process, the key is to determine with relative accuracy the likelihood that things will either operate properly or fail to do so. To provide top management with a realistic snapshot (see **figure 1**), it is critical to cost out these issues (see item 11 in **figure 3**). While costs for merging IT operations are unlikely to stop a merger or takeover from proceeding, it is helpful for management and the firm's board of directors to have a realistic picture. In particular, underestimating the challenges and facing the problems down the line is less likely to happen (see **figure 1**). Accordingly, management needs to be given this information in a form that is easy to understand. This knowledge can be considered when setting up the budget to synchronize or merge IT operations before the final price is negotiated between the parties. Getting the transitional budget for synchronizing or merging processes, functions and applications before the final price tag is determined will save a lot of time and grief thereafter. Without it and a realistic plan, IT staff members will be busy extinguishing fires, instead of pushing ahead to merge the operations according to plan.

Figure 3—Key Elements and Considerations to Be Investigated

1. Reviewing a profile of the information systems team, including background and qualifications
2. Developing a profile of hardware, operating and network systems, and application software and databases
3. Reviewing the operating system and software application licenses (servers, PCs and mobile devices)
4. Reviewing the information systems lease and maintenance contacts
5. Reviewing policies and procedures regarding system use
6. Assessing services and relationships with third-party service providers, such as outsourcers
7. Examining the information systems plan
8. Reviewing privacy and security policies and controls used for determining violations (e.g., by using the COSO checklist at *http://blog.cytrap.eu/?p=189*)
9. Examining security metrics and key performance indicators (KPIs) used for providing baseline indicators regarding such criteria as policy violations, data security breaches and legal compliance assessments[7]
10. Reviewing the effectiveness of the group's system of internal controls covering all material controls, including financial, operational and compliance controls, and risk management systems (including property rights, information assets and data)
11. Developing an integration plan for merging the two enterprises, including alternatives, timelines, needs and requirements (options must be costed out)

Note: In practice, the above considerations are most likely used as part of categories that will involve more considerations and questions. In fact, it is very likely that a due diligence questionnaire will be made up of about 100 questions.

Preparing for Due Diligence With Security Metrics

Security metrics can help identify impediments to a potential merger or industrial sale down the line due to differences in information systems, configurations and processes. Generally, information security and risk management require measurable security. Hence, during the due diligence process, the acquirer's IT security staff members are likely to ask for such data. MITRE[8] groups measurable security into the following main areas:

- Threat
- Vulnerability
- Configuration management
- Asset management

There are many metrics that can be used, but while some metrics are extremely popular with *Fortune* 500 companies,[9] their usefulness is not always obvious. For instance, an indicator that provides metrics regarding the percentage of machines infected by a computer virus tells little about the vulnerability of data stored on that PC's hard drive against various newly emerging malware threats. Accordingly, a KPI used by the firm may indicate that every 10th PC in the organization is infected by some type of malware (e.g., worm). However, end-user training may have resulted in a level of awareness that prevents employees from opening such file attachments, thus preventing these PCs from becoming a zombie of a botnet that sends out spam. Thus, the likelihood of such a threat becoming a critical security incident (e.g., several PCs being infected and becoming part of a botnet used for spamming) is not very likely. Having a regularly updated antivirus program running on the PCs and the firm's mail server will further reduce this risk. Hence, this type of KPI may be interesting to a techie, but it will reveal little, if anything, about the possible risk of a large botnet operating on the to-be-acquired firm's local area network.[10]

Security metrics must be strategic in focus, so the KPIs provide management with a realistic overview of the risk issues to be dealt with regarding a merger or an acquisition.

What about key risk indicators?

The objective of due diligence is straightforward and simple. The acquirer is interested in minimizing its exposure to the problems and pitfalls that can arise when making an acquisition. To be able to make an informed decision regarding an acquisition candidate and increase the chances of success, the board needs to be presented a set of key risk indicators (KRIs) pertaining to security issues.

KRIs are measures that indicate the level of and changes in an organization's risk profile. This is achieved by focusing on the root causes of potentially significant risk events and exposures. KRIs provide an early-warning system to management, underscoring the areas where predefined thresholds are being exceeded and, thus, highlighting potential danger spots. The use of KRIs is one of the recommendations for sound operational risk management and, thus, is an essential component of Basel II-related efforts. In many cases, a group of KRIs provides the best management information for a meaningful assessment.

What set of KRIs the due diligence team wants to calculate and present to the people making the final decision about the acquisition is open to question. But, usually, it begins based on an extensive checklist that was used addressing legal compliance, best practice and policy issues, and if controls were implemented and remedial action was taken to achieve satisfactory performance levels.[11] Thereafter, key risks regarding IT security and postmerger activities must be identified, including the risk owners (who is responsible for the risk and will lead changes and improvements during the postmerger phase?). The causes of these risks and, most important, the risk indicators must be identified.[12]

How can the organization build a strategic set of KRIs and KPIs to help improve operations and prepare the firm for due diligence?

While technical people tend to focus on impact management, it is often narrowed down to critical incidents. Here, KPIs focusing on such issues can provide important information to system staff members and engineers, such as the type of information collected with these two questions:

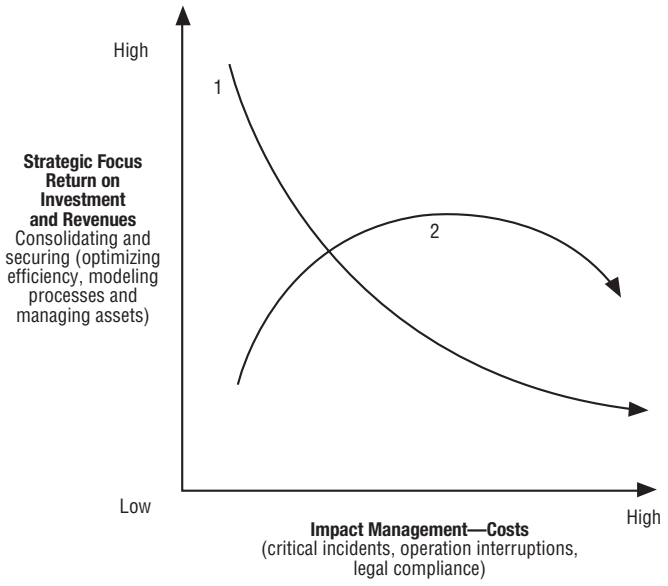
- What is the percentage of workstations (including notebooks) with automatic protection in accordance with policy?
- What is the percentage of software changes that were reviewed for security impacts in advance of installation?[13]

KRIs differs from KPIs in that the latter are meant as a measure of how well something is being done, while the former is an indicator of the possibility of future adverse impact.

As **figure 4** illustrates, however, managers are primarily concerned about what the risk might be that such a critical incident will occur, how it might affect daily operations at the plant, and legal compliance issues.[14] Accordingly, violations of privacy policy are critical if one can show how this might relate to data security breach laws and possible liability issues.[15]

Figure 4 indicates that privacy issues (see the X-axis—critical incidents) and violations may have an effect on the effective consolidation and realigning of business processes in the new enterprise (i.e., after the merger).[16] The link to these strategic issues must be shown. Accordingly, while answers to the two questions listed previously might be interesting to some people, they are of little significance in merger negotiations. Naturally, KPIs that neither address nor relate to operational issues and possible interruptions in business processes will not make it easy to get decision makers' attention. If KPIs do relate to strategic and critical operational issues and concerns, however, the communication of such information will be of great interest to management and the board of directors. Accordingly, using as a basis or starting point something that management understands very well will, naturally, support one's efforts in getting one's point across. Equally important, receiving the resources outlined in a premerger budget for postmerger activities needed for smoothing the integration process will be more likely if management understands why this is critical and what the consequences could be if it is not addressed. An example is taking the COSO checklist for internal controls[17] as the basis for developing six critical KPIs regarding information security and privacy protection. Using security metrics and relating these measures to COBIT will make it easier to put them within a larger framework of auditing.[18]

Figure 4—Preparing IT Security and Compliance



In **figure 4**, the key issue is to find the low-hanging fruit that can be eliminated relatively easily, without too great of a cost. It is obvious that curve 1 will get the greatest attention by the board, while curve 2 might not, unless one can provide clear-cut examples (e.g., the cost of notifying subjects about a data security breach is high from an administrative perspective as well as a bad publicity point of view).

Conclusion

Information security and risk management issues are becoming increasingly important in the due diligence process.

In today's global and continually changing economy, most mergers and acquisitions involve companies engaged in international trade. In addition, enterprises typically adhere to certain regulatory requirements, such as those that compel them to ensure that their service provider meets stringent controls in handling corporate data. Due diligence from the enterprise may require its service provider to produce an independent audit report to ensure that such controls are in place.

As with other areas of due diligence review, compliance reviews regarding best practices, information assets, risk management and information security help in protecting the buyer from unknown compliance issues, which may have the potential of escalating out of control if discovered at a later date.[19] Postclosing discovery of an information asset or risk management compliance issue may not only cause significant financial loss, but also result in stressful customer, affiliate and government relations. Companies should include an information asset and risk management due diligence compliance review module as part of the overall due diligence proceedings of a merger or acquisition of a company.

To prepare for due diligence, it is necessary to streamline control and audit work. Moreover, focusing on those strategic matters regarding risks and IT security during due diligence will certainly get the greatest attention. As a result, the

necessary decisions can be made to streamline postmerger or takeover adjustments.

A well-executed due diligence process regarding IT security shows that the firm uses a method and tools that are considered to be effective and in line with best practice. Concerning the general legal notion of due diligence, the firm can also reduce the risk for being held responsible for deleterious consequences, as having not exercised due diligence down the line—a further headache that is not needed since it detracts from what is really important: quickly creating the synergies that were the reason for merging the organizations in the first place.

Reference

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *www.coso.org*

IT Governance Institute, *Control Objectives for Information and related Technology* (COBIT), USA, 1998-2007

Wegner, D.M.; R.ö Wenzlaff; R.M. Kerker; A.E. Beattie; "Incrimination Through Innuendo: Can Media Questions Become Public Answers?," *Journal of Personality and Social Psychology*, vol. 140, 1981, p. 769-777

Endnotes

[1] Bhatia, M.; "IT Merger Due Diligence: A Blueprint," *Information Systems Control Journal*, vol. 1, 2007, p. 46-49

[2] For example, if a user tries to decide about backing up the computer's hard drive or encrypting data stored on the drive in case the laptop is stolen, the user has neither the knowledge about the complete range of the possible outcomes (e.g., compliance and liability issues) nor their probabilities.

[3] Hertwig, R.; G. Barron; E.U. Weber; I. Erev; "Decisions From Experience and the Effect of Rare Events in Risky Choice," *Psychological Science*, vol. 15, no. 8, 2004, p. 534-539

[4] See *http://blog.cytrap.eu/?p=188*.

[5] *Op. cit.*, Hertwig, *et al*. Koehler, J. J.; L. Macchi; "Thinking About Low-probability Events: An Exemplar-cuing Theory," *Psychological Science*, vol. 15, no. 8, 2004, p. 540-546

[6] See *http://blog.cytrap.eu/?p=186*.

[7] See *http://blog.cytrap.eu/?p=74*.

[8] MITRE, Making Security Measurable: A Collection of Information Security Community Standardization Activities and Initiatives, January 2007, *http://makingsecuritymeasurable.mitre.org*

[9] Pironti, J.P.; "Key Elements of a Threat and Vulnerability Management Program," *Information Systems Control Journal*, vol. 3, 2006, p. 52-56

[10] See *http://blog.cytrap.eu/?p=61*.

[11] For more information, including a start rating of these issues, see Urs and Nahum's security checklist at *http://regustand.cytrap.eu/?p=1*.

[12] See the flowchart at *http://blog.cytrap.eu/?p=236*.

[13] Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census-Government Reform Committee, US House of Representatives Corporate Information Security Working Group, *Report of the Best Practices and Metrics Teams*, 10 January 2005, *http://makingsecuritymeasurable.mitre.org*

[14] Drake, A.; J. Jeschke; "Security and Regulatory Compliance—A Quantitative Risk Management Approach," *Information Systems Control Journal*, vol. 4, 2004, p. 19-22

[15] See the infosec checklist at *http://blog.cytrap.eu/?p=190*.

[16] Cilli, C.; "Privacy: An Opportunity for IS Auditors," *Information Systems Control Journal*, vol. 4, 2005, p. 48-51

[17] See *http://blog.cytrap.eu/?p=189*.

[18] See *http://blog.cytrap.eu/?p=188*.

[19] Gattiker, U.E.; "The Changing Role of the IT Auditor: A European Perspective," *Information Systems Control Journal*, vol. 3, 2005, p. 22-23

Urs E. Gattiker, Ph.D.
has worked both as a professor and in the trenches dealing with IT control issues. He serves on various committees including, but not limited to, the Expert Advisory Group of the European Union's European Network and Information Security Agency (ENISA), and was vice chair of the Advisory Board of the EU Security and Dependability Task Force. He is director of CASEScontact.org, an early warning system. Together with colleagues, he develops and applies risk and compliance assessment tools helping clients achieve greater value creation (see also *http://blog.CyTRAP.eu*). Since 2005, Gattiker has been a member of ISACA's *Journal* Editorial Committee.

Information Systems Control Journal is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *Information Systems Control Journal*.