

Insights on IT risk
February 2010



Top privacy issues for 2010





Information serves as an integral part of most business processes. Organizations cannot survive without information and the supporting systems, third parties and manual activities that collect, derive, process, store and make available the information. Organizations rely on information and, therefore, are at risk when the information is degraded. In addition, information often imposes obligations to the organization, whether because a law or regulation requires it, or fiduciary duty demands it.

Enterprise governance, risk and compliance (GRC) represents the actions that an organization takes to achieve its performance objectives and manage risk. This includes information risk and the organization's obligations over the information it owns, produces, uses and makes available to others. Organizations use different kinds of information – financial, business, intellectual property, etc. – each with its own unique governance, risk and compliance considerations. Personal information is one such information category, and in this publication we take a closer look at the specifics of personal information and privacy risk.



Introduction to privacy risk management and compliance

This document introduces the related topics of privacy risk management and compliance, describes how they must be addressed integrally to be effectively managed, discusses how effective management can lead an organization to increased value and presents a framework for managing privacy risk and compliance holistically. This document also introduces the top privacy issues for 2010 in the context of the privacy framework. The privacy framework allows for the management of risk, maintenance of compliance and support to business initiatives that involve personal information. Presenting the top issues in the context of the privacy framework, therefore, provides a window to the direction and approach organizations should take to address these issues.

Top privacy issues for 2010

Every organization that handles personal information – whether for consumers, customers, employees or business partners – faces a number of obligations related to privacy and the protection of that information.

Since 2001, when Ernst & Young published our first annual update on privacy concerns and the top issues that organizations would face in the year ahead, one thing became clear – many issues are persistent and don't neatly expire at the end of a year. That being said, these issues do evolve and manifest themselves differently to fit the current state of events. This document details those developments in light of the ongoing changes in the privacy and data protection landscape.

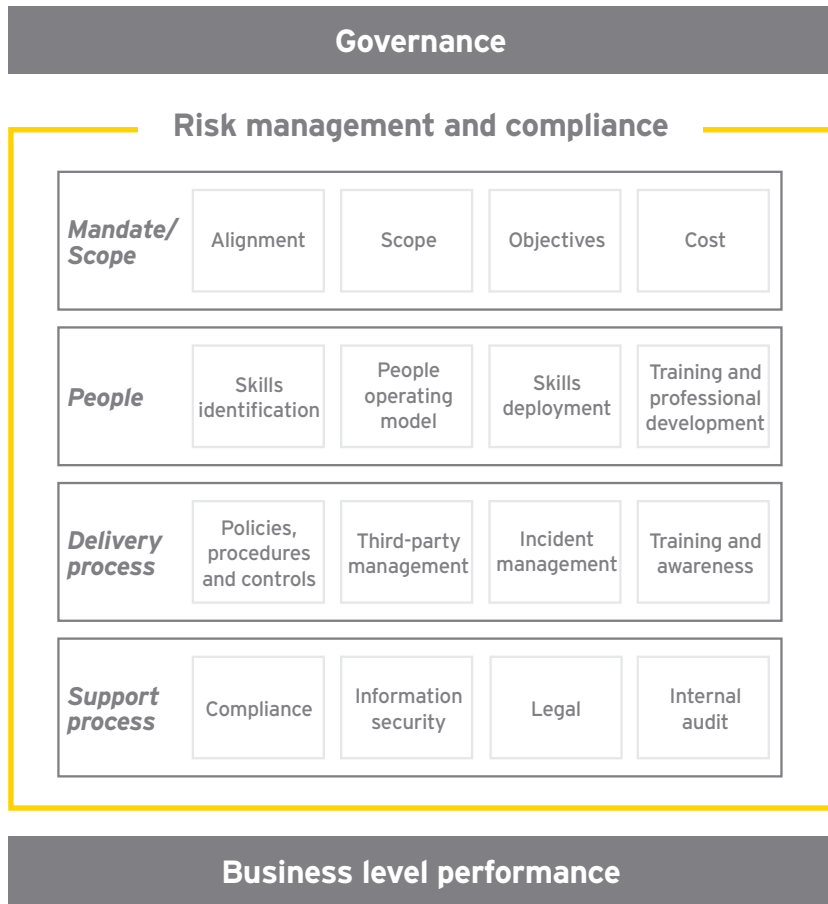
While privacy in earlier years may have been considered more of a marketing hook, focused on customer preferences, privacy in recent years is associated with the potential for abuse – inappropriate access to or exposure of information resulting in identity theft and fraud. This year we add to these alarming concerns the regulatory changes across the globe, as well as the lingering effect of the economic crisis.

The key challenge in managing risk and compliance with regard to personal information in such an environment is governing the use and protection of that information completely and consistently across increasingly complex and distributed enterprises. This is where the privacy framework takes on a level of higher importance. We focus on what the organization needs to do – and in fact needs to do well – at the corporate, business unit and affiliate levels to effectively manage and govern privacy risk and compliance across the enterprise.



The privacy framework

The privacy framework explains what an organization needs to do well to be able to effectively manage privacy risk and compliance. The business level performance layer describes the organization's use of personal information throughout its business processes and considers the infrastructure of systems and third parties. The risk management and compliance layer defines the people, processes, and technology used to protect and govern the use of personal information throughout the organization. Atop them both, the governance layer defines how all that is managed.



Governance

The governance layer defines the roles and responsibilities necessary for managing the use and protection of personal information at the corporate and business unit levels. Governance can often be considered the formal and informal allocation of responsibilities, accountabilities and ancillary duties and obligations of the various parties within the organization and among the third parties involved in processing the information. It may involve formal corporate governance regimes and also informal processes deep within a specific business unit.

Business level performance

The business level performance layer describes the organization's understanding or determination of where and how it processes personal information, including its accounting of the processes, systems, databases and third parties involved with processing personal information. This layer is composed of the infrastructure serving the personal information to business processes. This may be accounted for in listings, databases or other information at the corporate level (e.g., an information technology application listing, the procurement department's vendor information) and at the business unit level (e.g., a business unit's process documentation).



Risk management and compliance

Risk management

Risk management includes the approach used for managing privacy risk across the organization. Risk management may be formal or informal, discrete or integrated with other business risk areas (e.g., through an enterprise risk management program), at a corporate level, through an IT risk management program or at a business unit level.

Compliance

Compliance is defined by the organization's programs, tools and other enablers to manage adherence with policies, regulation and other obligations around the use and protection of personal information. This aspect of the framework often includes the roles of internal audit, the compliance office, the legal department, the IT security department, the audit committee and other parties within the organization involved with oversight. Some compliance and monitoring may be performed at the corporate level, but this aspect also addresses the specific compliance and monitoring processes established within the business processes of the organization.

Policies, procedures and controls

This component of the framework includes the enterprise and business unit policies, procedures and controls concerning the use and protection of personal information. These may include corporate and business unit policies, procedures and standards related to privacy, information security, records management, acceptable use of technology, human resources management, customer service and other functions that process personal information. These may also include the processes and controls used to enforce policy and other compliance obligations, and monitoring of those processes and controls to ensure they remain intact and effective. They may be from administrative, technical, physical, contractual, regulatory or other measures. They may be established at the corporate level (e.g., a common authorization process, a product development process, a system development lifecycle) or specific to a business unit function (e.g., work steps in a customer marketing process, technical controls over the transfer of information, physical protection of a specific facility). Quite often this represents the corporate or business unit information security program and the specific IT security controls established over the processing of information (e.g., at the network, operating system, middleware, database and application levels). It would also address security controls in end-user computing technology and devices such as in personal data assistants (PDA), other portable computing devices, and portable media.

Third-party management

Third-party management includes the processes that account for the protection of information, including performing due diligence during the selection process, putting controls in place – both contractually and for the secure transfer of the information – and building a solid basis of comfort that the third parties using the personal information are able to protect it and govern its use. This aspect of the privacy framework may entail processes within corporate or business unit procurement departments, legal departments and other supporting groups, along with the specific operational processes of the business unit supported by the third party. We use the term third party more broadly than just the term vendor or service provider. Third parties are any other entity that processes personal information on behalf of or in conjunction with the organization, or with whom the organization exchanges personal information.

Incident management

Incident management involves the process, documented in a comprehensive plan, which provides an effective and orderly response to events and potential events involving personal information, including related regulatory requirements such as breach notification. Much broader than just information security response programs or just breach notification steps that may be needed in some cases, an effective incident management program spans discovery, analysis, response, escalation, reporting, and remediation phases of an incident.

For each of these components, the organization must determine not only what to do, but the extent to which the component is addressed, such as the following:

- ▶ Informally or formally?
- ▶ Integrated with other risk and compliance efforts, or separately?
- ▶ At the corporate level, within the business units or at affiliates?

This allows the organization to manage privacy at a level reasonable to the risks and that meets the more specific compliance obligations and processes set forth by regulations and contracts.

Top privacy issues for 2010

Regulatory landscape



The top privacy issues for 2010 cover a wide range of topics. They are each addressed by several different elements of the privacy framework, as indicated.

In the United States, although there is no overarching privacy law, a complex arrangement of federal laws and even more complex state laws govern the use of personal information in different industries and contexts.

The changes brought about by the HITECH Act¹ (part of the ARRA² that was signed into law in February 2009) are still keeping many companies busy in 2010. This law amended HIPAA³ and has established requirements that reach far beyond the healthcare industry by stating the data protection responsibilities of business partners and vendors that handle protected health information (PHI) on behalf of healthcare organizations. Other provisions in the HITECH Act underscore existing HIPAA requirements and specify enhancements related to their implementation. The HITECH Act also adds requirements around breach notification for protected

health information, which is a new consideration and goes further than most of the existing breach notification rules that had focused on financial information and identity theft. The implementation process that organizations will go through to address these new requirements will continue beyond 2010 as the U.S. Department of Health and Human Services (HHS) and the Federal Trade Commission continue to provide guidance and final requirements for the different provisions.

Outside the US, national data protection laws are well established in Europe, Canada and some Pacific Rim countries. Whereas data protection authorities have identified the need to develop consistent privacy standards (such as in the recent Madrid resolution⁴), the laws vary greatly on many issues. Privacy regulations in different countries continue to evolve. Breach notification requirements are at different stages of consideration and development across the globe. In addition, other regulators (other than privacy commissioners, such as financial industry regulators) are increasingly involved in enforcing the rules over handling personal information. This means that the security and protection of personal information is generally a requirement, no matter where it is held and to whom it is transferred.

In keeping up with the changing regulatory landscape, have you:

- ▶ Recently reviewed the regulatory changes in jurisdictions in which you operate and have you assessed your compliance with them?
- ▶ Updated your policies to reflect the changes in the regulations that affect your organization?

1. Health Information Technology for Economic and Clinic Health (HITECH) Act
 2. American Recovery and Reinvestment Act (ARRA)
 3. Health Insurance Portability and Accountability Act (HIPAA)
 4. See <http://www.privacyconference2009.org/media/Publicaciones/index-iden-idweb.html>



Incident management



The need for effective and timely management of privacy events and incidents remains a critical issue for all organizations. Potential compromises occur frequently, even in the best-run organizations. In the US, the need for effective incident management is made increasingly important by breach notification requirements that apply more broadly. It used to be that an incident resulted in notification if sensitive identifiers such as Social Security numbers or bank account information were lost or stolen. With the HITECH Act, breach notification is triggered more readily, when protected health information, a far broader category of information, is potentially exposed.

In Europe, the regulatory changes will directly affect the telecommunications industry, but in France, for example, broader regulations affecting all industries are finding more solid ground and a regime of more general breach notification requirements are being put in place. Data protection authorities in general are arguing for voluntary notification in the absence of strict rules. Organizations should plan their approaches to incident management carefully, even when the rules in some jurisdictions have not been precisely stated.

Incident management processes now require a greater level of sophistication in organizations not only to assess what information was potentially exposed, but also, in the case of protected health information, to assess the likely impact on individuals. Therefore, formal, effective and repeatable processes to determine the nature of an event and the steps to take in response are essential. Training of staff is critical as well, so that they know what might constitute an "incident" or "event" that warrants the attention of management. In other cases, inappropriate reactions to events may open the organization up to more damage than is warranted by a situation. Deliberate processes managed by cognizant executives are a must.

In establishing your organization's incident preparedness, have you:

- ▶ Established a process to manage incidents and events involving personal information and to address applicable regulations?
- ▶ Addressed risks to information by implementing effective procedures and controls to prevent incidents from happening?



Cloud computing



The traditional roles of outsourcing and the extended enterprise are stretched by the increased popularity of cloud computing. Clouds and other utility computing, challenge our traditional approaches as the control and custody of personal information is further ceded. While organizations may have chosen in the past to avoid cloud technologies and the possible privacy and security challenges they bring about, in this economic climate, the cost reduction benefits that such solutions offer have brought many organizations to reassess whether these transformational technologies are right for them.

There are three common cloud service delivery models: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS). There are four common cloud service deployment and consumption modalities: private, public, managed and hybrid. It is the combination of the service delivery model with the service deployment model that sets the basic cloud computing risk profile.

Organizations must first address some key considerations before engaging with cloud providers. Cloud computing adds a new type of outsourcing arrangement for the organization that may not fit neatly with the current approach for procurement and vendor management. The ability to keep such arrangements within the current set of data protection expectations is key and should not be diminished. Making sure that the organization's key stakeholders are comfortable with the risk-benefit ratio (e.g., cost reduction through outsourcing staff, software and storage of information) is critical for the effective long-term adoption of such approach as well. Of course, not all processes and information should be ushered to the new frontier of technology, and making the decision on what and when to convert to new solutions is a step organizations must carefully contemplate, especially where limitations exist over the supervision and assurances provided by the service provider.

As you move your information to the clouds, have you:

- ▶ Inventoried your processes and systems and assessed which may be better candidates to be moved to the cloud based on their privacy risk exposure?
- ▶ Considered the implications of the trans-border transfers of your information in the cloud?
- ▶ Identified what privacy and security considerations your organization will be comfortable with before moving personal information to the cloud?

Service provider audits



2010 marks an important change in the way service providers will be able to provide assurances over their processes and control environments to their customers and business partners. The now ubiquitous SAS 70 report is changing. The SAS 70 report is an assurance tool that auditors use to address business processes that have an impact on the financial statements of those relying on them. However, the SAS 70 has become in the past years, inappropriately so, the assurance tool many companies put their trust in as it relates to how their service providers protect personal information.

But change is coming. In 2010, expect the American Institute of Certified Public Accountants (AICPA) to launch the overhaul of service organization reporting. The new assurance tool, which will be under a different title, will allow the inclusion of controls that are beyond those of the integrity of financial information, thereby allowing the report to address privacy and data protection controls, among other controls.

The prevalence of SAS 70 and the existing reliance on this report for general vendor management considerations suggests that the new reporting standard will have a significant impact for many organizations. Organizations will reassess the type of audits they undergo and the type of control frameworks they expect their vendors to adopt. The AICPA has previously developed privacy criteria titled Generally Acceptable Privacy Principles (GAPP). Many organizations have used the GAPP in developing their privacy programs and some have already audited their programs based on these criteria. It is the GAPP that is most likely to be used as the criteria for privacy and data protection in the new service organization reporting standards.

In serving your business partners, have you:

- ▶ Assessed your current reliance on SAS 70 reports in your vendor management process for broader data protection purposes?
- ▶ Have you identified the extent of privacy and security controls you would like to have assessed as part of the audits they undergo?



Encryption



Personal information protection has to cover information wherever it is and wherever it is going. The practice of encrypting portable devices, portable media and electronic communications (including email messages and their attachments) is commonplace. While this may have been a cutting-edge idea or a leading practice just a year or two ago, in 2010, the encryption of personal information at rest and in transit should be standard operating procedure.

In some of the emerging regulations, such as those from Massachusetts and Nevada in the US, certain categories of personal information must be encrypted in specific circumstances, such as their transfer using email over the internet. Where not a direct requirement, according to most breach notification laws, encrypted information that is lost does not commonly require notification. In 2010, this exclusion applies also to the HITECH Act notification requirements over protected health information. This is another reason for many organizations – including those that do not neatly fall within the health care industry, but handle information for its members – to apply encryption where it is warranted.

For many organizations, the use of encryption is not new. In fact, it has been part of the protection of specific systems and processes that have given rise to a wide patchwork of encryption tools, technologies and solutions. Eclectic as they are, each adds to the increasing challenge of encryption key management and brings technical limitations in applying them across different systems and operations. For many such organizations, it is no longer the mere addition of encryption – the benefit of enhanced protection over personal information – that is the goal, it is the effective use of encryption technology.

For many organizations, encryption will come to mean maturing and streamlining the use of existing procedures and solutions. It will also mean identifying specific tools and applying them consistently; upgrading from folder-based to full-drive encryption of portable media for better coverage; and using encryption technology less reactively, on an issue-by-issue basis, but rather more holistically with an eye on the organization's broader compliance and risk management needs.

With an eye on encryption, have you:

- ▶ Identified encryption solutions for the security of portable media and communications containing personal information?
- ▶ Identified opportunities to manage those solutions more effectively so encryption can be more commonly available and cost effective?
- ▶ Inventoried your systems and information to identify where encryption solutions will be most relevant for compliance and risk management?



The cost of compliance failures



Crime and fraud related to personal information are on the rise. In light of the identity theft, financial fraud and even medical identity theft scenarios being perpetrated, regulators are seeking and often receiving greater enforcement powers. In the US, the HITECH Act has drastically changed the cost of compliance failures related to protected health information. The HHS has shown a clear course for conducting more audits of companies after it was criticized in an inspector general report for not doing enough. The HITECH Act also brought business associates under the HHS enforcement umbrella – a significant number of organizations, many of which were previously far from the HHS reach. Furthermore, the HITECH Act calls for the FTC and state attorneys general to take an active role in enforcing health information privacy and security.

In other countries, regulators such as national data protection authorities and financial and telecommunications regulators have become more active with inquiries, audits and enforcement activities – sometimes in response to employee and customer complaints, other times as part of proactive initiatives. Many have been seeking stronger enforcement powers and sanctions. For example, in the United Kingdom, the Information Commissioner has increased the level of vigilance for pursuing cases and has been granted authority to impose fines of up to US\$800,000 for serious privacy breaches.

2010 will bring about an increased number of regulatory audits and fines paid by organizations that do not implement privacy controls effectively. The increased number of industries and jurisdictions that are subjected to breach notification requirements is likely to drive much of that activity. Note that the HITECH Act requires organizations to report incidents directly to the HHS or the FTC, and some of the breach notification laws models also put notification to the regulator as a key requirement.

With the expectation of more vigilant enforcement and higher fines for noncompliance, have you:

- ▶ Reviewed your compliance with the regulations affecting your operations across different jurisdictions?
- ▶ Updated your processes and controls to adequately meet your compliance requirements?



Governance



Many organizations have established privacy offices to manage their risk and compliance obligations over personal information. These offices have grown in some cases to include several privacy professionals. Because privacy management depends on many professionals across the organization, the network of those involved in protecting personal information has likely grown and formalized over time as well.

The changes in the economy and the landscape of privacy management affect the governance considerations in many organizations, in some cases in contradictory directions. While the risk to personal information only increases as fraud based on such information grows, some organizations are going through restructurings and reductions of their workforces that affect privacy. These organizational changes may range from modifying the make up of the privacy office or, less directly, when positions across the organizations that have some part in the management of privacy (e.g., in IT, legal, procurement) are changed or eliminated. As organizations acquire others, the challenge of privacy management further increases as the combined organization is dealing with broader scope of responsibility over personal information and streamlining the use of information that may have different commitments associated with it. Merged organizations pose an even larger challenge, when dissimilar policies and procedures must be harmonized.

As your organization has adapted to the challenging financial times, have you:

- ▶ Assessed the impact of changed and eliminated positions across your organization on privacy governance?
- ▶ Considered whether your privacy office is still adequately equipped to deal with the organization's key risks and compliance obligations?



GRC technology enablement



The increasing complexity of GRC frameworks, including those for privacy, has driven the need to automate common GRC activities, including management, measurement and reporting. Normally through software tools, organizations can align their specific risks; legal and regulatory requirements; compliance objectives; and business strategies to their own business processes and controls so that risk management and compliance activities are structured, comprehensive and not left to chance. Out-of-the-box GRC software can get an organization only so far; it is the customization and configuration of these tools that allow a specific organization to manage its specific requirements and its specific activities.

Common GRC activities suitable for technology enablement include risk identification and management; compliance requirement organization; mapping of controls and compliance requirements to specific business processes; incident management; and dashboarding and reporting. Use of GRC tools can result in stronger GRC activities, reduced costs, more accurate reporting and a stronger regulatory compliance posture.

In 2010, more privacy offices will be using GRC tools to monitor controls and survey their organizations on specific areas of risk and compliance. As the use of GRC tools matures within the organization, more areas of privacy management will be monitored and consequently better reporting on progress and gaps will be generated. As other groups within the organization that are tasked with elements of privacy management incorporate GRC to their operations, the privacy office visibility further increases and the ability to react to specific challenges improves.

As you consider integrating GRC tools to your privacy management efforts, have you:

- ▶ Identified areas for improving compliance and risk monitoring across critical operational areas?
- ▶ Considered how to harmonize GRC reporting and record keeping across operations and processes?



Transformational technology



Technology continues to transform business. That's not new. However, getting a handle on the new technology that is transforming business is critical to transforming how organizations need to manage privacy.

Devices that can contain information are increasingly prevalent; they are used for both work and home purposes, blurring the lines between the two, and results in ceding of control over the devices and the information to employers, service providers and others. These devices are increasingly networked, resulting in the addressability of previously unconnected devices. More and more are becoming "smart" and interactive.

In addition to these devices, there is a proliferation of repositories for personal information on the web, and of new ways to provide interconnectivity and interaction. This means that there is more personal information in more places under the control of more entities.

New rules are expected related to specific techniques and technologies, such as with behavioral tracking and advertising on the internet, the use of radio frequency identification (RFID) applications and the implementation of the Smart Grid. These emerging technologies will bring specific regulatory and self-regulatory requirements to govern their implementation.

Finally, cloud and utility computing afford new economies and efficiencies to information processing, but it spreads the custody and control of personal information well beyond the organization's traditional boundaries. The result is that information about people is held in a variety of logical and physical objects, and controlled by a variety of entities. These technologies are not only changing business, they are changing who and what has custody and control over personal information. They are changing the way that organizations manage privacy.

As your organization expands its use of new technologies and architectures, have you:

- ▶ Determined how you will adapt your privacy risk management to address the risk related to the loss of direct control and custody over personal information?
- ▶ Actively begun to address the regulatory compliance, and control impacts over mobile devices and cloud computing?



Looking forward

These issues deserve more than a simple “check-the-box” exercise. Each one should be addressed as part of the comprehensive and deliberate management of privacy risk and compliance. Founded on business level performance and governance, an effective program relies on controls, monitoring, compliance activities and other assurances to help make sure an effective operation is in place.

Privacy has an impact on the business risks and compliance of every enterprise, and more so for global entities. Management and boards of directors should ensure that their organizations are adequately positioned to manage privacy across the enterprise. Ernst & Young will track these issues and will continue to work with its clients to develop recommendations for addressing the challenges.



About Ernst & Young

At Ernst & Young, our services focus on our individual clients' specific business needs and issues because we recognize that every need and issue is unique to that business.

Information technology is one of the key enablers for modern organizations to compete. It gives the opportunity to get closer, more focused and faster in responding to customers, and can redefine both the effectiveness and efficiency of operations. But as opportunity grows, so does risk. Effective information technology risk management helps you to improve the competitive advantage of your information technology operations, to make these operations more cost efficient and to manage down the risks related to running your systems. Our 6,000 information technology risk professionals draw on extensive personal experience to give you fresh perspectives and open, objective advice – wherever you are in the world. We work with you to develop an integrated, holistic approach to your information technology risk or to deal with a specific risk and information security issue. We understand that to achieve your potential you need a tailored service as much as consistent methodologies. We work to give you the benefit of our broad sector experience, our deep subject-matter knowledge and the latest insights from our work worldwide. It's how Ernst & Young makes a difference.

For more information on how we can make a difference in your organization, contact your local Ernst & Young professional or any of the people listed in the table below.

Contacts

Global		
Norman Lonergan (Advisory Services Leader, London)	+44 (0) 20 7980 0596	norman.lonergan@uk.ey.com
Paul van Kessel (IT Risk and Assurance Services Leader, Amsterdam)	+31 88 40 71271	paul.van.kessel@nl.ey.com
Advisory Services		
Robert Patton (Americas Leader, Atlanta)	+1 404 817 5579	robert.patton@ey.com
Norman Lonergan (Europe, Middle East, India and Africa Leader, London)	+44 (0) 20 7980 0596	norman.lonergan@uk.ey.com
Nigel Knight (Far East Leader, Shanghai)	+86 21 2228 8888	nigel.knight@cn.ey.com
Isao Onda (Japan Leader, Chiba-shi)	+81 4 3238 7011	onda-s@shinnihon.or.jp
Doug Simpson (Oceania Leader, Sydney)	+61 2 9248 4923	doug.simpson@au.ey.com
IT Risk and Assurance Services		
Bernie Wedge (Americas Leader, Atlanta)	+1 404 817 5120	bernard.wedge@ey.com
Paul van Kessel (Europe, Middle East, India and Africa Leader, Amsterdam)	+31 88 40 71271	paul.van.kessel@nl.ey.com
Troy Kelly (Far East Leader, Hong Kong)	+81 2 2629 3238	troy.kelly@hk.ey.com
Giovanni Stagno (Japan Leader, Chiyoda-ku)	+81 3 3503 1100	stagno-gvnn@shinnihon.or.jp
Iain Burnet (Oceania Leader, Perth)	+61 8 9429 2486	iain.burnet@au.ey.com





About Ernst & Young

Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 144,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

For more information, please visit www.ey.com.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients.

The Ernst & Young organization is divided into five geographic areas and firms may be members of the following entities: Ernst & Young Americas LLC, Ernst & Young EMEA Limited, Ernst & Young Far East Area Limited and Ernst & Young Oceania Limited. These entities do not provide services to clients.

About Ernst & Young's Advisory Services

The relationship between risk and performance improvement is an increasingly complex and central business challenge, with business performance directly connected to the recognition and effective management of risk. Whether your focus is on business transformation or sustaining achievement, having the right advisors on your side can make all the difference. Our 18,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and superior client experience. We use proven, integrated methodologies to help you achieve your strategic priorities and make improvements that are sustainable for the longer term. We understand that to achieve your potential as an organization, you require services that respond to your specific issues, so we bring our broad sector experience and deep subject-matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where the strategy is delivering the value your business needs. It's how Ernst & Young makes a difference.

© 2010 EYGM Limited.
All Rights Reserved.

EYG no. AU0447



In line with Ernst & Young's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.