



 **ERNST & YOUNG**

Quality In Everything We Do

10th Annual Global Information Security Survey

Achieving a Balance of Risk and Performance

Contents



Foreword	1
Introduction: Achieving a Balance of Risk and Performance	2
Summary of Key Findings	3
Opportunities for Improvement	4
Aligning Information Security with the Business	5
Driving Information Security	10
Managing Information Security	14
Staffing Information Security	17
Benchmarking Information Security	20
2008 and Beyond	24
Survey Approach	27

Foreword



Paul van Kessel
Global Leader
Technology and
Security Risk Services
Ernst & Young

Ten years ago, we launched the first Ernst & Young Global Information Security Survey and have since seen the effort materialize into one of the longest-running annual surveys within the global information security arena.

Each year — and this year is no different — we see the business environment become more complex and the scope of information security expand. New technologies, global connectivity, and increased regulatory requirements continue to push information security to new levels.

We have come to realize that the focus and drivers for information security may change over the years, but the need to protect information assets remains vitally important to global business.

There is evidence that organizations are beginning to recognize that information security can deliver more than just protection for information. Significant performance improvements are being realized that impact the bottom line and elevate information security from a tactical solution to a strategic imperative.

The indications are encouraging that information security is gaining the attention it deserves, but our survey also reveals that many organizations are struggling to acquire the experienced resources needed to act on it.

My personal thanks to all of our survey participants for taking the time to share their views on information security. My colleagues and I hope you find this survey report useful. We welcome the opportunity to talk with you personally about your specific information security risks and opportunities for improvement.

Introduction: Achieving a Balance of Risk and Performance

A Look Back: In this report, we take the opportunity to look back over the results of our previous information security surveys to provide additional insights into how the challenges facing the information security function have evolved and how organizations have reacted to address their security needs.

Information security remains an important component of risk management. However, improving overall business performance is emerging as a critical objective.

In this 10th annual Ernst & Young Global Information Security Survey, we gauge the current state of information security and the major factors shaping its future.

Consistent with previous years, our 2007 survey results show that many companies are making progress in mitigating risks and improving their information security. Primarily driven by regulatory pressures, management's awareness of information security has also increased.

Along with these positive gains, increased expectations for improving performance and helping meet business objectives have emerged.

About the Report

In this report, we take a closer look at:

- how organizations are aligning information security with their business objectives
- what is driving the need for and improvements in information security
- how organizations are managing their information security function
- how organizations are staffing information security

In each section, we provide current survey results, together with comparisons with results from previous years to highlight any significant trends. We also identify and discuss potential opportunities for improvement from both risk mitigation and business performance perspectives.

This report is designed to help organizations to obtain a deeper understanding of current information security trends, as well as to focus their efforts on areas where we expect improvement may be most necessary.

Summary of Key Findings

Information Security is Improving

This year's Ernst & Young Global Information Security Survey shows that organizations continue to improve their information security, but remain challenged to find the right balance between risk mitigation efforts and performance based initiatives.

Aligning Information Security with the Business

- Meeting business objectives is a growing focus for information security.
- Information security is now more integrated into overall risk management.
- Information security remains isolated from executive management and the strategic decision making process.

Driving Information Security

- Improving IT and operational efficiency are emerging as important objectives.
- Compliance continues to be the primary driver of information security improvements.
- Privacy and data protection have become increasingly important drivers of information security.

Managing Information Security

- Organizations rely on audits and self-assessments to evaluate the effectiveness of their information security programs.
- Organizations are demanding more from vendors and business partners in managing third-party relationships.

Staffing Information Security

- The greatest challenge to delivering information security projects continues to be the availability of experienced IT and information security resources.

Opportunities for Improvement

Moving Toward a Balance of Risk and Performance

The 2007 Ernst & Young Global Information Security Survey shows that many organizations now view information security as more than just risk mitigation and look for real performance improvements from the implementation of security initiatives.

Aligning Information Security with the Business

- Leverage business relationships to better meet business objectives.
- Continue to improve alignment with overall risk management efforts.
- Involve information security in corporate strategic decision making processes.

Driving Information Security

- Approach information security from a business improvement perspective to better leverage investments.
- Consider using privacy and data protection as a competitive advantage in the market.
- Build upon compliance initiatives to establish a sustainable compliance program.

Managing Information Security

- Use a combination of self-assessment, internal audit, external audit, and benchmarking to effectively evaluate and monitor information security.
- Adopt more formal and consistent procedures for managing the risks in third-party relationships.

Staffing Information Security

- Investigate alternative staffing options to help address the growing challenge of the availability of experienced and trained information security resources.

Aligning Information Security with the Business

A Look Back: In 2003, less than 29% of our survey participants reviewed their information security policies and procedures for consistency and alignment with business objectives on an annual or more frequent basis.

Source: 2003 Ernst & Young Global Information Security Survey

During the first ten years of the Global Information Security Survey, there has been a positive evolution in the role of information security. Once considered by management as “a cost of doing business,” much like an insurance policy, information security today is considered as not only necessary, but critical to the business.

Information security can no longer focus solely on the operational aspects of security to protect corporate assets. In previous surveys, we found an increasing number of respondents saying information security should become more proactive and less reactive in its approach. Our 2007 survey shows that information security practitioners are doing a better job of aligning their initiatives with the strategic objectives of the organization and becoming proactive participants in their organizations’ overall risk management.

A key challenge for information security leaders will be their ability to balance tactical demands, react to changes, and sustain operational activities, while elevating the role of information security to form part of the strategic decision-making processes of both corporate and business unit leaders. It must cross the threshold of integration with enterprise risk management and compliance efforts and increase the capability and stature of the function beyond the act of asset protection.

Information security is increasingly earning a place at the table when important and highly visible initiatives are being planned.

Aligning Information Security with the Business

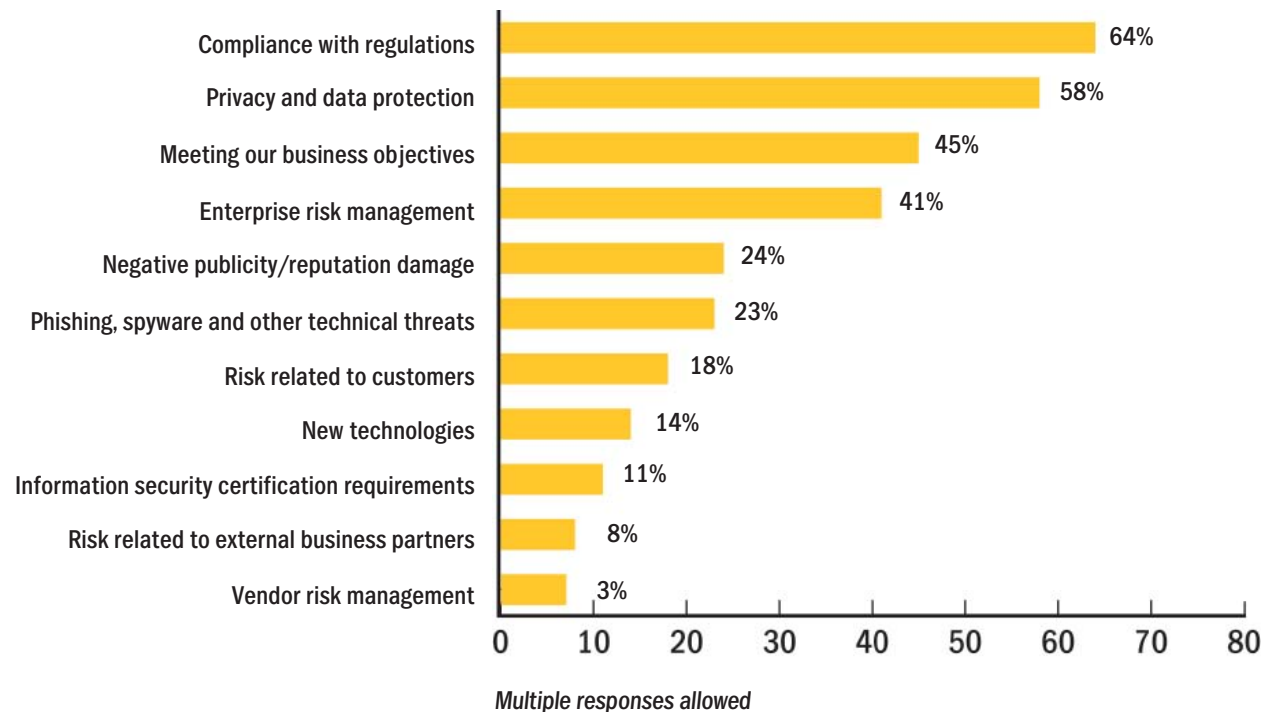
Key Findings

Meeting business objectives is a growing focus for information security.

In 2007, compliance remained the number one driver of information security. There is, however, a growing upward trend in the number of organizations where information security initiatives are driven by the need to meet business objectives. Nearly half of our respondents affirmed that meeting business objectives was an important driver, an increase over last year and representing a move to third greatest driver of information security initiatives.

This result supports the growing trend that information security is moving toward greater business objective alignment. As a result, traditional drivers like technology advances and technical vulnerabilities tend to be deferred or addressed as part of the organization's compliance efforts. This allows information security to focus more on business initiatives — a result supported by this year's survey — as fewer than 15% of respondents see technology as an important driver.

How organizations rank the top three drivers that most significantly impact information security practices in their organization



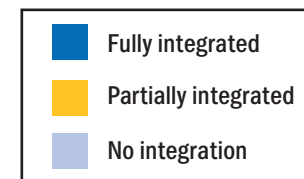
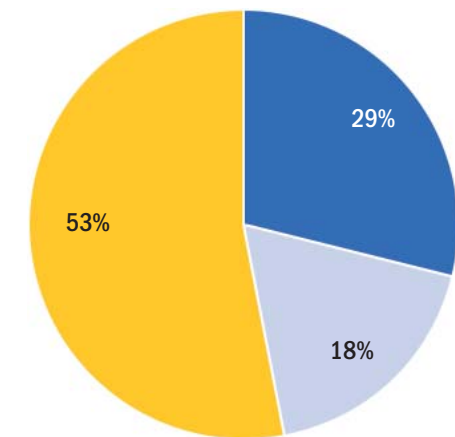


Information security is now more integrated into overall risk management.

A powerful message from this year's survey is the proportion of respondents who acknowledge they have partially or fully integrated their information security functions with risk management operations (82%), compared with 40% in 2005 and 43% in 2006. With regulatory compliance as a major integration stimulus, the proportion of organizations that have fully integrated both functions nearly doubled, from 15% in 2006 to 29% in 2007.

Is this an indicator that information security will no longer be a part of the IT function? We don't think so. Rather, this result substantiates the growing trend to integrate the information security function along strategic/governance lines for regulatory compliance and operational and architectural lines within the IT function. This is being driven not only from a regulatory perspective, but from the growing lines of security demarcation.

Degree of integration between IS function and overall risk management

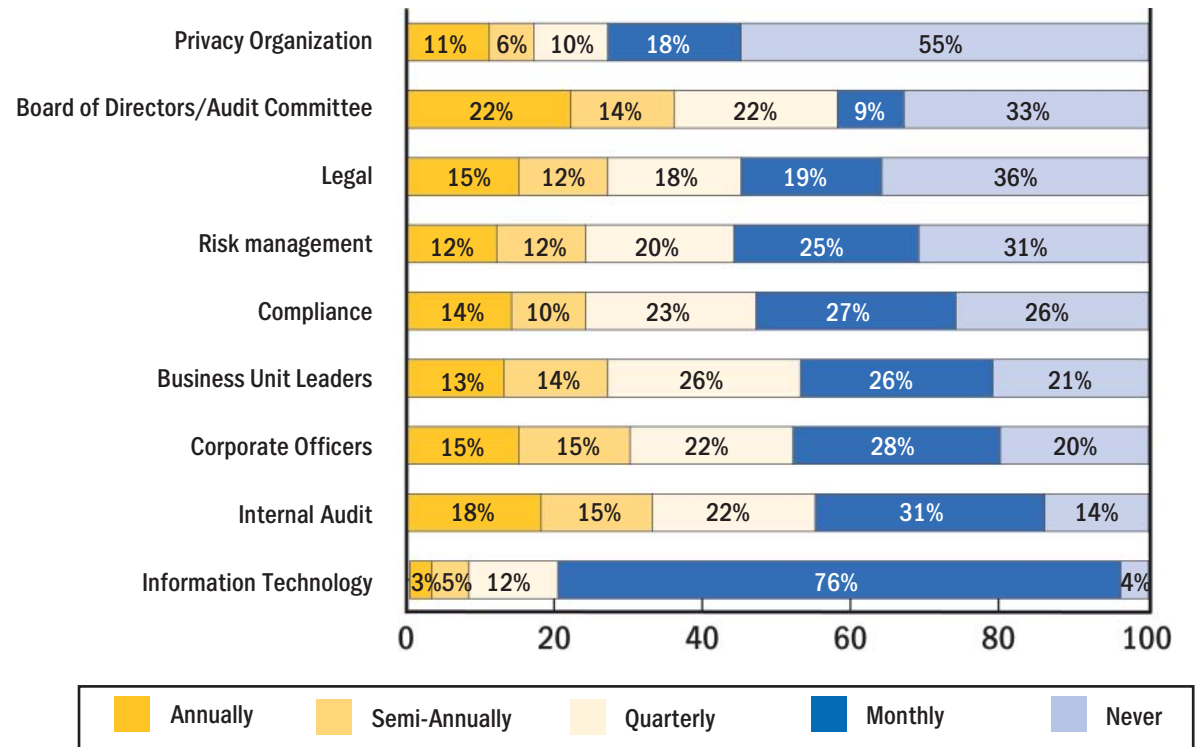


Aligning Information Security with the Business

Information security remains isolated from executive management and the strategic decision making process.

Although there is a recognizable integration of security within the overall risk management process, there are concerns that this is driven more by initiatives than strategic management direction. This year's survey suggests that monthly meetings are three times more likely to occur between the information security team and IT leaders than they are between information security and corporate officers and business unit leaders. The infrequency of meetings or other interactions between information security and senior executives provides an unfortunate indication that information security is still not as closely connected with executive leadership as it should be. The majority of information security functions meet less than once a quarter with leadership and 20% of respondents said their information security groups do not meet with corporate officers or business unit leaders.

How often the individuals responsible for delivering information security services meet with the following internal groups or individuals to discuss or understand their business objectives and information security needs





The Opportunities

Leverage business relationships to better meet business objectives.

Making information security considerations an integral part of an organization's strategic planning activities has numerous benefits. The process begins when the information security function capitalizes on the business-level relationships it develops with key executives — even though those relationships may transcend traditional, prescribed reporting lines. Information security must evolve from being a reactive and risk-driven entity that simply protects physical and intellectual property, into an agent of positive change within the organization by proactive involvement in strategically important activities.

Early participation allows an information security function to help the business identify and resolve — or at least be made aware of — issues that impact the achievement of strategic business objectives. This is a role we expect to strengthen as organizations continue to grow their compliance and risk management capabilities.

Continue to improve alignment with overall risk management.

We expect compliance efforts to continue to support integration of security and risk management and assume more of an independent governance role to help manage and sustain compliance initiatives. The continued connection between these functions enhances the organization's ability to use information security more strategically in addressing compliance and business objectives. We expect this role to strengthen as organizations increase their compliance and risk management capabilities.

Involve information security in corporate strategic decision making processes.

Routine reporting and dialogue with executive leadership is an effective way to increase visibility and establish the strategic value of information security. This approach provides two distinct advantages: first, the proactive involvement of information security

fosters a proficient contributor role for it with executive leadership, helps to shape strategic business decisions, reduces the time to move from concept to delivery, and provides an advisory role on matters related to risk.

Second, frequent dialogue with executives creates a greater awareness of issues and challenges that face information security. As a result, executives are more likely to be aware and supportive of resource needs, whether they relate to budgets, technology, or personnel. Taking these steps should tremendously improve the awareness of information security and help elevate its perceived value beyond that of regulatory compliance.

Driving Information Security

A Look Back: In 1998, remote access was a primary driver for information security, with more than 80% of our survey participants providing some degree of remote access to their organization. Dial-up was the most common access technology at 69% and the Internet was at only 20%.

Source: 1998 Ernst & Young Global Information Security Survey

Not surprisingly, the issue of regulatory compliance continues to be the motivating factor driving information security in 2007. This has been the most pressing issue since 2005, when compliance overtook common worms and viruses as the top driver of information security. However, the compliance push has also raised management's awareness of information security, to the point where the information security function is now viewed as integral to business operations.

The need to detect and protect the organization from threats and viruses has become a principal driving force in managing risk and supporting business needs, for example, balancing data protection and collaboration. This is a positive indication that business awareness of the value of information security continues to increase and that leadership sees its performance-enhancing potential.

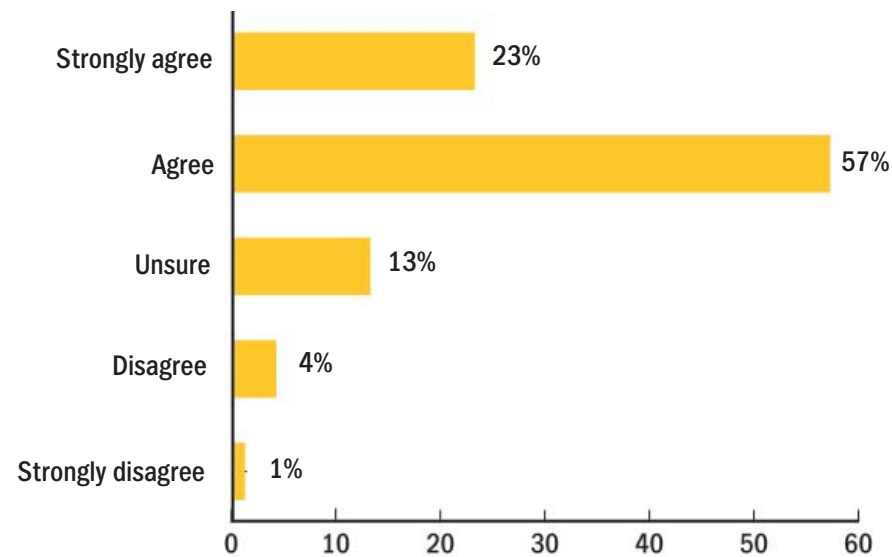
Key Findings

Improving IT and operational efficiency are emerging as important objectives.

For years, information security has been trying to establish a business identity that promotes and adds value to the organization rather than being viewed as an IT overhead and an obstacle to operational efficiency. Today, information security is viewed as a positive contributor whose capabilities and level of importance within the organization have increased due to its support of compliance efforts, a view shared by 82% of respondents in this year's survey. In addition, eight out of ten organizations believe that information security's contributions have resulted in improvements to overall information technology's operational efficiencies, and nearly six out of ten indicate information security has been instrumental in enabling strategic initiatives. Both findings point to the increasing importance and value being attached to the information security function.



Compliance with regulatory obligations in general has actually improved the organization's information security



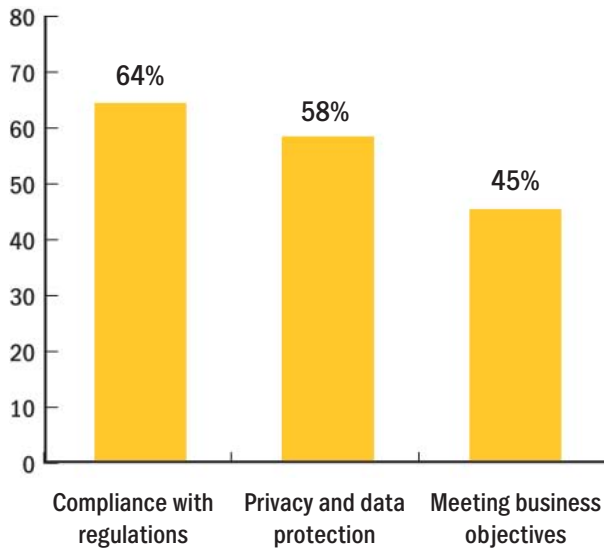
Compliance continues to be the primary driver of information security improvements.

For many years, common threats posed by worms and viruses were the key driver of information security, but that changed more than two years ago, when compliance became one of the top ten drivers of information security and in 2005 overtook worms and viruses as the leading driver. The shift resulted not only because compliance became an executive or board-level issue, but also because of the organization's growing proficiency over time in handling the more common threats.

Today, the trend of compliance-driven information security improvements continues, as 64% of respondents still rank compliance as the principal driver. However, we have seen a slight drop in the percentage from last year. Compliance was also the top-ranked influencer in integrating information security with the organization's overall risk management function.

Driving Information Security

Top three drivers that impact information security practices in the organization

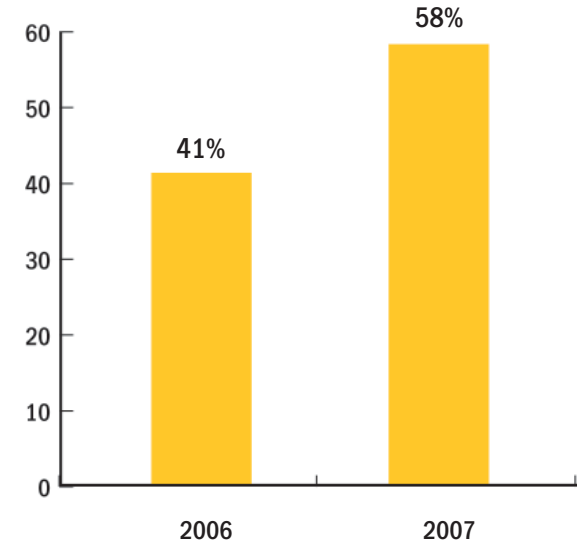


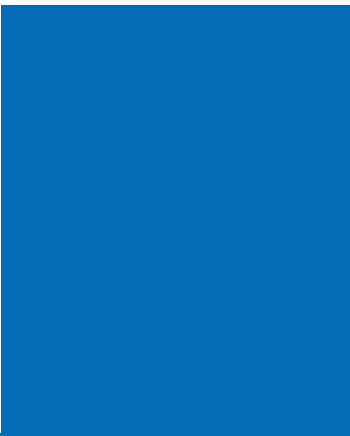
Multiple responses allowed

Privacy and data protection have become increasingly important drivers of information security.

It is clear that more organizations are paying attention to the implications of data loss or theft in the wake of well-publicized incidents and executive leadership is taking seriously its stake in ensuring that adequate controls and protection are in place. A significantly higher proportion of this year's survey respondents — 58% versus 41% in 2006 — ranked the protection of privacy and data as one of the top three business drivers, with 73% of CEOs and 64% of CIOs placing a high level of importance on protecting privacy and data assets.

Privacy and data protection as top driver for information security practices (2006 vs. 2007)





The Opportunities

Approach information security from a business improvement perspective to better leverage investments.

Information security must continue to demonstrate and increase its value to the business. Executive leadership has taken notice and information security functions should take every opportunity to build and maintain the growing relationship. The increased visibility is shifting the perspective that information security is predominantly “risk-focused” toward the notion that it supports the business — forming a balance between operational performance and risk management. This shift will enable more effective planning and allow information security and the business to act together to better mitigate risks and improve business performance.

Consider using privacy and data protection as a competitive advantage in the market.

Of the leading information security issues, privacy is a growing driver primarily because it is highly consumer-driven. Media stories about privacy breaches, identity thefts, and the loss of personally identifiable information have not only heightened consumer awareness, but have stimulated a sense of the leadership’s personal accountability and the absolute need to give priority to privacy and data protection. When information security is well executed, organizations have a prime opportunity to expand the controls developed during compliance efforts, and use the protection of privacy and data as a competitive advantage in the market.

Business entities that demonstrate leading practice in implementing strong privacy safeguards and enforcing information security controls can leverage these attributes of their business as competitive differentiators to increase market share, reputation, and profitability.

Build upon compliance initiatives to establish a sustainable compliance program.

We expect the regulatory and compliance environment to continue to influence the information security agenda. There is an opportunity for information security to strike a balance between compliance and the support of business objectives. Building a sustainable compliance program, information security can establish a position to respond to regulatory change while maintaining its business focus.

Regulatory compliance is a powerful catalyst for companies to invest in mitigating business risk through a sustainable compliance program. To assist in the development and maintainability of compliance programs, organizations should look to standards-based information security models defined by ISO 27002 and the Information Security Forum’s *The Standard of Good Practice for Information Security* as example resources for guidance.

Managing Information Security

A Look Back: In 2002, only 21% of our survey participants reported outsourcing any information security activities to a third party.

Source: 2002 Ernst & Young Global Information Security Survey

Information security has come full circle with security functions moving from a decentralized model in the early 1990's back to a centralized one. Today, 82% of our survey respondents say they have returned to a centrally structured function. The move back to a centralized structure is not surprising, given the extensive compliance pressures and the expanding risk management role of information security.

Organizations are looking at ways to assess and measure the effectiveness of their information security. This year's survey indicates that many organizations have looked to self-assessment, benchmarking, internal and external audit, and independent third-party assessments to evaluate their security program effectiveness.

As organizations look to outside parties for core business assistance, the ability to effectively measure information security effectiveness has run into additional challenges. When the responsibilities of an external party increase, the importance and impact that the third party can have on an organization is significant. This year's survey indicates respondents are expecting more from their external relationships, almost mandating that these suppliers adhere to the client's standards, policies, and procedures.

Key Findings

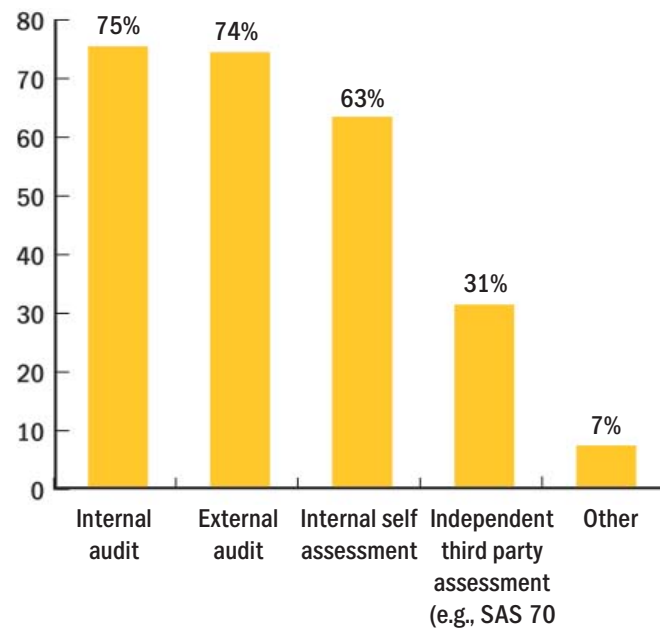
Organizations rely on audit and self-assessment to evaluate the effectiveness of their information security programs.

In order to effectively manage expanding boundaries of compliance and information security, organizations use a combination of approaches as mentioned earlier.

Sixty three percent of organizations assess their information security functions by self assessments. Of those, 91% are using corporate policies, procedures and internal standards as a basis. Nearly three quarters of respondents rely on formal internal and external audit results. Six out of ten evaluate their security management approach, implementation, and controls using industry-recognized information security standards like ISO 27001: 2005 and 27002:2005. Finally, nearly 40% of the respondents use independent assessment techniques such as SAS 70 or other third party assessments to evaluate their security programs.



How organizations are evaluating their information security posture

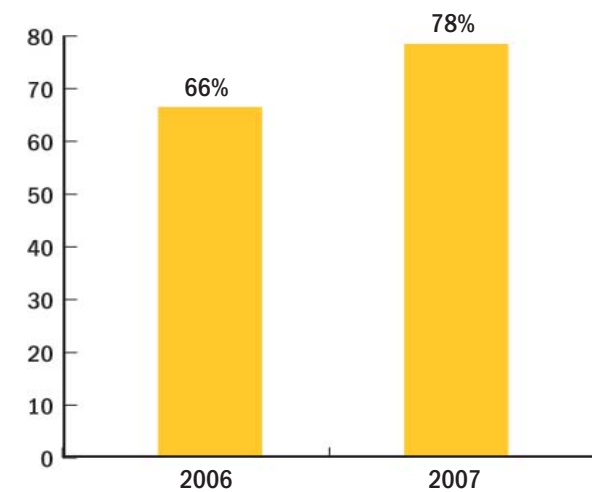


Organizations are demanding more from vendors and business partners in managing third-party relationships.

Both IT and information security are forming more relationships with third parties, whether in the form of strategic business relationships, outsourced operational capabilities, resource augmentation, or assistance with executing tactical initiatives. However, with these relationships come increased risks. The capabilities of information security and the required controls to protect the organization must not be diminished by the use of third parties or the services they provide. Our survey shows a substantial increase in the requirement of third parties, business partners, and vendors to abide by the policies, procedures, and standards of the client organization; an increase of 12 percentage points from 66% in 2006 to 78% in 2007.

In addition, almost half of the respondents also require the third-party organization to have its own information security and privacy policies and procedures in place — an increase of seven percentage points from last year — in order for it to do business with the client organization.

Organizations that require third parties to be able to support their policies, procedures and standards



Managing Information Security

The Opportunities

Use a combination of self-assessment, internal audit, external audit, and benchmarking to effectively evaluate and monitor information security.

Businesses continue to look for ways to improve: through new services, markets, technology advances, and relationships. Organizations need to continuously assess, improve, and monitor the capabilities of the information security function. The use of a range of effective tools for evaluating information security will enable them to do so. Self-assessment, in particular, is an efficient way for organizations to assess the function.

By involving IT as well as business entities in the process, compliance with organizational policies and regulations is improved. Self-assessment also provides a means for information security to identify risk and potential solutions that can be communicated as a business case for budget and resource requests.

In addition to self-assessment, organizations need to expand their use of standards-based evaluations. These standards provide consistent approaches and offer guidance to help organizations improve the maturity of their information security programs.

Adopt more formal and consistent procedures for managing the risks in third-party relationships.

With the use of third-party relationships, which we believe will continue to increase, there is a need for the third party to have access to the organization's business systems or information. With this increase, there is an inherent increase in risk. Organizations need to recognize and manage the increased risk by properly managing relationships and making sure the outside resource conforms to the organization's security objectives. Although a majority of companies have such procedures in place, more organizations should adopt formal arrangements to manage third-party relationships, including the use of independent audits to monitor compliance and increase the confidence level that third parties are taking the necessary steps to protect the organization's assets.

Staffing Information Security

A Look Back: In 1997, only 57% of our survey participants had dedicated information security personnel.

Source: 1997 Ernst & Young Global Information Security Survey

Successfully managing the human resource aspects of any business, especially the recruitment and retention of good talent, is crucial to any organization's success. This is even more vital for information security and an issue that we can trace as far back as 1997.

The 2007 participants ranked human resource constraints, both from IT and information security perspectives, as the most significant challenge that organizations face in delivering information security projects.

What has changed is the greater importance respondents attached to having the right information security talent as part of the organization. The lack of skilled resources ranks even higher than financial and technological limitations, which have traditionally been major barriers.

Key Findings

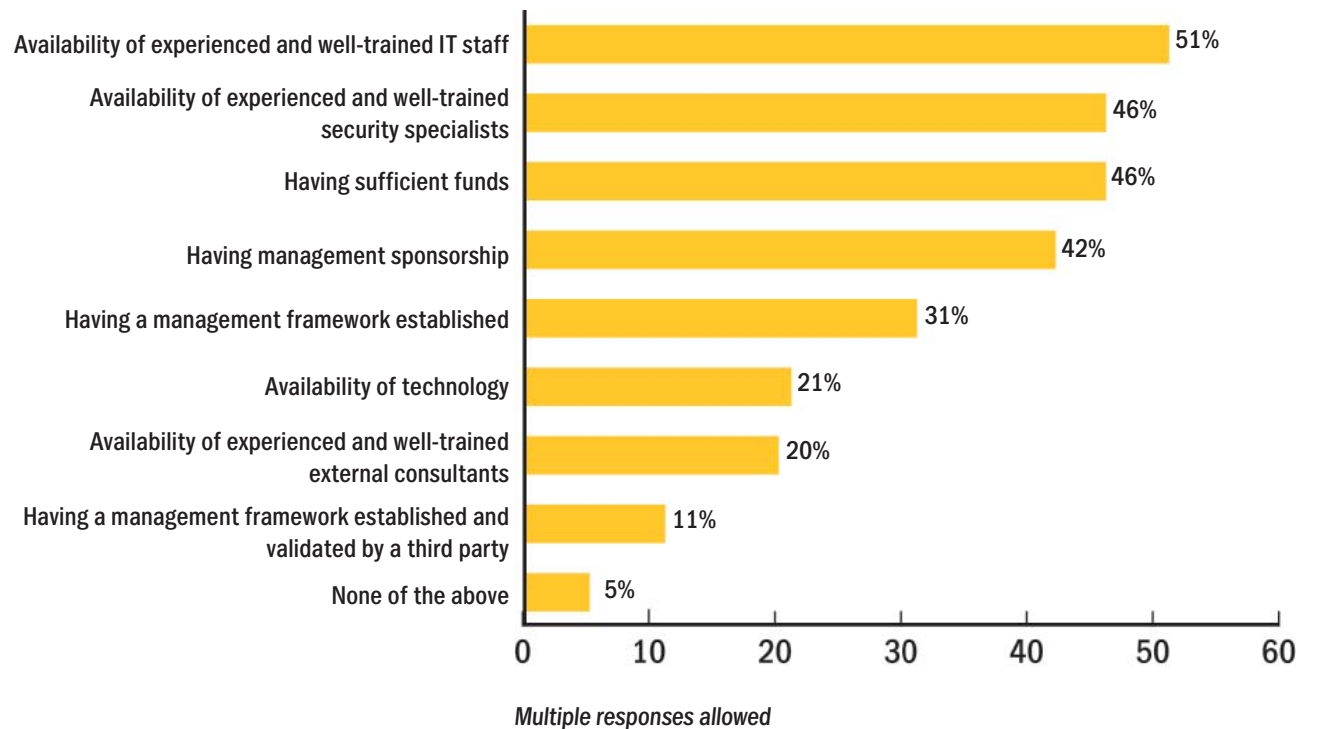
The greatest challenge to delivering information security projects continues to be the availability of experienced IT and information security resources.

As the priorities and objectives of information security shift, finding the right human resources inside or outside of the organization will continue to be a growing concern for information security. The lack of skilled resources can ultimately disrupt an organization's ability to make strategic business decisions and execute them. The survey shows, not surprisingly, that the lack of experienced resources is an important consideration in the decision to seek third-party assistance. Many factors impact an organization's ability to find and keep experienced and well-trained resources, including emerging business models, technology advances, and balanced investments. Each of these can place different demands on the skill sets the organization either has at its disposal or must obtain.

Staffing Information Security

It is important to recognize that changes to the business may require the organization to reevaluate its resource needs and capabilities. This rapidly changing resource environment appears to be one of the major reasons why more than 60% of survey respondents have turned to outsourcing certain elements of information security. This reduces the need for organizations to acquire and maintain certain hard-to-acquire skill sets in-house. The availability of competent individuals ranked first and second among the challenges, while finding well-trained, experienced external consultants is far less difficult. In addition, there are certain capabilities that are simply more cost effective to outsource, which is likely the reason that 75% of the respondents are using third parties for attack and penetration testing, with another 47% using outside resources for information security architecture design, procedure development, and training and awareness programs.

Percentage of respondents reporting the following areas present the greatest challenge to their organization in delivering strategic information security projects





The Opportunities

Investigate alternative staffing options to help address the growing challenge of the availability of experienced and trained information security resources.

The well-recognized talent shortage in IT and information security can be a challenge for many organizations, but it can also be an opportunity to rethink how information security reacts to resource demands. As we discussed in the section, “Aligning Information Security with the Business” (which supports our observation that organizations are starting to segment information security), we believe that the realignment along strategic, governance, operational, and architectural functional lines provides an opportunity for information security to evaluate new resource pools that were unavailable in the past.

For example, the increased integration of information security and risk management has led to resource requirements shifting from being primarily technical to risk and controls-based with

a technical aptitude. With information security’s diminished concentration on the technical and operational aspects of the business, resources from other parts of the organization such as Internal Audit have the technical aptitude and the audit experience to address risk and compliance needs.

Organizations need to act to ensure, however, that the shift away from the technical and operational elements does not create gaps in the more traditional areas of information security.

In addition, third parties will continue to play a valuable role in filling resource gaps and their use should be considered to augment information security roles, especially when highly skilled and experienced personnel would not be a sustainable long-term option for the organization. Our survey shows that using third-party resources can be a productive exercise in cost management, while meeting the expanding demands for information security professionals.

Benchmarking Information Security

A Look Back: In 2005, more than half of the organizations participating in our survey had formally adopted an information security standard (e.g., ISO, IS Forum) or planned to so in the near future.

Source: 2005 Ernst & Young Global Information Security Survey

Strategic Benchmarking Information Security

For the second year in a row, Ernst & Young assisted organizations evaluate and benchmark their information security programs against the globally accepted security standard ISO 27002:2005, formerly known as ISO 17799:2005.

Last year's survey indicated that organizations were using independent third-party information security assessments to establish and understand their information security position to drive security and risk mitigation efforts.

In 2007, services like Ernst & Young's ISO 27002 benchmark evaluation continued to help organizations gauge their efforts and proactively adjust when regulatory changes are anticipated. In addition, many organizations are leveraging the information as a value added opportunity to move beyond tactical initiatives.

Advances in cyberspace and virtualization have led to the rapid development of an information society. Organizations can leverage these advances to create new business opportunities, meet market demands by changing operational and business models, and drive new technology investment decisions.

With each new opportunity for global collaboration between strategic partners or create self-directed customer solutions, the lines of security demarcation move further away from the center. This means that the complexities of protecting the business are likely to increase.

The ISO 27002 benchmark survey helps organizations establish strategic approaches and evaluate their business entity security capabilities to manage the blurring lines of security.



Ernst & Young ISO 27002 Evaluation

The use of an independent security evaluation in conjunction with the knowledge and experience of the Ernst & Young security professional can help organizations to:

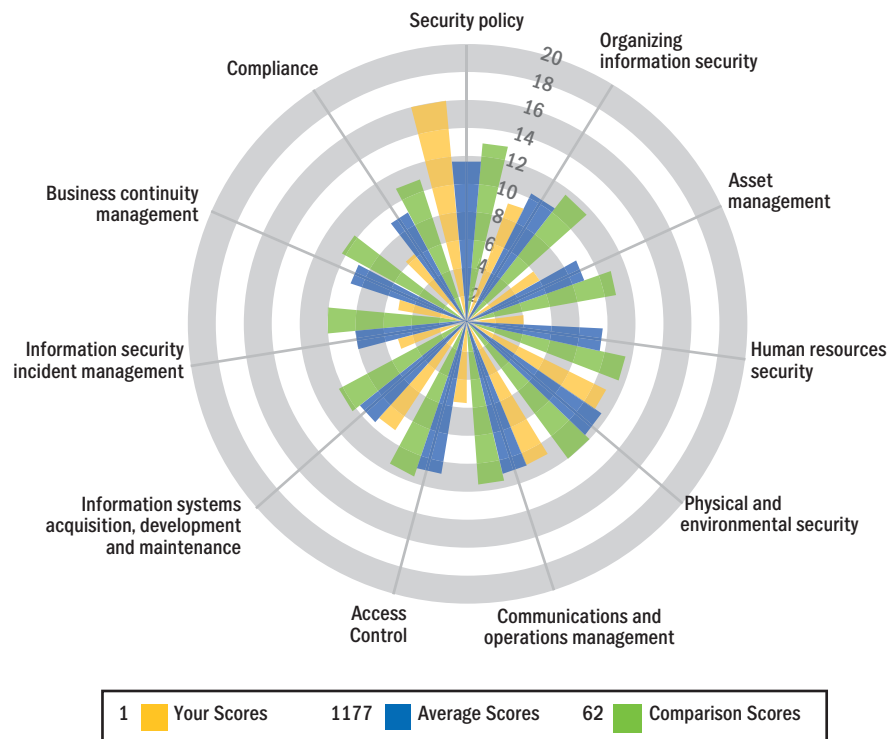
- Understand the extent of standards-based coverage versus their information security program
- Provide a year-over-year performance indicator of their information security program
- Evaluate business entities against themselves and their competitors using a common language
- Conduct a confidential and objective comparative analysis of their information security in contrast to similar organizations and industries
- Identify opportunities to improve information security across an organization's environmental and operational domains

Ernst & Young's global security professionals assisted nearly 1,200 organizations in 46 countries during the last two years' ISO 27002 surveys. The collection of survey data from the participants across 11 ISO domains provides an innovative way for organizations to evaluate and assess their capabilities and gives them a unique ability to compare themselves against the other participants.

ISO Benchmark Survey Reporting

Organizations participating in the ISO security survey are provided with online access to their individual benchmark reports upon completion of the survey questionnaire. The benchmark report provides a point-in-time perspective of the organization's self-assessed maturity level for each of the ISO security categories. The participating entity's score in each category is graphically represented along with a comparative average score for all other participants. Additional comparison can be made for a particular industry segment, country, or size of business.

Benchmarking Information Security

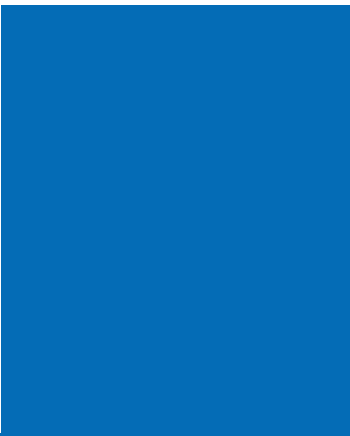


Using the Information

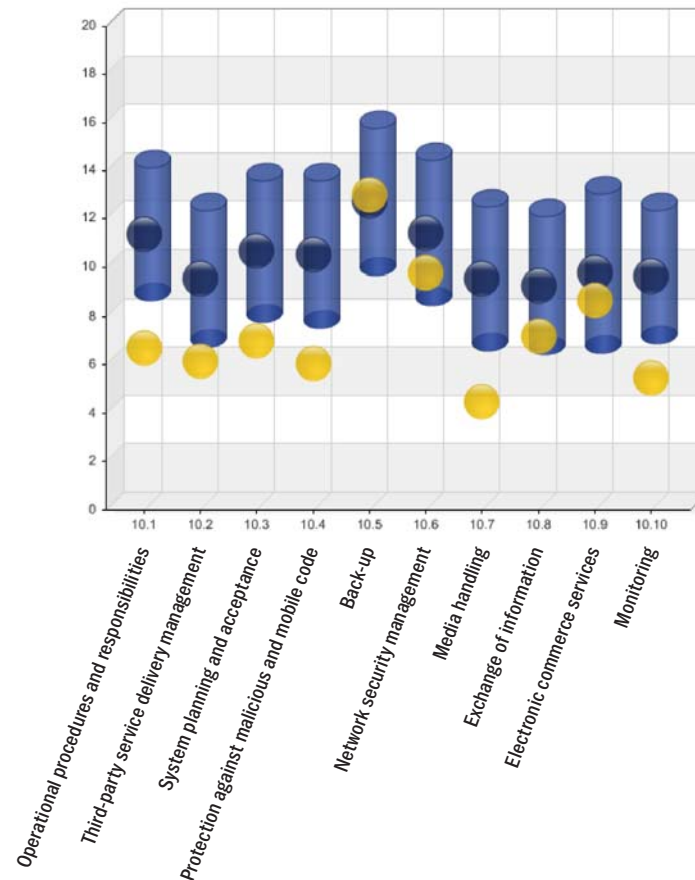
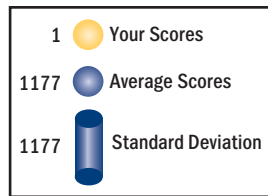
The “radar” graph is used to examine the relative comparison of each category. Areas where the organization’s scores are much higher or lower than the total average are indications that these areas may require further examination and analysis.

In order to support additional analysis and to establish a better understanding of specific ISO domains, the benchmark report includes detailed pipe-diagrams. Like the radar chart, the pipe-diagrams represent the respondent’s relative maturity for each of the subcategories that make up an ISO domain and compare responses against the average responses and a deviation that represents the middle two-thirds of all participants.

Together, the two reports help organizations understand their information security position by establishing a baseline score they can use to periodically evaluate their information security and respective business entities.



Communications and Operations Management



When first evaluating the survey data, the initial tendency may be to consider high maturities as good and low maturities as a need for improvement. We caution against this approach as policies, resources, and the organization’s risk tolerances for each category must be carefully considered as part of the analysis when actually determining improvement areas. For support in interpreting the results or assistance with a detailed analysis, contact your local Ernst & Young office.

2008 Survey: How To Participate

Organizations, their subsidiaries, and business entities that wish to participate in the ISO 27002 benchmark evaluation can do so at no cost by contacting their local Ernst & Young office or by visiting Ernst & Young online at www.ey.com/giss and completing our request form.

2008 and Beyond

A Look Back: In 1998, less than 8% of our survey participants conducted electronic commerce via the Internet. However, 75% reported they would expand their use of the Internet for business transactions if the security of the medium were ever improved.

Source: 1998 Ernst & Young Global Information Security Survey

Key Thoughts to Consider: 2008 and Beyond

An often-repeated statement is that the more things change the more they stay the same. For security, it's no different. For thousands of years, people have tried to protect what they had. Civilizations built great walls, huge fortresses, used different mechanisms and secrets to protect something valuable.

Societies have had the fundamental desire over ages to keep their valuables protected, while at the same time share the beauty and richness of them with others — no matter what was defined as the item or how great its value was. Yesterday and today, people have tried to apply the same core security principles to new technologies, new markets, and new organizations. Today, the central imperative concerns are confidentiality, integrity, and availability of information and resources.

However, when the traditional principles have been applied, the objectives were compromised. Over-protection renders the valuable object useless while under-protection leaves it exposed. On one hand, extreme security and controls prohibit usability. On the other, low security and control left things without practical restraint.

The key message to take away from this 2007 Global Information Security Survey into 2008 and beyond is balance: allow a more natural balance of risk and performance. Don't abandon security for performance and conversely, don't abandon performance for security. Whether your organization is small or large, local or global, the right balance produces the best results.



Aligning Information Security with the Business

Information security has always struggled with the fact that it was disconnected from the business. Compliance efforts have opened the doors much more widely for the information security function to make major strides in aligning with the business. We believe that initiatives such as Identity and Access Management will continue to make headway because of the added value measures like these can bring in terms of reduced costs — for resources such as help desks — enabling entry to new markets and allowing customers to get the resources they need — and improved IT efficiencies — by automating many of the processes still performed manually.

Driving Information Security

The primary driver, compliance, has begun to enter the maintenance cycle from a maturity model perspective. This isn't to say that it won't continue to be an important driver for 2008; instead, it will become an organization's standard mode of operating. Every new regulation appears to build upon the last, so regulatory impact will be significantly less than it has been over the last few years. In aligning with the business, information security will start to improve the balance of risk and operational performance by reexamining its role in many organizations to focus on becoming more efficient and effective in the execution of its responsibilities. The drivers for 2008 that will start to become more important are those that focus on the service delivery functions and the improved operational efficiencies that can be obtained. Finally, expanding markets will also require information security to address data leakage and protection, and the need to strike the balance between making information available, yet secure.



2008 and Beyond

Managing Information Security

As this report highlights, the information security function has become more important than ever. Almost all organizations would agree that this function is critical to the success of the business. Information security will continue to evolve and with that evolution, new demands on monitoring its effectiveness will become more important. Organizations need to continue assessing their information security effectiveness. The trend for 2008 will be around proactive, continuous monitoring of information security functions and controls. Security Information Management will become more important, as a way not only to collect information, but also to report on it. Security dashboards will start to become more prevalent as organizations look to improve upon the reporting of the security position to executive leadership and the business.

Staffing Information Security

Doing more with less has been a familiar mantra for information security professionals for years. The challenge is in addressing the issue. Traditional information security staffing models will be changed in 2008 as organizations look for ways to fulfill their staffing gaps. Security strategists will be more aligned with business strategists and will report into different parts of their organizations. Security architects will move more in line with IT architects and the security operational functions will be blended with business unit operational functions. Also, these roles will start to be filled by non-traditional information security professionals, as non-IT resources may fill some gaps and third-party organizations take on an even more important role.

Survey Approach

A Look Back: In 1997, for the first time, Ernst & Young's Information Security Survey polled senior management from companies in 29 countries, not just in North America.

Source: 1997 Ernst & Young Global Information Security Survey

The 10th Annual Ernst & Young Global Information Security Survey was developed with the help of our assurance and advisory clients in more than 50 countries.

This year's survey was conducted between May 2007 and August 2007. Nearly 1,300 organizations across all major industries participated.

Methodology

The two questionnaires used in the survey (the executive questionnaire and ISO 27002-based benchmark questionnaire) were distributed internationally to designated Ernst & Young

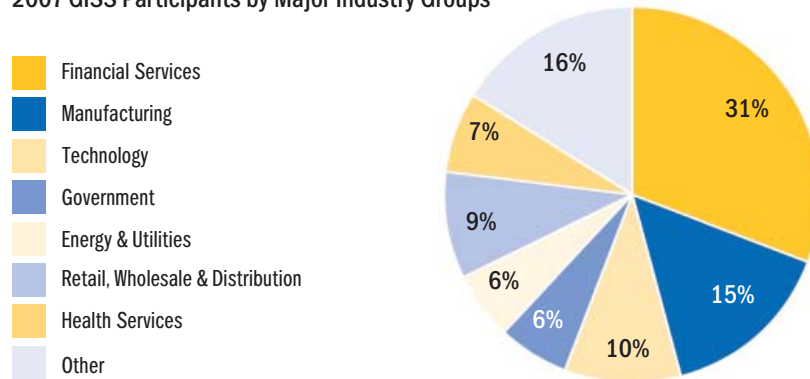
professionals in each country practice within the Ernst & Young network, along with protocol instructions to provide consistent administration of the survey process.

Most of the executive questionnaire results were gathered from face-to-face interviews with the leaders of information security in participating organizations. When this was not possible, the questionnaire was administered electronically. The ISO 27002-based benchmark questionnaire results were gathered via a secure Web site, where information security teams within the participating organizations logged in to complete the questionnaire.

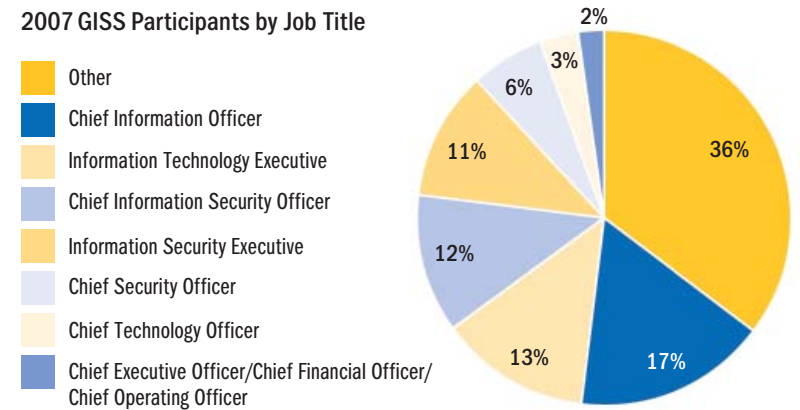
Survey Approach

Profile of 2007 Survey Participants

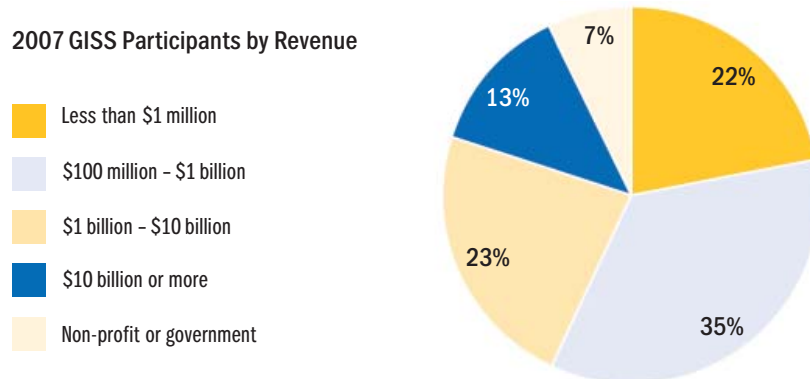
2007 GISS Participants by Major Industry Groups



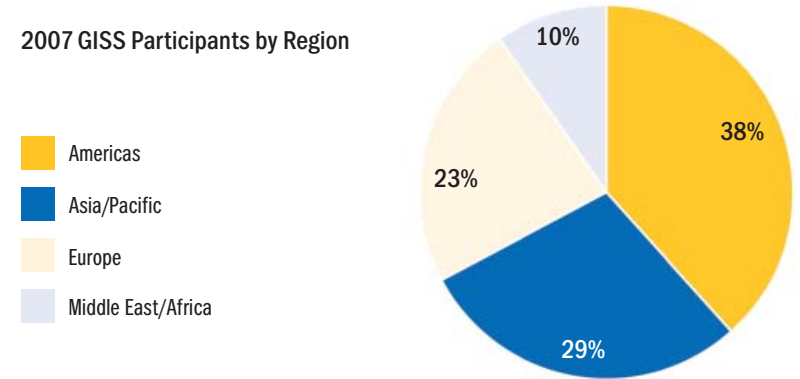
2007 GISS Participants by Job Title



2007 GISS Participants by Revenue



2007 GISS Participants by Region



About Ernst & Young

Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 130,000 people are united by our shared values and an unwavering commitment to quality.

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.

ERNST & YOUNG

www.ey.com

© 2007 EYGM Limited. All Rights Reserved.
EYG No. DZ0033

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.