

Public Sector IT Risk Management

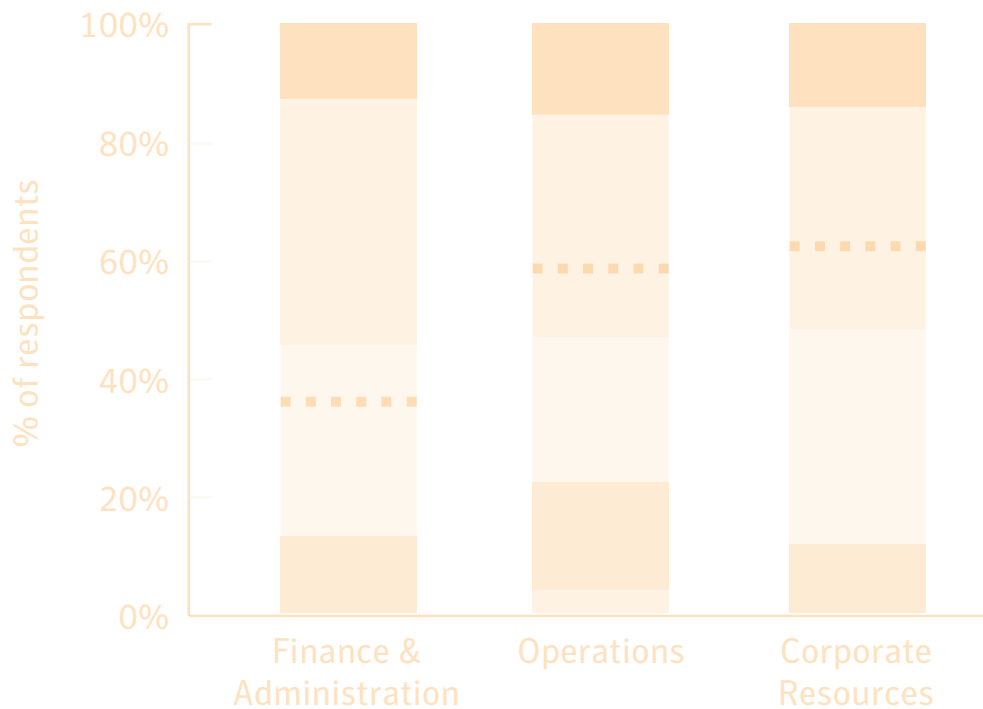
An IT Risk Management Sector Report

Volume 1

Executive Summary

IT Risk Management can help public sector organizations avoid or mitigate risks in e-government and shared services initiatives. Public sector organizations rate themselves effective at classifying and managing IT assets, less effective at securing information assets throughout their lifecycle—and particularly weak in secure application development. Benchmarked against Best in Class standards, they show well-balanced investments across process and technology controls. Further investments in staff training and secure application development should help them improve their overall capability to manage IT Risk as they move toward shared, citizen-centered IT services.

IT Risk by Bu



Introduction

The Internet is transforming the ways governments and citizens interact. As governments rely on Information Technology (IT) for better efficiency and quality and consistency of service, IT Risk Management helps them identify and mitigate IT risks—including security, availability, performance and compliance elements—so they can make a thoughtful, careful transition to more efficient, citizen-focused operations and services. This paper examines public sector trends in IT, sources of IT Risk, and the effectiveness of IT Risk Management controls.

Public sector IT trends

National, regional and municipal governments worldwide are investing in e-government and shared services initiatives:

- **E-government** is a broad category of IT initiatives to improve the speed and quality of government-citizen interactions. It represents an attempt catch up to the private sector in online service delivery. An example is Australia's 2006 e-Government Strategy, focusing on relationships with businesses, non-governmental organizations, and citizens, as well as government operations.¹
- **Shared services** consolidate operations and service delivery across organizational units to improve efficiency and reduce costs. In the United States, for example, the President's Management Agenda aims to identify and consolidate such duplicate services.²

Both initiatives are significant for governments and the societies they serve. They offer substantial direct benefits, helping to cut costs as they improve service quality. And they can pay for themselves, by public sector productivity improvements that drive economic competitiveness. The European Commission's eGovernment Observatory calls Information and Communication Technology "the most powerful government lever for increasing overall productivity and economic competitiveness."³ And even modest government cost reductions can have meaningful effects on economies that struggle to grow even one or two percent per year.

1. Australian Government Information Management Office. *Responsive Government, a New Service Agenda 2006 e-Government Strategy* (Canberra: Department of Finance and Administration, Australian Government, March 2006), 8.
2. CIO Counsel. *Federal Chief Information Officer Council Strategic Plan FY 2007 – 2009*. (www.cio.gov: Chief Information Officer Council) 11.
3. IDABC eGovernment Observatory. *The Impact of eGovernment on Competitiveness, Growth and Jobs*. (Brussels: IDABC Pan-European eGovernment Services) 23.

Required investments

Both e-government and shared services initiatives demand improvements in the capabilities of public sector IT and management personnel, improved availability for key citizen services, and better security for systems and data accessible over public networks.

People investments—E-government and shared services initiatives can be only as effective as the systems, processes, and staff available to support them. Anticipating a skills shortfall, governments everywhere are taking steps to upgrade IT staff capabilities. For example, the US Government CIO Council's 2007 to 2009 Strategic Plan includes developing “a cadre of highly capable IT professionals with the mission-critical competencies to meet agency goals.”⁴

Availability investments—E-government requires that agencies and ministries keep citizen services available around the clock. A citizen who once went to the County Clerk's office for a building permit may now expect to get that permit online any time of day—and “after-hours” provisioning is particularly important to small business owners. Systems supporting key applications may need to expand availability to accommodate new service expectations.

Security investments—Shared citizen-facing systems expose interactions and information to greater risks than the isolated systems they replace. In the wake of well-publicized database breaches, governments are moving aggressively to secure interagency, interjurisdictional, and public interactions, and protect citizens' private information. For example, the U.K. government is implementing identity-management solutions to help “public and private sectors to manage risk and provide cost-effective services trusted by customers and stakeholders,”⁵ and the US government spent \$5.5 billion—9% of its 2006 IT budget—securing IT investments.⁶ Securing interactions with citizens and protecting their private information are fundamental responsibilities, but also improve productivity by releasing resources once consumed by “firefighting.”

4. CIO Counsel. *op. cit.*, 4.

5. Cabinet Office. *Transformational Government Enabled by Technology*. (London: Cabinet Office, November 2005) 13.

6. Office of Management and Budget. *FY2006 Report to Congress on Implementation of the Federal Information Security Management Act of 2002*. (Washington D.C.: Office of Management and Budget) 1.

IT Risk Management and government IT initiatives

IT Risk Management aligns the costs and efforts of IT risk mitigation with an organization's strategic and financial goals. IT Risk managers mitigate risks by deploying and monitoring key process and technology controls. How effectively they do so determines their residual levels of IT Risk, and the resources free to apply to other strategic initiatives.

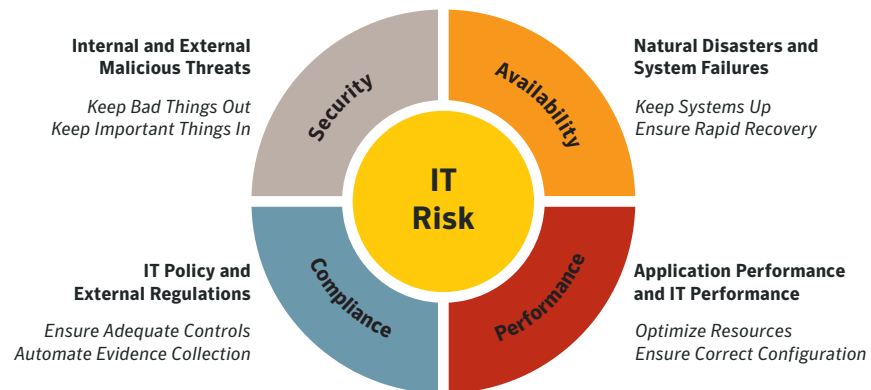


Figure 1: IT Risk spans four areas, each with its own set of drivers and potential impacts.

E-government and shared services initiatives spotlight the need for balance, and IT Risk Management helps achieve that balance. Today, for example, multiple isolated authentication processes add cost, complexity, and risk to government operations. But in a future shared services environment, security failures may compromise multiple systems instead of just one, and availability failures may render multiple systems inaccessible. IT Risk Management disciplines guide risk-mitigation efforts in this balancing act within the context of an agency or ministry's goals, resources, and capabilities.

What drives public sector IT Risk?

Symantec's February, 2007 *IT Risk Management Report* reports results from a survey of 310 IT professionals, 25% of whom represent national, regional, or local governments, nongovernmental organizations (NGOs) or educational institutions. Details of the survey and sample may be found in the full report, available online.⁷

To identify IT Risk drivers, participants rated IT risks associated with each of seven business processes. Public sector participants' Critical or High ratings are presented in Figure 2, benchmarked against corresponding ratings from the private sector.

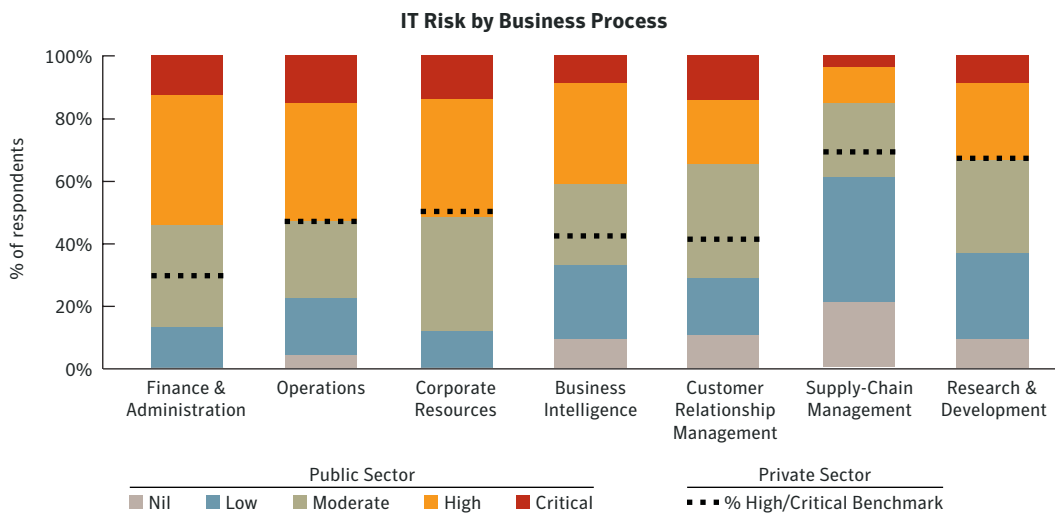


Figure 2: IT risks associated with key business processes by participants from the public and private sectors. The area of the top two bars indicates High or Critical ratings by public sector participants; the area above the dotted line indicates corresponding ratings from the private sector. In both groups, Finance and Administration processes received the highest proportion of High or Critical ratings.

Among public sector participants a majority—55%—rate IT risks associated with Finance and Administration High or Critical; a full 71% of participants from the private sector do so. But fewer public sector participants associate High or Critical levels of IT Risk with external-facing processes: Business Intelligence, Customer Relationship Management (CRM), and Supply-Chain Management (SCM). This disparity is not surprising. E-government exposes agencies—often for the first time—to elevated service expectations from citizens who see themselves as customers, not passive recipients. Because the sheer scale of many government IT systems and user populations extends deployment cycles, exposure of systems and data to external IT risks may not yet be a practical reality.

Public and private sectors face different compliance IT risks—from laws, regulations, or IT policies governing information handling or processing. To measure their perspectives on compliance risk, Symantec asked participants to rate how much risk each of six categories of regulation introduced into their organizations. Figure 3, on the following page, shows the results.

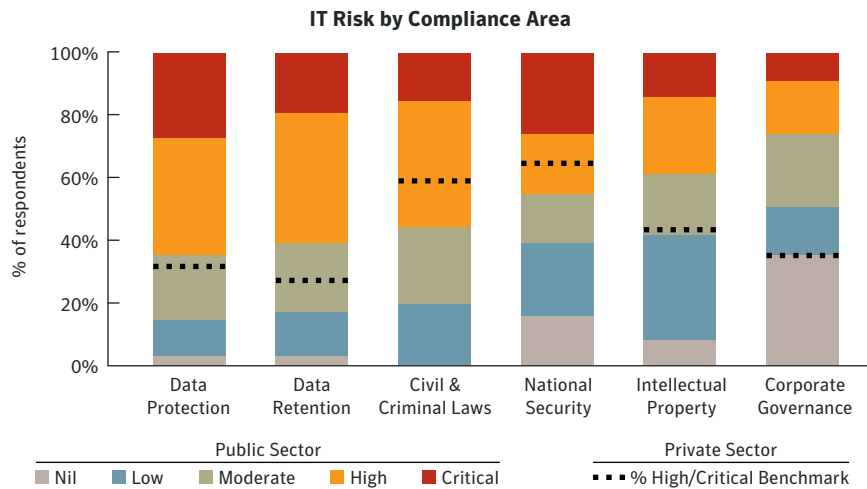


Figure 3: IT Risks associated with key compliance areas by participants from the public and private sectors. Ratings are indicated as in Figure 2. Compliance issues associated with data received the most High or Critical ratings from both groups. More public sector participants gave high ratings to National Security and Civil and Criminal areas; more private-sector participants applied those ratings to Corporate Governance.

Public and private sectors share the view that Data Protection and Retention carry the greatest compliance risk. The importance of these issues will grow as shared services pass confidential personal information across agencies and systems, increasing both its risk exposure and citizens' expectations for the highest standard of protection.

As expected, more public sector participants see compliance risks related to the civil and criminal law and national security as important. In contrast, more participants from the private sector expressed concern about compliance risks introduced by corporate governance requirements—65% of them rated these risks High and Critical, compared to only 26% of public sector participants. But as governments and other public sector organizations expand their internal governance efforts, the current gap between their ratings and those of the private sector may shrink.

Managing IT Risk—process and technology controls

Despite wide awareness of IT Risk Management principles, few organizations have integrated them into formal programs. This section compares risk-management process and technology controls in public and private sectors.

Symantec has identified eight technology and eight process controls that represent best practices for managing IT Risk. They are derived from international standards including ISO/IEC 17799:2005,⁸ COBIT,⁹ and ITIL.¹⁰ Symantec has refined them based on its own experience dealing with highly effective organizations, and expanded them to include availability and performance as well as security and compliance.

8. *Information Technology – Security Techniques – Code of Practice for Information Security Management. (ISO/IEC 17799:2005(E)).* (Geneva: International Organization for Standardization, 2005).

9. *Aligning COBIT, ITIL and ISO 17799 for Business Benefit.* (Rolling Meadows, IL: IT Governance Institute and Norwich, UK: Office of Government Commerce, 2005).

10. *IT Infrastructure Library, <http://www.itil.co.uk>.* (Norwich, UK: Office of Government Commerce).

Process controls

IT professional's ratings of their organizations' effectiveness in deploying key process controls are shown in Figure 4. Differences between public and private sectors are most visible in Asset Inventory Classification and Management, for which 43% of public sector organizations rated their organizations more than 75% effective, compared to only 35% of organizations from the private sector.

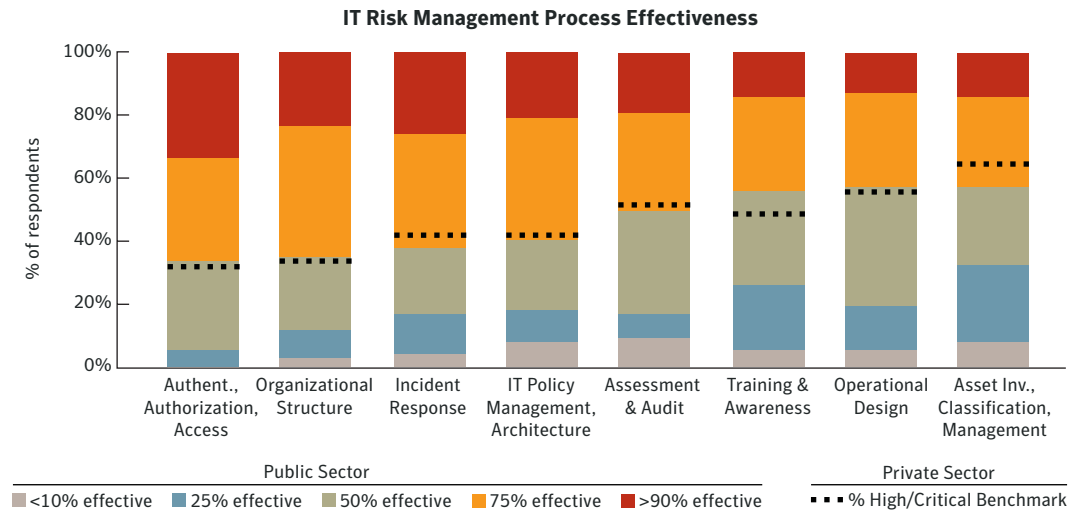


Figure 4: Effectiveness of organizations' process controls for managing IT Risk, arranged from left to right in decreasing frequency of rated effectiveness.

The *IT Risk Management Report* raised concerns about the low effectiveness ratings for Asset Inventory Classification and Management. Asset inventory classification and management is fundamental to good risk analysis, and is an area in which governments have traditionally performed well.¹¹ But while the public sector's strong performance is encouraging, the 75% rating seems low in context of the US Federal Information Security Management Act (FISMA) finding that 88% of major federal information systems are certified to meet FISMA standards.¹²

11. E.g., the 2007 *Secure Computing* award to the UK Government's Central Sponsor for Information Assurance http://www.cabinetoffice.gov.uk/csia/information_for_the_public_sector/risk_management/index.asp

12. Office of Management and Budget. *FY2006 Report to Congress on Implementation of The Federal Information Security Management Act of 2002*. (Washington D.C.: Office of Management and Budget) 22.

Technology controls

Public sector performance ratings in deploying technology controls mirror the private sector's for Network, Protocol and Host Security, and Resilient Infrastructure, as shown in Figure 5. The shortfall for Secure Data Lifecycle Management is consistent with the public sector's perception of lower risks associated with Data Retention Compliance (Figure 3), because retention management is a key element of Secure Data Lifecycle Management.

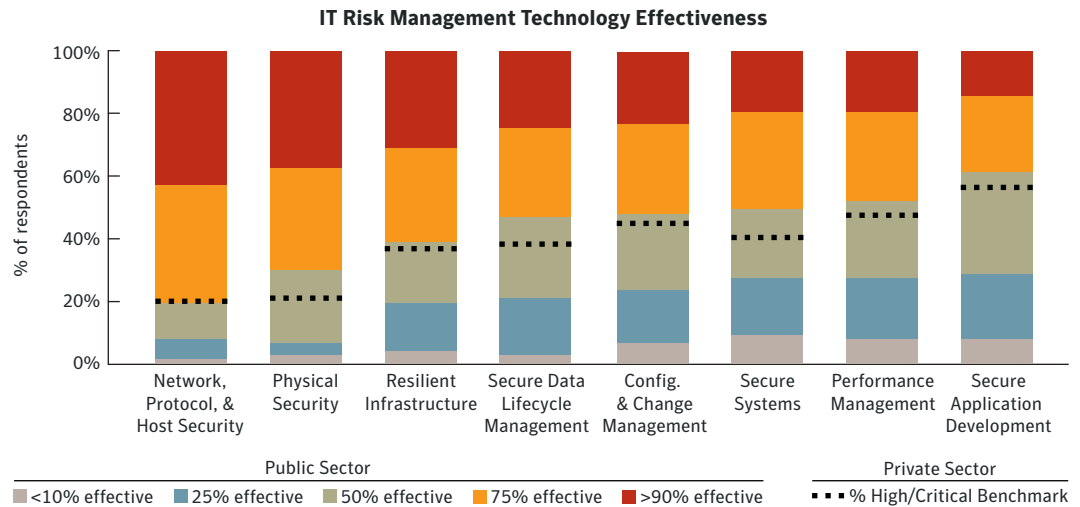


Figure 5: Effectiveness ratings for organizations' technology controls for managing IT Risk, arranged from left to right in decreasing frequency of rated effectiveness.

Public sector organizations should examine closely the less effectively deployed technology controls at the right of Figure 5. These provide foundations for important business processes. For example, Change and Configuration Management is critical to system availability and security, helps avoid costs to maintain and adapt antiquated systems, and reduces risks of system outages. Disciplined Change and Configuration Management can relieve pressures on agency and department budgets and unscheduled funding requests.

Secure Application Development is the poorest-performing technology control for both public and private sectors, although it is among the most important for any organization rolling out new initiatives. Applications with security flaws are costly to maintain, prone to external threats, and wasteful of citizen resources. International Data Corporation (IDC) *Government Insights* observes that governments in the Asia-Pacific region are now focusing on building secure application development environments,¹³ suggesting growing awareness of this deficiency and initiatives to correct it.

Achieving Best in Class IT Risk Management

To identify the factors that help organizations achieve Best in Class IT Risk Management, we ranked survey responses into quartiles according to their overall effectiveness across the 16 process and technology controls identified above.

The *IT Risk Management Report* showed that the highest-ranking quartile—the Best in Class organizations—experience fewer incidents than lower quartiles, despite facing *higher* levels of Compliance and Business Process risk. This finding suggests that Best in Class controls help organizations safely navigate riskier business environments.

Figure 6 extends this analysis to public sector organizations. The public sector appears in the Best in Class quartile to the same degree—25%—as in the sample as a whole, with better representation among national than regional or local governments.

Benchmarked against the Best in Class, public sector organizations have smaller gaps to fill among process controls (left graph) than among technology controls (right graph). Public sector shortfalls are greatest for Assessment and Auditing, Training and Awareness, and IT Policy Management and Architecture controls.

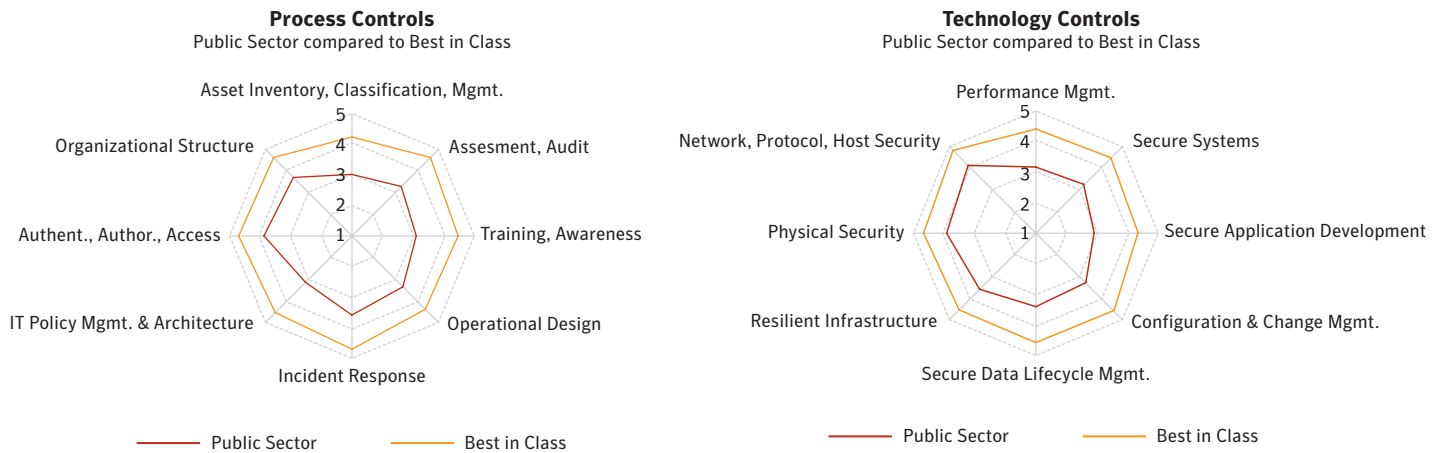


Figure 6: Process (left) and technology (right) control effectiveness scores for Best in Class and public sector organizations. Best in Class organizations show effective performance across most or all measures (shown as distance from the graph's center), rather than disproportionate emphasis on a few.

Their increased pace of investments in IT staff may be intended to remedy the low public sector ratings for Training and Awareness processes. A recent Symantec-sponsored IDC study found that well-trained teams average 10% greater productivity than under-skilled teams.¹⁴ As they move towards electronic delivery of shared services, IT Risk training for IT and other professionals will help them manage risks and deliver promised benefits to citizens.

Among technology controls, the public sector rates itself closest to Best in Class performance for Physical Security, and for Network, Protocol and Host Security. The sector's largest shortfalls appear in Secure Application Development, Secure Systems Build and Deployment, and Performance Management. These lower ratings are consistent with the recommendation above that these organizations focus on mitigating risks during application development. Improvements will help public sector organizations avoid raising security risks as they deploy their new e-government and shared services solutions.

Highly effective organizations deploy more controls, and deploy each of them more effectively. In IT Risk Management, the path from good to great leads from tactical, technical reactions to inclusive, forward-looking strategies, in balanced programs that optimize investments across all controls for greatest impact. We encourage readers to evaluate their own performance on these controls as a first step toward investments to help measure and manage IT Risk.

Conclusions

As public sector organizations drive to improve operational efficiency and deploy e-government initiatives, they will face new IT risks among their other challenges. As they share services across agencies, the service impacts of IT security and availability incidents will be more widely distributed.

Public sector organizations have already started to raise their investments in personnel, scalability and security initiatives to mitigate these and other risks. A more capable work force will monitor and manage the full spectrum of IT risks more effectively. On-demand availability of key services and information will meet higher, customer-driven service requirements. And more robust security will meet responsibilities and expectations for protection of personal data, build trust in new systems and services, and reduce barriers to adoption.

No survey can cover all the risks facing every organization; each should assess its own IT risks and manage them in balance with its own goals and resources. “One size fits all” approaches—especially in the public sector—invite mismatched and poorly designed IT Risk Management strategies that could threaten agencies and the citizens they serve.

Best in Class organizations operate effectively in high-risk environments by deploying a full spectrum of process and technology controls effectively and seamlessly. Through disciplined planning and careful implementation, more public sector organizations can reach their high standard of effectiveness.

About Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world.

The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries.

More information is available at www.symantec.com

Confidence in a connected world.

For specific country offices and contact numbers please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

Copyright© 2007 Symantec Corporation. All rights reserved. Symantec and the Symantec logo are trademarks or registered trademarks of the Symantec Corporation or its affiliates in the U.S. and other countries.
7/07 12741597