

Enterprise Risk and Technology Management

An Executive Summary of a Landmark Report

By The Institute of Internal Auditors

“Directors have a responsibility to oversee risk management in the organizations they serve. One primary source of risk is information technology. For most companies, IT includes employees’ use of personal computers. In a new research report, The Institute of Internal Auditors offers comprehensive guidance on the management of PC use in order to mitigate financial and operational risk for this important asset. This report is essential reading for IT managers, internal audit committees, chief security officers, and anyone attempting to bridge the gap between IT policy and board-level business decisions.”

— Roger W. Raber, CEO and President, The National Association for Corporate Directors, December 1, 2003

The full report “PC Management Best Practices: A Study of the Total Cost of Ownership, Risk, Security, and Audit” can be ordered from The Institute of Internal Auditors (The IIA) at: http://www.theiaa.org/iaa/bookstore.cfm?fuseaction=product_detail&order_num=482.

■ INTRODUCTION

“Good internal control is no longer just a best practice...it’s the Law!”

— PricewaterhouseCoopers, *IIA Technology Audit Forum*, July 24, 2003.

The global regulatory and legal environment is tightening around the issue of information security. Businesses must protect the privacy and integrity of financial and sensitive third-party information or face increasing risk of government intervention and legal liability. For any business with networked and Internet-connected computing systems, this requires comprehensive and documented infrastructure security management based on industry best practices.

A recent report by The Institute of Internal Auditors provides groundbreaking support for this challenge. The report is called, *“PC Management Best Practices: A Study of the Total Cost of Ownership, Risk, Security, and Audit.”* Zeichner Risk Analytics LLC, a leader in business risk management, calls it the *“first-ever risk framework for managing personal computing security.”*

The report from the IIA explores the impact of PC fleet management practices on key business issues, including information security, enterprise risk, regulatory compliance, legal liability, business process efficiency, revenue generation and total cost of ownership (TCO). The report is a practical guide to maximizing business value from PC investments and uses language that is as meaningful to executive boards as to IT specialists. It provides a comprehensive framework, business justification and recommendations for moving toward PC management best practices that enable an organization to maintain a more secure, agile and cost-effective PC infrastructure.

This paper extracts some of the key messages from that report, highlighting the importance of an up-to-date, well-managed PC infrastructure in addressing:

- Rising security threats
- New regulatory requirements
- Rapidly evolving liability issues

ABOUT THE INSTITUTE OF INTERNAL AUDITORS

The Institute of Internal Auditors (The IIA) is the leading professional organization for the internal audit profession, a recognized authority in the field and a key source of authoritative research and information. Its membership includes over 85,000 professionals working in private and public organizations worldwide.

The IIA defines internal auditing as: *“an independent, objective assurance and consulting activity designed to add value and improve an organization’s operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.”*

Internal audit teams typically have direct lines of communication with upper management, including the board of directors. With respect to information technology, these professionals can be instrumental in providing a common framework for aligning the goals and strategies of business, financial and IT decision makers. A working relationship with the internal audit team should be a top priority for all high-level IT managers.

The full report is must reading for IT managers, internal auditors, financial analysts, security specialists, and anyone associated with enterprise risk, technology management and security. It is available at: http://www.theiia.org/iaa/bookstore.cfm?fuseaction=product_detail&order_num=482.

■ THE SECURITY IMPERATIVE

Security threats are increasing.

Digital threats to Internet-connected systems and networks are growing in volume, sophistication and potential damage. Businesses must be aware of these threats, understand the exposure they face, and manage their technology infrastructure to cost-effectively mitigate risk.

According to the IIA:

- *“Information security is the number one issue for the American technology community”*
- *“...an active hacker community is ready to capitalize on detected vulnerabilities.”*
- *“...sources indicate the actual costs of security events are actually greater than previously estimated, and a single event can cost millions of dollars.”*
- *“Many organizations are under the impression that their traditional insurance policies cover network security and cyber-related risks, but this is rarely the case. Most standard insurance policies specifically exclude network related incidents.”*

Strong PC security is essential.

As external access to internal applications has become commonplace, perimeter security solutions, such as network firewalls, no longer provide sufficient protection against the volume and complexity of incoming traffic. A security-hardened PC infrastructure adds an essential layer of additional protection.

According to the IIA:

- *“Virtually every aspect of PC fleet management has an impact on information security — from platform choices and software management to upgrade cycles and end-user education.”*

- *“The stakes are high, and IT organizations should have formal processes in place to regularly monitor, evaluate, and enforce internal controls to ensure compliance with internal objectives, legislation, regulations, agreements, and insurance coverage provisions.”*
- *“Internal control and security elements such as firewalls, virus protection, intrusion protection, software maintenance and patching, event logging, encryption, authentication, and end-user awareness programs should be carefully controlled and integrated into a larger security framework.”*

A poorly managed or out-of-date PC infrastructure raises critical security issues.

Threats are constantly evolving, and security precautions must be updated accordingly. Software upgrades, security patches and hardware lifecycles should be actively managed to balance risks and costs.

According to the IIA:

- *“A single out-of-compliance PC can present a vulnerability that poses significant risk to the enterprise.”*
- *“Out-of-date operating systems are particularly vulnerable to digital attack, since the vendor no longer provides patches for newly discovered security vulnerabilities.”*
- *“Old PCs can significantly increase enterprise risk, especially if they are running older operating systems that are no longer supported by the vendor. These old, unsupported configurations should be eliminated from the environment.”*

Staying current with technology and actively managing PC lifecycles are critical components of enterprise security.

Businesses must balance the acquisition and deployment costs for new systems and software against the higher cost and risk associated with older PCs and operating systems. Formal risk, TCO and change management strategies are essential to establish optimal lifecycle solutions that deliver full business value.

According to the IIA:

- *“Improving the efficiency of patch management processes and keeping your PC and server infrastructure up-to-date are among the most cost-effective steps toward enhancing security.”*
- *“Fundamental advances in PC platform security have been underway for several years, and the recent generation of platforms, operating systems, applications, and management tools enable better security at lower costs than was possible with older systems.”*
- *“Newer operating systems, such as [Microsoft] Windows 2000 or Windows XP, provide logging capabilities for auditing security events. This is important for compliance and forensic investigation, and for understanding attacks to resolve vulnerabilities and limit damage.”*
- *“Although many companies have corporate policies and procedures, only through automated solutions can a company keep a fleet of PC’s in compliance with patch and virus updates.”*

■ REGULATORY COMPLIANCE AND LEGAL LIABILITY

PC security management is becoming a business requirement.

Governments and regulatory bodies around the world are establishing financial integrity and privacy regulations to improve oversight in today’s increasingly global and digitally-connected economy. Businesses need to be aware that these regulations will materially impact baseline expectations for technology management. The IIA report provides a COSO model for compliance with Sarbanes-Oxley and similar regulations, and a framework for more secure network computing.

According to the IIA:

- *“In a networked business environment, PC management requirements will be impacted by virtually all legislation and regulation that addresses the integrity, reliability, or privacy of business information.”*

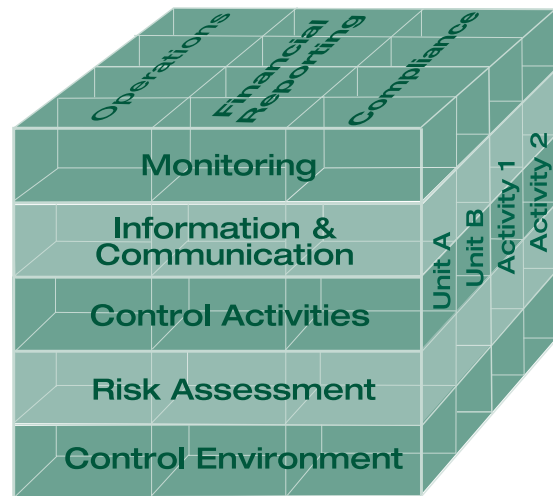


Figure 1.
The COSO “Internal Control Integrated Framework” model is recommended by The IIA for establishing and documenting a comprehensive infrastructure security solution.

- *“Even regulations that do not explicitly focus on security may have substantial consequences for IT in general, and PC fleet management in particular. Examples include the International Financial Reporting Standards (IFRS), Basel II Accord, the Corporate Law Economic Reform Program (CLERP), the Gramm-Leach-Bliley Act (GLB), the Sarbanes-Oxley Act (SOA) and the Health Insurance Portability & Accountability Act (HIPAA).”*
- *“The PC plays a complex role in many core issues, including security, privacy, information and control reliability, risk management, governance, and even critical infrastructure protection and national defense.”*
- *“The COSO model can serve as a successful framework to document the key controls of the networked PC environment.”*

Due diligence in PC security is essential to limit legal liability.

Most businesses process and store large volumes of sensitive information on systems that are connected to their PC infrastructure, and to the Internet. Though legal issues will continue to be defined in precedent-setting court cases, the trend is toward holding companies liable for private information that is compromised by inadequate security solutions.

According to the IIA:

- *“The Steptoe & Johnson report offers compelling evidence that a failure to protect customer and third-party information residing on an organization’s systems and network will expose that organization to potential litigation and substantial risk.”*
[<http://www.steptoec.com/publications/274a.pdf>]
- *“A software security patch policy, and similar PC controls, should be based upon industry best practices to mitigate potential liability.”*
- *“Reducing enterprise risk can improve bottom line performance by reducing material impacts resulting from exploited vulnerabilities. Benefits may also be reflected in reduced insurance premiums.”*

■ MANAGING BUSINESS RISK

Decision makers must look at the full business, financial and technical implications of the PC infrastructure.

The issues are complex, and there is no one-size fits all solution. A formal approach to risk management is recommended, so businesses can align PC management strategy with core business objectives.

According to the IIA:

- *“A comprehensive understanding of the total costs and risks associated with the PC infrastructure is essential to drive organizations toward the kinds of formal strategies, policies, and best practices that are appropriate for such a large and distributed enterprise asset.”*
- *“These pressures make it all the more essential to closely evaluate the economics of the full PC lifecycle including acquisition, deployment, support, and replacement; to understand the value-at-risk with respect to the PC infrastructure; and to integrate this evaluation with broader enterprise risk assessments.”*
- *“As the criticality of information processed in the networked PC environment increases, so does the need for an improved control structure. Automated solutions become a must as the organization grows.”*

A holistic approach to PC fleet management is a competitive advantage.

Due to the scope of the PC infrastructure, and its critical importance in most business processes, it should be closely managed, using proven best practices, formal financial models and comprehensive internal controls.

According to the IIA:

- *“This report is a call to action for auditors and management to address the control, security, and efficiency of their networked PC infrastructure.”*
- *“The PC infrastructure has become a strategic business asset, and should be managed accordingly.”*

- *“Perhaps the most essential point is that companies must look holistically at their PC environment in terms of costs, risk and value and manage their replacement schedules accordingly. As evidenced by our research results, overall costs can be reduced by viewing the PC as more than just a commodity, and addressing the complete vendor and service relationship as a single equation.”*

■ STRATEGIC INVESTMENT IN THE PC INFRASTRUCTURE

A full assessment of business, financial, and technical considerations leads naturally to the adoption of PC management best practices, including regular system upgrades.

A PC environment with up-to-date hardware and software is a core business advantage, especially if it is efficiently managed using automated tools and processes. To validate this in their own environment, IT managers should work closely with financial specialists in their organization to establish appropriate models for understanding business risk and TCO.

According to the IIA:

- *“The apparent savings of postponing new PC acquisitions must be weighed against the costs and risks of maintaining older PCs.”*
- *“By bringing both technical and financial expertise to bear on PC management issues, an enterprise can migrate toward best practices and optimized refresh cycles in a controlled fashion that delivers (and documents) better ROI at each step in the process.”*
- *“There is a strong tendency for businesses—especially under difficult economic conditions—to retain PCs as long as they serve their main function. After all, it is hard to argue with the immediate cost savings of delayed acquisition. Yet, as already mentioned, 70 to 80 percent of the total cost of PC operation is unrelated to acquisition and deployment costs, and older PCs are inherently more costly to manage and secure.”*

BEYOND RISK MITIGATION— REDUCING TOTAL COST OF OWNERSHIP

According to The Institute of Internal Auditors, PC management best practices, such as standard configurations, automated management tools and regular upgrades of the installed base, can decrease total costs by 20 to 25 percent in a typical organization. These steps can also make it far less costly to effectively manage software updates—including security patches, virus definitions and firewall profiles—which are essential to overall platform security.

According to the IIA:

- *“For many business decision makers, it seems obvious that PCs should be kept as long as they seem to adequately serve their core function. Yet a closer look reveals it is generally more cost-effective to replace PCs on a regular schedule.”*
- *“Older PCs are more prone to problems and failure than newer machines, as is reflected in the costs for extended warranties.”*
- *“Retaining PCs for longer periods also forces IT organizations to maintain a greater variety of operating systems across the PC fleet. A diverse fleet of PCs and operating systems adds complexity to the costs of maintenance, support, asset management, monitoring, and software updates.”*
- *“...there is no one-size-fits-all solution, but a 3-year upgrade cycle for desktops and a 2-year cycle for laptops seems to deliver best overall value for most organizations, especially when instituted as part of a comprehensive best practices program that includes standardized hardware and software configurations and automated tools for core management functions.”*

■ CONCLUSION

“The better you understand and document the costs, risks, and value associated with your current environment, the more effectively you can evaluate the real benefits—and justify the costs—of infrastructure and operational upgrades.”

— The Institute of Internal Auditors, *PC Management Best Practices: A Study of the Total Cost of Ownership, Risk, Security, and Audit*, Mark Salamasick & Charles Le Grand, 2003

In recent years, leading IT organizations have made substantial progress in defining and implementing best practices for PC fleet management. Advances in platforms, operating systems and management applications have played—and continue to play—a critical role in this evolution. In light of today’s growing security and regulatory requirements, businesses must be aware of these developments, and embrace advanced tools and strategies for reducing risk and improving the value of their PC infrastructure.

The research by The IIA puts the critical importance of PC management best practices into clear perspective for business decision makers. It provides a compelling business case for maintaining an up-to-date and well-managed PC infrastructure in order to:

- Improve information security,
- Comply with new and evolving laws and regulations,
- Reduce legal liability,
- Qualify for network insurance to cover residual business risk.

The IIA report has been strongly endorsed by the National Association of Corporate Directors, one of the most influential professional organizations for corporate board members and high-level executives. We recommend that IT managers share this document, and the full IIA report, with their internal audit, financial, security and executive management teams. It can provide common ground for understanding key issues, and a strong framework for moving forward cost-effectively.

To order a copy of the full IIA report—*PC Management Best Practices: A Study of the Total Cost of Ownership, Risk, Security, and Audit*—visit the IIA Web site at: http://www.theiia.org/ia/bookstore.cfm?fuseaction=product_detail&order_num=482.

Intel, and the Intel logo are trademarks or registered trademarks of Intel Corporation. Copyright ©2003 Intel Corporation. All Rights Reserved. 1203/RS/ITF/xx/PDF

300307-001

* Other names and brands may be claimed as property of others.

