



Today's IT Organization – Delivering Security, Value and Performance Amid Major Transformation

Assessing the Results of Protiviti's 2014 IT Priorities Survey

Powerful Insights. Proven Delivery.®

protiviti[®]
Risk & Business Consulting.
Internal Audit.

INTRODUCTION

If there is one word to describe the state of IT organizations in 2014, it is **transformation**.

Protiviti's 2014 IT Priorities Survey confirms that IT transformation has become the new normal for companies: Nearly two-thirds of respondents (63 percent) reported that some form of "major IT transformation" is under way in their organizations. Even more important: Not only is IT altering its structure, the function is also transforming its fundamental mission. IT's objective is shifting from leveraging technology in support of the business to the higher-reaching goal of protecting and enhancing business value.

This shift also is evident in the changing role and ever-increasing workload of the CIO. Seventy percent of CIOs said they see themselves as a future CEO, according to a recent survey by *The Wall Street Journal*.¹ CIOs are certainly putting in the work to get there: The issues and activities identified in our study by CIOs and IT executives indicate they need to address these items in order to keep the business running and support challenging strategic initiatives.

In fact, responses from all of our participants – more than 1,100 – indicate IT functions have scores of significant priorities and likely are being pulled in multiple directions to address countless critical challenges. Among the most notable for 2014:

- **Enhancing and protecting business value** – The integration and alignment of IT planning and business strategy represents a paramount priority. In fact, enhancing and protecting the value of the organization – via data security as well as other IT risk management and business continuity capabilities – is top-of-mind not only for IT organizations, but also for their organizations' boards and executive management teams.
- **All eyes are on security** – Massive security breaches continue, with some organizations being questioned by congressional committees in recent months. More than ever before, this has IT departments – as well as boards and executive management – on edge, on notice and, in some cases, testifying under oath. Strengthening privacy and security around the organization's systems and data is now a top priority across all industries.
- **Managing and classifying all that data** – As the need for stronger information security intensifies, CIOs and IT professionals are seeking out more effective ways to stratify the importance of the information they have, and organize and secure the growing volume of data they must manage.
- **Strengthening IT asset – and data – management** – Companies are seeking to improve their data and information governance programs, a need no doubt driven by the growing use of mobile devices and applications, social media, and the continued integration of cloud computing into IT strategy and processes.
- **More mobile, more social** – Mobile commerce management, mobile security and mobile integration remain focal points for IT departments in 2014, even as security-related priorities compete for their time and resources. A similar trend holds for social media, as organizations continue to rely on IT to support their investment in social media activities while improving the integration of these capabilities with other IT assets.

Protiviti

March 2014

¹ Bussey, John, "CIOs Eye the Corner Office," *The Wall Street Journal*, Feb. 10, 2014: <http://online.wsj.com/news/articles/SB10001424052702304680904579364641778947268>.



METHODOLOGY

More than 1,100 respondents, including CIOs, IT vice presidents and IT directors, participated in our study, which was conducted within the prior 90 days. We are very appreciative and grateful for the time invested in our study by these individuals.

Participants answered more than 100 questions in 10 categories:

- Technical Knowledge
- Managing Security and Privacy
- Defining IT Governance and Strategy
- Managing Application Development
- Deploying and Maintaining Solutions
- Managing IT Infrastructure
- Managing IT Assets
- Management and Use of Data Assets
- Ensuring Continuity
- Organizational Capabilities

For each of these categories, respondents were asked to rate, on a scale of one to 10, the level of priority for them and their organizations to improve in different issues and capabilities. A “10” rating indicates the issue is a high priority while a “1” indicates the issue is a low priority.

We have classified each of these issues with an index of 6.0 or higher as a “significant priority” for IT functions. Those with an index of 4.5 through 5.9 are classified as a “moderate priority” and those with an index of 4.4 or lower are classified as a “low priority.”

TECHNICAL KNOWLEDGE

Key Findings

- IT project and program management are deemed to be critical priorities, as are ERP systems – this is understandable given that many organizations are undergoing a major IT transformation.
- CIOs and IT organizations are focused on fortifying their overall IT governance and risk management capabilities in multiple areas that continue to evolve, including virtualization, cloud computing, data governance and smart device integration.
- Not surprisingly, privacy and information security issues are top-of-mind, with U.S. data breach and privacy laws, ISO/IEC 27001 and 27002, the NIST Cybersecurity Framework, and mobile commerce security ranking as significant priorities.

Commentary

It is both interesting and telling to find IT project management at the top of the priorities list in this category, with IT program management trailing close behind. As we noted in our Introduction, nearly two out of three organizations today are undergoing a major IT transformation. Many transformative projects include the selection and implementation of new ERP systems, another highly ranked priority. More companies are looking to expand and deepen their project and program management capabilities because of the very complex, and often lengthy, IT projects and programs they have underway.

Security and privacy standards, ranging from various data breach and privacy laws throughout the United States, to the recently updated ISO/IEC 27001 and 27002 information security standards,² and to the final NIST Cybersecurity Framework,³ also rank as critical priorities. Understandably, CIOs and IT professionals at all levels of the organization want to strengthen their security and privacy knowledge as well as their organization's information security capability. With corporate and national security hinging increasingly on data security and protection, new regulations, rules and guidance will continue to materialize, requiring CIOs and their staffs to ensure their systems are up-to-date and in compliance.

Achieving this goal will not be easy, given the IT function's other priorities – among them, strengthening knowledge and capabilities related to virtualization, cloud computing, smart device integration, and data governance and big data – together with the slippery nature of emerging cyberattacks. Organizations in all industries continue to experience security breaches – sometimes massive ones – with the aftermath often including an appearance before Congress to testify. More than ever, CIOs and IT staff – as well as boards of directors and executive management – are on edge and on notice. IT organizations must ensure they are highly vigilant in establishing strong security and privacy measures, and prepared to respond (rather than reacting) quickly when a data breach strikes.

² *Information Technology Flash Report*, “Security Standards ISO/IEC 27001 and 27002 Have Been Revised: What Are the Significant Changes?”, October 17, 2013, Protiviti: www.protiviti.com/en-US/Documents/Regulatory-Reports/Information-Technology/IT-Flash-Report-ISO-27001-27002-101713-Protiviti.pdf.

³ *Protiviti Flash Report*, “Cybersecurity Framework: Where Do We Go From Here?”, February 25, 2014: www.protiviti.com/en-US/Documents/Regulatory-Reports/Information-Technology/IT-FlashReport-NIST-Cybersecurity-Framework-Where-Do-We-Go-From-Here-022514-Protiviti.pdf.

Finally, all of the priorities in this category, from IT project and program management to ERP systems and virtualization, underscore the need for strong business analysis and risk management capabilities, which will help IT executives and staff members bridge the gap between IT and the business, and engage organization executives and business-unit owners in a more effective manner.

Overall Results, Technical Knowledge


Technical Knowledge	Priority Index
IT project management	6.5
Virtualization	6.5
Cloud computing	6.3
Data governance	6.3
IT program management	6.3
Data breach and privacy laws (various U.S. states)	6.2
ERP systems	6.2
ISO/IEC 27001 and 27002	6.2
BYOD policies/programs	6.1
Cloud storage of data	6.1
Mobile commerce security	6.1
NIST (cybersecurity)	6.1
PMP	6.1
Smart device integration	6.1
Big data	6.0
ISO 31000	6.0
Mobile commerce integration	6.0
Social media security	6.0
CISM	5.9
CISSP	5.9
COBIT	5.9
European Union Data Directive	5.9
Mobile commerce policy	5.9
Social media integration	5.9
CISA	5.8
PCI DSS	5.8
Social media policy	5.8
CGEIT	5.7
FISMA	5.7
GSEC	5.7
HITRUST CSF	5.6

Key Questions to Consider

- Is your IT function devoting sufficient resources to maintaining current knowledge of ISO 31000, ISO/IEC 27001 and 27002, state-, country- and region-specific data breach and privacy laws (including the European Union Data Directive and, in the U.S., NIST and FISMA), as well as related directives and guidance?
- Are your existing data governance, IT project management and IT program management sufficient in light of ever-changing data security risks?
- Has the IT function developed mobile commerce and social media policies that clearly convey the security requirements to employees who engage in mobile commerce and/or social media activities?
- Does the IT function maintain a “bring your own device” (BYOD) policy that serves as the foundation for a current, secure and business-value-enabling BYOD program?
- How are mobile commerce, social media and BYOD policies monitored and audited? Are these reviews integrated into the audit plan?
- Is current in-house knowledge of cloud computing, virtualization and big data capabilities and risks sufficient? How is this internal knowledge cultivated and, when necessary, supplemented and enhanced?
- Are you currently using cloud computing resources in your environment? What applications are running in that environment? What data do you allow to be processed there? Who was involved in making/approving that decision?
- Does the IT function’s knowledge of existing and emerging areas – ranging from ERP systems to cloud computing, smart device integration and data governance – enable swift, comprehensive and effective response to data breaches?
- To what degree is IT leadership providing the funding and support necessary for staff members to strengthen their knowledge and expertise through professional certifications? And along with these certifications, is your organization ensuring IT staff members gain meaningful experience in these areas?

Focus on CIOs/IT Executives and Large Companies

Technical Knowledge – Results for CIOs/IT Executives and Large Company Respondents			
Technical Knowledge	Overall	CIOs/IT Executives ⁴	Large Company Respondents ⁵
IT project management	●	●	●
Virtualization	●	●	●
Cloud computing	●	●	●
Data governance	●	●	●
IT program management	●	●	●
Data breach and privacy laws (various U.S. states)	●	●	●
ERP systems	●	●	●
ISO/IEC 27001 and 27002	●	●	●
BYOD policies/programs	●	●	●
Cloud storage of data	●	●	●
Mobile commerce security	●	●	●
NIST (cybersecurity)	●	●	●
PMP	●	●	●
Smart device integration	●	●	●
Big data	●	●	●
ISO 31000	●	●	●
Mobile commerce integration	●	●	●
Social media security	●	●	●
CISM	●	●	●
CISSP	●	●	●
COBIT	●	●	●
European Union Data Directive	●	●	●
Mobile commerce policy	●	●	●
Social media integration	●	●	●
CISA	●	●	●
PCI DSS	●	●	●
Social media policy	●	●	●
CGEIT	●	●	●
FISMA	●	●	●
GSEC	●	●	●
HITRUST CSF	●	●	●

 Significant Priority
Index of 6.0 or higher
  Moderate Priority
Index of 4.5 to 5.9

⁴ Includes responses from CIOs and Vice President-level executives.

⁵ Companies with revenues of US\$1 billion or more.

MANAGING SECURITY AND PRIVACY

Key Findings

- Among all of the IT organization's many responsibilities, managing security and privacy ranks among its most vital priorities.
- Preparing for, monitoring for and responding to security incidents – swiftly and effectively, based on an established policy and tested processes – understandably is deemed to be a critical concern.
- Other significant priorities include enterprise data classification and management, identity and access management, and IT user management, as well as technical infrastructure configuration.
- Organizations are continuing to evolve their third-party/vendor management programs, especially in light of recent security breaches undertaken by using vendor credentials.

Overall Results, Managing Security and Privacy

Managing Security and Privacy	Priority Index
Developing and maintaining security and privacy standards	6.4
Monitoring security events	6.4
Implementing security/privacy solutions and strategies	6.3
Incident response success (containment, recovery)	6.3
Incident response policy and preparedness	6.3
Incident response reaction time	6.3
Managing user identities and access	6.3
Managing and classifying enterprise data	6.2
Managing application users	6.2
Managing IT users	6.2
Managing technical infrastructure configuration	6.2
Clarity about third-party compliance readiness (partners, vendors)	6.0
Managing contractors	6.0
Managing third-party vendors	6.0
California Security Breach Information Act (SB 1386)	5.9
U.S. Gramm-Leach-Bliley Act (GLBA)	5.8
U.S. Health Insurance Portability and Accountability Act (HIPAA)	5.8

Commentary

As reports of occurrences of corporate and governmental data breaches increase in frequency and magnitude, managing and protecting IT systems and data – which includes monitoring security events and improving different facets of incident response, among other activities – is an increasingly important priority. Developing and maintaining these capabilities requires establishing – and communicating – a security and privacy strategy, executing this strategy (e.g., managing applications,

users, technical infrastructure and third-party vendors), managing security incidents when they arise, and monitoring changing regulatory compliance requirements and real-world risks to ensure the strategy remains effective.

Each of these activities is important and is closely related to other priorities identified in our results, including:

- Improving nearly every facet of incident response
- Managing application users and third-party vendors
- Maintaining clarity about the compliance readiness of vendors and trading partners
- Managing and classifying enterprise data

The emphasis on incident response underscores the increasing realization by IT functions and C-suite executives that data breaches are a matter of “when,” not “if.” In fact, the focus within our survey findings on the entire incident response lifecycle – from monitoring to actual response time – points to a growing demand for rigorous preparedness anchored by up-to-date incident response policies and trusted processes.

Key Questions to Consider

- Does the information security team and leadership have appropriate visibility?
- What is the current state of your organization’s security-event monitoring and security-incident response capabilities? On what basis do you rate this?
- Is your security-event monitoring support being performed in-house, through a managed security services provider (MSSP) or both? Is this effective for you? How do you determine that?
- Does your organization have a security/privacy strategy in place? If so, how is the strategy communicated throughout the organization, as well as monitored and audited?
- Does the IT strategy include an incident response plan? Has this plan been updated to include potential events stemming from new technologies (mobile/cloud) or application approaches (social media)?
- Have the right functions/people been involved in the creation of the incident response plan?
- Are third-party vendors and trading partners addressed in your security/privacy strategy?
- How is vendor compliance with your security and privacy policies and standards (including incident response preparedness) monitored?
- How are internal security threats monitored, managed and communicated?
- How would you rate your company’s data-security incident response preparedness? What is your approach to rating this?
- What steps are in place to test and improve incident response speed as well as the quality of the overall incident response capability?
- How well does the IT function and senior management team understand what comprises “sensitive” organizational data and information?

- How clear is your organization regarding which applications leverage sensitive information and who is afforded access to them?
- How are you classifying and managing your organization's data – both internally and through your third-party vendors?
- Is there a formal data classification program in use to help manage both the effectiveness and efficiency of the overall data security/privacy capability?
- Precisely who is responsible for monitoring IT's compliance with relevant legal and regulatory requirements related to data security and privacy? How often? What is the performance trend?

Focus on CIOs/IT Executives and Large Companies

Managing Security and Privacy – Results for CIOs/IT Executives and Large Company Respondents			
Managing Security and Privacy	Overall	CIOs/IT Executives	Large Company Respondents
Developing and maintaining security and privacy standards	●	●	●
Monitoring security events	●	●	●
Implementing security/privacy solutions and strategies	●	●	●
Incident response success (containment, recovery)	●	●	●
Incident response policy and preparedness	●	●	●
Incident response reaction time	●	●	●
Managing user identities and access	●	●	●
Managing and classifying enterprise data	●	●	●
Managing application users	●	●	●
Managing IT users	●	●	●
Managing technical infrastructure configuration	●	●	●
Clarity about third-party compliance readiness (partners, vendors)	●	●	●
Managing contractors	●	●	●
Managing third-party vendors	●	●	●
California Security Breach Information Act (SB 1386)	●	●	●
U.S. Gramm-Leach-Bliley Act (GLBA)	●	●	●
U.S. Health Insurance Portability and Accountability Act (HIPAA)	●	●	●

 Significant Priority
Index of 6.0 or higher
  Moderate Priority
Index of 4.5 to 5.9

DEFINING IT GOVERNANCE AND STRATEGY

Key Findings

- IT strategy/organization priorities, which rank among the highest in our study, reflect a clear shift in objectives from leveraging technology investments in support of the business to protecting and enhancing business value.
- IT executives and their staffs are looking to enhance their contributions to the company's value by improving the integration and alignment of IT planning with business strategy and also by improving their use of key performance indicators (KPIs).
- To protect organizational value, respondents plan to develop and maintain better security and privacy standards while also improving the way IT costs and benefits are monitored.

Overall Results, Defining IT Governance and Strategy

Defining IT Governance and Strategy	Priority Index
Integration/alignment of IT planning and business strategy	6.5
Key performance indicators (KPIs)	6.5
Monitoring IT costs and benefits	6.5
Developing and maintaining enterprise information architecture	6.4
IT risk analysis and reporting	6.4
Long-term and short-term planning	6.4
Managing project quality	6.4
Monitoring and achieving legal/regulatory compliance	6.4
Defining metrics and measurements for monitoring IT performance	6.3
Developing and maintaining end user support policies and standards	6.3
Developing and maintaining operations management policies and standards	6.3
Maintaining IT controls design and operating effectiveness	6.3
Managing and monitoring policy exceptions	6.3
Reporting IT activities and performance	6.3
Defining IT roles and responsibilities	6.2
Defining organizational placement of the IT function	6.2
Negotiating, managing and monitoring customer service-level agreements (SLAs)	6.2
Negotiating, managing and monitoring information quality	6.2

Commentary

The integration of IT planning and business strategy ranks as the one of the highest overall priorities, among all categories, in this year's survey. This type of strategic undertaking also helps explain why 63 percent of respondents reported that their organizations are undergoing a major IT transformation. Without question, linking IT and business strategy is a top-of-mind issue for today's IT functions.

According to our results, IT executives and professionals also recognize the important relationship between protecting value and enabling value. As the business value companies derive from their data and information assets increases, the value of these assets – and therefore the need to protect them – also rises. This explains, in great part, why developing and maintaining security and privacy standards, monitoring IT costs and benefits, and monitoring and achieving legal/regulatory compliance also qualify as top priorities.

In addition, IT leaders and their teams are committed to improving the way IT costs and benefits and IT performance (through KPIs) are monitored and measured. They are benchmarking themselves to demonstrate the value they bring as well as highlight areas for improved performance, showing a desire to manage their transformative activities in a way that positively affects the bottom line.

Key Questions to Consider

- To what extent are the CIO and IT leadership team collaborating with the business to identify potential business opportunities and threats proactively that require IT support and inclusion in IT planning?
- To what degree is your IT planning integrated and aligned with business strategy? How is your senior IT leadership team working to ensure this alignment exists and is sustained as the business strategy changes?
- How can the IT function's long-term and/or short-term planning be improved?
- Is the IT strategy enabled by IT risk analysis and reporting?
- Who is responsible for developing, evaluating, maintaining and monitoring data security and privacy standards?
- How is IT working with the finance, compliance and/or risk function to improve the effectiveness and efficiency of IT's compliance management program and processes?
- How are IT costs and benefits – and IT performance – measured, monitored and managed?
- What sort of benchmarking activities are used to compare the IT function's performance to other IT organizations?

Focus on CIOs/IT Executives and Large Companies

Defining IT Governance and Strategy – Results for CIOs/IT Executives and Large Company Respondents			
Defining IT Governance and Strategy	Overall	CIOs/IT Executives	Large Company Respondents
Integration/alignment of IT planning and business strategy	●	●	●
Key performance indicators (KPIs)	●	●	●
Monitoring IT costs and benefits	●	●	●
Developing and maintaining enterprise information architecture	●	●	●
IT risk analysis and reporting	●	●	●
Long-term and short-term planning	●	●	●
Managing project quality	●	●	●
Monitoring and achieving legal/regulatory compliance	●	●	●
Defining metrics and measurements for monitoring IT performance	●	●	●
Developing and maintaining end user support policies and standards	●	●	●
Developing and maintaining operations management policies and standards	●	●	●
Maintaining IT controls design and operating effectiveness	●	●	●
Managing and monitoring policy exceptions	●	●	●
Reporting IT activities and performance	●	●	●
Defining IT roles and responsibilities	●	●	●
Defining organizational placement of the IT function	●	●	●
Negotiating, managing and monitoring customer service-level agreements (SLAs)	●	●	●
Negotiating, managing and monitoring information quality	●	●	●

 Significant Priority
Index of 6.0 or higher
  Moderate Priority
Index of 4.5 to 5.9

MANAGING APPLICATION DEVELOPMENT

Key Findings

- Protecting value – via risk management and security – is among the application development priorities.
- Other key areas of focus include collaboration platforms such as SharePoint, and mobile application development.

Overall Results, Managing Application Development

Managing Application Development	Priority Index
Risk management	6.1
Collaboration platforms (for example, SharePoint)	6.0
ERP application security	6.0
Mobile application development	6.0
Project monitoring and control	6.0
Requirements management	6.0
Configuration management	5.9
Decision analysis and resolution	5.9
ERP system "bolt-on" applications (BI, CRM, etc.)	5.9
ERP system implementation	5.9
Organizational performance management	5.9
Software selection	5.9
ERP system selection	5.8
Object-oriented programming	5.8
Organizational process performance	5.8
Organizational training	5.8
Scrum development methodology	5.7
Spiral iterative framework	5.7
Spreadsheet risk	5.7

Commentary

IT organizations clearly want to strengthen risk management practices surrounding application development. This focus applies both to the development of mobile apps as well as to more traditional areas, including the security of ERP, business applications and the software – such as business intelligence and customer relationship management (CRM) systems – integrated with these enterprise systems.

Along with strengthening risk management, other specific components of application development, including the use of collaborative platforms (e.g., Microsoft SharePoint) and improved project monitoring and control, requirements management and configuration management, rank as key priorities.

Another notable priority is project monitoring and control. This reflects a need among many organizations to improve project management capabilities and implement more robust project portfolio management.

Key Questions to Consider

- How can risks related to applications development be managed more effectively? What are the top risks that exist, and how can these issues be addressed?
- Has your overall ERP system security kept pace with changes to the data environment, as well as the system's integration with newer applications (e.g., CRM, BI, BPM, HRIS, etc.)?
- How do you manage and monitor risks related to application development as the nature of applications under development changes?
- Is the IT function managing mobile application development in a secure manner that helps drive business value?
- Are collaboration platforms deployed in a way that enhances application development?
- Are project monitoring and controls applied to the development process current and effective?

Focus on CIOs/IT Executives and Large Companies

Managing Application Development – Results for CIOs/IT Executives and Large Company Respondents			
Managing Application Development	Overall	CIOs/IT Executives	Large Company Respondents
Risk management	●	●	●
Collaboration platforms (for example, SharePoint)	●	●	●
ERP application security	●	●	●
Mobile application development	●	●	●
Project monitoring and control	●	●	●
Requirements management	●	●	●
Configuration management	●	●	●
Decision analysis and resolution	●	●	●
ERP system "bolt-on" applications (BI, CRM, etc.)	●	●	●
ERP system implementation	●	●	●
Organizational performance management	●	●	●
Software selection	●	●	●
ERP system selection	●	●	●
Object-oriented programming	●	●	●
Organizational process performance	●	●	●
Organizational training	●	●	●
Scrum development methodology	●	●	●
Spiral iterative framework	●	●	●
Spreadsheet risk	●	●	●

● Significant Priority
Index of 6.0 or higher
● Moderate Priority
Index of 4.5 to 5.9

DEPLOYING AND MAINTAINING SOLUTIONS

Key Findings

- IT functions are focused on managing changes in third-party applications, as well as applications developed in-house.
- Managing the system development lifecycle – the developing and acquiring of applications – also ranks high on the IT priorities list.

Overall Results, Deploying and Maintaining Solutions

Deploying and Maintaining Solutions	Priority Index
Developing and maintaining application interfaces	6.1
Managing changes – third-party applications	6.1
Managing changes – applications developed in-house	6.1
Developing applications	6.0
Acquiring applications	5.9

Commentary

Based on these results, it appears organizations are struggling with coordination across the business as they deploy solutions and updates. They also are challenged with deploying solutions that are owned by a third party and perhaps even hosted offsite.

Key Questions to Consider

- Who is responsible for overseeing changes to third-party applications?
- How is this process monitored and audited?
- Who is responsible for deciding whether a new application should be developed internally or acquired?

Focus on CIOs/IT Executives and Large Companies

Deploying and Maintaining Solutions – Results for CIOs/IT Executives and Large Company Respondents			
Deploying and Maintaining Solutions	Overall	CIOs/IT Executives	Large Company Respondents
Developing and maintaining application interfaces	●	●	●
Managing changes – third-party applications	●	●	●
Managing changes – applications developed in-house	●	●	●
Developing applications	●	●	●
Acquiring applications	●	●	●



Significant Priority
Index of 6.0 or higher



Moderate Priority
Index of 4.5 to 5.9

MANAGING IT INFRASTRUCTURE

Key Findings

- There is increasing emphasis on improving the management and administration of backup and recovery, along with a need for better storage management and planning.
- IT functions also are looking to strengthen database change management, IT infrastructure change management, job processing and network performance planning.

Overall Results, Managing IT Infrastructure

Managing IT Infrastructure	Priority Index
Managing and administering backup and recovery	6.3
Storage management and planning	6.2
Database change management	6.1
IT infrastructure change management	6.1
Managing and maintaining job processing	6.1
Network performance planning	6.1
Operating system change management	6.1
Managing data center environmental controls	6.0
Platform performance planning	6.0

Commentary

As organizational supplies of data surge, the need to store, manage and protect (i.e., back up) this data, particularly in the cloud, becomes more complicated. Increased and better data storage and data-management techniques are required to harness the potential value of this raw information. This area often requires large doses of tactical and technical work, a fact that accounts for needing additional resources ranking as a key priority elsewhere in our survey.



More important, these priorities clearly reflect the emerging responsibilities of IT as a key enabler of business success and continuity. The push for these improvements frequently originates from strategic concerns identified by executive management and the board of directors, who realize that planning and managing the technical infrastructure well is key to the success and resilience of the business.

Key Questions to Consider

- Are our current storage, management, backup and recovery capabilities keeping pace with our organization's growing supply of data, and are future capabilities appropriately planned?
- Do our storage management capabilities support and align with the ways in which we classify, manage and protect our organizational data?
- Are our data center operations meeting current processing needs as well as the requirements of our business continuity management (BCM) policies and programs?
- Are BCM considerations integrated into storage-management investment decision-making?
- How does our IT function ensure we continue to meet rising business demands with regard to network performance?

Focus on CIOs/IT Executives and Large Companies

Managing IT Infrastructure – Results for CIOs/IT Executives and Large Company Respondents			
Managing IT Infrastructure	Overall	CIOs/IT Executives	Large Company Respondents
Managing and administering backup and recovery	●	●	●
Storage management and planning	●	●	●
Database change management	●	●	●
IT infrastructure change management	●	●	●
Managing and maintaining job processing	●	●	●
Network performance planning	●	●	●
Operating system change management	●	●	●
Managing data center environmental controls	●	●	●
Platform performance planning	●	●	●

 Significant Priority
Index of 6.0 or higher
  Moderate Priority
Index of 4.5 to 5.9

MANAGING IT ASSETS

Key Findings

- Monitoring and accounting for IT assets has grown more complex due to smart device proliferation, growing workforce mobility and the IT function's reliance on external partners.
- In this environment, software and hardware deployment, along with managing software licensing and compliance, are the most significant IT asset management priorities.
- Of particular concern are retirement issues, including but not limited to licensing recovery and sensitive data contained on retired assets.

Overall Results, Managing IT Assets

Managing IT Assets	Priority Index
Software deployment	6.2
Hardware deployment	6.1
Managing software licensing and compliance	6.1
Accounting for IT asset management	5.9
Determining outsourcing strategy and approach	5.9
Managing audit process (SAS 70, SSAE 16, others)	5.9
Managing contract analysis and renewal	5.9
Managing hardware maintenance agreements	5.9
Managing IT asset retirement – IT asset refresh	5.9
Monitoring and reviewing contracts/billings	5.9
Monitoring external service-level agreements	5.9
Monitoring IT assets	5.9
Negotiating and establishing agreements	5.9
Managing IT asset retirement – employee/contractor termination	5.8

Commentary

If a company's IT asset management approach isn't transforming, it should be. The steady adoption of smartphones and tablets, along with the recent and rapid adoption of cloud computing, software-as-a-service models and business apps, has greatly complicated IT asset management processes. Mobile commerce, social media proliferation for business purposes and BYOD practices are further dividing the attention of IT managers, pointing to the need for clear and comprehensive asset management policies.

Given these new and complex challenges amid a flurry of new devices and mobile apps, it is no wonder that we find the deployment of software and hardware at the top of the priority list in this category, together with licensing and compliance issues. Equally important is the retirement of hardware and software assets.

Furthermore, organizations have been challenged to deploy enterprise software solutions, such as Microsoft Windows versions. Such deployments have a strong impact on the business and usually require multiple years to complete successfully.

Key Questions to Consider

- How can IT collaborate more effectively with the procurement, finance and accounting, and compliance functions to ensure that external relationships involving IT assets are structured, managed and monitored in a risk-savvy manner?
- Who is responsible for network planning and engineering, and ensuring any network build-out is right-sized?
- Are third-party agreements concerning IT assets managed in accordance with relevant auditing standards, such as SSAE 16 (the standard that replaced the legacy SAS 70 audits)?
- Who is responsible for creating, maintaining and monitoring controls and other risk-management considerations related to the deployment, maintenance and retirement of software and hardware assets?
- What policies (e.g., infrastructure, operations, BYOD, mobile commerce) govern the deployment and retirement of IT hardware and software assets?
- Are your current ITAM policies, processes and technologies, and organizational structure (people, roles, etc.) sufficient in light of the rapidly evolving nature of certain IT assets?

Focus on CIOs/IT Executives and Large Companies

Managing IT Assets – Results for CIOs/IT Executives and Large Company Respondents			
Managing IT Assets	Overall	CIOs/IT Executives	Large Company Respondents
Software deployment	●	●	●
Hardware deployment	●	●	●
Managing software licensing and compliance	●	●	●
Accounting for IT asset management	●	●	●
Determining outsourcing strategy and approach	●	●	●
Managing audit process (SAS 70, SSAE 16, others)	●	●	●
Managing contract analysis and renewal	●	●	●
Managing hardware maintenance agreements	●	●	●
Managing IT asset retirement – IT asset refresh	●	●	●
Monitoring and reviewing contracts/billings	●	●	●
Monitoring external service-level agreements	●	●	●
Monitoring IT assets	●	●	●
Negotiating and establishing agreements	●	●	●
Managing IT asset retirement – employee/contractor termination	●	●	●

 Significant Priority
Index of 6.0 or higher
  Moderate Priority
Index of 4.5 to 5.9

MANAGEMENT AND USE OF DATA ASSETS

Key Findings

- Multiple areas within data asset management, from governance and business intelligence to master data management (MDM), analytics support and data lifecycle management, are key priorities.

Overall Results, Management and Use of Data Assets

Management and Use of Data Assets	Priority Index
Business intelligence and reporting tools	6.1
Data analytics platforms and support	6.1
Data and information governance program	6.1
Data lifecycle management	6.1
Master data management	6.1
Short- and long-term enterprise information management strategy	6.1
Big data initiatives	5.9
End user adoption of data tools	5.9

Commentary

With advances in cloud computing, software-as-a-service models and data analytics, it has become very difficult to discuss IT asset management without assessing the need to better manage business intelligence and organizational data – wherever it resides. According to our survey, 70 percent of organizations use offshore resources to augment and support their IT activities. This illustrates one important way in which data asset management differs from traditional IT asset management – where the asset is located. This translates into different management tactics for IT assets and data assets.

Organizations are continuing to struggle with how to get at data and derive value from it. They also are being challenged by legacy infrastructure that supports data repositories, which can limit the ability to access data in more meaningful ways.

Our survey results indicate that organizations consider the creation and maintenance of a data and information governance program to be a foundational element of sound data asset management. Thus, master data management and data analytics platforms are clear priorities for IT organizations. These priorities point to an increased understanding of the IT function's role as the organization's protector of value (managing master data in a secure manner) and enhancer of business value (by providing and managing the analytics that underpin strategic decisions).

Key Questions to Consider

- Does your organization have a formal data and information governance program in place? If so, who is responsible for overseeing the program?
- How is this program communicated and monitored throughout the organization?
- How is IT working with internal audit to ensure that the data and information governance program is an effective risk-management mechanism?
- Is the IT function regularly conducting short- and long-term enterprise information planning?
- How is this information planning integrated into IT planning and overall business strategy?
- Are data assets managed in a way that is both secure and able to drive business value through specific capabilities and tools, including data analytics and business intelligence?
- How is master data management quality/security governed and monitored?
- What are the most important data-related risks related to the use of third-party vendors and outsourcers, and how are these risks managed and monitored?
- How are external vendors' data management practices integrated into internal audit's work plans?

Focus on CIOs/IT Executives and Large Companies

Management and Use of Data Assets – Results for CIOs/IT Executives and Large Company Respondents			
Management and Use of Data Assets	Overall	CIOs/IT Executives	Large Company Respondents
Business intelligence and reporting tools	●	●	●
Data analytics platforms and support	●	●	●
Data and information governance program	●	●	●
Data lifecycle management	●	●	●
Master data management	●	●	●
Short- and long-term enterprise information management strategy	●	●	●
Big data initiatives	●	●	●
End user adoption of data tools	●	●	●

 Significant Priority
Index of 6.0 or higher
  Moderate Priority
Index of 4.5 to 5.9

ENSURING CONTINUITY

Key Findings

- IT functions are focusing on the development, ongoing maintenance and testing of business continuity programs and IT disaster recovery plans.
- Another key priority is ensuring that IT aspects of BCM programs align with business objectives and needs, and have the support of executive management.

Overall Results, Ensuring Continuity

Ensuring Continuity	Priority Index
Business continuity management and disaster recovery program testing	6.2
Developing and maintaining IT disaster recovery plans	6.2
Ensuring business alignment	6.2
Designing and maintaining business continuity strategies	6.1
Ensuring executive management support and sponsorship	6.1
Developing and maintaining business resumption plans	6.0
Developing and maintaining crisis management plans	6.0
Developing and maintaining risk assessment/business impact analysis	6.0

Commentary

Extreme weather events and global supply chains, along with the ever-increasing challenge of supporting a more mobile and remote workforce, are among the many reasons why companies should develop, maintain, monitor and continually upgrade their business continuity management (BCM) capabilities. Two years ago, global economic losses from natural disasters and other weather-related events cost the increasingly connected global economy \$186 billion in losses, sharply raising BCM-related questions in the minds of organization leaders.⁶ In addition, man-made forms of disruption – cyberattacks being among the most notable – also must be planned for from a BCM perspective.

To ensure effectiveness, a BCM program must be expansive: It should address business recovery requirements, strategy design, plan design and implementation, training and awareness, testing (including scenario planning) and ongoing maintenance, and compliance monitoring and auditing.⁷

With organizations relying overwhelmingly on technology systems, applications and data to conduct business, IT functions must provide leadership and initiative in BCM efforts – at both a strategic and tactical level. Our results show that IT professionals are sharply aware of the need for BCM initiatives and intend to focus significant resources on the development and maintenance of IT disaster recovery plans (a central component of BCM), as well as on the testing of BCM programs and specific plans. More importantly, they plan to ensure executive support and sponsorship in this effort and full alignment of their effort with the business plan overall – another indicator of the transformation of IT.

⁶ “U.S. Dominated Global Disaster Losses in 2012: Swiss Re,” by Andrew Freedman, ClimateCentral.org, April 1, 2013: www.climatecentral.org/news/us-dominated-global-disaster-losses-in-2012-insurer-reports-15814.


⁷ For more on BCM, see Protiviti’s *Guide to Business Continuity Management: Frequently Asked Questions, Third Edition*, 2013: www.protiviti.com/en-US/Documents/Resource-Guides/Guide-to-BCM-Third-Edition-Protiviti.pdf.

Key Questions to Consider

- Who in the IT function is responsible for developing and maintaining IT disaster recovery plans as well as ensuring that current IT considerations are addressed in the overall BCM program?
- Does IT play a central role in organizational BCM and disaster recovery activities?
- How are BCM considerations and requirements integrated into IT investment and procurement plans and processes?
- Are business interruptions and crises stemming from potential data breaches taken into account in your current BCM program?
- How is the BCM program monitored to ensure that it reflects changes to IT infrastructure, applications, external relationships and data?
- How are IT-related BCM and disaster recovery capabilities, activities and updates shared with executive management and the board of directors, and how is feedback from these levels incorporated into the BCM planning process?
- How frequently do you test the BCM plans that are in place? How are the results of these tests reviewed, analyzed and acted upon?
- How can new/emerging technology tools and capabilities be used to strengthen the effectiveness of the overall BCM program?

Focus on CIOs/IT Executives and Large Companies

Ensuring Continuity – Results for CIOs/IT Executives and Large Company Respondents			
Ensuring Continuity	Overall	CIOs/IT Executives	Large Company Respondents
Business continuity management and disaster recovery program testing	●	●	●
Developing and maintaining IT disaster recovery plans	●	●	●
Ensuring business alignment	●	●	●
Designing and maintaining business continuity strategies	●	●	●
Ensuring executive management support and sponsorship	●	●	●
Developing and maintaining business resumption plans	●	●	●
Developing and maintaining crisis management plans	●	●	●
Developing and maintaining risk assessment/ business impact analysis	●	●	●

 Significant Priority
Index of 6.0 or higher
  Moderate Priority
Index of 4.5 to 5.9

ORGANIZATIONAL CAPABILITIES

Key Findings

- Leadership (within your organization), recruiting IT talent, working effectively with executives, and coaching/mentoring mark the top priorities.

Overall Results, Organizational Capabilities

Organizational Capabilities	Priority Index
Leadership (within your organization)	6.0
Recruiting IT talent	6.0
Working effectively with business-unit executives	6.0
Working effectively with C-level/senior executives	6.0
Coaching/mentoring	5.9
Working effectively with outside parties	5.9
Working effectively with regulators	5.9
Dealing with confrontation	5.8
Developing outside contacts/networking	5.8
Leadership (in outside organizations, groups, etc.)	5.8
Leveraging outside expertise	5.8
Negotiation	5.8
Six Sigma	5.8

Commentary

All of the priorities identified by respondents in this category involve important relationships that IT professionals maintain throughout – and beyond – the organization.

To strengthen and expand their own skill sets, CIOs and IT executives and professionals are looking to build better relationships with C-level executives, business-unit executives and the board of directors. Senior-level IT executives also expressed a desire to strengthen their relationships with regulators, a crucial activity given the high probability of new data-security regulations and rules coming down the pike soon. In addition, our respondents reported that they are interested both in the recruitment of IT talent (including the possibility of bringing in nontraditional candidates for certain IT roles) and in leveraging outside resources to meet their burgeoning responsibilities.

These priorities provide further evidence that IT is no longer an island. Instead, CIOs and their staffs are pursuing organizational goals that will help them thrive as business collaborators, business-value builders and business leaders.

Key Questions to Consider

- Does IT leadership provide formal and informal opportunities for staff to work with, and learn from, business colleagues throughout the organization as well as with business-unit and C-level executives?
- Are current IT recruitment and talent management practices meeting the function's resource needs? How might these practices be strengthened to meet future resource needs?
- How are senior IT executives working with, and learning from, their partners in the legal, compliance and risk management functions to build and strengthen their own relationships with regulators?
- What monitoring and communications mechanisms are in place to ensure that IT professionals stay informed of emerging legislative and regulatory developments that could affect the IT organization?
- What leadership development offerings (formal and informal) are made available to rising IT managers?
- How can coaching/mentoring offerings be made available to a larger number of IT managers and staff?

Focus on CIOs/IT Executives and Large Companies

Organizational Capabilities – Results for CIOs/IT Executives and Large Company Respondents			
Organizational Capabilities	Overall	CIOs/IT Executives	Large Company Respondents
Leadership (within your organization)	●	●	●
Recruiting IT talent	●	●	●
Working effectively with business-unit executives	●	●	●
Working effectively with C-level/senior executives	●	●	●
Coaching/mentoring	●	●	●
Working effectively with outside parties	●	●	●
Working effectively with regulators	●	●	●
Dealing with confrontation	●	●	●
Developing outside contacts/networking	●	●	●
Leadership (in outside organizations, groups, etc.)	●	●	●
Leveraging outside expertise	●	●	●
Negotiation	●	●	●
Six Sigma	●	●	●

 Significant Priority
Index of 6.0 or higher
  Moderate Priority
Index of 4.5 to 5.9

METHODOLOGY AND DEMOGRAPHICS

More than 1,100 respondents, including chief information officers, chief technology officers, chief security officers, chief information security officers, and other IT executives and professionals, participated in our study, which was conducted within the past 90 days. We are very appreciative and grateful for the time invested in our study by these individuals.

All demographic information was provided voluntarily and not all participants provided data for every demographic question.

Position

Chief Information Officer	8%
Chief Security Officer	11%
Chief Information Security Officer	9%
Chief Privacy Officer	3%
Chief Technology Officer	6%
Chief Financial Officer	3%
IT VP/Director	16%
IT Manager	22%
General Manager	4%
Supervisor	5%
Other	13%

Industry

Manufacturing	19%
Technology	19%
Professional Services	8%
Financial Services	7%
Energy	5%
Retail	5%
Telecommunications	5%
Healthcare	4%
Government/Education/Not-for-profit	3%
Insurance	3%
Services	3%

Communications	2%
Consumer Products	2%
Media	2%
Real Estate	2%
Utilities	2%
Other	9%

Size of Organization (by Gross Annual Revenue)

\$20 billion or greater	10%
\$10 billion - \$19.99 billion	8%
\$5 billion - \$9.99 billion	13%
\$1 billion - \$4.99 billion	26%
\$500 million - \$999.99 million	21%
\$100 million - \$499.99 million	11%
Less than \$100 million	11%

Type of Organization

Public	37%
Private	53%
Not-for-profit	3%
Government	6%
Other	1%

Organization Headquarters

North America	91%
South America	6%
Asia Pacific	1%
Europe	1%
Middle East	1%

ABOUT PROTIVITI

Protiviti (www.protiviti.com) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit, and has served more than 35 percent of FORTUNE 1000® and FORTUNE Global 500® companies. Protiviti and its independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

About Our IT Consulting Services

In today's rapidly evolving technological environment, a trusted adviser – one who not only provides relevant insights, but delivers a combination of strategic vision, proven expertise and practical experience – can enhance the value of your business with technology.

Our global IT Consulting practice has helped CIOs and IT leaders at more than 1,200 companies worldwide design and implement advanced solutions in IT governance, security, data management, applications and compliance. By partnering with us, you ensure that your IT organization performs with the same focus and excellence with which you manage day-to-day business operations. We will work with you to address IT security and privacy issues and deploy advanced and customized application and data management structures that not only solve problems, but add value to your business.

PROTIVITI GLOBAL IT CONSULTING PRACTICE

Kurt Underwood
Global Leader – IT Consulting
kurt.underwood@protiviti.com

GLOBAL IT CONSULTING MANAGING DIRECTORS

Tom Andreesen
thomas.andreesen@protiviti.com

Samir Datt
samir.datt@protiviti.com

Hernan Gabrieli
hernan.gabrieli@protiviti.it

John Harrison
john.harrison@protiviti.com

Greg Hedges
gregory.hedges@protiviti.com

Rob Hustick
rob.hustick@protiviti.com

Senthil Kumar
senthil.kumar@protivitiglobal.com.kw

Mike Lane
michael.lane@protiviti.com

Sidney Lim
sidney.lim@protiviti.com

Mark Lippman
mark.lippman@protiviti.com

Chris Loudon
christopher.louden@pgs.protiviti.com

Masato Maki
masato.maki@protiviti.jp

Ronan O'Shea
ronan.oshea@protiviti.com

Ed Page
ed.page@protiviti.com

Michael Pang
michael.pang@protiviti.com

Michael Porier
michael.porier@protiviti.com

Aric Quinones
aric.quinones@protiviti.com

Siamak Razmazma
siamak.razmazma@protiviti.com

Anthony Samer
anthony.samer@protiviti.com

Mike Steadman
mike.steadman@protiviti.com

Andrew Struthers-Kennedy
andrew.struthers-kennedy@protiviti.com

David Taylor
david.taylor@protiviti.com

Tomomichi Tomiie
tomomichi.tomiie@protiviti.jp

SOLUTION THOUGHT LEADERS

Managing the Business of IT

IT Governance & Risk Management

Jonathan Wyatt
jonathan.wyatt@protiviti.co.uk

IT Operations Improvement

Jeff Weber
jeffrey.weber@protiviti.com

Portfolio & Program Management

Steve Cabello
steve.cabello@protiviti.com

Strategy & Alignment

Michael Schultz
michael.schultz@protiviti.com

Managing Security & Privacy

Security Strategy & Policy

Cal Slemp
cal.slemp@protiviti.com

Identity & Access Management

Ryan Rubin
ryan.rubin@protiviti.co.uk

Incident Response & Forensics

Rocco Grillo
rocco.grillo@protiviti.com

Security Operations Centers

Michael Walter
michael.walter@protiviti.com

Data Security & Privacy

Jeff Sanchez
jeffrey.sanchez@protiviti.com

Vulnerability & Penetration Testing

Scott Laliberte
scott.laliberte@protiviti.com

Managing Applications & Data

Software Services

Scott Gracyalny
scott.gracyalny@protiviti.com

Business Intelligence

Matt McGivern
matt.mcgivern@protiviti.com

ERP Solutions

Carol Raimo
carol.raimo@protiviti.com

Risk Technologies

Scott Wisniewski
scott.wisniewski@protiviti.com

THE AMERICAS

UNITED STATES

Alexandria	Kansas City	Salt Lake City
Atlanta	Los Angeles	San Francisco
Baltimore	Milwaukee	San Jose
Boston	Minneapolis	Seattle
Charlotte	New York	Stamford
Chicago	Orlando	St. Louis
Cincinnati	Philadelphia	Tampa
Cleveland	Phoenix	Washington, D.C.
Dallas	Pittsburgh	Winchester
Denver	Portland	Woodbridge
Fort Lauderdale	Richmond	
Houston	Sacramento	

ARGENTINA*

Buenos Aires

CHILE*

Santiago

PERU*

Lima

BRAZIL*

Rio de Janeiro
São Paulo

MEXICO*

Mexico City
Monterrey

VENEZUELA*

Caracas

CANADA

Kitchener-Waterloo
Toronto

ASIA-PACIFIC

AUSTRALIA

Brisbane
Canberra
Melbourne
Perth
Sydney

INDIA

Bangalore
Mumbai
New Delhi

INDONESIA**

Jakarta

CHINA

Beijing
Hong Kong
Shanghai
Shenzhen

JAPAN

Osaka
Tokyo

SINGAPORE

Singapore

SOUTH KOREA

Seoul

EUROPE/MIDDLE EAST/AFRICA

FRANCE

Paris

ITALY

Milan
Rome
Turin

THE NETHERLANDS

Amsterdam

GERMANY

Frankfurt
Munich

UNITED KINGDOM

London

BAHRAIN*

Manama

QATAR*

Doha

KUWAIT*

Kuwait City

UNITED ARAB EMIRATES*

Abu Dhabi
Dubai

OMAN*

Muscat

SOUTH AFRICA*

Johannesburg

* Protiviti Member Firm

** Protiviti Alliance Member