DECEMBER 2012

BUSINESS TECHNOLOGY OFFICE

Protecting information in the cloud

IT and business executives need to apply a risk-management approach that balances economic value against risks.

James Kaplan, Chris Rezek, and Kara Sprague

The use of highly scaled, shared, and automated IT platforms—known as cloud computing—is growing rapidly. Adopters are driven by the prospects of increasing agility and gaining access to more computing resources for less money. Large institutions are building and managing private-cloud environments internally (and, in some cases, procuring access to external public clouds) for basic infrastructure services, development platforms, and whole applications. Smaller businesses are primarily buying public-cloud offerings, as they generally lack the scale to set up their own clouds.

As attractive as cloud environments can be, they also come with new types of risks. Executives are asking whether external providers can protect sensitive data and also ensure compliance with regulations about where certain data can be stored and who can access the data. CIOs and CROs are also asking whether building private clouds creates a single point of vulnerability by aggregating many different types of sensitive data onto a single platform.

Blanket refusals to make use of private- or public-cloud capabilities leave too much value on the table from savings and improved flexibility. Large institutions, which have many types of sensitive information to protect and many cloud solutions to choose from, must balance potential benefits against, for instance, risks of breaches of data confidentiality, identity and access integrity, and system availability.

The cloud is here to stay

Refusing to use cloud capabilities is not a viable option for most institutions. The combination of improved agility and a lower IT cost base is spurring large enterprises to launch concerted programs to use cloud environments. At the same time, departments, work groups, and individuals often take advantage of low-cost,

Takeaways

Even companies that have so far resisted cloud computing may soon find that opting out is no longer a viable strategy, given the twin imperatives of increasing agility and reducing costs.

Rather than forbidding use of the cloud, organizations must understand the risks and benefits of both public- and private-cloud offerings.

A business-focused risk-management approach can allow large institutions to protect their data while taking advantage of more efficient, flexible solutions.

easy-to-buy public-cloud services—even when corporate policies say they should not.

High growth and value expectations

Corporate spending on third-party-managed and public-cloud environments will grow from $28 billion in 2011 to more than $70 billion in 2015, according to IDC. However, total spending on the cloud is much larger than these estimates indicate because the figures do not reflect what enterprises spend on their private-cloud environments. Eighty percent of large North American institutions surveyed by McKinsey are planning or executing programs to make use of cloud environments to host critical applications—mostly by building private-cloud environments. At several of these institutions, executives predict that 70 to 75 percent of their applications will be hosted in cloud environments that will enable savings of 30 to 40 percent compared with current platforms.

Using external cloud offerings can yield even more pronounced savings. Some executives cite examples of 60 to 70 percent savings by replacing custom-developed internal applications with software-as-a-service alternatives sourced from the public cloud. In addition, according to recent McKinsey research, 63 percent of business leaders who responded agreed that the cloud can make their entire organization more business agile and responsive.

The rise of bottom-up adoption

Truly cloud-free organizations are extremely rare—and in fact may not exist at all. If you think you are the exception, you are probably wrong. Regardless of any “no cloud” policy, the democratized nature of cloud purchasing reduces the middleman role played by traditional IT departments and makes central control difficult. Users are subscribing directly to cloud services, from online storage and backup to media services and customer-relationship-management solutions, paying via credit card. Developers are using infrastructure-as-a-service and platform-as-a-service solutions for testing code and sometimes for hosting applications.

Ironically, forbidding cloud offerings may lead to users subscribing to less secure solutions. An employee using a credit card may not be sufficiently security inclined or aware to purchase the enterprise-class version of cloud software. That same individual might have been perfectly willing to use cloud service providers endorsed by his or her organization had they been available.

Risks and opportunities

Using the cloud creates data-protection challenges in public-cloud services as well as private-cloud environments. However, traditional platforms at most organizations have significant information risks that actually can be mitigated by moving to a more highly scaled and automated environment.

Risk of contracting for public cloud

Decades of experience matured the practice of writing contracts for telecommunications network services and traditional outsourcing arrangements. Terms and conditions exist for allocating liability for security breaches, downtime, and noncompliance events between providers and enterprises. They may be unwieldy, but they are well understood by providers, law firms, and—in many cases—CIOs and CROs.

Contracting for the cloud is different in many ways. Highly scaled, shared, and automated IT platforms, for example, can obscure the geographic location of data from both the provider and customer. This is a problem for institutions dealing in personally identifiable information because often they must keep some customer data in certain jurisdictions and face regulatory action if they do not. At this point, banking CIOs and CROs that we have interviewed largely do not believe that most public-cloud providers can give them the guarantees they require to protect their institutions from this type of regulatory action. Another novel challenge presented by the cloud is how to conform to regulatory and industry standards that have not yet been updated to reflect cloud architectures.

At some level, for the cloud, we are simply in the early days of contracting for enterprise-class services. How to draft the required terms and conditions will remain an open question until litigation has identified the critical issues and legal precedent has been established for resolving those issues.

Risk of aggregation in private-cloud environments

The current state of data fragmentation at many enterprises provides a peculiar kind of risk-management benefit. Dispersing sensitive customer data across many platforms means that a problem in one platform will affect only a subset of a company's information. Fragmentation may also limit the impact of a security breach, as different platforms often have varying security protocols.

In contrast, consolidating applications and data in shared, highly scaled private-cloud environments increases the honeypot for malevolent actors. There's much more valuable data in one place, which raises the stakes for being able to protect data.

Risk-management advantages of the public and private cloud

Both public- and private-cloud solutions can provide data-protection advantages compared with traditional, subscale technology environments. Cloud solutions improve transparency—for example, the centralized and virtualized nature of the cloud can simplify log and event management, allowing IT managers to see emerging security or resiliency problems earlier than might otherwise be possible. Likewise, in cloud environments, operators can solve problems once and apply the solutions universally by using robust automation tools.

Perhaps more important, technology organizations can focus investments in security capabilities on a small number of highly scaled environments.

A risk-management approach to exploiting the cloud

In many large institutions, information security traditionally has been a control function that used policies limiting what IT managers and end users could do in order to reduce the likelihood of data loss, privacy breaches, or noncompliance with regulations. We believe that IT organizations must now adopt a business-focused risk-management approach that engages business leaders in making trade-offs between the economic gains that cloud solutions promise and the risks they entail. It is still the early days of cloud computing, and risk-management decisions are highly dependent on the specifics

Exhibit 1
Comparing deployment models highlights options.

		Physical location	Physical segregation	Operational control
Traditional deployment	**Traditional on premises**	On premises	Yes	Customer
	Traditional off premises[1]	Off premises	Yes	Shared
Cloud deployment	**Private on premises**[1]	On premises	Yes	Customer
	Virtual private[1]	Off premises	No	Shared
	Community[1]	Off premises	No	Shared
	Private off premises	Off premises	Yes	Shared
	Public/multitenant[1]	Off premises	No	Vendor

[1]Deployments may be geography specific, geography agnostic, or geography ignorant (ie, you may or may not know where data are physically stored).

of the situation, so there are no hard-and-fast rules. However, some rough principles for managing cloud-information risk are emerging.

Consider the full range of cloud contracting models

"Public cloud" and "private cloud" are useful simplifications, but there are other models (Exhibit 1) that may provide attractive combinations of control and opportunities to tap vendor capabilities:

- One option is on-premises managed private-cloud services, in which third-party vendors provide a service that operates like an external cloud offering but is located in an enterprise's own facility and is dedicated to the organization.

- Some flavors of virtual private clouds can be used; these are similar to public clouds in that the solution is externally managed, but like private clouds, they offer dedicated capacity, such as resource pools, that are reserved for each client.

- Community clouds feature infrastructure that is shared by several organizations and meets the needs of a specific community of users. Community clouds may, for example, provide industry-specific solutions that ensure compliance with relevant regulations.

To complicate things further, the maturity of technological and organizational solutions varies by deployment type and by application, vendor, and specific configuration.

Pursue a mixed-cloud strategy

Different workloads and data sets have vastly different stakes when it comes to data protection, depending on the nature of the application and which phase of the software life cycle it supports—for instance, development and test

versus live production. The public cloud can be a good option for developing and testing software, since this usually does not involve sensitive data. Any workload that includes personally identifiable customer information will require careful consideration before it could be hosted in a public-cloud environment. Control of data access is also important in order to protect confidential business information and intellectual property. Essentially, any

Exhibit 2
Data must be managed and protected.

Types of information[1]		Typical workloads
Confidential business information	• Trade secrets (eg, formulae, designs, methods, processes, code, devices) • Financial, tax, and insurance records (eg, transactions, trades, revenues, costs, prices, compensation) • Operations data (eg, enterprise resource planning, supply-chain management, customer-relationship management) • Other commercial information (eg, marketing plans, customer lists, contracts, IT architecture)	• Enterprise apps • Content creation and management • Transaction management
Published intellectual property	• Copyright (eg, digital-rights management, media) • Patent (eg, designs, processes) • Trademark (eg, graphics, URLs)	• Content distribution • Engineering, design apps • Content creation and management
Legal/ e-discovery (eg, communication, working papers)	• Generally legal-mandated retention (eg, e-mails, memos, phone logs) • Specific lawsuit- or subpoena-driven retention • Internal-policy-governed retention and destruction • Nonmandated retention (eg, phone calls, videoconferences)	• Communication (eg, voice over Internet protocol, e-mail) • Collaboration apps (eg, wikis)
Regulated information	• HR and employment (eg, Equal Educational Opportunities Act, Americans with Disabilities Act) • Medical (eg, Health Insurance Portability and Accountability Act) • Financial (eg, Fair and Accurate Credit Transactions Act) • Governmental (eg, Freedom of Information Act, Video Privacy Protection Act) • Technology and telecommunications (eg, customer proprietary network information) • Other regulated information	• Hospital-information systems apps (health/medical) • HR apps • Monitoring/audit
IT information	• Activity and access logs (for dynamic monitoring, audits) • Policy, rules, and authorizations • Identity and authentication	• Systems management • Security/identity • Process/policy

[1]While data are paramount, any evaluation should also address infrastructure, applications, and people.

Exhibit 3
A mixed-cloud strategy will strike the best balance of technology benefits and risk management.

	Workload-fit characteristics	Examples
Legacy systems	• Would require replatforming • Independent software vendor will not support third-party virtualization or converged infrastructure	• Mainframe apps • Unique workloads
Private cloud	• Tailored business applications • Memory- or bandwidth-intensive workloads • Significant integration and cross-application orchestration • Compliance-regulated processes or information • Mission-critical service-level agreements	• Enterprise resource planning • Supply-chain management • Data access, analytics • Custom apps
Public cloud (IaaS[1])	• Variable/peak application demands	• Test and development • Nonmission-critical, departmental applications
Public cloud (SaaS[2])	• Horizontal, nondifferentiated workloads • Configuration vs customization to meet business needs • 99.9% uptime acceptable • Only basic archiving or e-discovery needs	• Mail • Collaboration • Time and expense • HR management • Customer-relationship management

[1]Infrastructure as a service.
[2]Software as a service.

data that has business value or is covered by regulation needs appropriate management and protection (Exhibit 2).

In addition, benefits from cloud migration can vary widely by workload. For example, consumer-commerce sites, where capacity demand spikes during major promotions or at certain times of the year, will benefit from taking advantage of the variable pricing available through highly scalable public clouds.

Sophisticated IT shops are developing tools to map workloads to cloud-based hosting options using criteria like mission criticality, sensitivity of data, migration complexity, and peak processing requirements. This will make it possible for IT staff to pursue a mixed-cloud strategy and drive workloads to the hosting options that best balance risk and economic value (Exhibit 3).

Implement a business-focused approach

Organizations that have mature risk-management functions—for example, large companies in heavily regulated industries such as banking—should establish a comprehensive risk-management approach for cloud computing that extends beyond technology solutions and the IT department. Design and implementation should cover

the policies, skills, capabilities, and mind-sets required of the IT and risk-management organizations, as well as the operating units. The risk-management methodology should address several elements, including transparency, risk appetite and strategy, risk-enabled business processes and decisions, risk organization and governance, and risk culture (Exhibit 4).

Transparency about the risks of breaches of confidential business information, intellectual property, and regulated information is essential to protecting sensitive data. Fortunately, centralized cloud platforms and expanded operational data available from these platforms allow managers to assess risks, discover breaches, design guidelines based on trade-offs

Exhibit 4
A risk-management approach requires changes across several dimensions.

	From	To
Transparency	A backward-looking view by risk type	A forward-looking view of existing and emerging risks based on all available data
Risk appetite and strategy	Hard limits of tolerance	A nuanced view across risk types and scenarios based on business decisions about trade-offs between risk and value
Risk-enabled business processes	Manual and error-prone risk processes	Standardized and monitored processes with clear delineation of oversight roles
Risk organization and governance	Established risk-team roles and structures	Enhanced risk-management talent and greater board involvement
Risk culture	A soft idea	Clear metrics and targeted interventions that foster a strong risk-management mind-set

For organizations engaged in wholesale cloud migrations, roles and responsibilities will require significant changes—moving from specialized roles, such as server or network managers, to broader roles for integrated service managers.

between risk and value, and in many cases automate the enforcement of these guidelines.

To a large extent, the rules for the data that certain groups of employees are authorized to access and the data that must remain in the private cloud can be enforced by the cloud platform itself. Data on the company's quarterly financial results, for instance, can be automatically blocked from leaving the secure environment of its private cloud until results have been officially released.

For organizations engaged in wholesale cloud migrations, roles and responsibilities will require significant changes—moving from specialized roles, such as server or network managers, to broader roles for integrated service managers. These service managers will be well positioned to steward business risks because their perspective is more comprehensive than that of specialized managers, for example, when making judgments on when to use private- or public-cloud resources.

Nonetheless, the democratized nature of cloud purchasing and usage constitutes risks that automated guidelines cannot fully address. The proliferation of wireless devices that can access cloud computing anytime and anywhere, for instance, extends the reach of the company's information infrastructure, but by doing so, the information also becomes more vulnerable to breaches. Among the risks: lost or stolen devices with sensitive data stored on them. This means that the mind-sets and behaviors of line staff and managers can have great impact on cybersecurity. As a result, companies must drive risk awareness across the organization and provide risk orientation for new and lateral hires. Linking compliance to compensation through clear metrics reinforces the culture shift.

• • •

The cloud in its many forms is an exciting development for enterprise IT, but it also creates new types of challenges in protecting sensitive information assets. A business-focused risk-management approach enables large institutions to strike the right balance between protecting data and taking advantage of more efficient and flexible technology environments.

James Kaplan is a principal in McKinsey's New York office, where **Chris Rezek** is a consultant; **Kara Sprague** is a principal in the San Francisco office.