THE WHITE BOOK OF...

Managing Hybrid IT

The de initive guide to maximizing the cloud, enabling innovation and redefining governance

shaping tomorrow with you

FUJITSU

THE WHITE BOOK OF...
Managing Hybrid IT

Contents

Acknowledgements

We would like to thank the following individuals for their valuable contributions to our research in developing this publication (listed alphabetically, by organization):

- Mike Capone, Chief Information Officer and Corporate Vice President of Product Development, ADP
- Vishy Padmanabhan, Global IT Practice Partner, Bain & Company
- Jim Reavis, Co-founder and CEO, Cloud Security Alliance
- Christopher Dailey, Head of Research, Dātu Health
- Don Crabtree, Principal Infrastructure Architect, Delta Air Lines
- Andrew Brabban, Director for Applications Portfolio, Fujitsu
- Cameron McNaught, Executive Vice President, Emerging Technologies and Solutions, Global Delivery, Fujitsu
- Dr David DeHaven, Dean of the School of Information Technology, Kaplan University
- Bill Limond, Chief Information Officer (interim), Medicines and Healthcare products Regulatory Agency
- Patricia Renzi, Principal, Milliman
- Scott Skellenger, Vice President and Chief Information Officer, RainTree Oncology Services
- Gareth Wylie, Head of Programmes, Telefónica Digital
- David Harkness, Vice President and Chief Information Officer, Xcel Energy
- Jim Stikeleather, Co-author, Business Innovation in the Cloud: Executing on Innovation With Cloud Computing

Preface

The White Book of Managing Hybrid IT is the latest in a series of research reports from Fujitsu that seek to document cloud utilization within organizations, offering guidance on the application and management of a technology where adoption is surging. It adds to our existing white books on cloud adoption, cloud security, big data, and mobilizing the enterprise.

It is clear from both our research and the extensive discussions that my peers and I have held with CIOs, partners and industry analysts that cloud is now part of the standard delivery model for IT services in many organizations today. From Fujitsu's perspective, we see cloud as the natural platform for delivering innovation and new types of applications, such as Big data, IoT, Mobility, as well as modernizing existing ICT systems. Cloud has a key role in underpinning our vision of a human-centric intelligent society, one where social and business innovation is driven by the intelligent use of information and communication technology.

This fifth installment of our **white book** series, produced in collaboration with Longitude Research, reviews several key questions associated with this acceleration in the adoption of cloud and the subsequent challenges that IT leaders are grappling with. In particular, it seeks to:

- Identify the issues that organizations are encountering as they look to manage multiple cloud solutions and integrate these into existing IT systems – a hybrid IT set-up;
- Explore the strategies companies are using to manage the performance, security and cost of this new world of hybrid IT effectively, while still giving business-unit leaders the freedom to use cloud technology as a platform for innovation;
- Assess how the relationship of IT with the wider business may need to change in the long term, as organizations adapt to the hybrid IT ecosystems they must build for the future;
- Define a new approach and solution for the integration, aggregation and management of this growing portfolio of cloud services that is effective for a new model of service procurement and deployment.

The organizations that most readily accept the new reality of hybrid IT, and reconfigure themselves to manage a radically different IT landscape, will find they are better positioned for the future. In particular, they will find themselves more able to innovate, less vulnerable to security risks and system-performance issues, and more responsive to the demands of their respective markets. In short, they stand to gain substantial competitive advantage by embracing the hybrid IT model as the way forward.

As cloud usage matures it is becoming clear that adopting cloud no longer delivers the level of competitive advantage it once did. In fact, not adopting cloud is, in many instances, becoming a competitive disadvantage. The advantage now is from unlocking the value in existing data and systems and marrying these to new ways of engaging customers and changing the way organizations operate etc.

By providing a clear guide to the hybrid IT world that CIOs and other IT leaders are facing today, we hope this book will be useful in helping to ensure success in your journey towards a deeper adoption of the cloud in your organization. As ever, we welcome your feedback and insights.

Shobhit Porwal
Head of Hybrid IT,
Fujitsu America, Inc.

Executive summary

- **Cloud-computing systems are business as usual for most organizations, with deepening adoption now focused on improving processes, increasing efficiency, and enabling innovation.** A significant number of organizations have moved beyond an experimentation stage with cloud, with widespread adoption that draws on multiple systems and providers. Across a range of sectors, this deeper uptake is enabling fundamental business transformations, including wholly new processes, shorter supply chains, and faster routes to market for new products.

- **Cloud has changed the way corporate technology projects are procured, deployed, and managed.** The reality today in many organizations is that business-unit leaders are directly driving many corporate IT projects, given the ease with which cloud systems can be bought. Businesses must react positively to this change by empowering these leaders to handle procurement and deployment better, while finding new ways to manage the challenges that these changes inevitably bring.

- **New approaches to governance are needed to avoid replicating old, fragmented-enterprise IT problems and to match the new pace of business.** As their organizations make use of multiple cloud solutions – and multiple cloud providers – IT leaders are finding a growing need to extend and adapt existing operational management and governance. The fact that most companies still retain a large investment in on-premises IT systems and applications further strengthens this need. Those who don't respond will find themselves tackling greater complexity, new security risks, concerns over under-delivery, and integration problems. IT leaders also need to find ways to allow the rest of the business to adopt and implement new applications quickly and easily, to avoid them simply bypassing IT altogether.

- **IT can help by providing the framework for a new era.** The creation of a governance framework to manage the full cloud lifecycle, from procurement to decommissioning, can help organizations grapple with the adaptation challenges ahead. Such a framework needs to ensure that, as new cloud services are introduced – and, increasingly, combined with existing systems and applications – there are clear policies on how these services are managed within the overall IT landscape.

- **The hybrid IT model cannot succeed without the right toolkit.** Governance models are not the only areas that need to adapt; organizations also need the appropriate tools to manage an increasingly hybrid IT environment. These tools need to ensure that the integration of this hybrid environment is done properly, operational management is effective, and that any associated risks are managed, while at the same time giving the wider business the freedom to innovate.

- **The role of the CIO is shifting from that of IT provider and procurer to that of adviser and broker.** CIOs remain drivers of their organizations' IT strategies, but, equally, they need to recognize that the rest of the business needs greater freedom to decide which systems to buy or use. In supporting this shift, many are reinventing themselves as brokers or advisers. In the longer term, there may need to be a more fundamental shift of the IT function as a whole, such as to a federated model. In this approach, the CIO remains at the center, owning a governance structure that helps guide the business, while becoming more closely aligned to business needs through a brokering model that delivers a portfolio of cloud and non-cloud services.

- **The public sector is often a leader when it comes to cloud procurement.** Many public-sector organizations are already making significant use of the benefits of cloud and, given the sensitivities over the proper use and security of public data, many public-sector bodies appear to be further down the road than their private-sector peers in adopting good practices. This is especially true of processes and governance relating to how cloud services are procured and how security is managed.

Meeting the hybrid-IT management challenge

Our research suggests that as organizations become more heavily reliant on cloud, drawing on wide-ranging services from multiple providers, they will need to review their approach to service integration and end-to-end service management. This is especially so for a hybrid world of public and private cloud systems, along with other non-cloud applications. In particular, attention needs to be given to the following three areas:

1. Process and policies

- Creation of central cloud-procurement agreements for business leaders to work from.
- The setting out of organizational standards and specifications that must be met by all cloud services.
- Aligning corporate risk appetite with cloud-procurement and implementation processes.
- Governance framework that covers the entire cloud life cycle, from identification and configuration to migration, management, and decommissioning.

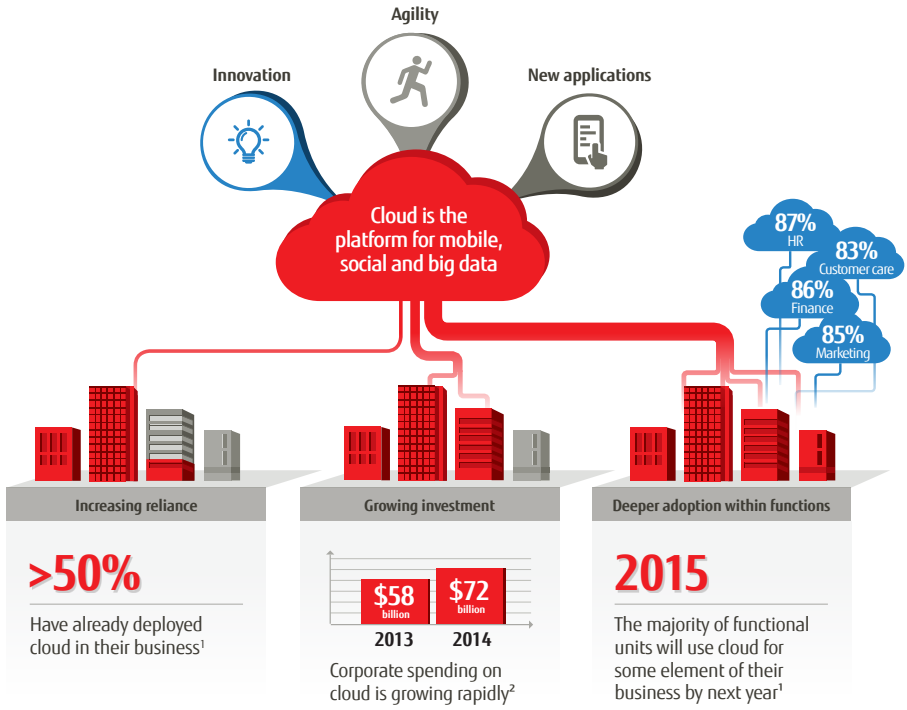
2. Operational management tools

- Providing a catalogue of available cloud and non-cloud resources for easy consumption by business.
- Reporting on usage of cloud services, and consolidating associated costs and cost allocation across the organisation.
- Integrating processes and data across hybrid IT systems.
- Monitoring and managing of all systems, with integration into existing service-management tools.
- Protecting the data held in the cloud, as well as those in non-cloud systems.
- Managing identity and access centrally across the whole IT environment, including cloud services.

3. Leadership and management

- Rethinking the CIO role – from IT provider and procurer to curator and broker of services.
- Embedding a new culture by educating the wider business on managing risk and cloud-governance processes.
- Up-skilling the workforce to enable this new model of IT adoption to thrive. Technical IT staff are fundamental to this, but program managers, service managers and procurement specialists all need to adapt as well.

Introduction: A pivotal platform



> **"From a business perspective, we are definitely more open to cloud services today than we were five years ago"**
>
> Don Crabtree, Principal Infrastructure Architect at Delta Airlines

Cloud technology is no longer being spoken about in terms of "if" or "when" – the conversation has moved onto "what next" and "how fast". This realization is leading organizations to rethink the way in which cloud solutions are being implemented, with an understanding that these systems will form a critical, and often dominant, component of their IT architecture in future.

Reservations about cloud systems have not been entirely swept away – data security, for instance, still remains a major concern. But, for many, the strengths of cloud far outweigh its perceived weaknesses, and organizations are learning how to combine cloud and non-cloud systems to address these concerns – for example by running workloads wherever most appropriate to meet their security and compliance considerations. Cloud investment trends reflect businesses' growing reliance on the technology: an April 2014 report from Forrester Research projects a rise in corporate spending on cloud services to US$72bn in 2014, up from US$58bn in 2013[2]. "From a business perspective, we are definitely more open to cloud services today than we were five years ago," says Don Crabtree, Principal Infrastructure Architect at Delta Airlines. "As a matter of fact, I think the business would probably like to go much faster than IT would."

1. "Global cloud survey: The implementation challenge", KPMG, February 2013.
2. "Cloud spending by companies outpaces predictions, Forrester says", Bloomberg, April 2014.

For many organizations, cloud technology has become a pivotal platform for innovation, for both internal processes and external customer propositions. Our research has uncovered diverse examples of businesses implementing cloud systems to gain competitive advantage. Some of these are profiled in this report, and they include decision-support tools, helping pharmaceutical companies to improve cancer treatment, faster computational support for the M&A due-diligence process, and the creation of a global HR platform, among other examples.

Multiple clouds, multiple leaders

The upshot of this success is that many organizations are moving towards a more advanced level of cloud maturity. In turn, many business-unit leaders are finding themselves taking the lead on adopting cloud-based services. "If you look at examples such as SalesForce.com®, they afforded swathes of frustrated sales and marketing directors the opportunity to deliver innovative benefits, such as enabling sales people to engage with customers in new ways – without having to turn the IT landscape upside down," explains Andrew Brabban, Director for Applications Portfolio, Fujitsu.

"If you look at examples such as SalesForce.com, they afforded swathes of frustrated sales and marketing directors the opportunity to deliver innovative benefits, such as enabling sales people to engage with customers in new ways – without having to turn the IT landscape upside down"

Andrew Brabban, Director for Applications Portfolio, Fujitsu

This trend of putting more power into the hands of other executives is creating myriad practical concerns for CIOs, from service-integration and data-security concerns through to optimizing capability as cloud adoption grows. In many cases, large organizations are creating scenarios whereby multiple business units are contracting multiple cloud vendors – sometimes overlapping, and collectively giving rise to enormous complexity[3].

For their part, business leaders must learn how to strike the right balance between managing the risk and complexity associated with a heavier reliance on cloud, while enabling the wider organization to make full use of its potential. This is a problem that resonates with Gareth Wylie, the Head of Programs at Telefónica Digital, a subsidiary of the Spanish telecommunications firm now incorporated back into the organisation's core business. "We were one part of the business that decided we needed to move quickly and implement a cloud solution. But others within the business have taken it upon themselves to do so in the absence of a global system being delivered, and that leaves us with some difficulties to overcome, given the reality of having multiple systems and trying to stitch them together," he says.

This report seeks to highlight the methods that leading organizations are employing to empower business units to adopt cloud systems, while still ensuring the necessary operational management and governance. It offers guidance for CIOs and other executives in creating a framework to achieve this, and points to practical examples of private- and public-sector organizations leading the way in this area. Finally, it considers where this road will lead in the long term.

3. "The entangled web of a multi-vendor cloud environment", ITpreneurs, March 2013.

1

Rethinking innovation and modernization opportunities

Cloud is changing how companies innovate and evolve both their business models and their supporting IT systems. Even just a few years ago, IT's role in enabling innovation and supporting transformation typically required a structured approach and solid leadership commitment. IT teams had to spend time understanding the needs of different business-unit leaders, before procuring and implementing the infrastructure and applications needed to achieve those aims. This process typically required long lead times, careful collaboration and communication, and ongoing leadership involvement. In short, the process was not particularly conducive to greater innovation.

By contrast, cloud makes it easy for organizations to try out different applications and technologies, with little cost or risk. Business leaders can quickly test different systems they believe may enhance how their functions operate, or that may pave the way for wholly new approaches. Any that don't work can simply be dropped – enabling a "quick to succeed, cheap to fail" approach.

As Jim Stikeleather, co-author of **Business Innovation in the Cloud: Executing on Innovation With Cloud Computing**, explains, cloud is the platform that enables organizations to exploit new types of applications – especially for mobility, social media and big data – to deliver exciting new results. "The primary interface between enterprises and their customers is now supported by the cloud, and it's completely changing the way companies engage with their market," he says.

Many others agree. Various executives interviewed for this report are putting this hugely powerful innovation and modernization platform to good use in diverse areas, both internally and externally, as the following examples highlight.

Internal innovation and modernization

Leading organizations are using cloud systems to deliver wide-ranging internal benefits, whether streamlining internal processes to increase efficiency and cut costs, or generating entirely new systems for business units to use.

Telefónica Digital has done just that, transforming its HR function into a global digital operation. Mr Wylie says the company sought to improve performance through better-targeted recruitment and development of its 6,000 employees. The task was made more difficult because the group had multiple HR teams across 16 countries, with different processes and different HR systems in place, ranging from very basic tools to high-end Enterprise Resource Planning (ERP platforms. "Putting a new cloud system in place enabled HR to implement global processes, including performance management, that have allowed us to better allocate our resources and target areas for improvement," says Mr Wylie.

"Putting a new cloud system in place enabled HR to implement global processes, including performance management, that have allowed us to better allocate our resources and target areas for improvement"

Gareth Wylie, Head of Programmes, Telefónica Digital

Elsewhere, multinational actuarial firm, Milliman, is using the computing power of cloud platforms to help smooth the M&A process. Patricia Renzi, Principal at the firm, highlights an example where, during an M&A analysis, the client wanted additional sensitivity testing at the last minute. "Analysis that could have slowed the transaction down for two weeks and added significant cost was managed in one hour through contacting the ops team and using the cloud to access 10,000 compute engines," she explains.

Cloud technology is also driving the modernization of existing IT applications. While the majority of legacy applications were built many years before cloud services existed, this should not prevent these systems from making use of the cloud. The most successful organizations are factoring this into their IT model, identifying legacy applications that could benefit from interaction with cloud services, and modernizing them so that cloud services can be added, even while these applications remain on-premises.

External engagement

Cloud services are also paving the way for enterprises to reshape their external proposition to customers. Companies are using the cloud to create new types of products and services; to take offerings to market more quickly; to open up new channels to engage consumers; and flexibly to support new growth areas within the business, rapidly scaling up or down in line with their level of success.

A recent marketing campaign run by a global soft-drinks manufacturer highlights the potential. The firm wanted to accompany the launch of a new line of its drinks brand with an online marketing campaign aimed at a young audience, engaging them through social-media channels and via its website, culminating in a series of brand-sponsored events. The marketing team potentially needed their IT platforms to support hundreds of thousands of entrants and to help organize the events. "While their IT department would have taken months to build the system they needed, by procuring a public cloud service they were able to run the campaign inside six weeks," explains Fujitsu's Mr. Brabban. "There was no need to build out support for thousands of users, and marketing could scale the service up as needed." As well as supporting a valuable campaign, the faster and lower-cost approach enabled the company's marketing team to run additional campaigns.

As organizations increasingly seek to realize the benefits of innovation and modernization that cloud can deliver, IT must ensure it can provide the necessary support. The wider business cannot act alone if the firm's overall enterprise
IT architecture is to remain intact, but, in order for IT skills and management capabilities to be fully exploited, the function needs to keep pace with the rest of the business. This is especially true given that applications are being modernized to interact with cloud, or wholly migrated onto off-premises platforms.

"The primary interface between enterprises and their customers is now supported by the cloud, and it's completely changing the way companies engage with their market"

Jim Stikeleather, co-author of **Business Innovation in the Cloud: Executing on Innovation With Cloud Computing**

2

Growing pains: Managing multiple clouds alongside existing IT

As the examples from the last chapter highlight, there is a clear case for cloud-based innovation and transformation. But, while enterprises in the early stages of cloud adoption may be able to fit cloud solutions into existing business processes with relative ease, those moving rapidly towards reliance on multiple cloud systems, often sourced from numerous providers, are running into some far more complex challenges. These typically fall into three broad groups: integration and service management; control and oversight; and the evolution of key roles. Each of these is discussed further here:

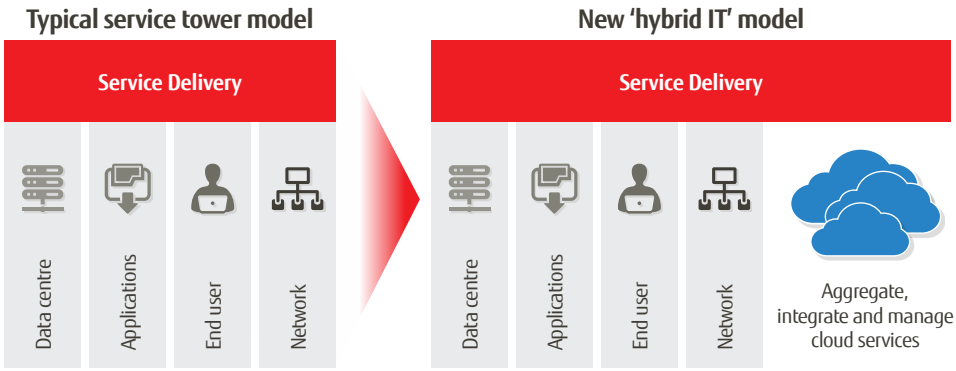
More cloud creates different challenges

Organizations are identifying new challenges as managing multiple clouds alongside traditional systems becomes the reality

1. Integrating and managing hybrid IT

As the rate of cloud adoption accelerates, and the issue of integrating and managing cloud alongside existing on-premises systems becomes more complex, companies are realising that introducing new cloud services is not always easy. The integration issues this raises cover a gamut of areas, including data, systems, and service integration, all of which must be dealt with effectively.

The importance of managing the service delivery of cloud and non-cloud systems alongside one another in a unified management model is becoming clear – organizations cannot afford to treat the two differently as cloud systems become more central to supporting the core business.



"The IT hub will undoubtedly shrink as the organization adopts more cloud solutions, but that hub has increasing numbers of spokes [cloud services] coming off it, many of which will need to communicate and interface with one another."

Don Crabtree, Principal Infrastructure Architect, Delta Air Lines

Complexity arises not only when integrating new cloud solutions with existing ones, but also with on-premises data centers, applications, and platforms. Dave Harkness, CIO at Xcel Energy, says his team spends a lot of time building integration between cloud and legacy systems. "We need to ensure we're holding the data we need to hold, and that we're enabling the cloud vendors to hold the data that we're willing to have them hold as well," he says. "So there is quite a bit of integration work that we have to do before we've rolled out most of these solutions."

Delta's Mr Crabtree says one of the biggest challenges organizations face is to ensure that cloud systems are communicating properly with one another, and with on-premises systems. "The IT hub will undoubtedly shrink as the organization adopts more cloud solutions, but that hub has increasing numbers of spokes [cloud services] coming off it, many of which will need to communicate and interface with one another," explains Mr Crabtree. Linking public cloud services with enterprise systems can be challenging, given the data-synchronisation issues involved. This task becomes even more difficult where business processes involve multiple systems. "Where a business process is required to cut across multiple applications, it further adds to the complexity of the application landscape, as well as adding to the cost of implementing and maintaining interfaces," adds Telefónica's Mr Wylie.

System integration is an issue that David DeHaven, Dean of the School of Information Technology at Kaplan University, has also struggled with in his attempt to implement a new cloud-based gaming platform for students. "We worked with our vendor on integration, who had done specific integrations in the past with a different online learning

platform. An assumption was made that they would naturally be able to integrate, but we discovered that this was not the case, and we had to build the integration solution ourselves," he explains.

Where large numbers of cloud systems are involved, it is no longer viable to link services, processes and data through point-to-point integrations. Instead, a more sophisticated solution is required, based on easily configured and open software tools, and which provides an integration hub with pre-defined connectors that can be configured quickly without lots of development expertise.

Once the cloud and non-cloud systems are integrated, the next challenge for the CIO lies in providing end-to-end management. Where the business has procured a cloud system, it may not even consider the need for the IT department to manage the system at the outset. "We are increasingly hearing about business units that have procured or built their own cloud service, perhaps on a public cloud service like Amazon® Web Services, and, once the system is up and in use, they then look to hand the system over to the IT department to manage it," explains Mr Brabban.

One of the end-to-end management challenges for CIOs is the operational headache of monitoring system performance where multiple cloud services have been adopted. Where business units have entered into contracts with cloud providers directly, it can leave the IT function without oversight of the underlying services that are delivering business processes. Often, the first time a problem becomes apparent is when a user reports it to the IT helpdesk – and, in extreme cases, this is when IT learns about the existence of the system for the first time, too.

It is critical that the CIO is able to monitor external systems in real time in order to manage their performance. This brings the challenge of managing a hybrid IT landscape in an integrated and consistent manner. In order to do so, the IT department needs management tools that can add new services quickly and easily, and to ensure it is flexible enough to manage services in both the traditional enterprise IT environment and in the cloud. However, existing enterprise-management solutions are often not able to do this.

2. Control and oversight

While the effective integration and management of cloud services and the safeguarding of data are likely to be top priorities for IT, there are also other key factors to consider, such as ensuring that systems are user-friendly and keeping costs to a minimum. In order to provide the necessary operational management, it is essential for IT to have oversight of the cloud services within the organization – from the procurement of individual systems right through to decommissioning. "One of the barriers to migrating applications to the cloud, especially core corporate applications, is the concern over losing the full overview of a process," says Mr Brabban. "This is especially so for large enterprises."

While empowering business leaders to buy cloud solutions ensures greater flexibility, these executives will, understandably, be less aware of the issues that might arise elsewhere in the business if IT has limited transparency. As one example, multiple user identities may be obtained for individual users as business units set up new services with different cloud providers. This creates unnecessary complexity for users, while CIOs are left with the task of trying to unravel these scattered pockets of service access.

Security issues also arise. If access for the entire organization cannot be tightly controlled through an identity-management service, it makes the task of provisioning and de-provisioning users across multiple services hard to police. If those leaving the organization do not have their access to external cloud services automatically switched off, then customer data is at risk of being stolen or misused – a scenario no modern business can afford to risk.

Security in the cloud isn't just about data governance – setting the policies around where data are held and who can access them – but also concerns the need for data protection. This involves not simply relying on the cloud provider to secure your data, but also establishing the policies to have the data backed up to a separate data store controlled by the organization. This could be another cloud service, or perhaps an on-premises data vault, depending on the sensitivity of the data.

Good data governance can also help to ensure compliance around how and when data can be accessed and used. One organization has built location awareness into its system to address this. When it identifies that an end user is accessing information from outside the corporate network – perhaps from a coffee shop or airport – it withholds access to certain data, bolstering security, while maintaining agility. (See **Managing security with multiple clouds** overleaf for more on other key security concerns.

If CIOs want to ensure that the business units can get the services they want quickly, while also providing the assurance that these services match governance requirements, then a catalogue of cloud and non-cloud IT services is needed. This allows the business to know what services already exist and makes it easy for the business units, their users, and IT to provision the different IT services the organization needs. It also provides the means to report on usage, to consolidate views on costs across the business, and to allocate costs or recharge accordingly.

The importance of obtaining cost transparency is highlighted by Mr Wylie as being crucial to managing costs. "Particularly in a large organization, perhaps with relatively autonomous business units, you could easily see local HR teams or other functions doing their own thing," he says. "This means that you're then tangled up with multi-year contracts that need to be honored, and you are missing out on the economies of scale that you would get if the agreements were pooled together across a wider user base – so you're adding to your bottom line unnecessarily."

Managing security with multiple clouds

The security of cloud systems has been a hugely contentious point since the technology was first brought to market. As organizations bring more cloud solutions on-board and deal with a greater number of providers, concerns around security deepen. In a recent EY study, 25% of respondents said that the use of cloud computing had increased their risk exposure over the last 12 months, and made them more vulnerable in respect of being attacked or harmed[4].

As organizations deepen their cloud engagement, IT's strength in overseeing security must not be lost. "The reality is, business units can go around, and will go around, central procurement functions, but all of that knowledge that IT has about managing systems can be very useful in helping the organization understand what to look for as they move more of their IT operations into the cloud," says Jim Reavis, CEO of the Cloud Security Alliance.

> "The reality is, business units can go around, and will go around, central procurement functions, but all of that knowledge that IT has about managing systems can be very useful in helping the organization understand what to look for as they move more of their IT operations into the cloud"
>
> Jim Reavis, CEO of the Cloud Security Alliance

The most significant cloud-security concerns for organizations are:

- **Sensitive data and business-critical information.** Working with multiple cloud providers makes it extremely important to understand the standards each is governed by, and where exactly organizational data are stored, given that some geographies are more hazardous than others.
- **Viability of services.** It is imperative that agreements with all service providers take into account the full lifecycle of related data, including the period it will be stored for, and how it will be dealt with once a cloud service is decommissioned.
- **Controlling access.** Being in control of which internal stakeholders have access to the information held in different cloud systems, and monitoring that centrally, is crucial.

4. "Under cyber attack, EY's global information security survey 2013", EY, October 2013.

To help organizations deal with this, Fujitsu has set out a 10-point security checklist[5]

1. Define approaches for identifying data to be protected and ascertain how to access this. Consider an access-control approach that incorporates and integrates in-house, outsourced and cloud systems.	❑
2. Clearly set out the organization's risk appetite and align cloud-procurement and implementation processes with this.	❑
3. Ensure a comprehensive understanding of legal and regulatory requirements applying to jurisdictions where providers are located and data are stored.	❑
4. Ensure that the relevant regulatory, corporate and industry standards apply to all providers.	❑
5. Build up relationships with trusted cloud-service providers.	❑
6. Create a cross-functional committee comprising IT, security and risk officers and key business units to work on cloud adoption and management.	❑
7. Refer to initiatives such as the Security, Trust and Assurance Registry (STAR)[6] when drawing up contracts with cloud providers, and conduct due diligence aligned with publicly available standards.	❑
8. Audit cloud-service providers' disaster-recovery plans and make appropriate provisions in response.	❑
9. Prepare for cyber attacks against both your organization and your cloud-service providers.	❑
10. Build the existing security team to incorporate a more diverse range of technical, contractual, and business-relationship skills.	❑

5. Checklist derived from "The White Book of Cloud Security", Fujitsu, 2011.
6. https://cloudsecurityalliance.org/star/

3. Changing role of the CIO

As cloud computing changes how businesses approach innovation, and the models and processes they employ, it is also driving enterprises to reassess how they consume IT, allocate technology budgets, and manage new services. This, in turn, is changing the role of CIOs, and the overall IT function.

While individual business units can see the advantages of cloud systems and are often driving the adoption of new tools, it is usually the CIO who remains responsible to the board for IT issues, whether on security, compliance, or performance. To handle this, CIOs will need to reassess their positions. "Looking forward, I think the CIO has to ensure the organization creates an environment where the integration and interface of these loosely coupled business functions can be brought into a harness or a framework, to enable some form of central cloud governance," says Scott Skellenger, CIO at RainTree Oncology Services.

"Many CIOs are realizing they need to become the broker or the enabler of ICT, not a provider, and they are evolving towards that"

Cameron McNaught, Executive Vice President, Emerging Technologies and Solutions, Global Delivery, Fujitsu

In particular, CIOs must concentrate on striking the right balance between fostering innovation and managing risk. Cameron McNaught, Executive Vice President of Emerging Technologies and Solutions at Fujitsu, argues that this involves repositioning, rather than entirely redefining, the role of the CIO. "Many CIOs are realizing they need to become the broker or the enabler of ICT, not a provider, and they are evolving towards that. They are becoming an internal adviser and framework provider, rather than the actual provider of the service," he says.

While a change in what is expected from a C-suite leader is inherently challenging, Mike Capone, CIO at ADP, a US multinational specializing in payroll and HR solutions, says a proactive approach is what's required. "The CIO should be the one leading the charge in terms of how we can leverage the cloud to make things work, and really partner with business and functional leaders on outcomes. This is a necessity. If you're kicking and screaming at this point, it's too late, they will either go around you, or, worse, they'll replace you," says Mr. Capone.

In the longer term, we may also begin to see an IT as a service (ITaaS)-type model emerging more strongly. This approach creates an operational model where the enterprise IT department acts as a distinct business entity, providing tailored services for the other lines of business. Here, the onus would be on IT to create a portfolio of services – some developed internally, some provided externally via dedicated contracts, and others sourced from cloud providers.

Surprise leaders? Lessons from the public sector

Government organizations are not commonly thought of as being at the forefront of technology innovation, with private-sector organizations usually leading the way. However, the scale and complexity of government departments, and the strict requirements they face in protecting national data, have required them to set high standards when it comes to cloud governance. In turn, leading public-sector agencies are providing insights for others. "There are definitely lessons the private sector can learn from the public sector," argues Bill Limond, an interim CIO from the Medicines and Healthcare products Regulatory Agency (MHRA)"For one thing, the security training is often far more comprehensive as government cannot risk any internal failings."

> **"There are definitely lessons the private sector can learn from the public sector. For one thing, the security training is often far more comprehensive as government cannot risk any internal failings"**
>
> Bill Limond, an interim CIO from the Medicines and Healthcare products Regulatory Agency (MHRA)

Easing procurement, limiting risk

Just as business-unit leaders are taking more control over cloud adoption, different government departments and agencies need to access their own services.

For example, the UK government has created a service called G-Cloud to manage the procurement of cloud services by different departments and to ensure consistent standards are adhered to. The system sets out a series of framework agreements with suppliers, covering all aspects of cloud services. The US government has made similar moves: in 2011, the then government CIO, Vivek Kundra, set out a Federal Cloud Computing Strategy, which outlined a foundation for cloud governance and procurement[7].

The Fujitsu Executive Vice President of Emerging Technologies and Solutions, Cameron McNaught, points to a similar practice being employed by several governments across Asia-Pacific. "They don't mind what cloud services their departments and agencies go out and buy, but they must be plugged into the framework they've set up, so they can govern it and protect themselves," he says.

There are clear benefits to this approach, but, most crucially, it gives departments the independence they need to find the best fit for their needs, while also ensuring that strict parameters are being observed.

7. "Federal cloud computing strategy", Vivek Kundra, The White House, February 2011.

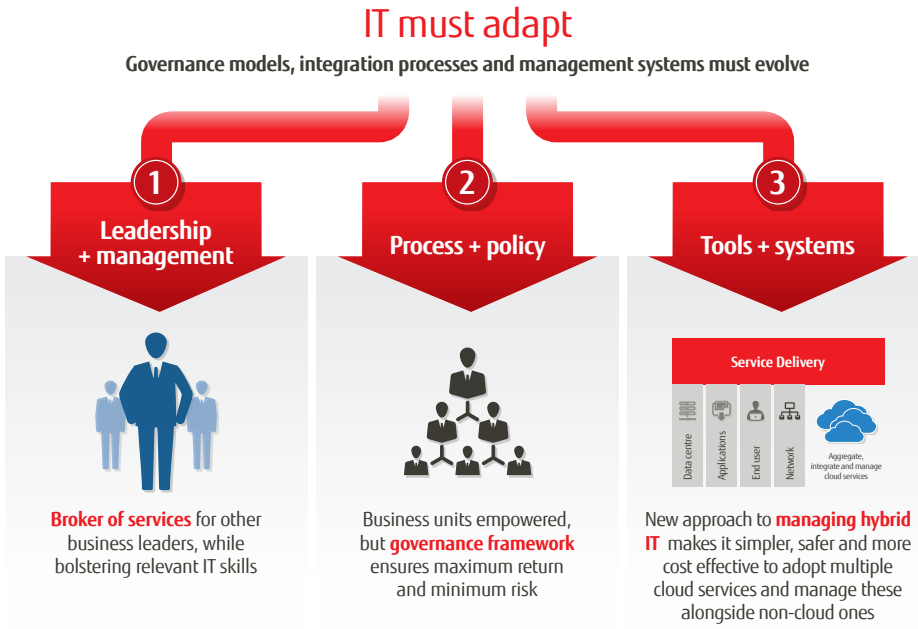
3

Navigating your cloud journey

As organizations begin to understand the deeper role cloud is playing, it is becoming clear that governance models, integration processes and management systems need to change to handle this emerging hybrid IT model.

With more IT decisions being led directly by the business units, how can organizations ensure that the necessary oversight is achieved? As Vishy Padmanabhan, Global IT Practice Partner at management consulting firm, Bain & Company, points out, investing in the right operating model – which includes development processes, operational processes and talent, and the right management and integration tools – to bring together cloud and non-cloud environments, has to be a critical priority.

Our research suggests that organizations should adopt a three-tiered approach to cope with the challenges ahead, evolving their overall IT leadership, their process and policy, and related tools and systems. Each of these is outlined here:



Leadership and management

"IT is a partner, but should not be the decision maker. You need your IT department to be a chief influencer, and they should rightfully have veto power if acquisition decisions are not reflecting the IT strategy"

Christopher Dailey, Head of Research, Datu Health

- Shift the primary focus of the CIO from being a provider of IT to a broker of services – both internal and external.
- Ensure IT takes the lead on educating the wider business on managing risk and governance processes.
- Hire and train cloud-savvy employees – technical staff, but also program and service management, and procurement specialists.
- Reskill the security team for a cloud era, drawing on new technical, contractual and business-relationship skills[8].

Process and policy

- Provide business units with a standard procurement-service agreement, defining the criteria new service providers must meet.
- Define the integration requirements for new systems before purchasing. This involves setting standards for common identity and access management, specifying integration into the end-to-end service management approach, and ensuring alignment of infrastructure, applications, and process.
- Create a portfolio of services that can be brokered to other business units – whether developed internally, provided via external contracts, or sourced from public cloud providers.

"You've got to have the right cloud governance in place and you've got to take it very seriously. The policies and processes in this area must be absolutely crystal clear across the whole organization"

Bill Limond, an interim CIO at the Medicines and Healthcare products Regulatory Agency (MHRA)

- Create a catalog of approved service providers and systems that meet organizational standards on security (including data protection and encryption policies), performance, and necessary regulatory standards.
- Build relationships with trusted cloud-service providers, and establish clear service level agreements (SLAs), ensuring they can be closely tracked.
- Audit cloud-service providers' disaster-recovery plans and make appropriate provisions in case of failure.
- Verify the availability of published application programming interfaces (APIs) for service provisioning, usage, and reporting.
- Ensure that the overall governance framework covers the entire cloud life cycle, from identification and configuration to migration, management, and/or decommissioning.

8. "The White Book of Cloud Security", Fujitsu, 2011.

"The CIO should be the one leading the charge in terms of how we can leverage the cloud to make things work, and really partner with business and functional leaders on outcomes"

Mike Capone, CIO, ADP

"Today's more cloud-reliant organizations need the tools that can aggregate all of the systems they have – enabling monitoring, recording, billing and provision in a single management interface"

Cameron McNaught, Executive Vice President, Emerging Technologies and Solutions, Global Delivery, Fujitsu

Tools and systems

- Establish a central management and reporting tool that enables the business to have oversight of costs for all cloud services.
- Provide an identity-management service that has a single sign-on for users to access all in-house, outsourced and cloud systems, and that can be monitored and managed centrally.
- Ensure the capability to back up data from cloud services and restore it onto different platforms.
- Ensure the ability to monitor and manage end-to-end services across both cloud and non-cloud environments.
- Check that your IT-service-management platforms can support ITaaS in the longer term.
- Provide the ability to integrate cloud and non-cloud applications seamlessly.

Q&A: Xcel Energy CIO Dave Harkness on selecting cloud services

The chief information officer of Xcel Energy, a US utility firm, explains how he maintains control of his organization's cloud network.

What are your key governance concerns around cloud systems, and how do you manage them?
We have a reference architecture that we've put together for both private and public cloud solutions. A lot of our governance is around the data and the security of the application, as well as a pretty thorough total cost of ownership.

What purpose does your cloud reference architecture serve?
One function of it is around how we build the integrations for different services, because you don't want to build a bunch of point-to-point stuff, you want them interfacing with your enterprise service bus (ESB) to make as much of that as standard as you can. You have to consider how easy it is going to be to build those interfaces, as, with some systems, a lot of integration work is needed before you can roll out the solutions.

Which other criteria should organizations assess when dealing with cloud providers and procuring new services?
Reliability is crucial – we pay a lot of attention to disaster recovery. We have really started to ramp up the analysis of the stability of cloud vendors, especially ones that are more critical to our day-to-day operation. So, if we're rolling out those capabilities that customers expect to have available 24/7, I want to know what that cloud vendor's disaster-recovery plans are. We also need to have a technology discussion, which is about asking, "what's your platform running on? And is it an Access database running in the background, or is it very mature technology?"

4

Re-engineering for cloud

Cloud computing is not just a passing phenomenon, but will be crucial to all organizations in the decade ahead.

Leading enterprises are already making extensive use of cloud technology – increasingly as a hybrid IT model integrating cloud systems with non-cloud – to innovate, seize new market opportunities, and secure a competitive advantage over rivals. A recent KPMG survey found that the vast majority of functional areas – including finance, HR and marketing – will already be using cloud in some form by 2015[9].

Although the pace of change varies widely across organizations, the overall direction of travel is clear. As this happens, both public- and private-sector organizations need to consider how best to allow business-unit leaders to exploit the cloud, while maintaining sufficient oversight of integration, security, service management, and cost issues. In particular, six key considerations stand out, which act as a cloud-maturity checklist for CIOs:

Cloud-maturity checklist for CIOs:

1. Do you have a clear understanding of your organization's level of cloud adoption? It is important to map out exactly how far different parts of the business have gone in terms of adopting cloud, gaining an overview of exactly how many cloud systems are in place and their impact on the organization, as well as what they intend to use in future.	❑
2. Does the organization have an effective governance framework in place for managing hybrid IT? In order to manage challenges such as security risks, integration problems and cost control, which arise as multiple cloud solutions are adopted and multiple cloud providers are utilized, it is crucial to ensure a central framework is in place. It is also vital that this framework can guide business units in procuring services, and that it enables IT to have effective oversight, while being able to provide operational management for these services.	❑

9. "The cloud takes shape", KPMG International, February 2013.

3. Are the necessary tools and systems in place to provide end-to-end service management as cloud adoption accelerates? IT needs the right tools to handle the operational management of cloud alongside non-cloud. This becomes even more pressing when the cloud services are no longer niche systems, but are delivering core business processes. The tools need to cover issues such as integration, performance, data security and access management.	❑
4. Have you achieved the right balance between IT oversight and business enablement for utilisation of cloud? While giving business leaders a free hand to adopt cloud systems opens up various risks, they must not be inhibited from seizing opportunities for innovation by any controls that are in place.	❑
5. How far has IT progressed towards becoming an enabler of, rather than provider to, the wider business? As organizations reach a greater level of cloud maturity, CIOs will need to evolve towards becoming brokers of cloud services for the wider business, as opposed to acting as the primary IT provider.	❑
6. Does your long-term vision for the IT function account for greater empowerment of other business leaders? As business unit leaders gain greater independence in sourcing and deploying IT services, the IT function may ultimately need to find wholly new operating models, such as ITaaS. Here, IT would operate as a distinct business entity, creating a portfolio of services for the rest of the business to utilize.	❑

4 Re-engineering for cloud

Fujitsu and managing hybrid IT

Cloud is no longer considered to be a new technology – it has become part of the standard delivery model for many CIOs today. At Fujitsu, we understand that as organizations grow their portfolios of cloud services, new challenges arise around the integration, aggregation and management of those portfolios, as well as for the existing, traditional IT services.

For more information on the Fujitsu approach to managing hybrid IT please contact us at:

http://www.fujitsu.com/us/solutions/cloud/hybrid-it/

Managing hybrid IT speak: Key terms explained

Access control: A way to control who and/or what may access a given resource, either physical (e.g. a server) or logical (e.g. a record in a database).

Certification: Documentary confirmation that a service, product, person or organization conforms to certain characteristics or possesses particular skills. This is often, but not always, subject to some form of external assessment.

Cloud architecture: The architecture of the systems involved in the delivery of cloud computing. This typically involves multiple cloud components communicating with one another over a loosely coupled mechanism (i.e. one where each component has little or no knowledge of the others).

Cloud-service provider: A service provider that makes a cloud-computing environment – such as a public cloud – available to others.

Data integration: The technical and business processes used to combine data from disparate sources into meaningful information.

Data residency: The location of data in terms of both the legal location (the country in which the cloud-service contract is enforced) and the physical location (i.e. the data centers where they are stored).

Hybrid IT: The result of combining internal and external services, usually from a combination of cloud services with on-premises systems, in support of a business outcome.

Identity federation: The provision of security to allow for a clean separation between the service being accessed and the associated authentication and authorization procedures. This enables secure collaboration across multiple systems, networks and organizations employing different security systems.

Interoperability: The ability of diverse systems and organizations to work together.

IT as a service (ITaaS): An operational model where the enterprise IT department acts and operates as a distinct business entity, creating services for the other lines of business within the organization.

Process integration: Efforts to create direct links between on-premises business applications and services on public clouds. It also constructs a business process linked with tasks requiring human decisions.

Real time: Real-time programs must guarantee a response (from event to system response) within strict time constraints. A real-time system may be one where the application is considered (in context) to be mission-critical.

Service integration: Allows an organization to manage IT-service providers in a consistent and efficient way, ensuring that performance across a portfolio of services meets the needs of the end users.

Service integration and management (SIAM): A framework for managing multiple IT suppliers, providing a single view of IT services to the rest of the business.

Service level agreement (SLA): Part of a service contract where the level of service is formally defined to provide a common understanding of services, priorities, responsibilities, and guarantees.

Single sign-on: A mechanism whereby a single action of user authentication and authorization permits access to multiple systems without the need to enter multiple passwords.

Systems integration: The joining of different subsystems into one large system to deliver a whole functionality.

For more information on FUJITSU Cloud, and to learn how we can assist your organization further, please contact us at:

Fujitsu America, Inc.

Address: 1250 East Arques Avenue Sunnyvale, CA 94085-3470, U.S.A.
Telephone: 800 831 3183 or 408 746 6000
Website: http://solutions.us.fujitsu.com
Contact Form: http://solutions.us.fujitsu.com/contact
Have a question? Email us at: AskFujitsu@us.fujitsu.com

Reference number: 3507