THE WHITE BOOK OF...

Cloud Security

The definitive guide to managing risk in the new ICT landscape

THE WHITE BOOK OF...
Cloud Security

Contents

Acknowledgments

In compiling and developing this publication, Fujitsu is very grateful to the members of its UK CIO Advisory Board and valued customers across the globe. Particular thanks are extended to the following for their contributions:

- **Nick Gaines, Group IS Director, Volkswagen UK**
- **Tony Mather, Chief Information Officer, Clear Channel International**

With further thanks to our authors:

- **Ian Mitchell, Chief Architect, Fujitsu UK and Ireland**
- **John Alcock, Information Assurance Consultant, Fujitsu UK and Ireland**

And our specialist contributors:

- **Darren Ratcliffe, VP & Global Cloud CTO, Fujitsu Global Business Group**
- **John Swanson, Information Assurance Consultant, Fujitsu UK and Ireland**
- **Mark Wilson, Strategy Manager, Fujitsu UK and Ireland**
- **Vincent Hughes, Senior Research Analyst, Fujitsu UK and Ireland**
- **Shane Tan Hua Beng, Consultant, Cloud Services, Fujitsu Asia Pte Ltd**
- **Johanna Heimonen, Business Director, Fujitsu Nordic**
- **Thomas A Hoover, IT Security and Compliance/Information Security, Fujitsu America Inc**

For any inquiries on Fujitsu's global cloud offering, please contact:
askfujitsu@uk.fujitsu.com

ISBN: 978-0-9568216-1-4
Published by Fujitsu Services Ltd.
Copyright © Fujitsu Services Ltd 2011. All rights reserved.
No part of this document may be reproduced, stored or transmitted in any form without prior written permission of Fujitsu Services Ltd. Fujitsu Services Ltd endeavours to ensure that the information in this document is correct and fairly stated, but does not accept liability for any errors or omissions.

Preface

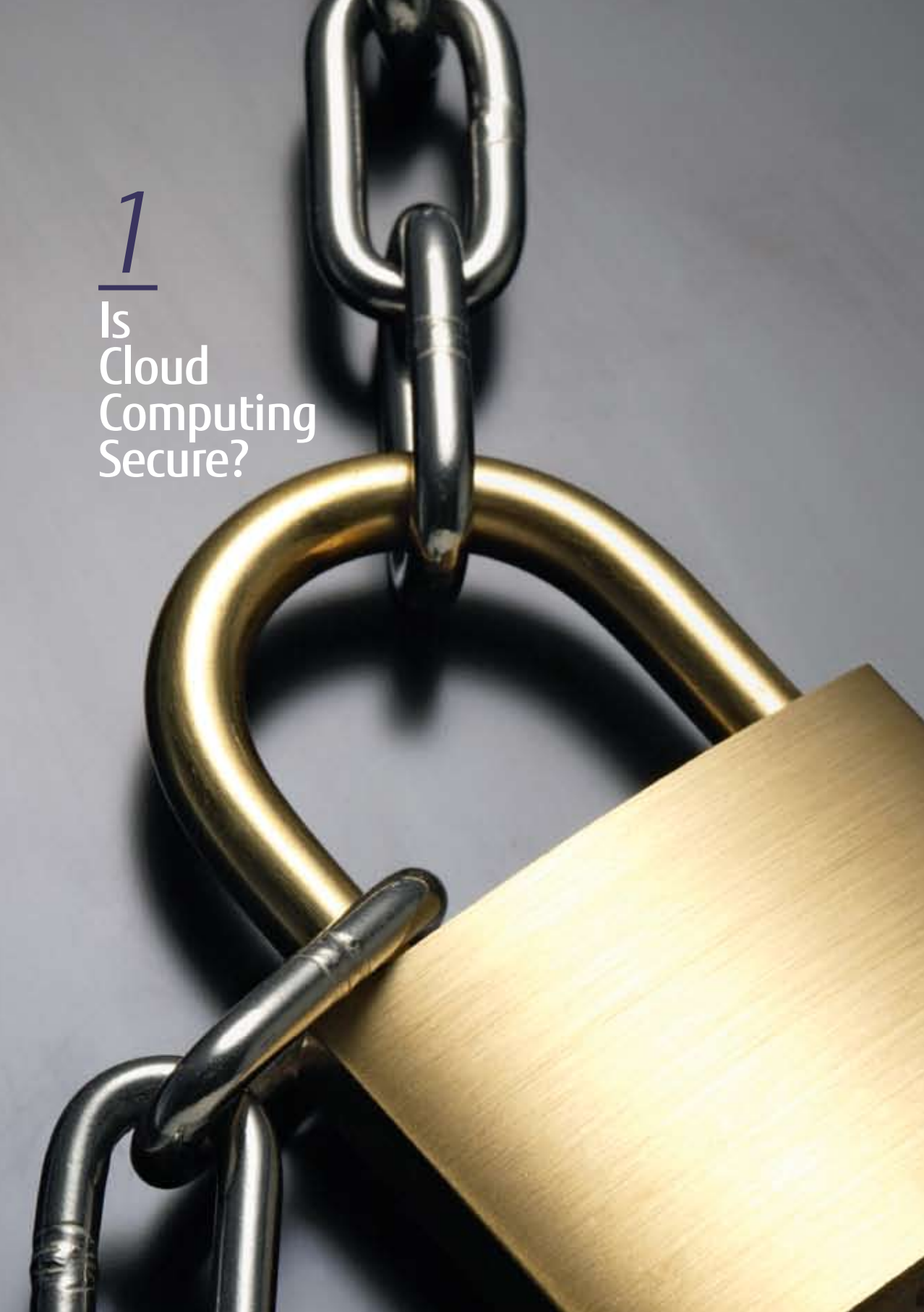
As we highlighted in the first book in this series, *The White Book of Cloud Adoption*, cloud computing is demonstrating its potential to transform the way IT-based services are delivered to organisations. What's more, there is little, if any, argument about the clear advantages of cloud: it is generally accepted that cloud adoption can and will create substantial business benefits through reduced capital expenditure and increased business agility. For most organisations, therefore, **the journey to cloud is no longer a question of "if" but rather "when"**, and a large number of enterprises have already travelled some way down this path.

However, there is one overwhelming question that is still causing many CIOs and their colleagues to delay their move to cloud: **Is cloud computing secure?** A simple answer is: Yes, if you approach cloud in the right way, with the correct checks and balances to ensure all necessary security and risk management measures are covered. Businesses that are already deep into their cloud programmes are reporting that security, while an extremely important consideration, is not a barrier to adoption.

That said, those CIOs ready to adopt cloud services are right to **place security at the top of their agendas**. After all, the consequences of getting your cloud security strategy wrong could not be more serious. As many unwary businesses have found to their cost in recent high-profile cases, a single cloud-related security breach can result in an organisation severely damaging its reputation – or, worse, the entire business being put at risk.

By providing a clear and unbiased guide to navigating the complexities of cloud security, we hope this book will help to ensure your cloud computing journey is as **trouble-free and beneficial** as it should be. Please let us know what you think – and how your cloud adoption progresses.

Cameron McNaught
Senior Vice President, Cloud, Global Business Group
Fujitsu



1 Is Cloud Computing Secure?

Summary

"Is cloud computing secure?" is invariably the first question CIOs proposing cloud solutions and services face from CEOs and senior colleagues. Yet those further along their cloud path are finding that, like all forms of information security, the question boils down to effective risk management. By employing multiple layers of defence and a robustly designed cloud architecture, organisations can confidently answer: "Yes, it is secure enough."

When Fujitsu released *The White Book of Cloud Adoption* in 2010 (see Appendix at the end of this book) to explain the pertinent issues for customers in a simple, digestible form, we didn't envisage how popular it would become. CIOs tell us it has helped clarify their own thinking and overcome many of their organisations' fears and misconceptions.

Those further along their cloud path are finding that, like all forms of information security, the question boils down to effective risk management

But while researching the book, we quickly realised the primary concern for those new to cloud was security. By contrast, organisations that had been using cloud for some time did not consider security an obstacle to adoption. (In fact, their biggest focus was, more justifiably, interoperability – ensuring different cloud providers' systems and services could talk to one another.)

The White Book of Cloud Adoption is still available and provides a comprehensive overview of the whole topic. But given the ongoing questions, we believe there is a need to explore the specific issues around cloud security in a similarly comprehensive fashion.

This second book in the series, *The White Book of Cloud Security*, is the result. Here, we explore the key issues surrounding cloud security for CIOs and their teams. From Fujitsu's position as a trusted cloud partner to leading organisations, we hope to pass on valuable advice and guidance about not only information security, but more broadly risk. This book will help CIOs make informed security decisions about their diverse cloud set-ups and better understand how to reap all the benefits of cloud without compromising their organisations' security.

Photograph: Corbis

Adapt and embrace

When it comes to cloud security, a CIO's objective remains the same as ever: to understand and manage risk. Yet perhaps the biggest risk of all is not embracing the opportunities cloud has to offer. Cloud gives an organisation a way to rethink its entire strategy for IT and business service provision, as well as the potential to improve its competitiveness and agility.

We hope to pass on valuable advice and guidance about not only information security, but more broadly risk

In addition, business functions and employees are increasingly demanding to use cloud applications and services that they believe improve their productivity and ability to innovate. Given these drivers, security teams, processes and solutions must adapt to embrace cloud, rather than reject it because it doesn't fit with all of their traditional approaches to security.

Rapid progress

Cloud is evolving at a phenomenal speed, even in the context of the fast-moving IT sector. As it evolves, so do the solutions and standards designed to address CIOs' concerns. Security standards are emerging – and constantly evolving – that directly address many of the challenges we already see today.

Different layers

In *The White Book of Cloud Adoption* (see Appendix at the back of this book), we outlined the different layers in the cloud services stack:

- **Infrastructure**-as-a-Service (IaaS)
- **Platform**-as-a-Service (PaaS)
- **Software**-as-a-Service (SaaS)
- **Business Process**-as-a-Service (BPaaS).

These layers – and their associated standards, requirements and solutions – are all at different levels of maturity. In this book, we explore cloud security and risk issues in a generic sense, rather than delving into the specific details of individual layers. But CIOs should remember when assessing providers (be they cloud service providers, existing IT suppliers, outsourcing companies or in-house IT) to ensure they compare like with like.

"The world of business is becoming more uncertain, as with new system architectures come new cyber threats. No longer can the mechanisms deployed in the past be relied on for protection"

Nick Gaines, Group IS Director, Volkswagen UK

Security characteristics of different types of cloud

	Private	Community	Public	Hybrid
Governance and enterprise risk management	☆ ☆ ☆	☆ ☆ ☆	☆	☆ ☆
Data residency and jurisdiction	☆ ☆ ☆	☆ ☆	☆	☆ ☆
Compliance and audit	☆ ☆ ☆	☆ ☆	☆	☆ ☆
Access control	☆ ☆ ☆	☆ ☆	☆	☆
Shared resources and data segregation	☆ ☆ ☆	☆ ☆ ☆	☆	☆ ☆
Security incident management	☆ ☆ ☆	☆ ☆	☆	☆ ☆
Physical security	Dependent upon service	Dependent upon service	Dependent upon service	Dependent upon service
Privileged users	☆ ☆ ☆	☆ ☆ ☆	☆	☆ ☆
Continuity services	Dependent upon business needs	Dependent upon business needs	Dependent upon business needs	Dependent upon business needs
Data disposal	☆ ☆ ☆	☆ ☆ ☆	☆	☆ ☆

The ratings assume each item on the left is implemented appropriately.

Not all clouds are equal

Although this book refers generically to "cloud", there are in fact several types of cloud. It is important to realise, too, that the type of cloud an organisation chooses is one of the biggest factors affecting risk. We choose to characterise these types as private, public and community clouds – or "hybrid" to refer to a combination of approaches.

Different types of cloud have different security characteristics. The table on page 10 shows a simple comparison. (The number of stars indicates how suitable each type of cloud is for each area.)

Security risks

Organisations with defined controls for externally sourced services or access to IT risk-assessment capabilities should still apply these to aspects of cloud services where appropriate.

But while many of the security risks of cloud overlap with those of outsourcing and offshoring, there are also differences that organisations need to understand and manage.

- **Processing sensitive or business-critical data** outside the enterprise introduces a level of risk because any outsourced service bypasses an organisation's in-house security controls. With cloud, however, it is possible to establish compatible controls if the provider offers a dedicated service. An organisation should ascertain a provider's position by asking for information about the control and supervision of privileged administrators.

- **Organisations using cloud services** remain responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subject to external audits and security certifications. Cloud providers may not be prepared to undergo the same level of scrutiny.

- **When an organisation uses a cloud service,** it may not know exactly where its data resides or have any ability to influence changes to the location of data.

- **Most providers store data in a shared environment.** Although this may be segregated from other customers' data while it's in that environment, it

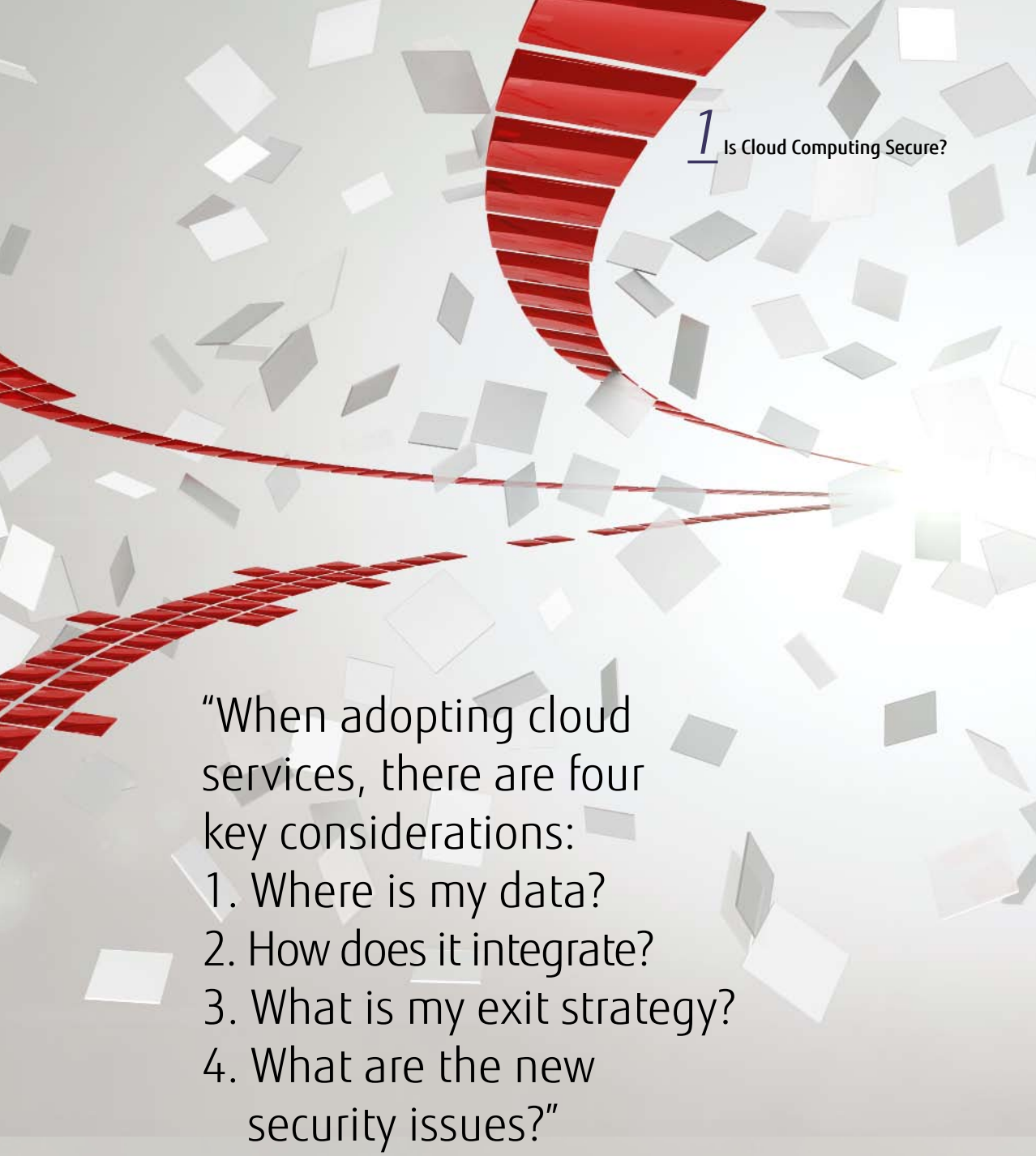
may be combined in backup and archive copies. This could especially be the case in multi-tenanted environments.

- **CIOs should not assume service providers will be able to support electronic discovery,** or internal investigations of inappropriate or illegal activity. Cloud services are especially difficult to investigate because logs and data for multiple customers may be either co-located or spread across an ill-defined and changing set of hosts.

- **Organisations need to evaluate the long-term viability of any cloud provider.** They should consider the consequences to service should the provider fail or be acquired, since there will be far fewer readily identifiable assets that can easily be transferred in-house or to another provider.

In short, no one security method will solve all these data protection problems so it is important to consider multiple layers of defence. Ideally, organisations should compartmentalise their cloud infrastructure and applications to apply the right controls in the right places and help contain the impact of security incidents.

No one security method will solve all these data protection problems so it is important to consider multiple layers of defence



"When adopting cloud services, there are four key considerations:
1. Where is my data?
2. How does it integrate?
3. What is my exit strategy?
4. What are the new security issues?"

Tony Mather, CIO, Clear Channel International

2

Cloud Security Simplified

Summary

As with all coherent security strategies, cloud security can seem dauntingly complex, involving many different aspects that touch all parts of an organisation. CIOs and their teams need to plot effective management strategies as well as understand the implications for operations and technology. In this section, we outline the key considerations.

The table on page 16 highlights all the different aspects of cloud security that CIOs need to consider. We have broken these down into the three following key areas:

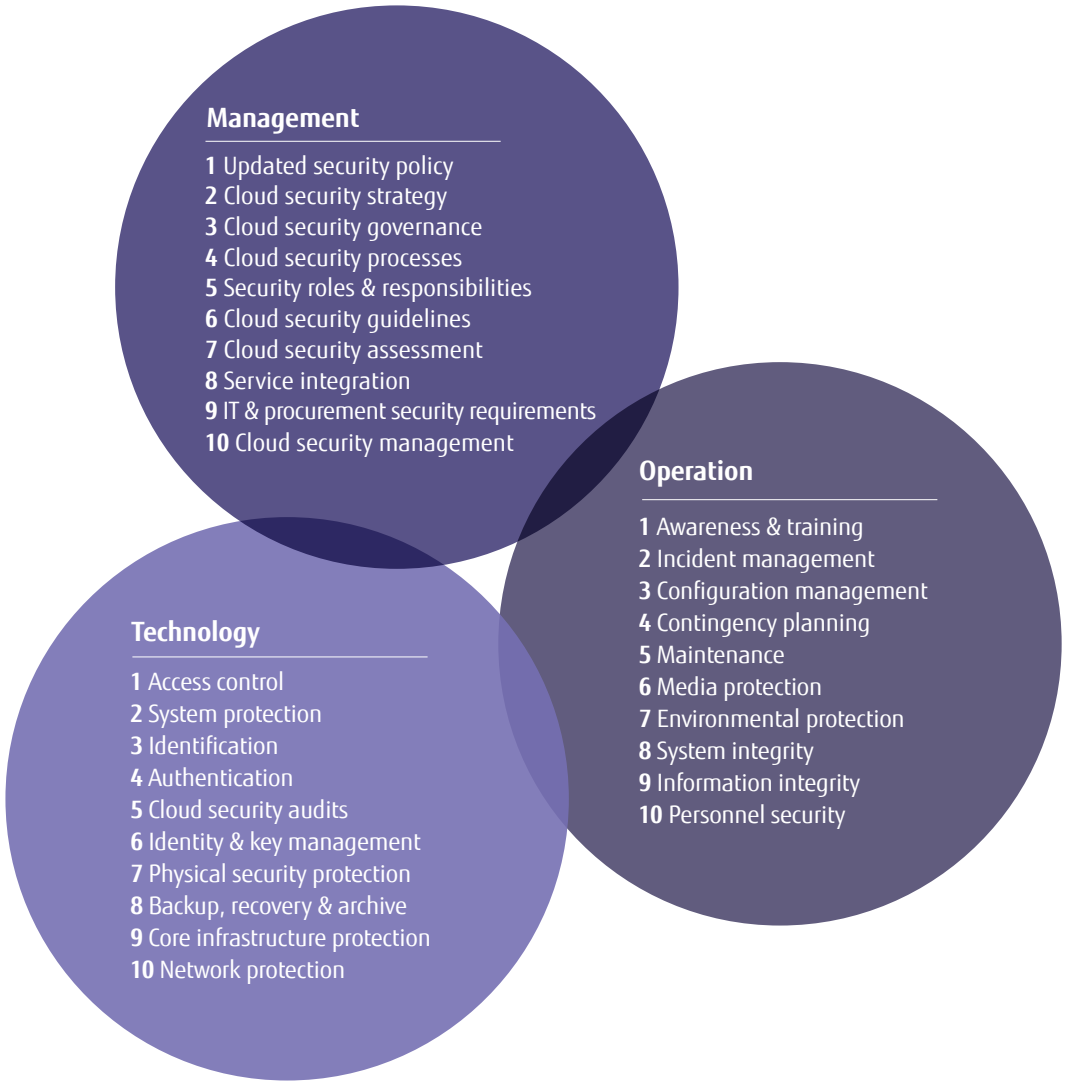
- **Management**
- **Operation**
- **Technology**

It provides an at-a-glance reference to the issues organisations need to address if they are to put in place effective cloud security strategies backed up with appropriate processes and technologies. On the following pages, there is a drill-down into each of these.

CIOs and their teams need to plot effective cloud security management strategies as well as understand the implications for operations and technology

Photograph: Corbis

Aspects of cloud security



Drilling down

The following is a brief explanation of each of the elements highlighted in the diagram.

Management

- **Updated security policy**

Amendments to the organisation's overarching security policy.

- **Cloud security strategy**

The organisation's strategy for security with respect to cloud. This should complement or be part of the organisation's existing overarching security strategy.

- **Cloud security governance**

The process for ensuring cloud security strategy and policy updates are adhered to.

- **Cloud security processes**

The security processes associated specifically with cloud and/or the amendments required to existing security processes in order to incorporate cloud.

- **Security roles & responsibilities**

Who is responsible for what with respect to ensuring the different elements of cloud security are implemented effectively.

- **Cloud security guidelines**

Advice and guidance provided to both business and IT teams regarding all aspects of security that affect them.

- **Cloud security assessment**

The ability to objectively measure the effectiveness of a given cloud service provider's security.

- **Service integration**

The integration of several cloud services at a management level.

- **IT & procurement security requirements**

Specific cloud security requirements that would need to be included in any procurement and/or IT project's overall requirements.

- **Cloud security management**

The overall day-to-day management of cloud security.

It is vital organisations ensure that their access control policies are still sustained by their use of cloud services

Operation

- **Awareness & training**

Educating employees about the security impact of cloud on their individual functions and roles.

- **Incident management**

Managing cloud-related problems and incidents.

- **Configuration management**

Ensuring the configuration of an organisation's service is appropriate and secure.

- **Contingency planning**

A pre-planned approach to business continuity, disaster recovery and the ongoing management (up and down) of cloud usage.

- **Maintenance**

The processes ensuring that anything in a cloud environment (or consumed from a cloud environment) is properly maintained and up to date.

- **Media protection**

Ensuring any data stored in a cloud environment is managed appropriately.

- **Environmental protection**

Ensuring an organisation's cloud service provider (and using that provider rather than internal IT) improves that organisation's environmental credentials.

- **System integrity**

Ensuring all cloud systems remain secure.

- **Information integrity**

Ensuring all information stored in a cloud environment is secure.

- **Personnel security**

Ensuring all personnel (both internal staff and employees of the cloud provider) are trustworthy and do not have the ability to compromise the service.

Technology

- **Access control**

Technology and software (including its configuration) that ensures the right person has access to the right data (and only the right data) for them.

- **System protection**

Technology to protect individual cloud systems from security risks such as distributed denial-of-service (DDoS) attacks.

- **Identification**

Technology to identify employees and other authorised personnel accessing a cloud service.

- **Authentication**

Technology to verify that an individual accessing a cloud system is who they claim to be.

- **Cloud security audits**

The tools and processes by which organisations ensure security (and associated systems and processes) are adequately maintained.

- **Identity & key management**

The management of security keys (e.g. encryption keys, SSL keys) and identities of the organisation's personnel.

- **Physical security protection**

Ensuring a provider has appropriate security controls for access to its buildings.

- **Backup, recovery & archive**

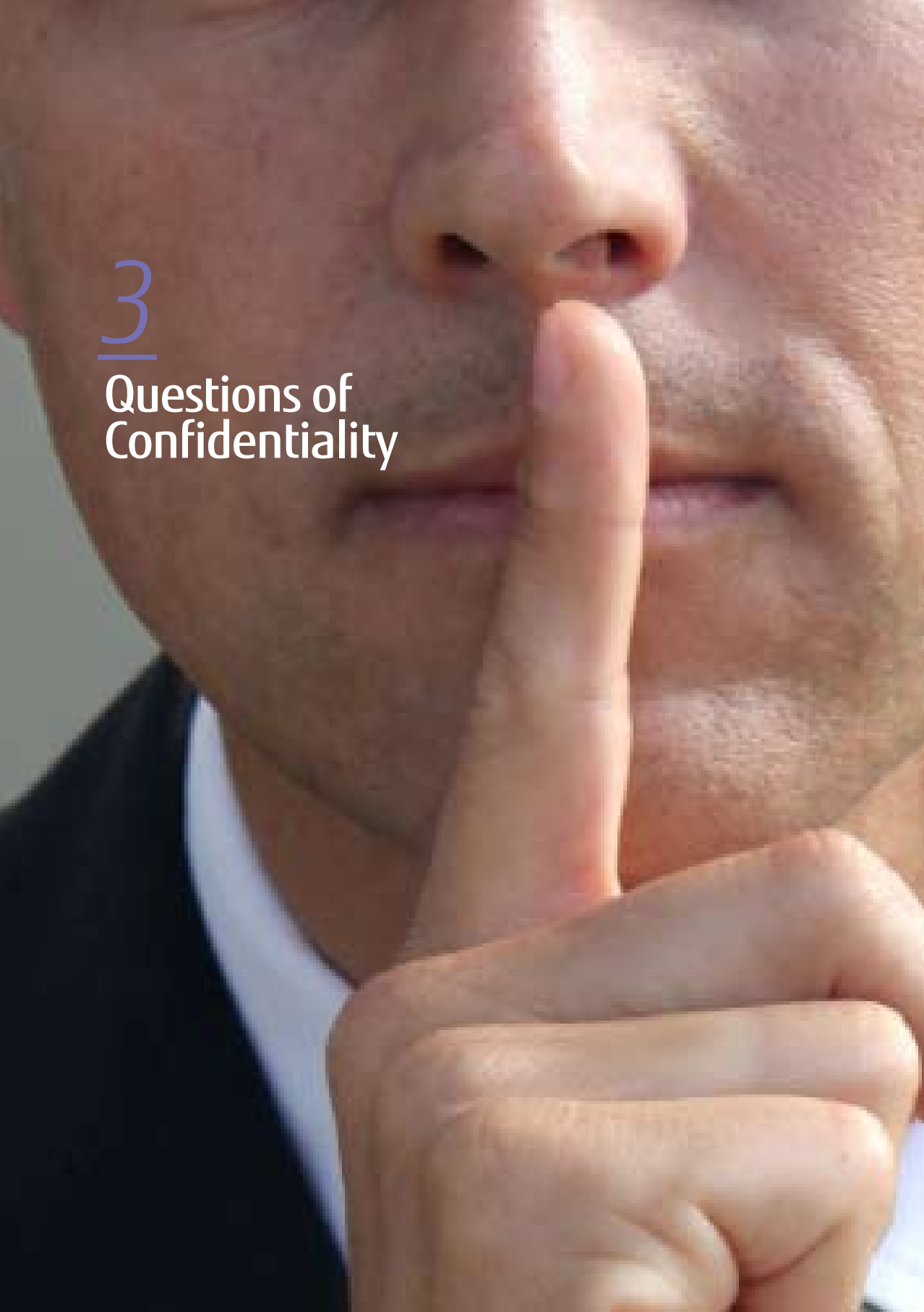
The tools and procedures for ensuring that data stored in a cloud system is available in the event of a catastrophic failure on the part of the provider.

- **Core infrastructure protection**

Protection of servers and other core infrastructure.

- **Network protection**

Protection of the internal network and the boundary of the network (where it connects to a cloud environment).



3 Questions of Confidentiality

Summary

Organisations adopting cloud services need to understand the implications for maintaining the confidentiality of personal or other sensitive business information. The key considerations are how the physical or legal location of data affects its use and ensuring only specified users and devices can view particular data. Buyers need to understand the regulatory frameworks under which they operate, assess potential providers and draw up suitable contracts to reflect regulatory obligations.

One of the greatest concerns for organisations coming to grips with cloud computing is confidentiality. Everyone expects certain information to be kept confidential in both their personal and professional lives and they expect the organisations for which they work, or with which they share their information, to maintain that assurance of confidentiality.

In the case of a fully-managed public cloud service, privacy and confidentiality risks are likely to vary according to the provider's terms of service and privacy policy. There's an even greater level of risk where providers reserve the right to change their terms and policies without recourse for existing customers.

> *"A key question needs to be: 'Am I adhering to local jurisdiction?"*
>
> *Tony Mather, CIO, Clear Channel International*

Data residency

When considering public cloud services, rather than private or community clouds, an organisation needs to understand the potential risk and impact of the secondary use of information. Secondary use of certain information by the provider may violate the laws or terms under which that information was collected. Given the variance in privacy legislation across different jurisdictions, the location where information is stored can have significant effects on the protection of privacy and confidentiality – as well as on the obligations of those who process or store the information.

Some regulatory bodies and the laws of certain jurisdictions establish privacy standards that can affect an organisation's decision to use a particular provider – particularly where that provider is offering a publicly-hosted shared service.

Photograph: Alamy

For example, the USA Patriot Act gives US law enforcement the right during the course of investigations into suspected terrorists to access information stored by providers, without having to inform data owners. Affected users of US-based cloud services would never know their information had been accessed.

Identify and classify

But while the location of data and the laws governing different jurisdictions are important considerations, it is also vital to understand the types of information stored and the appropriate level of risk associated with the loss of particular data.

It is vital to understand the types of information stored and the appropriate level of risk associated with the loss of particular data

By identifying and classifying data, it is possible to consider the most appropriate location in which to store particular information. For example, some data may be too sensitive for a public cloud but can still exist in a private one. For other data, technologies such as tokenisation could provide the answer. This is where a sensitive piece of information is replaced with a reference code and the actual data is held in another database, hosted elsewhere.

A joined-up approach

The key consideration for any organisation is to define a joint approach among architecture, data management, compliance and security teams, in order to identify the data that needs to be protected, and the legal and regulatory obligations that pertain to that data. Using this combination of skills and experience, an organisation can determine the appropriate level of protection while still ensuring the data can be accessed when and where necessary.

Legal or physical location?

It is important to understand the laws that may relate to the legal location of data (i.e. the location of the legal entity that holds the data – such as the cloud provider) rather than its physical location.

Information in a cloud environment may have more than one legal location at any one time, with differing legislative implications. In some cases, a provider may, without giving notice to its users, move information from jurisdiction to jurisdiction, from provider to provider or from machine to machine.

Provider policies

An organisation might determine that particular data can be safely stored in a cloud environment. But even if this is the case and there are financial or other compelling

"The real horror story for cloud users would be seeing other people's data"

Tony Mather, CIO, Clear Channel International

business reasons for doing so, it is important to consider whether a provider has:

- **Documented procedures** for co-operation with local law enforcement agencies, in order that organisations understand exactly what action would be taken in the event of a data-access request
- **A contractual agreement** that prohibits exposure of data without approval, so customers have notice of any proposed hand-over of data to authorities
- **The ability to specify that data reside** in particular legal jurisdictions when delivering cloud services to customers in particular countries (to comply with data protection regulations that require data to be stored in given regions).

Contract for confidentiality

Where data residency is an important issue, organisations must make sure that this is reflected in the contractual arrangements with their providers. It is important to look for clear policies and practices in order to make an informed decision about the privacy and confidentiality risks.

When drawing up cloud service contracts, organisations should consider adding data confidentiality clauses to ensure providers do not cause them to breach local data legislation because of that providers' compliance with another jurisdiction's laws.

Some cloud service providers may be more secure than in-house IT, especially for organisations with less mature or poorly-resourced IT functions

Access control

The other key consideration for ensuring the confidentiality of cloud-based data is access control. Cloud-hosted data can be accessed through more channels and in more locations than data hosted in the organisation. With a potential multitude of devices and remote users seeking access from different global locations, via a mix of public and private Wi-Fi, mobile networks and fixed connections, it is vital organisations ensure confidential information is not compromised and that their access control policies are still sustained by their use of cloud services.

The challenge of multiple logins

Having multiple logins for different services is likely to reduce access security. This is because it makes users more likely to store passwords insecurely on their devices or paper rather than committing them to memory. Therefore when defining access control mechanisms for cloud applications and data, organisations should try to ensure their approach is integrated with their in-house models.

Many organisations are using single sign-on (SSO) to alleviate the security issues presented by multiple logins. This can result in added complexity where there are multiple cloud providers in addition to internal services. Organisations should ascertain whether it is appropriate to partner with one or more trusted identity providers, so SSO can be continued. The access control model should also clarify who determines the trusted and trusting parties, and how.

Granular data control

Different parts of the business generally only require access to a certain subset of the organisation's data. For example, it's unlikely that retail staff would need to access their organisation's legal and commercial applications. It may therefore be worth considering role-based access control to further reduce the risk of confidential information falling into the wrong hands. Indeed, it will be increasingly desirable to control access to data at a much more granular level (we explore this further in Chapter 7).

A question of context

Despite the broad organisational trend towards "device agnosticism", in terms of security, businesses may consider certain types of device "more worthy" than others. Limiting access to services on this basis is referred to as context-sensitive access control. This means users' levels of access to data are governed by the devices they're using and their locations or types of connection.

For example, a smartphone app accessing sensitive data over a cellular network may have only limited access, while a company-maintained PC (or even the same smartphone) directly connected to the company LAN may have full access.

Caution: evolving architectures

As cloud evolves, new security architectures will emerge to govern access control. Some of these will be very simple – for example, ensuring individual applications are protected from attacks. Others will be more complex, such as the example above. CIOs should keep abreast of these developments and ensure they do not lock their organisations into particular solutions until they are confident that the solutions will meet business needs.

Monitor, control, log

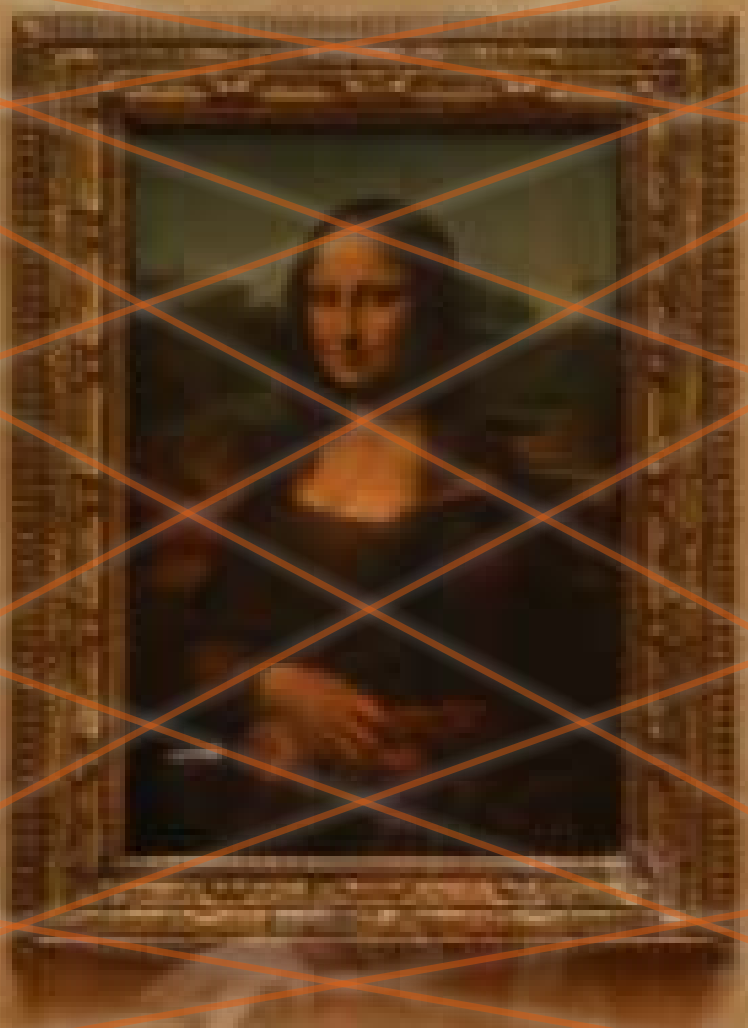
Organisations must ensure there are appropriate controls for both business users and IT support staff with "super user" privileges. It is important that the cloud provider monitors the use of such privileges, has appropriate behavioural controls in place and logs all data access so that it can provide audit trails to enable the investigation of potential security breaches and unauthorised access.

Cloud can be safer

Sometimes, cloud providers (as with outsourcers) are subject to greater scrutiny than the organisations using them. For example, a customer may demand a provider carries out background checks on all its employees, even though it does not apply a similar level of diligence to its own people. Some cloud service providers may therefore be more secure than in-house IT, especially for organisations with less mature or poorly-resourced IT functions.

4

Ensuring Integrity



Summary

An organisation moving sensitive business data to a cloud environment must take steps to ensure that its data is safe, genuine and accurate. Failing to do so can have both legal and operational consequences. It is therefore important to take data integrity into account as part of the due diligence process when selecting cloud providers.

Protecting the integrity of data in a cloud environment is vital. Organisations must:

- **Ensure that data stored** using cloud services has not been tampered with
- **Thoroughly address** all compliance-related issues
- **Ensure their reputations** are protected by working with trusted providers.

It is important to ensure providers comply with any regulatory, corporate, industry or other standards relating to cloud services. They must also be able to provide the information their customers require in order to meet their own obligations.

It is important to ensure providers comply with any regulatory, corporate, industry or other standards relating to cloud services

To this end, they should be able to demonstrate that:

- **Their systems are secure** (e.g. through certification)
- **They can provide** an adequate data-audit trail
- **Their terms of use** do not jeopardise customers' own legislative requirements or ethical codes.

While some of the means for doing so are similar to the steps outlined in Chapter 3, organisations also need to consider a number of specific areas.

Managing multiple providers

Cloud solutions are often based on data entry via web applications and organisations may use separate vendors for functions like HR management and payroll services, with no cross-checking or reconciliation among them. This may be

Photograph: Shutterstock

a good reason to use one provider for related applications or to employ a cloud services aggregator that offers intermediate transaction management functions.

Acceptable use and ethical fit

Reputations take many years to establish but can be damaged or destroyed in a matter of days. It's vital to build trusted relationships with cloud providers in order to maintain and protect the reputations of all parties.

Providers all have their own terms of service defining acceptable use. Often these are designed to protect them against violations of laws on terrorism, pornography and so on, in a similar vein to the acceptable-use terms many organisations already have in place for internal IT.

Any organisation consuming cloud services must be comfortable with its provider's terms and indeed the ethical position these represent. For example, if a provider was found to be in breach of any legal or moral codes, how would that reflect on users of the service? Organisations therefore need mechanisms to understand providers' policies and their implications, particularly in regard to the providers' standards of conduct.

Tamper-proofing data

The IT industry is notoriously volatile, and the growing cloud sector in particular is likely to see many mergers and acquisitions

How can the owner of information held in a database ensure its data has not been tampered with, either deliberately or accidentally? This is a concern even for internal systems, but cloud adds additional complexity through multi-tenancy (multiple customers sharing the same physical systems and storage media) and the use of external operational staff.

While other security controls must also be used, confirming data has not been altered (either deliberately or inadvertently through a process failure) is generally achieved by checking that the data's computational hash (a mathematically-determined code derived from the data) is still the same as it was originally. Ideally, the verification should take place using a hash that's been agreed in advance, to avoid what is known as a man-in-the-middle attack, in which the original hash is replaced with the amended data's hash at the point of verification between the systems transmitting and requesting information.

As it is not always practical to agree hashes in advance, it is common to use digital certificates to assert information is from a trusted source. This approach is commonly used in secure Internet transactions through encryption (for example, the HTTPS protocol for secure website access) but it can also be used to sign data transmissions. It is possible for malicious third parties to deliver false certificates, so organisations should maintain a list of trusted certificate providers to establish a chain of trust.

Understanding certification and standards

There are a number of common certifications and standards that providers use to bolster their claims of security and data integrity. The most frequently used are:

- **ISO 27001** – the current standard certification for the operation, monitoring, maintenance and improvement of information security management systems
- **ISO 27002** – recommendations for information security management (not currently certifiable)
- **ISO/IEC 20000** – specifies the minimum process requirements an organisation must establish to be able to provide and manage IT services to a defined quality
- **ISO 9001** – the most common of a number of quality management certifications. Being certified demonstrates a provider is driven to continually improve its internal, customer-facing and regulatory systems and processes.

Auditing and compliance

Although cloud computing is a relatively new development, data centre management is not. There are already proven tools and formal processes for auditing and testing the security aspects of data centres. For example:

- **Field tests** for fail-safety
- **Regular security** exercises
- **Formal frameworks** for security testing (such as penetration tests)
- **Independent** security audits
- **Reports to customers** on past service levels.

Buyer beware

None of an organisation's legal and regulatory compliance responsibilities are transferred to a provider when the organisation adopts cloud services. While the provider might be obliged to operate in conformance with particular requirements, responsibility for data, service levels, infrastructure, uptime and so on remains with the buyer. Organisations must therefore ensure:

- **They understand** how the service will be provided
- **They conduct due diligence** investigations into the provider's stability
- **Providers' reporting** is adequate. (E.g. are the tools appropriate? Are the dashboards fit for purpose?)

E-discovery

Electronic discovery (e-discovery) is a legal term referring to searches of stored data in the event of litigation. In a public cloud, this can create significant difficulties. An organisation should ensure questions relating to e-discovery are answered satisfactorily prior to contracting with a provider.

Mergers and acquisitions

Equally, an organisation needs to understand what happens to its data and services in the event of a provider entering into a merger or acquisition. The IT industry is notoriously volatile, and the growing cloud sector in particular is likely to see many mergers and acquisitions.

Data protection

When cloud applications hold personally identifiable information, organisations must ensure providers protect this adequately and in compliance with the local data protection laws that govern the information in question. For large, multi-region cloud solutions, this can be a complex scenario. The main data protection risks to the business are:

- **Loss of data** by the provider
- **Unauthorised access** to data the business holds
- **Malicious activities** targeting the provider
- **Poor internal IT** security on the part of the provider.

Organisations must assess the risks of these hazards and understand their potential impacts on the business before adopting a cloud service.

"Infrastructure providers may offer the integrity and security required, but in the longer term this has to be designed into the application for cloud services"

Nick Gaines, Group IS Director, Volkswagen UK

5 The Risk of Service Disruption

Summary

Amid ongoing reports of cloud services being brought down by both malicious attacks and providers' technical and operational failures, CIOs need strategies to mitigate the risk of disruption to business services. Before contracting, they should carefully assess providers' processes for managing availability. However, they will also need to accept that occasional outages are inevitable and plan accordingly.

The cloud availability conundrum

When it comes to availability, cloud services pose something of a conundrum for CIOs. On the one hand, the independence of such services from the organisations using them, the varied methods of connection available to users and the fact these services are central to the provider's business mean they are likely to remain live if local problems hit their customers' businesses. On the other, organisations using cloud services may be very dependent on public network links, and risk becoming "collateral damage" in incidents affecting service providers.

Organisations using cloud services may be very dependent on public network links, and risk becoming "collateral damage" in incidents affecting service providers

Attacks and failures

The activities of so-called "hacktivist" groups, such as LulzSec and Anonymous, show that organisations with poor security processes can suffer considerable reputational and financial damage. The technology media also frequently highlights service outages at major cloud providers that have occurred because of natural disasters, or technical or operational failures.

Is downtime the "new normal"?

The point of highlighting these outages is not to criticise. These stories hit the press because of their huge impact. They do, however, need to be viewed in context. Some commentators suggest this is the "new normal" and that businesses must learn to live with and manage outages, just as they have learned to cope with the odd power cut, dead phone line or train breakdown.

It's also worth considering whether existing internal or outsourced services can maintain similar availability rates. How long does it generally take to resume normal service following an incident? It may be that a few minutes of downtime

Photograph: Alamy

is acceptable. Organisations requiring very high availability might consider designing their infrastructure to span multiple regions and maybe even multiple cloud providers, just as in a private infrastructure set-up they might have multiple data centres, communications paths and power sources.

Mitigating the risk

Organisations choosing to use cloud services need to accept the risk that availability might occasionally be eroded by network downtime, data centre outages and other single points of failure. They can mitigate some of this risk by selecting an enterprise-strength cloud provider, but this will cost a little more. Where availability of data and applications is important to an organisation, however, they would be unwise to select a provider on price alone. Rather, they should investigate and compare potential providers' availability, and disaster recovery and business continuity plans in order to make an informed choice.

CIOs and staff responsible for procurement will need to identify and negotiate effective terms and conditions that mitigate any perceived exposure to risk and cost. At the same time, providers will be trying to standardise terms and minimise contractual differences among their customers. While the cloud space is still maturing, these tensions will continue. But we expect providers to eventually develop a standard approach that will satisfy all but the most demanding customers.

Tried and tested tactics

Many of the same service management disciplines and best practices that are usually applied to traditional IT will still apply in a cloud environment – for example, business continuity and disaster recovery planning.

Many of the same service management disciplines and best practices that are usually applied to traditional IT will still apply in a cloud environment

Business continuity

Outsourcing to a cloud provider does not outsource the responsibility for an effective and up-to-date business continuity (BC) plan. Organisations must assess the risks and understand the impact of any move to cloud on their BC plans (for example, the implications of accepting different SLAs from multiple providers). Effectively managed, however, cloud can have benefits for BC, for example in relation to testing and development. Using cloud services, new systems can be built, scaled and tested rigorously without affecting existing internal infrastructure, systems and processes.

Disaster recovery

Cloud contracts rarely include disaster recover (DR) provisions or financial penalties for failing to recover services within a specific timeframe following an incident. Some cloud infrastructure providers don't take responsibility for customer data. Buyers must understand a provider's DR plans and ensure they meet their overall requirements.

In addition, organisations need to ensure outsourced cloud services are incorporated into in-house DR plans. This includes so-called "shadow IT" (cloud systems outside the control and possibly implemented without the knowledge of the IT department). The considerations are similar to those involved in protecting business-critical "applications" developed using Excel spreadsheets or an Access database. CIOs must ensure they don't hinder business innovation and agility, but at the same time need to identify and monitor shadow IT so that it can be incorporated into overall DR plans.

It's also worth remembering that cloud can actually significantly simplify and reduce the cost of DR. Providers can offer standby infrastructure and platforms on a pay-per-use basis that can rapidly be brought up to speed in the event of disruptions affecting both internal and externally-sourced systems and services.

Overcoming attacks

A single cloud infrastructure will generally be used by a number of the provider's customers. A significant proportion of these customers will share not only a common network infrastructure but a common computing, memory and storage infrastructure. Organisations need to be aware that an attack that targets any of the provider's customers who share the same cloud environment is likely to affect their own ability to access services.

Organisations also increase the risk of suffering a distributed denial-of-service (DDoS) attack if they use multiple providers (although conversely this can also reduce the impact of any attack since it's unlikely all of an organisation's providers will be hit at the same time).

Buyers should question potential providers carefully to understand the mechanisms they have in place to detect, classify and trace DDoS attacks. They should also ask for full details of the providers' capabilities and how they scale their services.

Evaluating alerts

CIOs must ensure their cloud providers can show documented processes for evaluating security alerts from operating system and application vendors. This is particularly critical, given the increasing number of zero-day threats (identified security holes that have not yet been patched). It's important that vulnerable systems are protected from attack until routine service packs and updates fix any problems. Indeed, organisations face a higher level of risk if they fail to ensure systems are patched in a timely manner than they do from untested patches that could have unwanted side effects. Even so, it's also important to understand the testing procedures a provider uses.

6

Putting It All Together

Summary

Many of the risks associated with cloud come about as a result of inadequate service integration. This is both a technical and a business process consideration. Organisations must be certain cloud services are effectively joined up – both with one another and with in-house systems and business services. They should identify and mitigate risks systematically in advance, ensuring providers can be effectively assessed, monitored and managed.

Organisations often have concerns that moving systems and data into a cloud environment will lead to a sprawl of services from different providers, with all the associated technical, management and contractual headaches this implies. To ensure an effective end-to-end service that seamlessly joins up systems, services and processes – both internal and external – effective integration is essential.

Organisations need to be certain everything joins up

Among other things, organisations need to be certain that:

- **Services** will work correctly
- **They can recover speedily** from service outages
- **They can manage multiple providers** effectively
- **They can demonstrate their systems** and processes are compliant
- **All the risks are clearly identified** and mitigated.

Joining the dots

Organisations need to ensure robust and effective interoperability across infrastructure, applications and processes, among multiple providers, and between external and internal systems and services. In other words, they need to be certain everything joins up.

Photograph: Pixelate.biz

From a risk perspective, to do this effectively, they need to understand where the potential gaps or threats to service delivery lie and then mitigate those risks systematically.

Integrating business services

Most organisations typically focus on interoperability at the technology or application level. But as more and more cloud providers offer business processes "as a service", CIOs must be able to guarantee effective integration and interoperability at that higher business-process level if they are to ensure continuity of service and operations.

Whose problem is it anyway?

Organisations need to be clear who is responsible for fixing any problem. They must work through potential outages and understand in advance whom to approach for a "fix". Where there are multiple providers, organisations should determine if they will work together to recover after an incident. (For example, cloud providers are sometimes unable to share information with others due to regulatory restrictions.) In addition, organisations' business continuity and disaster recovery plans will need to factor in their cloud providers' own plans (see Chapter 10).

Warning: keep exits clear

To gain the full benefits of cloud, organisations need to maintain the freedom to switch providers should the need arise

Ultimately, cloud computing will be a utility – and to gain the full benefits of this model, organisations need to maintain the freedom to switch providers should the need arise. This should be addressed at the beginning of any cloud procurement so that the exit arrangements and obligations are fully understood at the outset. It is absolutely critical that organisations ensure service termination and/or transition to another provider is covered in the contracted terms and conditions.

Five further considerations

Other key aspects organisations must consider if they are to ensure effective service integration include the following:

1. Consistency of reporting

Organisations should be clear of the hierarchy of their cloud providers and, where possible, ensure there is a consistency of input into reports in terms of format and context. This is especially the case for reports that aggregate information across multiple providers.

2. Managing multiple providers

When dealing with a number of cloud providers delivering different services, an organisation should identify a logical single point of control and management.

3. Contractual security assurance

Organisations must be sure providers will deliver adequate protection and security throughout the life of the contract.

4. Managed security

Organisations must ensure providers offer adequate managed security services with appropriate support levels. This should include 24/7 access to support, vulnerability management and appropriate protection services.

5. Incident management

Organisations must understand how providers' incident management processes will join up with their own investigation and resolution processes.

7

Data is King

Summary

When applications and data no longer sit exclusively inside an organisation, it stops making sense to treat the firewalled boundary of the data centre as the primary line of defence. As cloud models evolve, businesses will need increasingly granular security controls at the application and data levels. This presents management, operational and technical challenges, but also enables exciting opportunities.

To ensure data confidentiality, integrity and availability, today's cloud providers offer capabilities such as encryption, segregation (to keep different customers' resources separate), rigorous access controls (to prevent unauthorised access to data) and scheduled data backups. But as cloud matures, organisations will need to rethink their security models fundamentally.

As cloud matures, organisations will need to rethink their security models fundamentally

Growing granularity

Currently, the data centre boundary (typically a demilitarised zone created by a series of firewalls) is the de facto standard "security wall" that protects access to an organisation's applications and data. But, in the cloud world, applications may not be inside the organisation's data centre. Consequently, security will be applied to applications and data at an ever more granular level. For example, firewalls will be built directly into applications and access to data will be controlled at the level of individual attributes within a record.

Understand and classify

For the model above to work, it is vital that organisations ensure data is accurately classified, so people can only access the specific information they're authorised to view – and so appropriate rules can be built into new applications and enforced automatically.

To classify effectively, the IT department will need a thorough understanding of the structure of the organisation's data and how it is used. Some data may not even be owned by the organisation (especially if it has been acquired from a

Photograph: Shutterstock

data marketplace – the data equivalent of an application store) and CIOs need to consider appropriate use and storage when moving such information into a cloud environment.

Grey areas of ownership

In other instances, it may not be clear whether the organisation, individual consumer or provider owns the data. Examples include website activity logs that reveal customer behaviour patterns or (even further abstracted) data regarding an organisation that is extracted from social networking sites. Organisations will need to clarify such grey areas in advance to ensure their use of cloud data is both secure and compliant.

A need for transparency

Organisations need to be confident their cloud providers' security provisions meet the standards claimed. Some researchers suggest current security models are not transparent enough. Although a provider may give guarantees of data confidentiality, integrity, secure auditing and resource isolation, an organisation should look for the detail of how the provider actually enforces these measures.

"Customer experience will be the measure of business success in real-time systems"

Nick Gaines, Group IS Director, Volkswagen UK

The problem of persistence

Some of the IT department's key technical cloud security concerns relate to the location and temporary persistence of transient data. Cloud applications are designed to be accessed through a browser. Web browsers, though, cache information and if an organisation is careless, unauthorised parties can access this stored data and gain access to confidential or sensitive information.

Tackling the technical challenges

IT departments can go some way to addressing these issues by employing a web architecture that makes only presentation data (i.e. the web page plus the data being shown) available to the browser, keeping the business logic secure within the application. This ensures that business logic and core data are protected from the casual viewer.

Some browser-based applications, however, will request a wide data set from the business logic layer and then use local script rules to present pieces of that information based on the user interactions with the page. Organisations should therefore be aware that caching of such a broad data set could pose a security risk.

A future solution

In future, we may see models where cloud applications are provided with individual security policies, enabling the tracking of data across cloud software components. By understanding which components are exposed to sensitive data in a multi-tenanted cloud environment, the application can constrain and potentially avoid security problems by isolating those components[1].

Three final considerations

1. Data stored within a cloud environment may need to reference data held within systems in the organisation's data centre. This data may be sensitive, as might the reference keys used. Organisations therefore need to consider security when integrating data across cloud providers and their internal systems.
2. Organisations must also consider the security of data connections when moving a service from one provider to another provider, in order to ensure the data maintains its integrity.
3. A related consideration is the size of the data being migrated during the transition. The volume of data may mean organisations cannot undertake such an activity without some interruption to the service.

Exciting opportunities

Despite the challenges involved, IT departments that tackle cloud data security effectively will open up exciting opportunities for their organisations. Businesses will increasingly be able to exploit the hidden value of their vast amounts of information, with analysis being possible ever closer to real time. They can employ new solutions such as "big data" analytics and complex event processing engines.

More exciting still is the move away from traditional relational database structures to more open architectures such as Linked Data. This concept is famously championed by Tim Berners-Lee, the inventor of the world-wide web, who urges organisations to publish structured data online in an open, machine-readable format. The result will be a "semantic web" where data from different sources can easily be connected and queried in real time.

Notes

1. See: http://www.computing.co.uk/ctg/news/2109259/cloud-tracked-ensure-security

8

The Cloud-Friendly Security Team

A. CLOUD
Chief Security Officer
Enabler of cloud adoption

Summary

As cloud-use increases, security teams need to ensure they are seen as enablers rather than blockers. That means they need to factor cloud into their existing systems and processes. They will also increasingly require skills in contractual and provider management, as well as a firm understanding of both their business's requirements and the security implications of a multiple-cloud landscape.

Cloud is already having a profound impact on security teams, not least because of the ease with which "shadow IT" can now proliferate within organisations (see Chapter 5). The issue is often exacerbated when the IT department and the security office are perceived as cloud "blockers".

While much of what security teams do will remain the same, they will nonetheless increasingly have to factor in cloud. Organisations must be prepared to restructure security teams to reflect any change of focus and ensure they have the capabilities to meet changing security needs.

Organisations must be prepared to restructure security teams to reflect any change of focus and ensure they have the capabilities to meet changing security needs

The seven steps towards an effective cloud security team

1. Develop a cloud strategy

Security teams should develop and own cloud security strategies as part of their organisations' broader information strategies. They should then review and revise security policies, procedures and processes to embed cloud into the security function and governance model. This may mean adding new policy statements or simply extending existing ones to encompass new concepts. It may also have knock-on effects on the security teams' approaches to compliance and audit activities.

2. Focus on a federated model

As cloud becomes more broadly adopted, the team will have to understand and adapt to a federated security model, where the authentication and authorisation

Photograph: Alamy, Shutterstock

between participating services are brokered and identity data is shared across the organisation's boundaries. A centralised model becomes unsustainable in a world where much of what needs securing actually resides outside the organisation. As ever more business services appear in a cloud context, the security team will need to encompass and address security issues related to process and technology integration.

3. Move closer to contracts and the business

The security team will also need to work with the legal department to ensure contracts with providers reflect the organisation's security requirements. To this end, it should develop, in collaboration with the commercial department, appropriate requirements and provider assessment criteria to ensure it obtains the appropriate levels of security, compliance and assurance around the services it is buying.

Many security teams have already been developing these skills as a result of outsourcing. Teams are changing from being providers themselves into more of a contract assurance function. They also need to become increasingly familiar with business functions in order to interpret business requirements and assess the potential impact of meeting those requirements with cloud services.

4. Manage multiplicity

Due to the perceived risk associated with cloud, the role of the chief security officer will become increasingly critical

Security teams in organisations that are using multiple cloud services also need to understand and manage the new risks this may present. For example, the organisation may enter into a contract with a Software-as-a-Service (SaaS) vendor that hosts its application on the same cloud infrastructure the organisation uses for some of its own legacy applications.

In this example, there is an obvious risk with availability. Less obvious is the potential risk of access to a wider set of data – the legacy data and the data in the SaaS application together might be more meaningful and therefore valuable.

5. Secure the exit

Upon termination of a cloud service contract, the security team needs to be satisfied that no residual sensitive data remains anywhere on the provider's systems. That includes operational databases, backups and archives. It is worth considering this eventuality at procurement time so the relevant obligations can be clearly set out in the contract.

6. Build diverse teams

Traditionally, security teams have largely comprised in-house technical staff. However, in a cloud world, the team may need to extend to include security representatives from providers, as well as from other parts of the business. Due to the perceived risk associated with cloud, the role of the chief security officer will become increasingly critical in terms of putting all the pieces together and ensuring the organisation's data and business logic are suitably protected.

7. Seek out security standards

It is much cheaper and easier to enter into contracts with providers if there are recognised standards against which they can be judged, rather than organisations having to draw up their own set of requirements. Cloud standards are still evolving, so the security team need to keep abreast of any new developments.

In summary, the security team needs more than ever before to facilitate good practice, especially through collaboration with the cloud service provider, rather than appear to be blocking the adoption of cloud capabilities. This means moving closer to a supporting – rather than an ownership – role.

9

The Cloud Security Checklist

Summary

A simple, two-part checklist to help CIOs determine whether both the security team and the rest of the organisation are fit and ready to use cloud securely.

In *The White Book of Cloud Adoption* (see Appendix), we included an assessment model to help CIOs prioritise the company's business systems and services for cloud adoption. This model provides a simple, objective mechanism for assessing the benefits of migrating a business system (or its function) into a cloud environment against the cost and complexity of doing so. The model also helps CIOs identify what type of cloud or cloud service, if any, would be appropriate for the different systems and services they may consider migrating.

This chapter takes that original adoption assessment model one step further and provides specific pointers on the key security and risk-related considerations when assessing any move to cloud.

The first part of the checklist (starting on the next page) allows a CIO to determine if the security team is ready for cloud. The second allows CIOs and their security teams to determine if the rest of the organisation and any proposed provider can offer genuine assurance of cloud security. In both cases, organisations must be able to tick *all* (not most) of the boxes before they can claim to be secure in a cloud context.

Effective cloud security involves considerations spanning the three broad areas of management, operation and technology (see Chapter 2). As with traditional outsourcing projects, organisations need to assess not only their own capabilities, but also those of any proposed cloud service provider. So the second part of the checklist helps CIOs to break down the various considerations by business area and assess both their own organisations' cloud security readiness and that of any cloud service provider under consideration.

As with traditional outsourcing projects, organisations need to assess not only their own security capabilities, but also those of any proposed cloud service provider

Photographs: Shutterstock

Is the security team ready for cloud?

	Security team
1. Is the security team aware of/knowledgeable about cloud?	❑
2. Does the organisation have a cloud security strategy with which its auditors would be happy?	❑
3. Has security governance been adapted to include cloud?	❑
4. Does the team's structure enable cloud security?	❑
5. Has the security team updated all security policies and procedures to incorporate cloud?	❑
6. Has the security team provided guidance to the business on how to remain secure within a cloud environment?	❑

Is the organisation/provider fit for cloud security?

Management	Organisation	Provider
1. Is everyone aware of his or her cloud security responsibilities?	❑	❑
2. Is there a mechanism for assessing the security of a cloud service?	❑	❑
3. Does the business governance mitigate the security risks that can result from cloud-based "shadow IT"?	❑	❑
4. Does the organisation know within which jurisdictions its data can reside?	❑	❑
5. Is there a mechanism for managing cloud-related risks?	❑	❑
6. Does the organisation understand the data architecture needed to operate with appropriate security at all levels?	❑	❑
7. Can the organisation be confident of end-to-end service continuity across several cloud service providers?	❑	❑
8. Does the provider comply with all relevant industry standards (e.g. the UK's Data Protection Act)?	❑	❑
9. Does the compliance function understand the specific regulatory issues pertaining to the organisation's adoption of cloud services?	❑	❑

Operation	Organisation	Provider
1. Are regulatory compliance reports, audit reports and reporting information available from the provider?	❑	❑
2. Does the provider have the right attitude to incident resolution and configuration management, even when services involve multiple providers?	❑	❑
3. Does using a cloud provider give the organisation an environmental advantage?	❑	❑
4. Does the organisation know in which application or database each data entity is stored or mastered?	❑	❑
5. Is the cloud-based application maintained and disaster tolerant (i.e. would it recover from an internal or externally-caused disaster)?	❑	❑
6. Are all personnel appropriately vetted, monitored and supervised?	❑	❑
7. Is the provider able to deliver a service within the required performance parameters?	❑	❑
8. Is it easy to securely integrate the cloud-based applications at runtime and contract termination?	❑	❑
9. Do you know the location from which the provider will deliver support and management services?	❑	❑
10. Do the procurement processes contain cloud security requirements?	❑	❑

Technology	Organisation	Provider
1. Are there appropriate access controls (e.g. federated single sign-on) that give users controlled access to cloud applications?	❑	❑
2. Is data separation maintained between the organisation's information and that of other customers of the provider, at runtime and during backup (including data disposal)?	❑	❑
3. Has the organisation considered and addressed backup, recovery, archiving and decommissioning of data stored in a cloud environment?	❑	❑
4. Are mechanisms in place for identification, authorisation and key management in a cloud environment?	❑	❑
5. Are all cloud-based systems, infrastructure and physical locations suitably protected?	❑	❑
6. Are the network designs suitably secure for the organisation's cloud adoption strategy?	❑	❑

The above checklist is intended to be a high-level guide to the areas organisations need to consider. There are also several very good evaluation models already on the market:

- **Cloud Security Alliance Security Guidance** for Critical Areas of Focus in Cloud Computing V2.1
- **Gartner ID G00209052:** "Determining criteria for cloud security assessment: it's more than a checklist"
- **Cloud Legal Project** at Queen Mary, University of London (http://www.cloudlegal.ccls.qmul.ac.uk/)
- **The German Federal Office** for Information Security's security requirements for cloud computing providers
- **Cloud security study** of the Fraunhofer Institute for Secure Information Technology (SIT).

In addition, further guidance can be found from the following websites:

- **www.first.org**
- **www.cloudsecurityalliance.org**
- **www.enisa.europa.eu**
- **www.nist.gov**

10

The Final word on Cloud Security

Summary

Organisations new to cloud say security is their number one concern. Indeed, many perceive it as a significant barrier to adoption. But those further along the cloud journey have a different perspective. While security is just as important for them, it is no longer a source of worry or apprehension. It has simply become another consideration in their risk management strategies and processes. Their experience informs future decisions about moving other services into (or sourcing them from) a cloud environment, thus helping them make ever further strides along their cloud path.

In this book, we have tried to pass on the insights we have gleaned working with customers all over the world to ease their transitions to cloud. Fujitsu's extensive analysis has led to the following conclusions:

- **The type of cloud** (public, trusted, private or hybrid) has the biggest single impact on the level of risk and its manageability.
- **To assure confidentiality,** organisations need to define approaches for identifying the data to be protected and ascertaining how to access that data. To do this, they should build relationships with trusted cloud service providers.
- **Organisations should consider** an access-control approach that incorporates and integrates in-house, outsourced and cloud systems.
- **To ensure data integrity,** organisations must understand how the provider guarantees data has not been tampered with.
- **To comply with regulations** (e.g. SOX, Basel III, CSA V2, PCI-DSS, ISO 27001, BS11000, HIPPA), organisations must ensure the relevant regulatory, corporate, industry or other standards apply (legally or contractually) to the provider.
- **Building a relationship** with a trusted cloud service provider helps organisations to maintain and protect their reputation.
- **From an audit perspective,** it is important that organisations know how cloud services are provided and they must ensure providers can give them the regulatory and audit information they require.

Security is no longer a source of worry or apprehension. It has simply become another consideration in risk management strategies and processes

Photograph: Alamy

- **Business continuity strategies** need to factor in an organisation's external cloud services. Organisations must understand the impact of accepting different SLAs from different providers.
- **Disaster recovery plans** need to include the cloud service provider's plans as well as in-house plans.
- **Organisations should be prepared** for attacks (e.g. distributed denial-of-service) against both themselves and their cloud providers.
- **Organisations need to ascertain** the interoperability of providers' offerings before buying. Otherwise, there is a risk that services from different providers across infrastructure, applications and process will not join up at runtime.
- **In multi-provider environments,** organisations need to be able to quickly determine who is responsible for fixing any problem that occurs. They should choose providers willing to work with others to resolve any issues expediently.
- **Reporting across multiple service providers** can be complex. Organisations must ensure consistency of input and format from their various providers.
- **Organisations will need to manage data** at an ever more granular level as cloud solutions evolve.
- **Cloud will have a profound impact** on the security team, which will require a more diverse range of technical, contractual and business relationship skills.

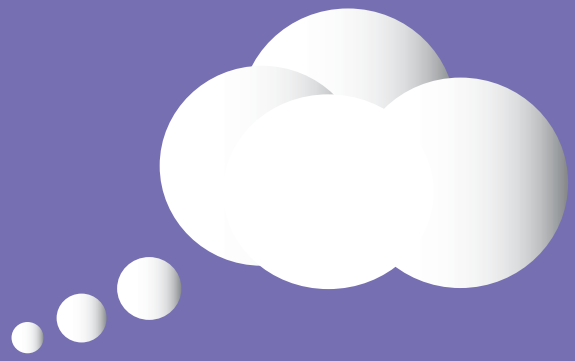
At Fujitsu, we recognise that for customers adopting cloud services, security is a key concern – and we take this very seriously

Organisations can use the cloud security checklist in Chapter 9 to ascertain how prepared their security teams and wider businesses are for cloud. There are also links to additional third-party models and frameworks for those who want to explore cloud security considerations in greater detail.

Fujitsu and cloud security

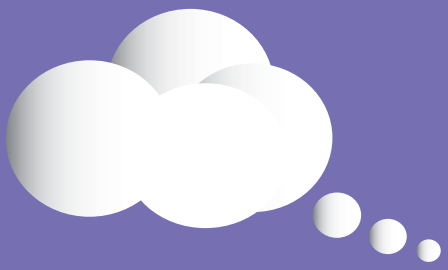
At Fujitsu, we recognise that for customers adopting cloud services, security is a key concern – and we take this very seriously. Our cloud offerings have built-in security mechanisms that address customers' concerns. We have a Cloud Security Committee focused on ensuring our cloud offerings are – and remain – secure. As an active member of the Cloud Security Alliance and other industry bodies, we are also firmly committed to the cause of furthering cloud security standards. Fujitsu's global expertise and experience in information assurance is widely recognised and means Fujitsu is ideally placed to assist customers in all areas of security, not least cloud security.

For more information on Fujitsu's cloud security capabilities and to learn how we can assist your organisation further, please contact us at: askfujitsu@uk.fujitsu.com



Cloud Security Speak: Key terms explained

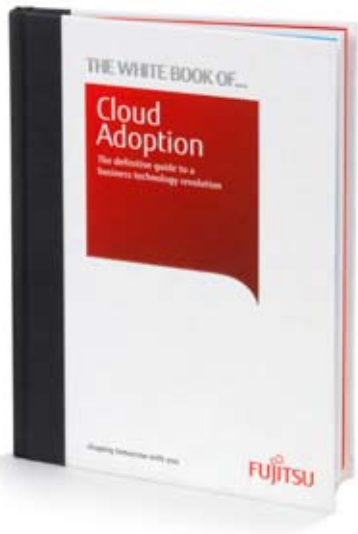
Access control	A way to control who and/or what may access a given resource, either physical (e.g. a server) or logical (e.g. a record in a database).
Architectural patterns	A design model that documents how a solution to a design problem can be achieved and repeated.
Availability	The proportion of time a system is in a functioning condition, based on a number of performance measures such as uptime .
Big data	Data sets that grow so large that they become awkward to work with using traditional database management tools. Typically contains many small records that are travelling fast.
Business continuity (BC)	(See also: Disaster recovery) Business continuity involves planning to keep all aspects of a business functioning amid disruptive events (whereas disaster recovery focuses on restoring or replicating the IT systems and services that support business functions).
Certification	Documentary confirmation that a service, product, person or organisation 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 buyer (CSB)	The organisation purchasing cloud services for consumption either by its customers or its own IT users. (Also referred to in this book as "the buyer".)
Cloud service provider (CSP)	A service provider that makes a cloud-computing environment – such as a public cloud – available to others. (Also referred to in this book as "the provider".)
Cloud services stack	The different levels at which cloud services are provided. Commonly: Infrastructure-as-a-Service (IaaS); Platform-as-a-Service (Paas); Software-as-a-Service (SaaS); Data-as-a-Service (DaaS); and Business Process-as-a-Service (BPaaS).
Confidentiality	The act of keeping data secret within a certain circle, where that information is not intended to be known publicly.
Context-sensitive	(When referring to a system) Exhibiting different behaviour depending upon the task or situation (for example, presenting data differently on different classes of device, such as personal computers, tablets and smartphones).
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 centres where it is stored).



Disaster recovery (DR)	(See also: Business continuity) The process, policies and procedures related to recovery or replication of technology infrastructure after a natural or human-induced disaster. DR is a subset of business continuity.
Distributed denial-of-service (DDoS) attack	An attempt to make a computing resource unavailable to its intended users by bombarding it with many simultaneous connection requests. "Distributed" refers to the use of multiple, dispersed systems to attack the resource.
Federation	The provision of security to allow for clean separation between the service being accessed and the associated authentication and authorisation procedures. This enables secure collaboration across multiple systems, networks and organisations employing different security systems.
Hash	A means of checking data integrity using a short code mathematically generated from the original data. Any accidental or intentional change to the data will change the hash value.
Hypertext Transfer Protocol Secure (HTTPS)	A secure protocol for the transfer of encrypted communications across a computer network.
Hypertext Transfer Protocol (HTTP) with SSL/TLS	Protocol to provide encrypted communication and secure identification of a network web server.
Integrity	In the context of data security, integrity means that the data cannot be modified without detection.
Interoperability	The ability of diverse systems and organisations to work together.
Linked data	A concept (famously championed by the web's inventor Tim Berners-Lee) in which structured data is published in a standard format so it can be interlinked and queried or read by both humans and machines. This facilitates the widespread use of multiple, diverse data sources in the creation of services and applications.
Non-repudiation	A service that provides proof of the integrity and origin of data together with authentication that can be asserted (with a high level of assurance) to be genuine.
Outsourced service provider/ managed service provider (OSP/MSP)	An external provider who manages and assumes responsibility for delivering a defined set of services, either proactively or as they are needed.
Patriot Act	The USA Patriot Act, a law enacted in the US, formerly known as the Uniting (and) Strengthening America (by) Providing Appropriate Tools Required (to) Intercept (and) Obstruct Terrorism Act of 2001.
Personally identifiable information (PII)	Data that, by its nature, is covered under privacy and data-protection legislation. This applies to information about both employees and consumers.
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 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.
Shadow IT	A term often used to describe IT systems and IT solutions built and/or used inside organisations without formal approval from the IT department.
Security information and event management (SIEM)	A solution to provide real-time analysis of security alerts generated by network hardware and applications; also used to log security data and generate reports for compliance purposes.
Single sign-on (SSO)	A mechanism whereby a single action of user authentication and authorisation permits access to multiple systems without the need to enter multiple passwords.
Security operations centre (SOC)	A business unit that deals with security issues on both an organisational and a technical level.
Tokenisation	The process of replacing a piece of sensitive data with a value that is not considered sensitive in the context of the environment in which it resides (for example, replacing an item of data with a reference to the actual data which is held in another database and hosted in a different environment).
Uptime	(See also: Availability) A measure of the time that a computer system has been available for service. Not to be confused with overall system availability, which will depend on a number of measures, including the uptime of individual components.
Vulnerability management	The cyclical practice of identifying, classifying, remediating and mitigating vulnerabilities.

Also in this series...



The White Book of Cloud Adoption:
The definitive guide to a business technology revolution

Extract from Chapter 1:
In pure business terms, cloud is essentially a flexible, scalable, pay-per-use model for the way IT services are delivered and consumed, typically through short-term contracts. With its pay-as-you-go model, cloud moves many IT costs from capital expenditure to operating expenditure; its "elastic model" means available IT capability can be flexed to mirror changing business demand; and it enables consumers of IT to have much greater transparency over their costs.

But there are different levels where that model can be applied – and the desired benefits attained:

- **Infrastructure-as-a-Service (IaaS)**
  Virtual machine services accessed over the network, providing compute and/or storage capabilities
- **Platform-as-a-Service (PaaS)**
  Platform software services (such as web, application, database servers, enterprise service buses and other middleware, with associated security mechanisms) on which web service-based applications can be built
- **Software-as-a-Service (SaaS)**
  Applications provided as a service from the cloud, with end-user licences procured or "released" in line with changing demand
- **Data-as-a-Service (DaaS)**
  Data or information delivered from the cloud either as raw data sets or consumed through an analytics interface
- **Business Process-as-a-Service (BPaaS)**
  Cloud-delivered business services that are aligned to business processes and associated measurable business outcomes.

To order a copy of this book, and for more information on the steps to cloud computing, please contact: askfujitsu@uk.fujitsu.com

Fujitsu Regional Offices

Europe, Middle East, Africa, India
FUJITSU (UK & IRELAND)
+44 (0) 870 242 7998
askfujitsu@uk.fujitsu.com
uk.fujitsu.com

FUJITSU TECHNOLOGY SOLUTIONS
(CONTINENTAL EUROPE, MIDDLE EAST, AFRICA & INDIA)
+49 1805 372 900
(14ct/min; mobile devices are limited to 42ct/min)
cic@ts.fujitsu.com
ts.fujitsu.com

FUJITSU (NORDIC REGION)
+358 45 7880 4000
info@fi.fujitsu.com
www.fujitsu.com/fi

North America
FUJITSU AMERICA , INC
+1 800 831 3183
globalcloud@us.fujitsu.com
www.fujitsu.com/us

Asia Pacific
FUJITSU HEADQUARTERS
+81 3 6252 2220
Shiodome City Center, 1-5-2 Higashi-Shimbashi
Minato-ku, Tokyo, Japan,105-7123
www.fujitsu.com

FUJITSU CHINA HOLDINGS CO LTD
+86 5887 1000
www.fujitsu.com/cn

FUJITSU (AUSTRALIA)
+61 9113 9200
askus@au.fujitsu.com
www.fujitsu.com/au

FUJITSU (NEW ZEALAND)
+64 4 495 0700
askus-nz@nz.fujitsu.com
www.fujitsu.com/nz

FUJITSU (KOREA)
+82 (080) 750 6000
webmaster@kr.fujitsu.com
www.fujitsu.com/kr

FUJITSU (SINGAPORE)
+65 6512 7555
fujitsucloud@sg.fujitsu.com
www.fujitsu.com/sg

Ref: 3369