Cloud Security checklist
Are you really ready for Cloud

Cloud Security Checklist

DISASTER RECOVERY

CONFIDENTIALITY

BIG DATA

ACCESS CONTROL

INTEGRITY

Introduction

Once you have assessed the benefits of migrating a business system or its function to the Cloud (See our White Book of Cloud Adoption), the next step is to consider the security and risk management implications of doing so.

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

If you approach cloud in the right way, with appropriate checks and balances to ensure all necessary risk management measures are covered, security is not a barrier to adoption.

This checklist enables you to make this assessment in two stages:

1   Determine how prepared the security team is for the move;

2   The readiness of the rest of the organisation by business area and any proposed provider's assurance of Cloud security.

The following provides a high-level guide to the areas organisations need to consider. Once ALL the boxes have been ticked, you can be sure you are operating in a secure Cloud context.

FUJITSU

shaping tomorrow with you

Cloud Security Checklist

1 Is the security team ready for the Cloud?

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

FUJITSU

shaping tomorrow with you

Cloud Security Checklist

2 Is your organisation /service provider ready?

Effective Cloud security considerations for the Organisation / Service provider spans three key areas:

- Management
- Operation
- Technology

Management

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"?
Organisation ■ Provider ■	Organisation ■ Provider ■	Organisation ■ Provider ■
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?
Organisation ■ Provider ■	Organisation ■ Provider ■	Organisation ■ Provider ■
7 Can the organisation be confident of end-to-end service continuity across several cloud service providers?	8 Can 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?
Organisation ■ Provider ■	Organisation ■ Provider ■	Organisation ■ Provider ■

FUJITSU

shaping tomorrow with you

DISASTER RECOVERY

CONFIDENTIALITY

BIG DATA

ACCESS CONTROL

Operation

1 Are regulatory complience reports, audit reports and reporting information available form the provider?

Organisation ■   Provider ■

2 Does the provider have the right attitude to incident resolutions and configuration management, even when services involve multiple providers?

Organisation ■   Provider ■

3 Does using a cloud provider give the organisation an environmental advantage?

Organisation ■   Provider ■

4 Does the organisation know in which application or database each data entity is stored or mastered?

Organisation ■   Provider ■

5 Is the cloud-based application maintained and disaster tolerant (i.e. would it recover from an internal or externally-caused disaster)?

Organisation ■   Provider ■

6 Are all personnel appropriately vetted, monitored and supervised?

Organisation ■   Provider ■

7 Is the provider able to deliver a service within the required performance parameters?

Organisation ■   Provider ■

8 Is it easy to securely integrate the cloud-based applications at runtime and contract termination?

Organisation ■   Provider ■

9 Do you know the loaction from which the provider will deliver support and management services?

Organisation ■   Provider ■

10 Do the procurement processes contain cloud security requirements?

Organisation ■   Provider ■

FUJITSU

shaping tomorrow with you

Cloud Security Checklist

Technology

1 Are there appropriate access controls (e.g. federated single sign-on) that give users controlled access to cloud applications?

Organisation ■   Provider ■

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)

Organisation ■   Provider ■

3 Has the organisation considered and addressed backup, recovery, archiving and decommissioning of data stored in a cloud environment?

Organisation ■   Provider ■

4 Are mechanisms in place for identification, authorisation and key management in a cloud environment?

Organisation ■   Provider ■

5 Are all cloud-based systems, infrastructure and physical locations suitably protected?

Organisation ■   Provider ■

6 Are the network designs suitably secure for the organisation's cloud adoption strategy?

Organisation ■   Provider ■

FUJITSU

shaping tomorrow with you

Closing remarks

At Fujitsu, we recognise that for companies adopting cloud services, security is a key concern. Our Cloud offerings have built-in security mechanisms that address business concerns and our Cloud Security Committee ensures our cloud offerings are founded in future-proof security principles. As an active member of the Cloud Security Alliance and other industry bodies, we are firmly committed to furthering cloud standards.

Further reading

- **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.enisa.europa.eu

www.cloudsecurityalliance.org

www.nist.gov

Contact us on:
Tel: +44 (0) 870 242 7998
Email: askfujitsu@uk.fujitsu.com
Web: uk.fujitsu.com