May 2010

Cloud Vendor Charter

Vendor Version

Not for distribution to customers

Disclaimer

Acknowledgements

This White Paper was developed by BASDA and its members as an initiative of the Cloud Special Interest Group (SIG).

Our special thanks go to:

Gary Ramsay and Conor Halpin of Opsource, Sarah Gathercole of Liquid Accounts, Bryan Richter of Mamut and David Turner of Unit4 for editing and compiling the document.

Published by BASDA, The Business Application Software Developers' Association, 92 High Street, Great Missenden, Buckinghamshire, HP16 0AN, UK, tel: +44 (0)1494 868 030, www.basda.org, e: info@basda.org

Additional copies of this document may be obtained from BASDA on +44 (0)1494 868 030; nominal price may be charged to cover our cost.

This document is part of series of documents produced by BASDA to aid our members and their customers in understanding cloud computing.

Other documents already released:
- Developing on The Cloud (White Paper)
- Cloud Vendor Charter for Customers

NOTE: This is a VENDOR ONLY version of the Charter – it contains notes to some of the charter sub-sections to give some background explanation or pointers for vendors when assessing compliance to the Charter.

This version should not be passed to non-vendor staff; a customer version of the Charter is also available – contact BASDA (www.basda.org) for more details.

Contents

1 Introduction

BASDA is the Business Application Software Developers' Association, a member-driven not-for-profit organisation where members benefit by sharing knowledge and expertise and working effectively as one voice to address strategic issues and evolving legal, political and technical influences that affect the business software industry.

Consequently, this Cloud Charter is primarily intended for software developers and independent software vendors (ISVs) that deliver their products and services through a Cloud or 'Software as a Service' architecture. However, other associated vendors and organisations may also choose to conform to the Charter.

2 Overview

The Cloud Vendor Charter outlines the minimum best practices that BASDA recommends be followed by Cloud Vendors to protect their customers' interests.

The Charter seeks to encourage a responsible approach to Data Management, Application Availability, Security and Customer Management throughout the lifecycle of the customer engagement.

The Charter aims to enhance the commercial success of both Customer and Vendor. Adhering to the Charter should not be overly burdensome for the Vendor but should assure the Customer that the Vendor deals with their business in a professional fashion and following industry best practices.

It is not the intention of the Charter to replace any of the existing industry standards such as ISO 27001, SAS 70, PCI DSS or Data Protection requirements. Where a Cloud Vendor is required to adhere to such standards, such adherence is implicit in accepting the Charter. However, customers should seek additional confirmation regarding specific standards compliance if that is critical to their organisation.

BASDA recognizes that no Charter can guarantee the commercial success of a Vendor organisation or provide a 100% guarantee against security breaches or systems failures. However adherence to the Charter will help reduce the chances of issues arising and mitigate the worst effects of such events.

Specifically we have considered:
- Security
- Reliability and Availability
- Application Life-Cycle management
- Customer Life-Cycle Management.

Across each of the four areas above consideration has been given to the following stages in the lifecycle of a customer engagement with the Vendor:
- Registration and On-boarding
- On-going operations
- Contract renewal
- Vendor migration

The Charter defines general minimum conditions whose effects cross all of the areas listed above and then describes some specific requirements for the sub-sections.

3 Cloud Vendor Requirements

3.1 Compliance requirements

All Vendors must adhere to the appropriate Data Protection Legislation as it applies to their customers.

Where specific industry compliance requirements exist Vendors undertake to meet those requirements and to undergo mandated audits.

3.2 Hosting

Cloud applications should be hosted at a location which meets the standards of a Tier 3 data centre[1]. Tier 3 describes the physical security and layout of a data centre together with redundant power, bandwidth and cooling.

NOTE FOR VENDORS: Few Cloud Vendors have the resources necessary to secure a data centre and provide the power, cooling and redundant bandwidth services necessary to guarantee a reasonable level of availability. Managed hosting that provides this level of service is readily available and at a reasonable cost. Furthermore most cloud infrastructure providers such as Amazon EC2, OpSource and RackSpace meet these requirements as a matter of course. This requirement will mean that Vendors will normally not be able to host at their own premise. This requirement immediately delivers a minimum standard of physical security and system availability.

1. (Following the four-tier classification system for data centre infrastructure and design by the Uptime Institute and generally accepted as industry standard.)

3.3 Back-up

All data should be backed up daily to an off-site location with a minimum two-day retention.

In other words:

• If a data storage device fails, or a data centre becomes unavailable the customer should not lose their data at least up to the previous day's operations; and

• A customer should be able to request the restoration of their data to a point at least two days prior in the event that some processing error occurs (e.g. an operator deletes data).

NOTE FOR VENDORS: Back-ups do not imply a disaster recovery strategy; simply that data is not lost. If a data centre was compromised there could be a significant delay (weeks) before a customer had access to their data, but it would not be lost.

Restoration of back-ups should be tested at least annually and also after any significant change in back-up strategy (e.g. new back-up software) or physical deployment (e.g. move to a new data centre). Evidence of back-up tests should be maintained.

NOTE FOR VENDORS: Back-ups cannot be assumed to be successful. When first deployed a back-up strategy must be tested and then tested at least annually to ensure that the process has not been compromised.

3.4 Data export

The Vendor should provide a mechanism, at no extra cost, for customers to take a copy of their core transaction data in a usable format (such as .csv).

NOTE FOR VENDORS:

• The definition of 'core transaction data' is intended to refer to the customer transaction information rather than all lookup/reference tables.

• An open question remains about archived data and how this can be exported by a Vendor. The intention is that the export should apply to on-line transaction information rather than off-line archived data.

• The implication of the description is that for the customer to 'take' a copy does not require a manual process from the Vendor but can be achieved by the customer through the user interface of the Vendor application.

• While the full data set may be of limited value without the application code, the customer at the very least can download their data and potentially upload it into a new system.

3.5 Complaints

The Vendor provides a mechanism for the Customer to register a complaint with the Vendor via electronic means (email, web-form) and for that complaint to be formally acknowledged, tracked and escalated within the Vendor organization.

3.6 Policies

Vendors commit to having a clear and published:

• Privacy Policy
• Complaints Policy
• Acceptable Usage Policy
• Support Policy.

3.7 Specific security requirements

Passwords: All Customer passwords should be encrypted (in the database and for transmission).

Security breach notification: If a security breach occurs or is suspected to have occurred customers should be notified of that breach as soon as possible and in any event not more than 12 hours after such a breach has been discovered. Vendors should have a formal procedure in place to deal with such notifications.

3.8 Service availability requirements

Issues often arise when the production environment is changed and so Vendors should have a documented release management policy. This policy should cover both application and environment (e.g. operating system, database, middleware) changes.

Vendors will provide automated monitoring and alerting of critical service components. Vendors will have a documented support policy to respond to alerts. The escalation process and response times by Vendor will be commensurate with the service criticality and hours of use by customers.

NOTE FOR VENDORS: The level of support and the escalation procedures will be different for different services depending on how critical they are. However in all cases there should be details of how Vendor responds to incidents, either from monitors or customer calls.

3.9 Specific customer management requirements

Customers should be provided with a mechanism to keep a complete copy of their contract or subscription agreement at the time of the agreement (for example the ability to print as a PDF). The Vendor will maintain a record of the actual terms of the agreement that was accepted by each customer.

It should be clear to customers who the legal contracting party is and who the billing entity is.

Vendors should allow customers reasonable termination clauses as part of the subscription agreements. This can include the option for the customer to notify them of their wish not to renew their contract at any time during their subscription. Specific limited time windows for such notifications (e.g. 30 days prior to an annual renewal) should not form part of an agreement.

Vendors should provide customers with reasonable notice of pricing changes. The notice period should be sufficient for the customer to plan and move off the service if they do not wish to continue using the service after the price adjustment.

Notes:

About BASDA:

www.basda.org

BASDA is the Business Application Software Developers' Association, a member-driven not-for-profit organisation where members benefit by sharing knowledge and expertise and working effectively as one voice to address strategic issues and evolving legal, political and technical influences that affect the business software industry. BASDA's members range from small, medium and large national & international software & service providers, primarily to businesses.

The BASDA's Cloud SIG Aims and Objectives

This Specialist Interest Group has been set up to raise the profile of business Cloud computing applications, exploring ideas around standards and best practice and producing deliverables that benefit both members, partners and end users.

- Ensure that members of BASDA understand both the potential and the implications for developing Cloud business applications.
- Inform and educate end users about Cloud business applications – the potential benefits and the considerations for implementation.
- Communicate with the wider industry and bodies that influence the future of Cloud computing