The CIO's Guide to Oracle Products and Solutions

Jessica Keyes

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN AUERBACH BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed on acid-free paper
Version Date: 20140623

International Standard Book Number-13: 978-1-4822-4994-1 (Hardback)

Library of Congress Cataloging-in-Publication Data

Keyes, Jessica, 1950-
The CIO's guide to Oracle products and solutions / Jessica Keyes.
pages cm
Summary: "This book is the go-to guide for all things Oracle. It provides management level guidance for successfully navigating and managing the Oracle-verse. Coverage includes executive level overviews of the Oracle product line - features and benefits; management best practices; user/developer lessons learned; management considerations; compliance and security considerations, and management metrics"-- Provided by publisher.
Includes bibliographical references and index.
ISBN 978-1-4822-4994-1 (hardback)
1. Oracle (Computer file) 2. Relational databases. I. Title.

QA76.9.D3K358975 2014
005.75'6--dc23 2014023833

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

5

Oracle Cloud

It should come as no surprise that Oracle is deep into all things "cloud." As shown in Figure 5.1, Oracle delivers a very broad selection of enterprise-grade cloud solutions, including software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). Table 5.1 shows the scale of Oracle's public cloud offerings. Virtually, all of their software is available for use on their public cloud.

As shown in Table 5.2, Oracle also delivers end-to-end managed cloud services across its broad portfolio of business applications, middleware, database, and hardware technologies.

Finally, as shown in Table 5.3, Oracle provides an integrated set of products and services to support private cloud applications, platforms, and infrastructure. The product and service set includes applications, lifecycle management, and security.

From a technical perspective, much of Oracle's cloud offerings are based on the Oracle Cloud File System. CloudFS, a storage management suite developed by Oracle Corporation, consists of a cluster file system called ASM Cluster File System (ACFS) and a cluster volume manager called ASM Dynamic Volume Manager (ADVM).

ACFS is a standard-based POSIX (Linux, UNIX) and Windows cluster file system with full cluster-wide file and memory-mapped I/O cache coherency and file locking. ACFS provides direct I/O for Oracle database I/O workloads. However, for better response time, ACFS implements indirect I/O for general purpose files that typically perform small I/O. CloudFS is designed to scale to billions of files and supports very large file and file systems sizes (up to exabytes of storage).

CloudFS is built on top of Oracle Automatic Storage Management (ASM) and Oracle clustering technologies to provide cluster volume and file services to clients. ADVM and ACFS leverage ASM striping, mirroring, and

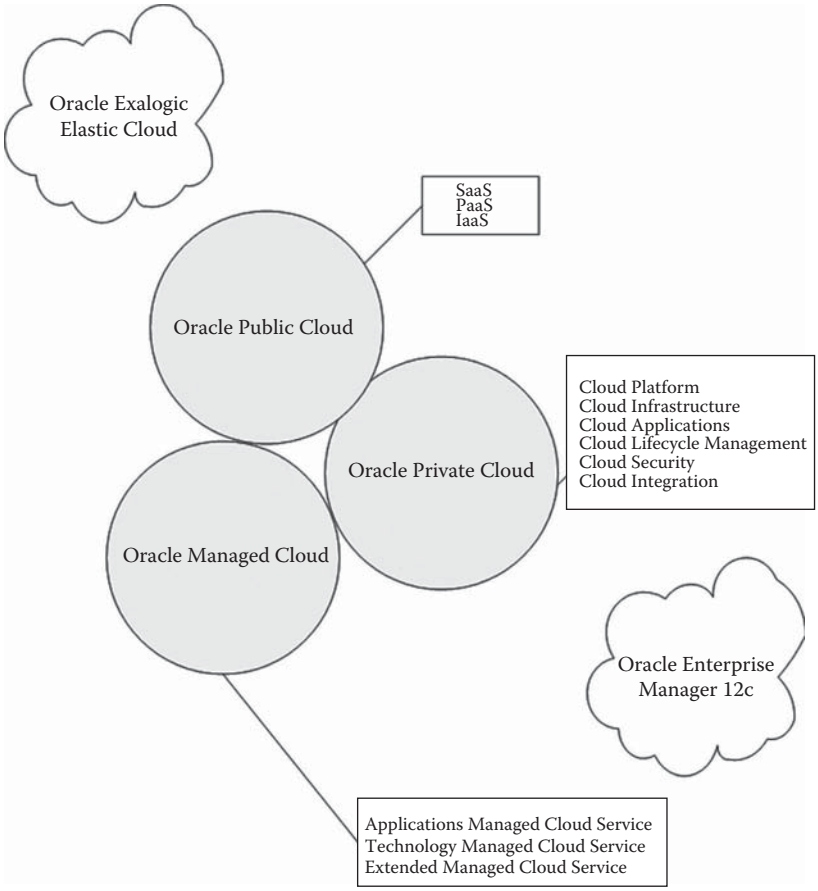

FIGURE 5.1
Oracle's cloud offerings.

automatic I/O rebalancing features to manage volumes that are dynamically resizable. ACFS supports Oracle database files as well as general purpose files.

Database as a Service (DBaaS) offers organizations accelerated deployment, elastic capacity, greater consolidation efficiency, higher availability, and lower overall operational cost and complexity. Oracle database 12c provides an innovative multitenant architecture featuring pluggable databases that makes it easy to offer DBaaS and consolidate databases on clouds. To support customers' move to this model, Oracle Enterprise Manager 12c adds new automation capabilities to enable quick provisioning of database clouds through self-service, saving administrators

TABLE 5.1

Oracle Public Cloud Offerings

Business Area	Product
Marketing	Oracle Eloqua
Sales	Oracle Sales Cloud: • Oracle Sales Cloud for Outlook • Oracle Sales Cloud Mobile • CX Integrations to Oracle Sales Cloud • Oracle Sales Cloud Customer Data Management
Service	Oracle Service: • Oracle RightNow Virtual Assistant Cloud Service • Oracle RightNow Analytics Cloud Service • Oracle RightNow CX Cloud Service May 2012 Release—Capabilities and Benefits • Oracle RightNow Chat Cloud Service • Oracle RightNow Cobrowse Cloud Service • Oracle RightNow Dynamic Agent Desktop Cloud Service • Oracle RightNow Dynamic Agent Desktop Cloud Service: Contact Center Experience Designer Feature • Oracle RightNow Dynamic Agent Desktop Cloud Service for Case Management • Oracle RightNow Email Management Cloud Service • Oracle RightNow Feedback Cloud Service • Oracle RightNow Government Cloud Platform Cloud Service • Oracle RightNow Guided Assistance Cloud Service • Oracle RightNow Innovation Community Cloud Service • Oracle RightNow Intent Guide Cloud Service • Oracle RightNow Outreach Cloud Service • Oracle Policy Automation for Mobile Devices • Oracle RightNow PCI Certified Cloud Platform Cloud Service • Oracle RightNow Platform • Oracle RightNow Social Experience • Oracle RightNow Self Service for Facebook Cloud Service • Oracle RightNow Social Monitor Cloud Service • Oracle RightNow Support Community Cloud Service • Oracle RightNow Virtual CIO Cloud Service • Oracle RightNow Web Self Service Cloud Service • Oracle Knowledge Release 8.5—Capabilities and Benefits • Oracle Knowledge Analytics

(Continued)

TABLE 5.1 (CONTINUED)

Oracle Public Cloud Offerings

Business Area	Product
	• Oracle Knowledge for Contact Center • Oracle Knowledge Solutions • Oracle Knowledge for Web Self Service • Oracle Knowledge Products and Oracle CRM On Demand • Oracle Policy Automation for Insurance • Oracle Policy Automation for Financial Services • Oracle Policy Automation Solution for Public Sector • Oracle Policy Automation Solution for Social Services • Oracle Policy Automation for Immigration • Oracle Policy Automation for Mobile Devices
Global human resources	Oracle Human Capital Management: • Oracle Human Capital Management • Oracle Global Payroll and Global Payroll Interface • Oracle Global Benefits Management • Oracle Performance Management • Oracle Goal Management • Oracle Talent Review and Succession Management • Oracle Workforce Compensation • Oracle Workforce Predictions • Oracle Transactional Business Intelligence
Talent management	Oracle Talent Management: • Oracle Talent Management Base • Oracle Taleo Recruiting Cloud Service • Oracle Taleo Onboarding Cloud Service • Oracle Performance Management • Oracle Goal Management • Oracle Talent Review and Succession Management • Oracle Workforce Compensation • Oracle Transactional Business Intelligence
Talent management for SMB	Oracle Taleo Business Edition
ERP	Oracle ERP: • Oracle Financials Cloud Service • Oracle Project Portfolio Management Cloud Service • Oracle Project Management Cloud Service • Oracle Project Resource Management Cloud Service • Oracle Task Management Cloud Service • Oracle Procurement Contracts

(Continued)

TABLE 5.1 (CONTINUED)

Oracle Public Cloud Offerings

Business Area	Product
	• Oracle Purchasing • Oracle Sourcing • Oracle Product Hub Cloud Service • Oracle Inventory and Cost Management
Enterprise planning	Oracle Planning and Budgeting Cloud Service
Financial reporting	Oracle Financial Reporting Cloud Service
Social networking	Oracle Social Network
Social marketing	Oracle Social Marketing: • Oracle Social Marketing Cloud Service • Oracle Social Engagement and Monitoring • Oracle Social Data and Insight
Build apps	Oracle Build Apps: • Database • Java • Developer • Documents • Business Intelligence • Mobile
Cloud marketplace	Apps from third-party vendors

time and effort. These new capabilities can help customers adopt Oracle Database 12c faster and pave the way to a DBaaS delivery model.

Oracle has also thrown a hardware solution into the mix. Oracle Exalogic Elastic Cloud is a computer appliance available since 2010. It is a cluster of x86-64 servers running Oracle Linux or Oracle Solaris preinstalled. Two 64-bit operating systems run on the server nodes of the appliance: Oracle Linux version 5.5 or Solaris 11. All servers have an installed cluster configuration of Oracle WebLogic Server and distributed memory cache Oracle Coherence. To run Java applications on a machine, there is a choice of HotSpot or JRockit. Management of the appliance is available in the Oracle Enterprise Manager toolset, which is also preinstalled in the appliance. A transaction monitor Tuxedo is optionally supplied.

Exalogic is being used by a wide variety of organizations, including the University of Melbourne, Food and Drug Administration (FDA), Amway, the Hyundai Motor Group, and the Bank of Chile.

TABLE 5.2

Oracle Managed Cloud Services

	Purpose	Features
Applications managed cloud service	With Oracle Applications Managed Cloud Service, the organization is able to choose the best deployment model for its business needs without lock-in. Oracle can manage applications onsite, through Oracle's partners, or at one of their data centers.	• Complete cloud-management services for any Oracle application • Ensures best practices across functional pillars in the cloud • Lets you manage your cloud applications any way you want • Offers choice of hosting @ Oracle, @ customer, @ partner, and hybrid options • Ensures enterprise-grade cloud security and performance
Technology managed cloud service	Oracle Technology Managed Cloud Service provides end-to-end management services delivered in the cloud and managed by Oracle.	• Delivers and manages Oracle technology and applications in the cloud • Uses standard configurations, including ITL-based compliant processes • Includes architecture design, monitoring, change management, security, and more • Provides hosting and management for the Oracle Technology Platform • Offers hosting and management for Oracle Engineered Systems
Extended managed cloud service	Oracle Extended Managed Cloud Service goes beyond core infrastructure and application management services to provide services that span the entire software life cycle, from migration, testing, and deployment to compliance and disaster recovery.	• Security services • Testing services • Transition services • Disaster recovery services

TABLE 5.3

Oracle Private Cloud

	Purpose	Features
Cloud platform	The Oracle Cloud Platform (also known as Platform as a Service [PaaS]) provides a shared and elastically scalable platform for consolidation of existing applications and new application development and deployment.	• Delivers greater agility through faster application development • Leveraging standards-based shared services and elastic scalability on demand • Includes database functionality based on Oracle Database and Oracle Exadata Database Machine • Features middleware technology based on Oracle Fusion Middleware and Oracle Exalogic Elastic Cloud • Engineered systems such as Exadata and Exalogic provide extreme performance and efficiency for mixed workloads
Cloud infrastructure	Oracle Cloud Infrastructure provides a complete selection of servers, storage, networking fabric, virtualization software, operating systems, and management software to support diverse public and private cloud applications.	• Flexible cloud infrastructure supports dynamic resource pooling, elastic scalability, and rapid application deployment • Includes Oracle Enterprise Manager, a complete cloud life-cycle management solution that allows you to quickly set up, manage, and support enterprise clouds and traditional Oracle IT environments from applications to disk • Built-in security and high availability • Application-aware virtualization and management capabilities

(Continued)

TABLE 5.3 (CONTINUED)

Oracle Private Cloud

	Purpose	Features
Cloud applications	Oracle's Cloud Applications are a complete and modular set of enterprise applications	• Complete and best-practice business processes across functional pillars in the cloud • Cloud applications any way you want them: in a public, private, or hybrid cloud • Global and enterprise-grade cloud security and performance to meet even the most-demanding requirements
Cloud life-cycle management	Oracle Enterprise Manager is Oracle's complete cloud life-cycle management solution. It provides self-service provisioning balanced against centralized, policy-based resource management, integrated chargeback and capacity planning, and complete visibility of the physical and virtual environment from applications to disk.	• Plan and set up the cloud with capacity and optimization planning, analysis, and recommendations, including definition of policies and rules needed to automate self-service provisioning • Build, test, and deploy applications on the cloud with an out-of-the-box, self-service portal • Track, report, and manage resource utilization and performance, including policy-driven scale-up and scale-down of resources; includes monitoring for cloud resource usage and request management • Meter, charge, and optimize your cloud with application-to-disk resource metering that tracks resource utilization and cost, ties back to internal billing and management reporting systems as needed, and automatically optimizes resources • Consolidate underutilized servers for migration to the cloud

(Continued)

TABLE 5.3 (CONTINUED)

Oracle Private Cloud

	Purpose	Features
Cloud security	Oracle Cloud Security leverages Oracle expertise in data security, identity management, and governance, risk, and compliance to provide a comprehensive, reliable solution for deployment in any cloud environment.	• Provides a comprehensive set of solutions to mitigate threats across your databases and applications • Deployed by thousands of leading organizations to address compliance for multiple government and industry regulations
Cloud integration	Oracle simplifies cloud integration by providing a unified and comprehensive solution to integrate disparate cloud and on-premise applications. Oracle cloud integration leverages Oracle Cloud Services as well as components from Oracle's SOA, BPM, and data-integration technologies.	• Comprehensive and unified set of components seamlessly integrating on-premises and cloud applications and services • Proven integration technologies deployed by thousands of leading organizations to ensure high reliability, real-time performance, and trusted integration • Leverages existing investments in Oracle database, middleware, applications, and hardware systems while working with third-party cloud applications

MANAGING THE CLOUD

Oracle's cloud products and services make it possible to run the entirety of an organization's business applications, and host all of its information assets, in the cloud. While many opt for a private cloud, more than a few organizations have moved to public or managed clouds. Thus, it is worthwhile to consider the cloud dynamic, including selection, legal issues, and security. The federal government's CIO Council carefully considered these issues (2012). This chapter aligns with their findings and recommendations.

The adoption of cloud computing represents a dramatic shift in the way organizations buy IT—a shift from periodic capital expenditures to lower cost and predictable operating expenditures. With this shift comes

a learning curve regarding the effective procurement of cloud-based services.

Cloud computing presents a paradigm shift that is larger than IT, and while there are technology changes with cloud services, the more substantive issues that need to be addressed lie in the business and contracting models applicable to cloud services. This new paradigm requires organizations to rethink not only the way they acquire IT services in the context of deployment, but also how the IT services they consume provide mission and support functions on a shared basis. Organizations should begin to design and/or select solutions that allow for purchasing based on consumption in the shared model that cloud-based architectures provide.

Cloud computing allows consumers to buy IT in a new, consumption-based model. Given the dynamic nature of end-user needs, the traditional method of acquiring IT has become less effective in ensuring the organization effectively covers all of its requirements. By moving from purchasing IT in a way that requires capital expenditures and overhead, and instead purchasing IT on-demand as an organization consumes services, unique requirements have arisen that organizations need to address when contracting with cloud service providers (CSPs).

Selecting a Cloud Service

The primary driver behind purchasing any new IT service is to effectively meet a commodity, support, or mission requirement that the organization has. Part of the analysis of that need or problem is determining the appropriate solution. Choosing the cloud is only the first step in this analysis. It is also critical for organizations to decide which cloud service and deployment model best meets their needs.

The National Institute of Standards and Technology (NIST) has defined three cloud computing service models: Infrastructure as a Service, Platform as a Service, and Software as a Service.

These service models can be summarized as:

1. *Infrastructure*: The provision of processing, storage, networking, and other fundamental computing resources
2. *Platform*: The deployment of applications created using programming languages, libraries, services, and tools supported by a cloud provider

3. *Software*: The use of applications running on a cloud infrastructure environment

Each service model offers unique functionality depending on the class of user, with control of the environment decreasing as you move from infrastructure to platform to software. Infrastructure is most suitable for users like network administrators, as organizations can place unique platforms and software on the infrastructure being consumed. Platform is most suitable for users like server or system administrators in development and deployment activities. Software is most appropriate for end users, since all functionalities are usually offered out of the box. Understanding the degree of functionality and what users will consume the services is critical for organizations in determining the appropriate cloud service to procure.

NIST has also defined four deployment models for cloud services: Private, Public, Community, and Hybrid. These service deployments can be summarized as:

1. *Private*: For use by a single organization
2. *Public*: For use by general public
3. *Community*: For use by a specific community of organizations with a shared purpose
4. *Hybrid*: A composition of two or more cloud infrastructures (public, private, community)

These deployment models determine the number of consumers (multitenancy) and the nature of other consumers' data that may be present in a cloud environment. A public cloud does not allow a consumer to know or control who the other consumers of a cloud service provider's environment are. However, a private cloud can allow for ultimate control in selecting who has access to a cloud environment. Community clouds and hybrid clouds allow for a mixed degree of control and knowledge of other consumers. Additionally, the cost for cloud services typically increases as the control over other consumers and knowledge of these consumers increases. When consuming cloud services, it is important for organizations to understand what type of data they will be placing in the environment and to select the deployment type that corresponds to the appropriate level of control and data sensitivity.

To choose a cloud service that will properly meet a unique need, it is vital to first determine the proper level of service and deployment.

Organizations should endeavor to understand not only what functionality they will receive when using a cloud service, but also how the deployment model a cloud service utilizes will affect the environment in which data is placed.

CSP and End-User Agreements

CSPs enforce common acceptable-use standards across all users to effectively maintain how a consumer uses a CSP environment. Thus, use of a CSP environment usually requires end users to sign terms-of-service (TOS) agreements. Additionally, organizations can also require CSPs to sign nondisclosure agreements (NDAs) to enforce acceptable CSP personnel behavior when dealing with data. TOS and NDAs need to be fully contemplated and agreed upon by both CSPs and organizations to ensure that all parties fully understand the breadth and scope of their duties when using cloud services. These agreements are new to many IT contracts because of the nature of the interaction of end users with CSP environments.

Terms of Service Agreements

Organizations need to know if a CSP requires an end user to agree to TOS in order to use the CSP's services prior to signing a contract. TOS restrict the ways consumers can use CSP environments. They include provisions that detail how end users may use the services, the responsibilities of the CSP, and how the CSP will deal with customer data. Provisions within a TOS may contradict organizational policies. Given that, organizations are advised to work with CSPs to understand what they require in order for end users to access a CSP environment and at the same time ensure that any TOS document incorporated into the contract is acceptable to the organization. If the TOS are not directly within the contract but only referenced within the contract, the TOS should be negotiated and agreed upon prior to contract award.

Additionally, TOS sometimes include provisions relating to CSP responsibilities, controlling law, indemnification, and other issues that are more appropriate for the terms and conditions of the contract. If these provisions are included within service agreements, they should be clearly defined. Furthermore, any agreements must address time requirements that a CSP will need to follow to comply with rules and regulations.

Nondisclosure Agreements

Some organizations require CSP personnel to sign NDAs when dealing with data. These are usually requested by organizations in order to ensure that CSP personnel protect nonpublic information that is procurement sensitive or affects predecisional policy, physical security, etc. Organizations will need to consider the requirements and enforceability of NDAs with CSP personnel. The acceptable behavior prescribed by NDAs requires oversight, including examining the NDAs' requirements in the rules of behavior and monitoring of end-user activities in the cloud environment. CSP and end-user agreements such as TOS and NDAs are important to both organizations and CSPs in order to clearly define the acceptable behavior by end users and CSP personnel when using cloud services. These agreements should be fully contemplated by both CSPs and organizations prior to cloud services being procured. All such agreements should be incorporated, either by full text or by reference, into the CSP contract in order to avoid the usually costly and time-consuming process of negotiating these agreements after the enactment of a cloud computing contract.

Service-Level Agreements

Service-level agreements (SLAs) are agreements under the umbrella of the overall cloud computing contract between a CSP and an organization. SLAs define acceptable service levels to be provided by the CSP to its customers in measurable terms. The ability of a CSP to perform at acceptable levels is consistent among SLAs, but the definition, measurement, and enforcement of this performance varies widely among CSPs. Organizations should ensure that CSP performance is clearly specified in all SLAs and that all such agreements are fully incorporated, either by full text or by reference, into the CSP contract.

Terms and Definitions

SLAs are necessary between a CSP and customer to contractually agree upon the acceptable service levels expected from a CSP. SLAs across CSPs have many common terms, but definitions and performance metrics can vary widely among vendors. For instance, CSPs can differ in their definition of uptime (one measure of reliability) by stating

that uptime is not met only when services are unavailable for periods exceeding one hour. To further complicate this, many CSPs define availability (another measure of reliability sometimes used within the definition of uptime) in a way that may exclude CSP planned service outages. Organizations need to fully understand any ambiguities in the definitions of cloud computing terms in order to know what levels of service they can expect from a CSP.

Measuring SLA Performance

When organizations place data in a CSP environment, they are inherently giving up control over certain aspects of the services that they consume. As a best practice, SLAs should clearly define how performance is guaranteed (such as response time, resolution/mitigation time, availability, etc.) and require CSPs to monitor their service levels, provide timely notification of a failure to meet the SLAs, and evidence that problems have been resolved or mitigated. SLA performance clauses should be consistent with the performance clauses within the contract. Organizations should enforce this by requiring in the reporting clauses of the SLA and the contract that CSPs submit reports or provide a dashboard so that organizations can continuously verify that service levels are being met. Without this provision, an organization may not be able to measure CSP performance.

SLA Enforcement Mechanisms

Most standard SLAs provided by CSPs do not include provisions for penalties if an SLA is not met. The consequence to a customer if an SLA is not met can be catastrophic (unavailability during peak demand, for example). However, without a penalty for CSPs in the SLA, CSPs may not have sufficient incentives to meet the agreed-upon service levels. In order to incentivize CSPs to meet the contract terms, there should be a credible consequence (for example, a monetary or service credit) so that a failure to meet the agreed-upon terms creates an undesired business outcome for the CSP in addition to the customer.

With many of the high-profile cases of cloud service provider failures relating to provisions covered by SLAs, as a best practice, organizations need SLAs that provide value and can be enforced when a service level is not met. SLAs with clearly defined terms and

definitions, performance metrics measured and guaranteed by CSPs, and enforcement mechanisms for meeting service levels will provide value to organizations and incentives for CSPs to meet the agreed-upon terms.

CSP, Organization, and Integrator Roles and Responsibilities

Many organizations procure cloud services through integrators. In these cases, integrators can provide a level of expertise within CSP environments that organizations may not have, thus making an organization's transition to cloud services easier. Integrators may also provide a full range of services from technical support to help-desk support that CSPs might not provide. When deciding to use an integrator, the organization may procure services directly from a CSP and separately with an integrator, or it may procure cloud services through an integrator as the prime contractor and the CSP as subcontractor. Whichever method the organization decides to use, the addition of an integrator to a cloud computing implementation creates contractual relationships with at least three unique parties, and the roles and responsibilities for all parties need to be clearly defined.

Contracting with Integrators

Integrators can be contracted independently of CSPs or can act as an intermediary with CSPs. This flexibility allows organizations to choose the most effective method for contracting with integrators to help implement their cloud computing solutions. As a best practice, organizations need to consider the technical abilities and overall service offerings of integrators and how these elements impact the overall pricing of an integrator's proposed services. Additionally, if an organization contracts with an integrator acting as an intermediary, the organization must consider how this affects the organization's continued use of a CSP environment when the contract with an integrator ends.

Clearly Defined Roles and Responsibilities

Whether an organization contracts with an integrator independently or uses one as an intermediary, roles and responsibilities need to be clearly

defined. Scenarios that need to be clearly defined within a cloud computing solution that incorporate an integrator include:

- How an organization interacts with a CSP to manage the CSP environment
- What access an integrator has to data within a CSP environment
- What actions an integrator may take on behalf of an organization

Failure to address the roles and responsibilities of each party can hinder the end user's ability to fully realize the benefits of cloud computing. For instance, if initiating a new instance of a virtual machine requires an organization to interact with an integrator, then this interaction breaks the on-demand essential characteristic of cloud computing.

The introduction of integrators to cloud computing solutions can be a critical element of success for many organizations. However, the introduction of an additional party to a cloud computing contract requires organizations to fully consider the most effective method of contracting with an integrator and clearly define the roles and responsibilities among CSPs, organizations, and integrators.

Standards

Standards are available in support of many of the functions and requirements for cloud computing. While many of these standards were developed in support of pre-cloud computing technologies, such as those designed for web services and the Internet, they also support the functions and requirements of cloud computing. Other standards are now being developed in specific support of cloud computing functions and requirements, such as virtualization.

Security

Placing data on an information system involves risk, so it is critical for organizations to ensure that the IT environment in which they are storing and accessing data is secure.

Because of the variability in risk postures among different CSP environments and differing missions and needs, the determination of the appropriate levels of security vary across organizations and across CSP environments.

Organizations must evaluate the type of data they will be placing into a CSP environment and categorize their security needs accordingly.

Based on the level of security that an organization determines a CSP environment must meet, the organization then must determine which security controls a CSP will implement within the cloud environment. Within this framework, organizations need to explicitly state not only the security impact level of the system (i.e., the CSP environment must meet high, moderate, or low impact level), but organizations must also specify the security controls associated with the impact level the CSP must meet.

Continuous Monitoring

After organizations complete a security authorization of a system based on clear and defined security authorization requirements detailing the security controls a CSP must implement on their system, organizations must continue to ensure that a CSP environment maintains an acceptable level of risk. In order to do this, organizations should work with CSPs to implement a continuous monitoring program. Continuous monitoring programs are designed to ensure that the level of security through a CSP's initial security authorization is maintained while organizational data resides within a CSP's environment.

Incident Response

Incident response refers to activities addressing breaches of systems, leaks/spillage of data, and unauthorized access to data. Organizations need to work with CSPs to ensure that CSPs employ satisfactory incident response plans and have clear procedures regarding how the CSP responds to incidents as specified in the organization's computer security incident-handling guidelines.

Organizations must ensure that contracts with CSPs include CSP liability for data security. An organization's ability to effectively monitor for incidents and threats requires working with CSPs to ensure compliance with all data security standards, laws, initiatives, and policies.

Generally, CSPs take ownership of their environment but not the data placed in their environment. As a best practice, cloud contracts should not permit a CSP to deny responsibility if there is a data breach within its environment. Organizations should make explicit in cloud computing contracts that CSPs indemnify organizations if a breach should occur, and the CSP should be required to provide adequate capital and/or insurance

to support their indemnity. In instances where expected standards are not met, then the CSP must be required to assume the liability if an incident occurs directly related to the lack of compliance. In all instances, it is vital for organizations to practice vigilant oversight.

When incidents do occur, CSPs should be held accountable for incident responsiveness to security breaches and for maintaining the level of security required by the organization. Organizations should work with CSPs to define an acceptable time period for the CSP to mitigate and resecure the system.

At a minimum, when implementing an incident response policy, organizations should ensure that:

1. CSPs are contractually complying with organizational security guidelines.
2. CSPs are accountable for incident responsiveness, including providing specific time frames for restoration of secure services in the event of an incident.

Key Escrow

Key escrow (also known as a fair cryptosystem or key management) is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys. Procedural and regulatory regimes in environments where the organizations own the systems storing and transporting encrypted data are fairly well settled. These regimes, however, become increasingly complex when inserted into a cloud environment.

Organizations should carefully evaluate CSP solutions to understand completely how a CSP fully does key management, including how the key's encrypted data are escrowed and what terms and conditions of escrow apply to accessing encrypted data.

Forensics

When an organization uses a CSP environment, it should ensure that a CSP only makes changes to the environment on pre-agreed-upon terms and conditions or as required by organization to defend against an actual or potential incident. Organizations should require CSPs to allow forensic investigations for regulatory, criminal, and noncriminal purposes, and

these investigations should be able to be conducted without affecting data integrity and without interference from the CSP. In addition, CSPs should only be allowed to make changes to the cloud environment under specific standard operating procedures agreed to by the CSP and organization in the contract.

Audit Logs

Organizations must work with CSPs to ensure that audit logs of a CSP environment are preserved with the same standards as are required by organizations. Organizations must outline which CSP personnel have access to audit logs prior to placing data in the CSP environment. All CSP personnel who have access to the audit logs must have the proper clearances as required by the organization. Essentially:

1. All audit/transaction files should be made available to authorized personnel in read-only mode.
2. Audit transaction records should never be modified or deleted.
3. Access to online audit logs should be strictly controlled. Only authorized users may be allowed to access audit transaction files.
4. Audit/transaction records should be backed up and stored safely off site.

Privacy Impact Assessments (PIA)

The PIA process helps ensure that organizations evaluate and consider how they will mitigate privacy risks while complying with applicable privacy laws and regulations governing an individual's privacy in order to ensure confidentiality, integrity, and availability of an individual's personal information at every stage of development and operation. Typically, organizations conduct a PIA during the security authorization process for IT systems before operating a new system and update.

Some of the normal PIA considerations to include are:

1. What information will be collected and put into the CSP environment
2. Why the information is being collected
3. Intended use of the information
4. With whom the information might be shared

5. Whether individuals will be notified that their information will be maintained in a CSP environment and what opportunities individuals have to decline to provide information that will be maintained in a CSP environment
6. What ability individuals have to consent to particular uses of the information, and how individuals can grant consent
7. How the organization and CSP will secure information in the cloud

In addition, a cloud computing PIA should focus specific attention on:

1. The physical location of the data maintained by the CSP
2. The retention policies that apply to the data maintained in a CSP environment
3. The mechanism by which an organization maintains control over data (e.g., by contractual provisions, nondisclosure agreements, etc.) that is maintained by CSPs
4. The means by which the CSP will terminate storage and delete data at the end of the contract or project life cycle

Data Location

Many CSP environments involve the storage of data across multiple facilities, often across the globe. Where data resides changes an organization's applicable legal rights, expectations, and privileges based on the laws of the country where the data is located. To fully understand who may have access to this data, organizations need to first consider the type of data they plan to place in a cloud environment and then review the laws and policies of the country where the cloud providers' servers are located.

Almost every country has different standards and laws for handling personal information that CSPs must meet if they maintain facilities within their borders. Some countries allow persons with rights of access to personal information that may not directly align with the legal framework in the United States. Other countries may permit law enforcement to request more data from cloud providers than within the United States. It may not be clear how the privacy laws and protections apply in these situations. In any situation where a CSP environment goes outside of US territories, there is a potential for conflict of law, and organizations must

take sufficient time to proactively consult with legal counsel about the possible ramifications.

Breach Response

When placing data that contains personally identifiable information (PII) in a CSP environment, organizations need to be aware of issues related to data loss incidents or breaches that are specific to the CSP environment. Organizations need to ensure that they can expand their breach policies and plans as required to ensure compliance with existing requirements for response. These policies must specify which parties are responsible for the cost and containment or mitigation of harm and for notifying affected individuals where required, as well as provide for instruction and requirements on terminating storage and deleting data upon expiration of the agreement or the agreement term and extension options.

It is important to ensure that an organization's breach policies and plans adequately address the new relationship between the organization and CSP, including the assignment of specific roles and tasks between the organization and the CSP, even before determination of ultimate responsibility in the case of a data breach. It is important to establish clear contractual duties and liability of the CSP for timely breach reporting, mitigation (i.e., administrative, technical, or physical measures to contain or remedy the breach), and costs, if any, of providing notice, credit monitoring, or other appropriate relief to affected individuals as appropriate under the circumstances. It is also important to address when the termination of services and assertion of the organization's rights of ownership, custody, transfer (return), or deletion of any data stored in a CSP environment will be invoked by the organization as a remedy for a breach. Finally, it is important to ensure that there are appropriate audit rights to permit compliance reviews.

SUMMARY

Oracle offers robust cloud services, but it is very important that the organization make a reasoned decision as to whether and which cloud services to utilize. The assessment must most importantly include level of support and security. Readers are also urged to review Cloud Procurement

TABLE 5.4

Notable 2013 Cloud Outages

Date	Cloud Provider Affected
January 2013	Dropbox
February 2013	Microsoft
March 2013	Microsoft
April 2013	Apple
August 2013	Amazon
	Google
September 2013	Amazon
October 2013	Microsoft
	Verizon
December 2013	Yahoo

Source: www.crn.com/slide-shows/cloud/240165024/the-10-biggest-cloud-outages-of-2013.htm.

Questions, Appendix 1 (available on CRC Press website http://www.crcpress.com/product/isbn/9781482249941), which provides a comprehensive worksheet for cloud vendor selection. Readers will also be interested in reviewing Appendix 2, which provides a detailed security checklist that can be used when accessing cloud vendors and web service providers. Finally, readers are urged to carefully examine the stability of the product. As you can see from Table 5.4, there have been quite a few notable cloud outages in the past year.

REFERENCE

CIO Council. 2012. *Creating effective cloud computing contracts for the federal government: Best practices for acquiring IT as a service*. Washington, DC: General Services Administration. http://www.gsa.gov/portal/mediaId/164011/fileName/cloudbestpractices.action (accessed March 21, 2014).