OPEN DATA CENTER ALLIANCE^{SM}

Cloud Coexistence with Extant Enterprise Systems

CONTRIBUTORS

- Dirk Becker—UBS
- Ed Simmons—UBS
- Jesse Schrater—Intel
- Jeff Sedayo—Intel
- Johan Minnaar—UBS
- Mariano Maluf—The Coca-Cola Company
- Matt Estes—The Walt Disney Company
- Pankaj Fichadia—National Australia Bank
- Ryan Skipp—T-Systems
- Tom Scott—The Walt Disney Company

v1.1

Open Data Center Alliance, Inc.
3855 SW 153rd Dr.
Beaverton, OR 97003 USA
Phone +1 503-619-2368
Fax: +1 503-644-6708
Email: admin@opendatacenteralliance.org

TABLE OF CONTENTS

CONTENTS

This paper is one in a series that the ODCA periodically publishes on key issues for the cloud computing industry.

LEGAL NOTICE

NOTICE TO USERS GENERALLY: Users of this document should not reference any initial or recommended methodology, metric, requirements, criteria, or other content that may be contained in this document or in any other document distributed by the Alliance (“Initial Models”) in any way that implies the user and/or its products or services are in compliance with, or have undergone any testing or certification to demonstrate compliance with, any of these Initial Models. The contents of this document are intended for informational purposes only. Any proposals, recommendations or other content contained in this document, including, without limitation, the scope or content of any methodology, metric, requirements, or other criteria disclosed in this document (collectively, “Criteria”), does not constitute an endorsement or recommendation by Alliance of such Criteria and does not mean that the Alliance will in the future develop any certification or compliance or testing programs to verify any future implementation or compliance with any of the Criteria.

LEGAL DISCLAIMER: THIS DOCUMENT AND THE INFORMATION CONTAINED HEREIN IS PROVIDED ON AN “AS IS” BASIS. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ALLIANCE (ALONG WITH THE CONTRIBUTORS TO THIS DOCUMENT) HEREBY DISCLAIM ALL REPRESENTATIONS, WARRANTIES AND/OR COVENANTS, EITHER EXPRESS OR IMPLIED, STATUTORY OR AT COMMON LAW, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, VALIDITY, AND/OR NONINFRINGEMENT. THE INFORMATION CONTAINED IN THIS DOCUMENT IS FOR INFORMATIONAL PURPOSES ONLY AND THE ALLIANCE MAKES NO REPRESENTATIONS, WARRANTIES AND/OR COVENANTS AS TO THE RESULTS THAT MAY BE OBTAINED FROM THE USE OF, OR RELIANCE ON, ANY INFORMATION SET FORTH IN THIS DOCUMENT, OR AS TO THE ACCURACY OR RELIABILITY OF SUCH INFORMATION. EXCEPT AS OTHERWISE EXPRESSLY SET FORTH HEREIN, NOTHING CONTAINED IN THIS DOCUMENT SHALL BE DEEMED AS GRANTING YOU ANY KIND OF LICENSE IN THE DOCUMENT, OR ANY OF ITS CONTENTS, EITHER EXPRESSLY OR IMPLIEDLY, OR TO ANY INTELLECTUAL PROPERTY OWNED OR CONTROLLED BY THE ALLIANCE, INCLUDING, WITHOUT LIMITATION, ANY TRADEMARKS OF THE ALLIANCE.

EXECUTIVE SUMMARY

Cloud services are increasingly prevalent in today's business landscape. However, cloud usage does not mean the elimination of traditional, on-premise IT systems hosted on private cloud or dedicated infrastructure. Enterprises have made substantial investments in technology, people, and processes to build, extend, and support technology portfolios and landscapes. Enterprises can be reticent to retire this investment even in the face of cost-effective and agile cloud platforms.

Despite a strong push to deploy applications to the cloud or consume cloud-based application services, many applications are still hosted within an enterprise's on-premise data center due to security, risk, and regulatory compliance obligations. This creates a hybrid IT deployment model: an on-premise landscape of existing or legacy systems, an off-premise cloud deployment of suitable IT capability.

This paper describes recommended approaches for integrating cloud deployments within an organization's preexisting management and control systems. Successful management of the integration between cloud-deployed solutions and existing infrastructure is critical. The ODCA believes that integration of cloud deployments with enterprise landscapes should consider people, process, technology, and operating models. Doing so encourages faster cloud adoption, leverages existing enterprise investments in IT landscapes, and helps govern safe cloud adoption through effective risk and compliance management.

PROBLEM STATEMENT

New cloud services are often adopted without consideration for the impact on existing enterprise management and control systems, business strategy, or operating models. This can lead to the proliferation of a new ecosystem—one where cloud solutions duplicate or overlap the existing IT landscape and operating model. When cloud services cannot integrate with legacy systems, the common coexistence challenges include:

- Misaligned enterprise architecture;
- Lack of data, service, and process integration;
- Inconsistent operational disciplines for incident, problem, and change management;
- Ineffective governance and compliance; and
- Incompatible security architecture and models.

Cloud integration must start with governance and control and then consider business process, applications, data, infrastructure, and organizational management controls. Integration should be addressed through the perspective of organizational roles involved in planning, delivering, and supporting IT services. This includes the traditional plan and build-and-run roles, as well as the modern agile and DevOps roles for service management.

Structured governance is required to constantly monitor performance, improve service effectiveness, and align with business objectives. Common governance models must address both the cloud and noncloud services leveraged by the enterprise.

DESIRED END STATE

Integration of the cloud with enterprise landscapes requires the following:

- Clear understanding of the cloud service from the cloud service provider,
- Refinement of governance controls and management processes to accommodate cloud services, and
- Investment in modernizing existing operating models and enterprise practices.

The goal of this paper is to share recommended approaches to:

- Integrate cloud services (private, public, or hybrid) with existing enterprise IT management and control landscapes;
- Implement consistent management and control practices across cloud deployments and existing enterprise landscapes; and
- Comply with risk, governance, and regulatory obligations.

SOLUTIONS TO COMMON CLOUD INTEGRATION CHALLENGES

A number of potential challenges occur when integrating cloud deployments with preexisting management and control landscapes:

Challenge	Potential Solution
Cloud adoption could create management complexity, duplication of processes, inconsistency, and manual processes for managing, governing, and controlling the enterprise assets located in the cloud.	Identify integration interfaces, queue management systems and the monitoring of these. Correct any deficiencies.

Continued

Challenge	Potential Solution
Processes and results of security architecture, governance, and operations are duplicated across legacy systems and cloud systems, hindering the achievement of the enterprise security objectives and posture.	Define a security operating model to integrate cloud services with the existing IT enterprise security domain and deploy accordingly (accommodating private, public, and hybrid models as needed).
Data management and governance are inconsistent for the enterprise across cloud and legacy deployments.	Update data policies and governance to include cloud services and then integrate controls accordingly.
Inconsistent service management across cloud deployments and legacy deployments impacts system functionality, availability, or performance.	Define interfaces to the Information Technology Infrastructure Library (ITIL) process environment and integrate the services between cloud provider and enterprise systems. Define the data required to enable active event management, source and target systems and interfaces, update frequencies, and process integration with the greatest possible automation.
Performance of business transactions may suffer.	Define message-handling systems and data-transfer systems and paths and then integrate cloud services accordingly. Analyze problems based on the defined interfaces and correct or update each as needed. Based on defined message queues and data exchange paths, perform business service monitoring on the transaction paths. Analyze and correct any bottlenecks.

In addition, a number of requirements should be met from the business governance perspective, including the following:

- Cloud service is technically performant and functional to the levels expected by the cloud consumer.
- Security is functional and complies with enterprise policies.

- Data governance is effective.
- Incident, problem, and change management are executed according to enterprise norms.
- Audit information is available to support compliance obligations.
- Business transactions perform to acceptable thresholds.

Considerations and approaches to these challenges are described under “Recommended Approaches for Cloud Integration” later in this document.

No matter what type of cloud services the enterprise elects to deploy, it will need to be integrated into the existing enterprise IT management and control landscape. This will enable the enterprise to proactively retain control, enable governance, and ensure compliance with policies and requirements. As multiple models and scenarios for this integration will be encountered, different considerations (including layers of integration) must be assessed and standard approaches defined for handling them. There will also be differences in integration between the enterprise and public, private, and hybrid cloud services, which should be considered.

REFERENCE MODEL FOR CLOUD INTEGRATION WITH ENTERPRISE LANDSCAPES

To successfully integrate cloud deployments into an existing business technology ecosystem, consideration must be given to the layers of the people, processes, data, and technologies involved. The following Information Technology Service Management model (ODCA Service Orchestration v2.0) based on ITIL provides a view of the integration areas between traditional systems and cloud deployments:

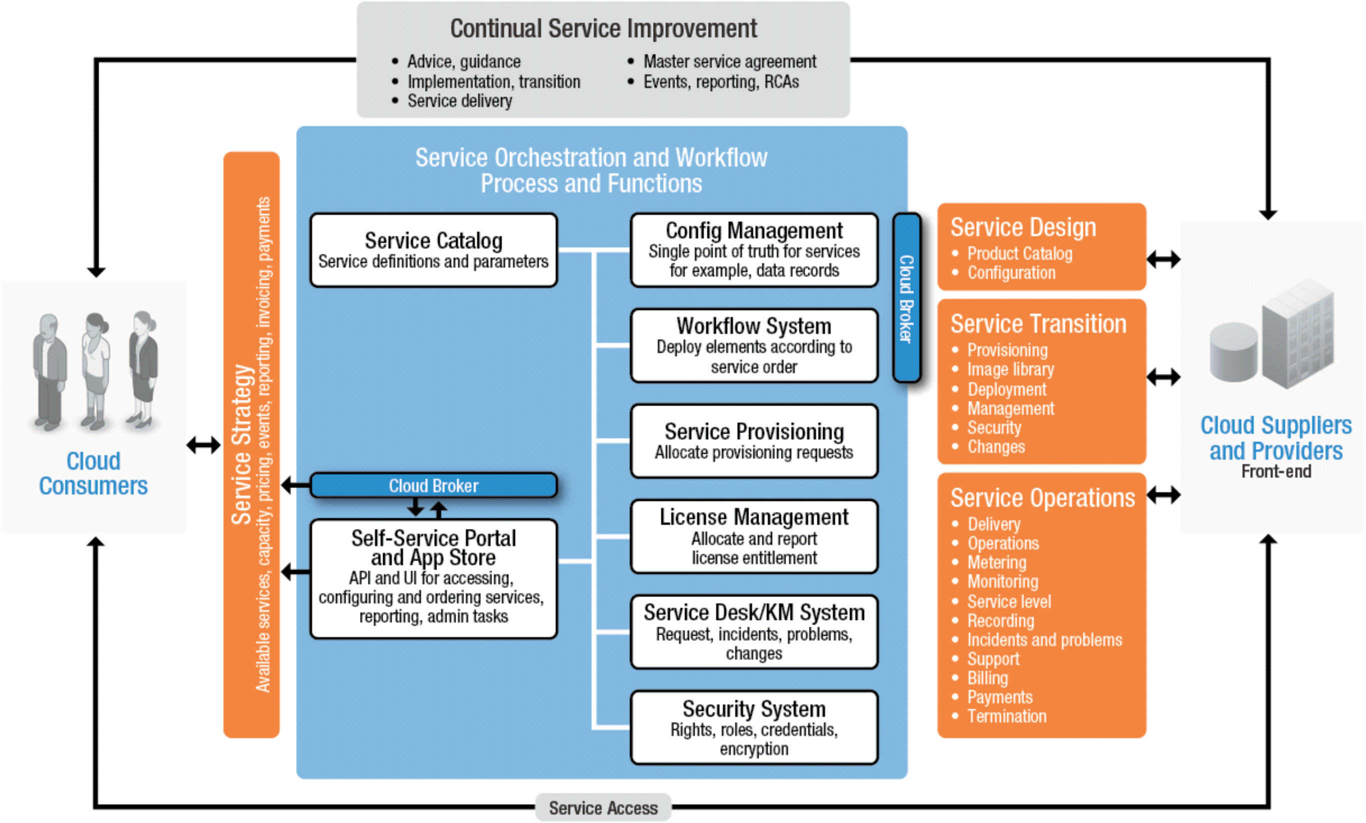
Continual Service Improvement
• Advice, guidance
• Implementation, transition
• Service delivery
• Master service agreement
• Events, reporting, RCAs
Service Orchestration and Workflow Process and Functions
Service Catalog
Service definitions and parameters
Config Management
Single point of truth for services for example, data records
Workflow System
Deploy elements according to service order
Service Provisioning
Allocate provisioning requests
License Management
Allocate and report license entitlement
Service Desk/KM System
Request, incidents, problems, changes
Security System
Rights, roles, credentials, encryption
Cloud Broker
Cloud Broker
Self-Service Portal and App Store
API and UI for accessing, configuring and ordering services, reporting, admin tasks
Service Strategy
Available services, capacity, pricing, events, reporting, invoicing, payments
Cloud Consumers
Service Design
• Product Catalog
• Configuration
Service Transition
• Provisioning
• Image library
• Deployment
• Management
• Security
• Changes
Service Operations
• Delivery
• Operations
• Metering
• Monitoring
• Service level
• Recording
• Incidents and problems
• Support
• Billing
• Payments
• Termination
Cloud Suppliers and Providers
Front-end
Service Access

Figure 1: Cloud Integration Model

RECOMMENDED APPROACHES FOR CLOUD INTEGRATION

Using the model illustrated above, a number of recommended approaches can be considered for each area or layer.

Service Management Layer

The components addressed and enabling the interactions are as follows:

A Master Services Agreement (MSA), as defined by the ODCA Usage Model: Regulatory Framework, is a contractual framework for which services can be commissioned based on predefined requirements, terms, and conditions. Make sure that an MSA is in place between the enterprise and every authorized cloud service provider, in order to define and control all interactions.

Service Strategy

Identify consistent processes and policies to govern and procure systems, including cloud systems, that follow an enterprise-wide procurement policy, risk framework, and control structures.

The service strategy should clarify the ownership of on-premise and off-premise services. Consider accountabilities and responsibilities using the responsible, accountable consulted, and informed (RACI) matrix for planning the services strategy.

Service Design

Technology staff should be innovative and flexible in how they adapt recommended approaches for service management in order to respond to continually changing technology landscapes. Adaptability is important because the characteristics of service management can change based on the technology environment and service solution—be it a legacy system, a cloud-based system, or a combination of the two. It is important to address the following:

- Define policies for use of off-premise cloud services with respect to control, governance, and partners.
- Design services to be agnostic to the environment (external or internal) with careful consideration of interoperability, business objectives, and service models.
- Balance integrated service management capabilities and cloud options to support optimal business results at an acceptable level of risk.
- Define a clear, complete description of services, including a definition of service levels, APIs, and service access points.
- Update the enterprise service catalogue with approved cloud services.

Service Transition

Service transition includes the following:

- Converting applications for cloud platforms,
- Identifying and transferring the necessary data,
- Setting up the environment, and
- Linking it back from the cloud into the enterprise management systems.

As applications are moved onto cloud platforms, two architectural styles must be considered.

Traditional bottom-up approach: Monitor infrastructure events and network data. Attempt to make sense of IT using predictive data analytics. It can be difficult to correlate and simulate the effects on any higher-level services that are directly or indirectly affected, related, or referenced.

Modern top-down approach: Have a constantly updated end-to-end model of related dependencies and data flows representing the real-world data. This makes it possible to simulate the potential impact of communication interruptions on higher-level services—providing a complete picture of the end-to-end value.

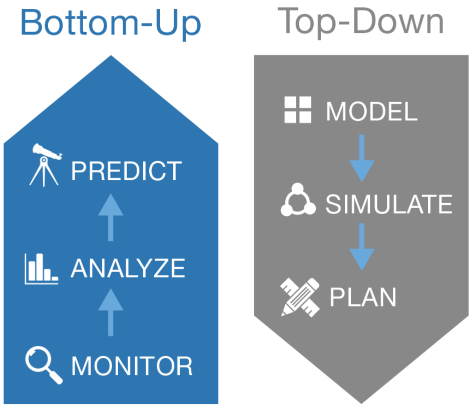

Figure 2: Side-by-side representation of top-down vs. bottom-up architecture

When the target state and the detected current state differ, there should be a structured process for addressing and correcting the difference. Security and vulnerability should be proactively scanned because monitoring both will identify any difference between expected value and detected value—indicating if there are any failures in the system.

Provider Organization Structure

Organizations need to understand the structure and account hierarchy of each cloud provider so that specific service integration layers can be mapped appropriately between the provider and the enterprise environment. Hierarchies often differ from provider to provider. It is important that individual account types can be rolled up to parents. Policies and tracking can be applied to the parents for greater control and predictability.

An organizational structure from a cost center or department perspective must be defined to which the cloud provider can report. Its record system should integrate the chargeback/showback of services. This enables ongoing budget tracking and planning for the enterprise. The additional benefit is individual business units can be made aware when they are carrying systems that are not needed anymore and could be potentially removed.

Service Operations

This takes place mostly with the cloud provider that delivers services to the relevant cloud consumers.

Controls

Organizations should define a set of policies and controls for securing systems that run exclusively in the cloud. Be sure to demonstrate how they must integrate with or connect back to the enterprise systems. Typically, access to control data is not part of cloud service offerings today. Have defined controls for the cloud to actively monitor the external cloud environment. Defined controls enable the enterprise to foresee issues or problems and proactively respond to them. Since cloud services run dynamically, it is important to ensure that the internal enterprise management and control environments are able to deal with real-time dynamic updates and information flow.

In the public cloud, service providers offer self-service portals and API-enabled services to review service performance, health checks, audit logs, and other metrics of cloud services. Enterprises should consider effective means to integrate these control systems with their internal management capabilities.

Change Management

Enterprises should integrate a structured and rigorous change management process with well-defined responsibilities. The process needs to be led by a change management team who can understand and sign off on system updates—dynamically for cloud processes and aligned to the existing enterprise systems. This team should own the changes to each sub-element of the system and synchronize the change event drivers so that each subsystem is updated as part of its lifecycle, in concert with the rest of the system. This same group is responsible for the end-to-end transactions as well, from a change-impact perspective.

Planning and Reporting

Capacity and performance management should provide a complete picture of both the on-premise and the cloud-based environments to ensure that services continue to perform as expected, cost efficiently.

Service management teams require adequate visibility into dependencies between all involved landscape elements—external and internal.

The horizontal distribution of network, storage, compute, and application in cloud services introduces challenges that were often nascent in traditional applications hosted within a company's own environment. This may become complex and challenging to control. The effect of the cloud is an overall system with a much broader distribution.

Responsibility

Enterprises should identify a dedicated team responsible for the integration and testing of cloud-based services with the enterprise systems and operations. Ensure that this team is adequately skilled and trained to integrate existing enterprise systems with cloud. This team becomes the “glue” between the different traditional skills and responsibilities prevalent in a complex enterprise and those required by the cloud provider organizations. If a team changes regularly, consistency is lost and the team needs to re-learn their expertise. They may repeat mistakes, costing time and money and creating security gaps. Identify exactly who supports which systems and where the service transfer points are for each element of the system.

Technology Layer

Service Layer

All capabilities provided in the cloud must be available through well-defined APIs. All access, including portlets, to these capabilities should only happen through these APIs and defined interfaces. These interfaces must be managed as services, including full life-cycle management and registration in a service catalogue.

Service Catalogue

As defined within the ODCA Usage Model: Service Catalog, an enterprise should provide a consistent service catalog across services that are implemented within traditional systems and for services that are enabled through cloud offerings. It should be used to describe and publish cloud services so that they can be discovered in a standard, repeatable, machine-readable way. Potentially, the enterprise can compare similar suppliers.

The service catalog may include an image library that holds and allocates reconfigured machine images for deployment across any supplier. Cloud consumers and suppliers could deposit images and control who can view and utilize them.

Service Portals and User Interfaces

Supported by a master services agreement, enterprises should authorize and determine which portals and APIs may and may not access and manage cloud-based services.

Cloud Provider Interfaces

Enterprises should clearly define the interfaces to and from the cloud provider. Implement control and management systems to monitor and secure the cross-boundary interactions—those of language; information format; network connection (addresses, speed, and capacity); transfer mode; functions and features; security requirements; and standard and customizable features, including APIs and GUIs.

If differences exist between cloud environment formats and the existing enterprise, use can be made of an API or translation interface for data transfer. This includes structured information production and consumption, semantic mediation, security mediation, service enablement, firewall management, transactional integrity, and holistic management of an integration chain.

Enterprises should create a clear strategy for dealing these interfaces. For each cloud service integration, determine which approach, method, and standard should generally be reused.

Configuration Management

Enterprises should predefine the variables allowed for cloud services to ensure compliance with business requirements such as availability and security. Configuration capabilities complement the service catalog by indicating available capacity and prices of the supplier’s environment at any one time. This can be used to support the conditional pricing, volume discounting, or spot market—a market where services are traded immediately. Additionally, predefined configuration management enables the customization of standardized services based on predefined service variables, such as the quality and location of storage.

Enterprises should create a map of all enterprise data artifacts and which types can exist in the cloud, how they should be managed, the related consistency points, and compliance requirements throughout the system.

Enterprises should define policies, governance structures, monitoring of data, data encryption requirements, and data retention parameters, For more information about configuration management, see Information as a Service Master Usage Model Rev1.0.

along with data protection requirements. Data maps should include source and destination format for all data elements; their structure (tables, graph nodes, objects, and files); and any authorized transformations or translations that happen along the way between enterprise and cloud.

Asset Management

A system for storing asset- and service-related information, as well as architectural and operational data, is an important dimension of configuration management for cloud services. Many enterprises have an established configuration management database, or CMDB, but it is very hard to integrate external cloud-based services into it. Dynamic assets are often not catered for in the CMDB design, and the information may not be available from the cloud service provider. For those users who opt to use a proxy between their enterprise and one or more SaaS providers, the proxy is one place where some of this data can be collected. This is very similar to functionality that some cloud brokers or cloud managers provide.

Consider including an asset management component in the enterprise architecture. Along with cloud-based asset and configuration management, the system could track for audit and compliance purposes and handle operational data tracking. Reporting, such as a list of interfaces, services, and cloud user accounts could feed back into the CMDB.

Maintaining Asset and Software Currency

Be clear up front with cloud providers on which version and patch level are integrated already. Identify which version your own systems can handle. Ensure these are recorded in the configuration management systems and change planning—synchronizing between the different environments. This means that a minimum set of configuration information must be available from the cloud service and captured per system.

Many enterprise configuration-management systems use the hardware, or machine, as their anchor reference. This may not be possible with a

PaaS or SaaS environment, so the anchor data reference for a system may need to move to a business unit or system reference.

Toolsets

Be wary of the proliferation and duplication of monitoring and telemetry toolsets between the existing enterprise standards and new cloud-based services. Alignment and management of the extended enterprise environment of cloud will become more complex with overlapping tool capabilities. Enterprises should consider cloud integration via data flow to a single monitoring solution. Strive to achieve a single pane of glass view for the cloud management and monitoring data, although admittedly the cloud monitoring may not provide the deep detail level we are accustomed to from the internal enterprise data center.

Create consistent backup and restore procedures with clear roles, responsibility, and custody definitions for the cloud-based services. This covers everything from reporting daily data protection events to alerting on unplanned events and recovery, such as service crashes, system moves, and disaster recovery.

Continuous Integration

Software deployment processes need to handle deployment onto both on-premise and cloud systems. The system elements located in and designed for the cloud accommodate regular function additions and scaling. Make sure the management and control systems support this continuous integration and scaling by means of a well-defined DevOps and continuous integration (CI) methodology. This also drives a requirement for in-house code repositories and cloud-based code repositories.

Plan for dynamic integration of the continuous transfer of ownership and accountability as elements move from development, user acceptance testing, and production in an ongoing process within the cloud service environment.

Service Provisioning

Determine the best routing and fit for any particular request and assign it to the relevant suppliers or subsystem. This can be established by identifying predefined criteria as described in TREC (the factors of trust, risk, eco-efficiency and cost) from the EC-sponsored OPTIMIS project.

Orchestrate Rather than Integrate

Focus on driving the configuration of resources via automated tooling-processes-catalogues, rather than developing each element to deliver on the exact business needs.

For more information about orchestration, see ODCA Usage Models "Service Orchestration Rev 2.0" and "Service Orchestration with TOSCA White Paper."

Middleware

Middleware can be a powerful connecting layer that enables cloud services. Control of middleware between cloud services and enterprise applications is important to ensure that security is maintained and that only authorized data flows according to expectations. This requires that control data be made available in both directions—back to the cloud-based system as well as to the enterprise monitoring environment. Be specific on what protocols and languages are authorized, such as web services, XML, JAVA, or C++.

Also consider the communication processes. Some are batch orientated while others are in real time or are queue-based. All parts of the system need to be aligned and monitored accordingly.

License Management

The cloud subscriber should implement a software library to catalogue all third-party software products that are licensed by the cloud subscriber in respect to cloud environments.

By developing and maintaining a software library catalogue, the cloud subscriber can more easily identify and access information about its third-party software licenses and support the analysis of migrating applications to the cloud.

Key objectives for license management in the cloud include enabling:

- License portability;
- Managing cost of licenses (internal and external);
- Monitoring of licenses to ensure compliance to terms and conditions; and
- Tracking use of deployed instances, decommissioning them when no longer used.

The cloud subscriber and cloud provider enterprise should develop, publish, and manage an internal software procurement policy that defines all terms of use in cloud environments.

According to the ODCA Software Entitlement Management framework, the cloud subscriber and cloud provider should develop and maintain a strong relationship with representatives from the respective software vendors. This requirement helps cloud subscribers and cloud providers to readily contact software vendor representatives with software queries, including the procurement of new licenses or amendment of existing licenses complying with the commercial conditions.

Service Desk and Knowledge Management

The service desk enables enterprises to meet business expectations and deliver interactive IT support services accessible anywhere, anytime.

To empower support teams with real-time collaboration and knowledge management of the cloud services that they are enabled to use, the support organization needs to transparently manage evolving complexities and knowledge across suppliers, consumers, and third parties.

The support organization should leverage recommended approaches across key ITIL service management processes for greater control and efficiency. This includes maximizing agent productivity with comprehensive end-user self-service capabilities. They should also leverage knowledge databases covering common questions, answers, and incident- and problem-related information pertaining to the cloud service.

Relevant information must be obtained from the involved cloud service providers for inclusion in the knowledge management systems that support the enterprise service desk. This can help minimize the number of problems and incidents overall.

Security and Compliance

When integrating cloud services with the enterprise, security is deployed on a federated basis. It requires standard protocols, such as SAML, for cloud consumer organizations to maintain their own user directories.. Cloud providers should establish well-defined trust relationships to permit access to their environments. These functions should define both the empowered users who are entitled to commission and configure systems as well as the end users of the services themselves. It includes aspects such as authorization levels to order further facilities.

User access should be authorized and revalidated for entitlement appropriateness and at planned intervals for both internal and external systems. For identified access violations, remediation must follow established user access policies and procedures.

The identification, assessment, and prioritization of risks posed by business processes that require third-party access to the organization’s information systems and data should be followed by a coordinated application of resources. This minimizes, monitors, and measures the likelihood and impact of unauthorized or inappropriate access. Compensating controls should be implemented prior to provisioning access to the cloud service.

Application vulnerability scans should be performed on systems both internal and external to the enterprise perimeters across the application stack. Application threats and threat methods must be updated constantly in the enterprise’s risk register. Regular application of security patches and fixes must accompany this life-cycle aspect and should be tracked in the enterprise CMDB. Static code scanning should also be performed regularly. Monitor the use of open source libraries and record their status in the CMDB. This includes vulnerability scanning and life-cycle authorized-change tracking. The security risk must be constantly updated.

For more in-depth information on security and compliance, see the ODCA best-practices paper "Architecting Cloud-Aware Applications Rev 1.0."

Tracking of shared software libraries is also important to remember, along with license and entitlement tracking.

Security Modularization

Enterprises should not give up the notion of security and control when extending the architecture (e.g., SOA or other cloud pattern) to include external or other cloud-based service elements. Create a predefined model for it that aligns the various participants of the system. Use a security, credentials, rights, access, and privilege perspective that integrates with the enterprise access management and control systems.

For each data access, the cloud-based system can query predefined roles and processes for data management in a centralized security system. This makes it simpler to manage data consistently.

If multiple data sources are able to reference an external modularized system for authorization and permission, policies and rules can be consistently applied among defined data classes and systems. It is also easier to update a policy if required, knowing that it will then be automatically and immediately applied to all data repositories that use the security source. This makes maintenance and auditing easier than if each subsystem has its own rules and policies that don't directly align to each other.

More information on security practices in cloud applications is available in ODCA's best-practices paper "Architecting Cloud-Aware Applications Rev 1.0."

By segregating data according to classes, management and control are focused and consistent.

Security Monitoring Services

Security monitoring should be updated to be aware of cloud services, as the systems and data are no longer necessarily protected by the corporate perimeter defenses. The cloud provider must also actively report defined security-related events to the enterprise security monitoring systems. Since some control of the cloud service is not in the hands of enterprise IT, the focus shifts to monitoring events and ensuring ongoing awareness against defined policies rather than actual control of the systems and data located in the cloud. Real-time response and processes are needed to ensure appropriate alignment to organizational requirements and protection.

Legal and Content Services

Protection and governance teams need to update the model for intellectual-property protection when external cloud services are adopted. This includes how they consider intellectual assets and how they understand, secure, and follow with data compliance requirements across multiple countries on multiple systems with varying control sets. The focus of control and protection may move to data assets and focus less on the applications themselves, which are hosted in the cloud, and more on the integrated processing concepts, which are proprietary to the enterprise.

This introduces additional new considerations for operations staff and data management and business continuity teams. These include potentially increasing the complexity of disaster recovery, service restoration, and data consistency and security.

Security and compliance teams must address the increased potential attack surface.

Penetration Testing

Define the various possible cloud service-based scenarios and the associated test for each scenario. These tests must be performed on the various subsystems where data is either transported or located. Define a frequency for repeating the test—for example, after each service update. This includes input/output validation and various penetration tests on each component in context of the reference architecture, as practically deployed in the enterprise.

Tests must address:

- Data security;
- Network security;
- Intrusion detection;
- Access and role control;
- Traffic and transaction anomalies;
- Unauthorized processes, such as malicious administration or similar activities; and
- Malware and similar.

Tests must also ensure that the related events are received with the correct priority in the enterprise control environment.

When the system is not under control of the enterprise, associated parties must negotiate and produce certification and demonstration of the necessary testing, results, and any required remediation.

CONCLUSION

While the use of cloud-based services brings significant advantages to an enterprise, retaining control of those services and the associated enterprise intellectual capital and assets brings a number of considerations to be solved. Enterprises must take time and plan how they will retain or establish that control. This paper has listed important aspects to consider. Use a layered approach that considers people, process, information, and technology aspects. Further cloud service adoption and cloud application development should become even easier and robust by leveraging various ODCA papers addressing cloud requirements, coexistence, and integration across planning, delivery, and operation of cloud services.