Open Group Standard

The Open Group Cloud Ecosystem Reference Model

This document is provided "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Any publication of The Open Group may include technical inaccuracies or typographical errors. Changes may be periodically made to these publications; these changes will be incorporated in new editions of these publications. The Open Group may make improvements and/or changes in the products and/or the programs described in these publications at any time without notice.

Should any viewer of this document respond with information including feedback data, such as questions, comments, suggestions, or the like regarding the content of this document, such information shall be deemed to be non-confidential and The Open Group shall have no obligation of any kind with respect to such information and shall be free to reproduce, use, disclose, and distribute the information to others without limitation. Further, The Open Group shall be free to use any ideas, concepts, know-how, or techniques contained in such information for any purpose whatsoever including but not limited to developing, manufacturing, and marketing products incorporating such information.

If you did not obtain this copy through The Open Group, it may not be the latest version. For your convenience, the latest version of this publication may be downloaded at www.opengroup.org/bookstore.

Technical Standard

The Open Group Cloud Ecosystem Reference Model

ISBN: 1-937218-46-1

Document Number: C141

Published by The Open Group, January 2014.

Comments relating to the material contained in this document may be submitted to:

The Open Group, Apex Plaza, Forbury Road, Reading, Berkshire, RG1 1AX, United Kingdom

or by electronic mail to:

ogspecs@opengroup.org

Contents

List of Figures

List of Tables

Preface

The Open Group

The Open Group is a global consortium that enables the achievement of business objectives through IT standards. With more than 400 member organizations, The Open Group has a diverse membership that spans all sectors of the IT community – customers, systems and solutions suppliers, tool vendors, integrators, and consultants, as well as academics and researchers – to:

- Capture, understand, and address current and emerging requirements, and establish policies and share best practices
- Facilitate interoperability, develop consensus, and evolve and integrate specifications and open source technologies
- Offer a comprehensive set of services to enhance the operational efficiency of consortia
- Operate the industry's premier certification service

Further information on The Open Group is available at www.opengroup.org.

The Open Group publishes a wide range of technical documentation, most of which is focused on development of Open Group Standards and Guides, but which also includes white papers, technical studies, certification and testing documentation, and business titles. Full details and a catalog are available at www.opengroup.org/bookstore.

Readers should note that updates – in the form of Corrigenda – may apply to any publication. This information is published at www.opengroup.org/corrigenda.

This Document

This document defines The Open Group Cloud Ecosystem Reference Model and provides guidance on how to apply it with The Open Group TOGAF® and ArchiMate® standards to develop an Enterprise Architecture. It has been developed and approved by The Open Group.

Enterprises are under increasing pressure to deliver greater business agility. Cloud solutions are rapidly and efficiently evolving to reach this end and at reduced overall costs. In order to deliver the agility and cost savings envisioned, an Enterprise Architecture of an enterprise's Cloud Ecosystem must be developed. This will allow rapid cloud solutions development and enhancement opportunities.

The Cloud Ecosystem of an enterprise provides critical and essential enabling capabilities to meet the demand for greater flexibility in delivering cloud business solutions. To address any gap in the enterprise's capabilities, an enterprise often collaborates with the participants of a Cloud Ecosystem (e.g., Cloud Service Providers, strategic vendors) and leverages participants' Cloud Services. However, the use of Cloud Services provided by participating external entities of a Cloud Ecosystem has implications on the Enterprise Architecture that require frequent assessments of changes in Cloud Services to ensure timely evolution. Approaching the Cloud Ecosystem within the context of an Enterprise's Architecture will provide the necessary alignment with the enterprise's strategic vision, goals, and objectives.

This standard is structured as follows:

- Chapter 1 (Introduction) is an introduction to this standard.
- Chapter 2 (Definitions) defines the general terms used.
- Chapter 3 (The Cloud Ecosystem Reference Model) defines the Cloud Ecosystem Reference Model. The Reference Model describes major actors and their inter-relationships, taxonomy, and architecture principles, and highlights a minimum set of Architecture Building Blocks (ABBs) to be realized and facilitated by at least one of the new or existing participants of an enterprise Cloud Ecosystem.
- Chapter 4 (Architectural Considerations for an Enterprise Cloud Ecosystem (Informative)) describes all the significant concepts in development, management, and governance of an enterprise Cloud Ecosystem.
- Chapter 5 (Using the Cloud Ecosystem Reference Model with the TOGAF Standard (Informative)) provides the informative case study of the "CloudEcoSource" organization to develop an Enterprise Architecture for the Cloud Ecosystem with the Cloud Ecosystem Reference Model. The chapter lists the TOGAF Architecture Development Method (ADM) phases and the steps needed to develop, manage, and govern the Cloud Ecosystem of the CloudEcoSource organization.

Intended Audience

This standard should be read by an Architect wishing to develop, manage, and govern an Enterprise Architecture for the Cloud Ecosystem. The intended audience of this standard includes but is not limited to:

- TOGAF practitioners
- Cloud Service Consumers and Providers
- Business and technical executives of an enterprise
- Business and technical architects
- Business and technical solution developers
- Business and technical operational team(s)
- Enterprise governance team(s)
- Enterprise business and management team

The information in this standard can be used stand-alone or with an encompassing Architecture Development Method (ADM), such as the TOGAF ADM. Integration with the TOGAF standard and extension steps are described in Chapter 5 of this standard.

Trademarks

Acknowledgements

The Open Group gratefully acknowledges the contribution of the following people in the development of this document, in particular the leadership of Tejpal (TJ) Virdi, Stephen Bennett, and Kevin Sevigny as co-chairs:

- Stephen G. Bennett, Oracle (Co-Chair)
- Stuart Boardman, KPN Consulting
- Henry Franken, Bizzdesign
- Ed Harrington, Architecting the Enterprise
- Sunil KempeGowda, CC and C Solutions
- Sreeparna Pal, Tata Consultancy Services
- Kevin Sevigny, Conexiam Solutions Inc. (Co-Chair)
- Emmanouil Tritsiniotis, Bizzdesign
- Tejpal (TJ) Virdi, The Boeing Company (Founding Chair)
- Vish Vishwanathan, CC and C Solutions
- Robert Weisman, Build The Vision

Referenced Documents

Normative References

Normative references for this standard are defined in Section 1.4.

Informative References

The following documents are referenced in this standard:

- An Architectural View of Security for Cloud, White Paper (W116), published by The Open Group, May 2011; refer to: www.opengroup.org/bookstore/catalog/w116.htm.
- An Information Architecture Vision: Moving from Data Rich to Information Smart, White Paper (W132), published by The Open Group, April 2013; refer to: www.opengroup.org/bookstore/catalog/w132.htm.
- Cloud Computing Portability and Interoperability, Open Group Guide (G135), published by The Open Group, April 2013; refer to: www.opengroup.org/bookstore/catalog/g135.htm.
- Cloud Security Alliance: TCI – A Quick Guide to the Reference Architecture; refer to: https://cloudsecurityalliance.org/wp-content/uploads/2011/10/TCI_Whitepaper.pdf.
- Cloud Security Alliance: TCI – Reference Architecture; refer to: https://cloudsecurityalliance.org/wp-content/uploads/2011/10/TCI-Reference-Architecture-v1.1.pdf.
- M.E. Iacob, H. Jonkers, D. Quartel, H. Franken, H.v.d. Berg: Delivering Enterprise Architecture with TOGAF® and ArchiMate®, BiZZdesign Academy 2012.
- NIST SP 500-292: NIST Cloud Computing Reference Architecture; refer to: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505.
- NIST SP 800-145: A NIST Definition of Cloud Computing; refer to: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.
- Security Principles for Cloud and SOA, White Paper (W119), published by The Open Group, December 2011; refer to: www.opengroup.org/bookstore/catalog/w119.htm.
- Service-Oriented Cloud Computing Infrastructure (SOCCI) Framework, Open Group Standard (C120), published by The Open Group, December 2011; refer to: www.opengroup.org/bookstore/catalog/c120.htm.
- UDEF: An Open Group Standard Supporting TOGAF Interoperability, Webinar (D008), published by The Open Group, September 2010; refer to: www.opengroup.org/bookstore/catalog/d008.htm.

- US Government: National Information Exchange Model (NIEM); refer to: www.niem.gov/technical/Pages/current-release.aspx.

1 Introduction

1.1 Objective

This standard defines The Open Group Cloud Ecosystem Reference Model and provides guidance on how to apply it with the TOGAF® and ArchiMate® standards to develop an Enterprise Architecture.

1.2 Overview

This standard defines the Cloud Ecosystem Reference Model. It also provides guidance on applying the Cloud Ecosystem Reference Model with the TOGAF and ArchiMate standards to develop, maintain, and govern an Enterprise Architecture for the Cloud Ecosystem.

The approach described in the standard enables practitioners to effectively align business and technical capabilities in creating architectural components, their inter-relationships, and to effectively manage interactions and relationships between the participants of the Cloud Ecosystem in order to minimize the impact of changes in Cloud Services (either developed by the enterprise itself or by participating entities of the Cloud Ecosystem).

1.3 Conformance

At the time of publication, there are no conformance requirements defined in this section for the purposes of this standard. Readers are advised to check The Open Group website for any conformance and certification requirements referencing this standard.

1.4 Normative References

The following standards contain provisions which, through references in this standard, constitute provisions of the Cloud Ecosystem Reference Model. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards.

- TOGAF® Version 9.1 Enterprise Edition, an Open Group Standard; refer to www.opengroup.org/togaf.
- ArchiMate® Version 2.1 Specification, Open Group Standard (C13L), published by The Open Group, December 2013; refer to: www.opengroup.org/bookstore/catalog/c113l.htm.

1.5 Terminology

For the purposes of this standard, the following terminology definitions apply:

Can Describes a permissible optional feature or behavior available to the user or application. The feature or behavior is mandatory for an implementation that conforms to this document. An application can rely on the existence of the feature or behavior.

Legacy Describes a feature or behavior that is being retained for compatibility with older applications, but which has limitations which make it inappropriate for developing portable applications. New applications should use alternative means of obtaining equivalent functionality.

May Describes a feature or behavior that is optional for an implementation that conforms to this document. An application should not rely on the existence of the feature or behavior. An application that relies on such a feature or behavior cannot be assured to be portable across conforming implementations. To avoid ambiguity, the opposite of “may” is expressed as “need not”, instead of “may not”.

Must Describes a feature or behavior that is mandatory for an application or user. An implementation that conforms to this document shall support this feature or behavior.

Shall Describes a feature or behavior that is mandatory for an implementation that conforms to this document. An application can rely on the existence of the feature or behavior.

Should For an implementation that conforms to this document, describes a feature or behavior that is recommended but not mandatory. An application should not rely on the existence of the feature or behavior. An application that relies on such a feature or behavior cannot be assured to be portable across conforming implementations. For an application, describes a feature or behavior that is recommended programming practice for optimum portability.

Will Same meaning as “shall”; “shall” is the preferred term.

1.6 Future Directions

It is anticipated that this standard will be updated to incorporate additional features and techniques to support the development of Enterprise Architecture with the Cloud Ecosystem Reference Model. It may also be aligned with future Open Group and international standards that overlap with the content of this standard.

2 Definitions

For the purposes of this standard, the following terms and definitions apply. Merriam-Webster's Collegiate Dictionary should be referenced for terms not defined in this section.

2.1 Cloud Ecosystem

A network of participating entities (e.g., Cloud Service Auditor, Cloud Service Broker, Cloud Service Consumer, Cloud Service Developer, Cloud Service Provider, Regulator, Supplier, Partner, etc.) each of which plays one or more roles in the provision, consumption, and evolution of Cloud Services.

- Ecosystem participants are not necessarily aware of all other entities in the Cloud Ecosystem but will in general affect or be affected by them.
- A Cloud Ecosystem is subject to internal factors and external factors.

2.2 Cloud Service Auditor

A party that can conduct independent examination of Cloud Service controls with the intent to express an opinion thereon. Audits are performed to verify conformance to standards through review of objective evidence. (Refer to NIST SP 500-292.)

2.3 Cloud Service Broker

An entity that manages the use, performance, and delivery of Cloud Services, and negotiates relationships between Cloud Service Providers and Cloud Service Consumers. (Refer to NIST SP 500-292.) Key capabilities provided by Cloud Service Brokers are:

- Cloud Service on-boarding
- Cloud readiness assessment
- Application and data migration
- Cloud Service Provider capabilities evaluation

2.4 Cloud Service Consumer

A person or organization is the principal stakeholder that maintains a business relationship with, and uses the service from, a Cloud Service Provider. (Refer to NIST SP 500-292.)

2.5 Cloud Service Developer

A person or organization that develops the technical as well as the business aspects of a (simple or higher-level) Cloud Service offering, which may be part of the organization of the Cloud Service Consumer or Cloud Service Provider. A Cloud Service Developer leverages the development and operational tools to develop and compose a service or set of services. (Refer to the SOCCI standard.)

2.6 Cloud Service Provider

A person, an organization; it is the entity responsible for making a Cloud Service available to interested parties. (Refer to NIST SP 500-292.)

2.7 Enterprise

The highest level (typically) of description of an organization which typically covers all missions and functions. An enterprise will often span multiple organizations. (Refer to the TOGAF standard.)

2.8 Infrastructure as a Service (IaaS)

The capability provided to the Cloud Service Consumer to provision processing, storage, networks, and other fundamental computing resources where the Cloud Service Consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The Cloud Service Consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls). (Refer to NIST SP 800-145.)

2.9 Platform as a Service (PaaS)

The capability provided to the Cloud Service Consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The Cloud Service Consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations. (Refer to NIST SP 800-145.)

2.10 Software as a Service (SaaS)

The capability provided to the Cloud Service Consumer to use the Cloud Service Provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The Cloud Service Consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. (Refer to NIST SP 800-145.)

3 The Cloud Ecosystem Reference Model

The Cloud Ecosystem Reference Model serves as an abstract foundation for the instantiations of architectures and business solutions of an enterprise. It defines a flexible and agile collaborative enterprise Cloud Ecosystem. It also provides for an effective digital customer experience for sharing business information securely regardless of its underlying data location.

The Cloud Ecosystem Reference Model ensures consistency and applicability of Cloud Services within a wide variety of Enterprise Architecture management frameworks. Figure 1 describes the relationships and dependencies between the various enterprise frameworks to manage the life cycle of Cloud Services utilizing the Architecture Building Blocks (ABBs) identified in the Cloud Ecosystem Reference Model to deliver enterprise business solutions. Please refer to the TOGAF standard for further explanation of the concepts associated with Architecture Development Methods (ADMs) and management of frameworks.

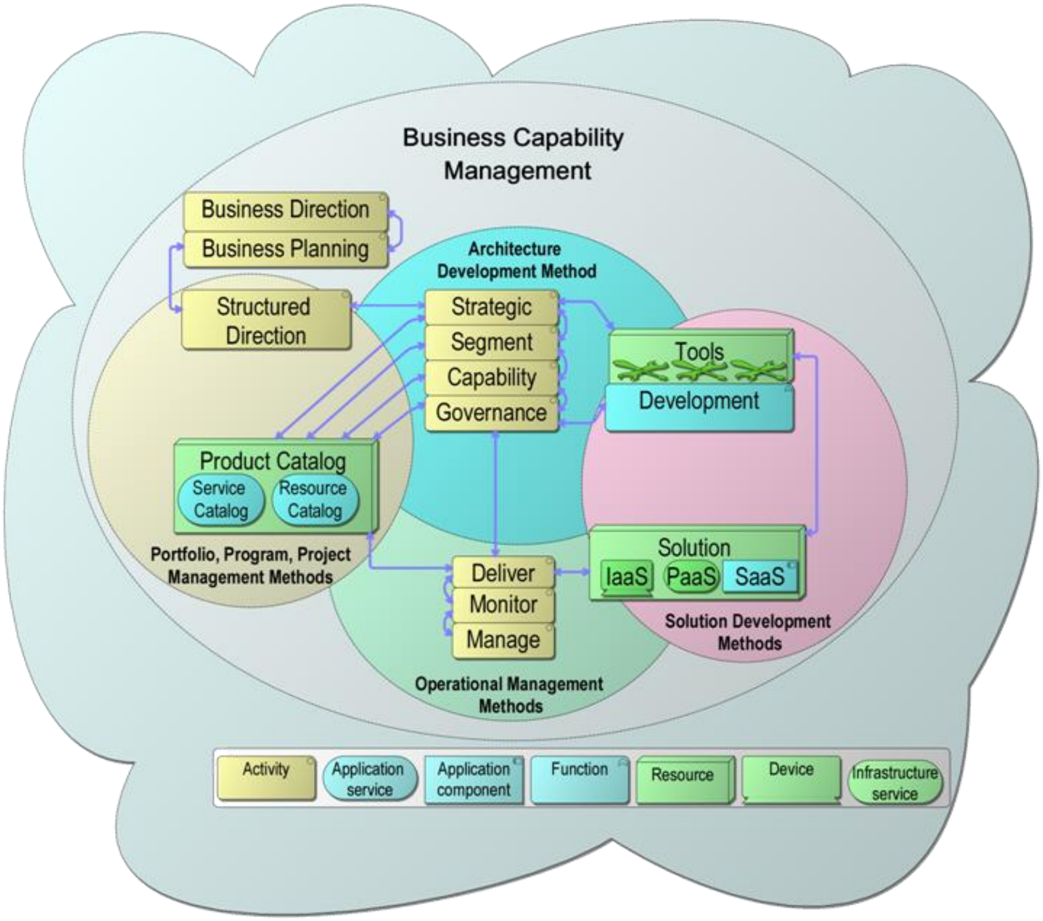

Figure 1: Managing Frameworks of an Enterprise Cloud Ecosystem

The Cloud Ecosystem Reference Model defines the major actors and their relationships and a minimum set of ABBs. The model describes the architectural capabilities to be realized and facilitated by at least one of the new or existing participants of an enterprise Cloud Ecosystem. The model establishes a common language for the various participants of an enterprise Cloud Ecosystem that supports the validations of Cloud Service Providers' solutions to achieve architectural integrity of business solutions of an enterprise.

ABBs of the Reference Model are described in Chapter 2 and Section 3.1.

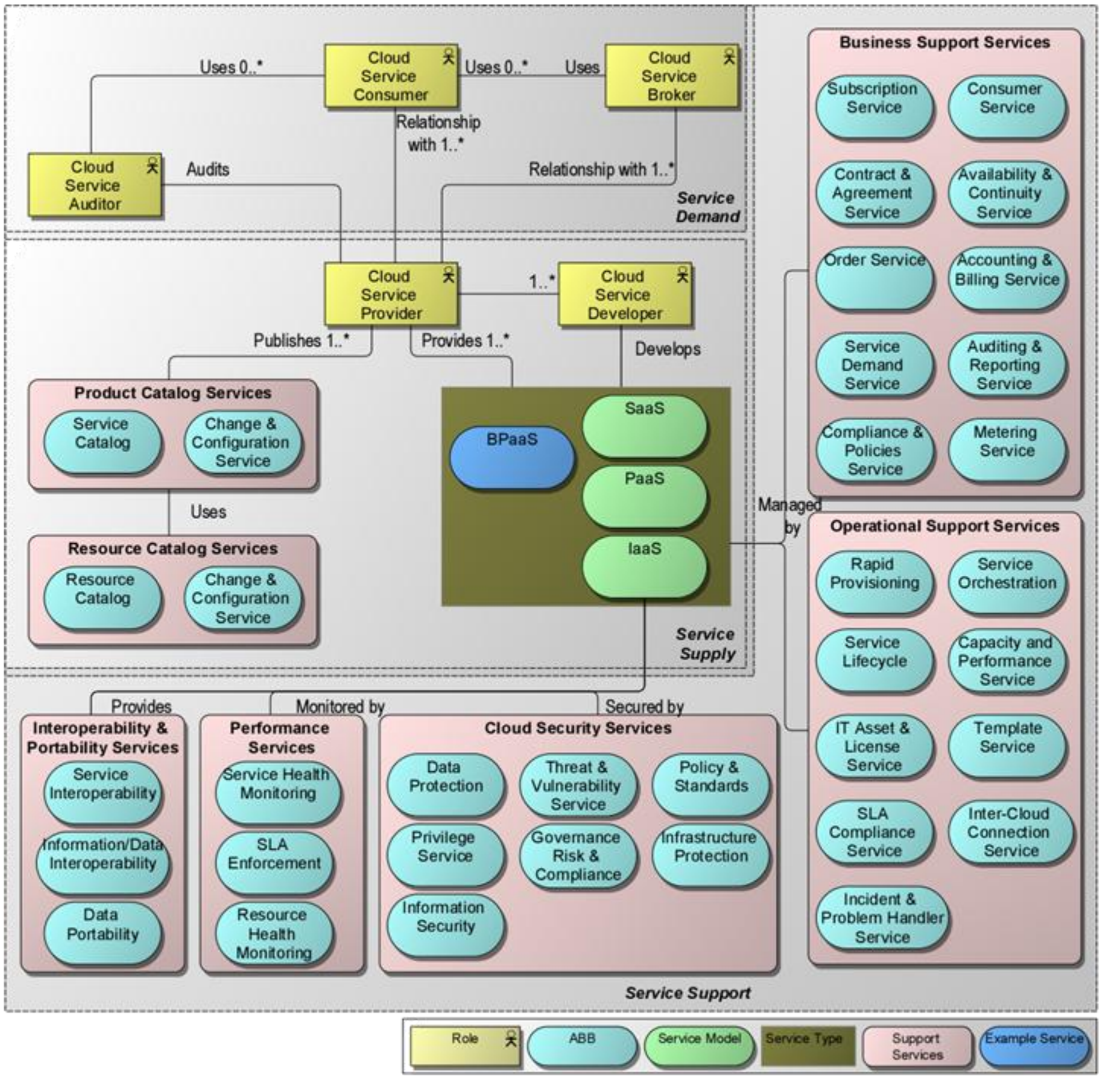

Figure 2: The Cloud Ecosystem Reference Model

The Cloud Ecosystem Reference Model should be considered as an extension of an Enterprise Architecture Model. The model can be used to define architecture for any specific scenario applicable for an enterprise utilizing Solution Building Blocks (SBBs) implemented by any new or existing participants of an enterprise Cloud Ecosystem. The visibility of these capabilities will vary according to the role(s) of the participants.

3.1 The Cloud Ecosystem Reference Model Taxonomy

This section describes the Cloud Ecosystem Reference Model Taxonomy to consistently apply a common business and IT taxonomy for interoperability.

3.1.1 Business Support Services

Business Support Services provide the business-related capabilities needed to simplify and support the end-to-end business activities of an enterprise Cloud Ecosystem. The following standard services will reduce complexity and simplify the enterprise business operations.

Table 1: Business Support Services ABBs of the Cloud Ecosystem Reference Model

Architecture Building Blocks (ABBs)	Description
Accounting & Billing Service	The Accounting & Billing Service generates and manages bills for the Cloud Service usage data using a set of predefined billing policies. Cloud Service Providers could allow production of one bill for multiple subscriptions of Cloud Services for the consumer and combining usage from multiple subscriptions to qualify for volume pricing discounts. It also manages other accounting-related activities (process payments, track invoices, etc.).
Auditing & Reporting Service	The Audit & Reporting Service provides a mechanism to record activities (including exceptions and events) and keeps them for an agreed time period to assist future investigations. Care must be taken to minimize the performance degradation and the risk of disruption to business processes. It generates reports to effectively perform client-facing business operations activities.
Availability & Continuity Service	The Availability & Continuity Service controls the redundancy, workload mobility between different Cloud Service Providers, and ensures that Cloud Services are built with high availability design practices and considerations.
Compliance & Policies Service	The Compliance & Policies Service defines, integrates, and aligns activities such as corporate governance and corporate compliance with applicable laws and regulations. It maintains an organizational structure, process, tools, and business policies to ensure adherence to applicable laws and regulations.
Consumer Service	The Consumer Service (*aka* Customer Management) provides an authoritative view to Cloud Service Consumers' information to ensure effective care is provided and information about consumer relationships is well managed.

Architecture Building Blocks (ABBs)	**Description**
Contract & Agreement Service	The Contract & Agreement Service handles contract life cycle (set-up, negotiate, close, terminate, etc.) and the ways in which various aspects of Cloud Services are offered and managed for Cloud Service Consumers. The contract states the terms and conditions for service usage (constraints, costs, and billing information) by the Cloud Service Consumer and includes applicable Cloud Service policies, Service-Level Agreements (SLAs) – availability, performance, etc. – to ensure that Cloud Service Providers provision services that meet the defined agreement.
Metering Service	The Metering Service is essential for billing/charging Cloud Services and their underlying resource usages (i.e., Cloud Services and resources allocation and consumption). It provides a metering capability with some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts).
Order Service	The Order Service controls the life cycle of Cloud Service orders (from a Cloud Service provisioning request capture to de-provisioning). It utilizes Cloud Service configuration, service life cycle, service orchestration (if required), and accounting and billing services.
Service Demand Service	The Service Demand Service is to understand the business demand for Cloud Services (e.g., in the case of IaaS, demand in the form of bandwidth, memory, CPU capacity, support personnel, etc.) based on the past business activity patterns combined with the future business growth estimate.
Subscription Service	Cloud Service Providers could enable multiple subscription models for charging Cloud Services' usage by utilizing the Subscription Service. These subscription models may include fixed, tier-based (e.g., Gold, Silver, and Platinum), pay-as-you-go payment terms (monthly, quarterly, annually). The Cloud Service Provider monitors allocation and consumption of Cloud Services and chargeback to its subscribed consumers based on subscription models.

3.1.2 Operational Support Services

Operational Support Services enable the capabilities for efficient business operations of an enterprise Cloud Ecosystem.

Table 2: Operational Support Services ABBs of the Cloud Ecosystem Reference Model

Architecture Building Blocks (ABBs)	**Description**
Capacity & Performance Service	The Capacity & Performance Service (*aka* Workload Management) allows efficient allocation and optimal use of underlying Cloud Resources. It analyzes performance of running Cloud Services in real-time and automatically adjusts the workload. If applicable, it utilizes external Cloud Service Providers' computing services by using inter-cloud connection services to meet the defined SLAs.
Incident & Problem Handler Service	The Incident & Problem Handler Service deals with any service-related incidents and associated problems and performs root cause analysis. It could store information in a knowledge support repository for further analysis that may include trend analysis to enable the evolution of the Cloud Services to prevent future incidents.
Inter-Cloud Connection Service	The Inter-Cloud Connection Service serves as a seamless connector from one cloud environment to another cloud environment (e.g., private cloud environment to external/public cloud environment) to enable Cloud Service interoperability. A Cloud Service connection ensures secure connectivity, traverses different network boundaries seamlessly, and enables performance improvement capabilities (e.g., compression).
IT Asset & License Service	The IT Asset & License Service controls licensing agreements of various aspects of Cloud Services that can be purchased and sold. Some Cloud Service Providers also allow Cloud Service Consumers to directly lease or buy licenses from the software/solution vendors or provide licenses on-demand.
Rapid Provisioning	Rapid Provisioning delivers architectural capabilities to quickly scale in or scale out computing resources normally delivered by at least one of the participating entities. Once self-subscribed to a catalog service, Rapid Provisioning capabilities automatically deploy Cloud Services based on a requested service capability. In a mature cloud environment, the Cloud Service Consumer could also have the capability to customize experience based on their role within the organization.
Service Life Cycle	Service Life Cycle (*aka* Service Delivery Management) controls the Cloud Services (including underlying Cloud Resources) life cycle from provisioning to de-provisioning dynamically (some Cloud Service Providers utilize workflow to manage the process). It also provides the visibility, control, and automation across cloud environments (e.g., private, public, and hybrid environments) to address business-critical challenges.
Service Orchestration	Service Orchestration serves as an efficient way to manage the Cloud Services (including underlying Cloud Resources) capacity and performance (it even instigates an external service gateway for workload management) automatically. It seamlessly coordinates Cloud Services in multiple cloud environments (e.g., internal/private and public cloud environments).

Architecture Building Blocks (ABBs)	Description
SLA Compliance Service	In order to ensure a high-level of service standards on Cloud Services, Cloud Service Consumers demand strict implementation of SLAs from Cloud Service Providers. Any degradation of service performance could have severe impact on revenue and end-user satisfaction. The SLA Compliance Service helps define SLAs and ensure their compliance and improve relationships with Cloud Service Providers. This service provides real-time assessment and SLA compliance reporting on Cloud Services.
Template Service	The Template Service provides re-creatable instances from service templates. In case of IaaS, the Template Service describes how the instances are to be configured (machine images, network connectivity, storage requirements, etc.) and deployed on a dynamic infrastructure environment. The Template Service also enables auto provisioning/re-deploying applications on a Cloud Service platform.

3.1.3 Cloud Security Services

Cloud Security Services provide the broad set of service capabilities to protect data/information, software, and the associated infrastructure services of an enterprise Cloud Ecosystem. Refer to The Open Group White Paper: Security Principles for Cloud and SOA for principles that are widely applicable as guidance to secure systems in all environments.

Table 3: Cloud Security Services ABBs of the Cloud Ecosystem Reference Model

Architecture Building Blocks (ABBs)	Description
Data Protection	In the information age, data is an asset. However, most data remains valuable only if it is protected. Data Protection needs to cover all data life cycle stages, data types, and data states. Data stages include create, store, access, roam, share, and retire. Data types include unstructured data, such as word processing documents, structured data, such as data within databases, and semi-structured data, such as emails. Data states include Data At Rest (DAR), Data In Transit (DIT) (also known as “data in motion” or “data in flight”), and Data In Use (DIU). The controls of Data Protection are data life cycle management, data leakage prevention, intellectual property protection with digital rights management, and cryptographic services, such as key management and PKI/symmetric encryption. (See TCI – A Quick Guide to the Reference Architecture.) The Enterprise Data Management function described below consistently applies security policies to all data types, data life cycle stages, and states.

Architecture Building Blocks (ABBs)	Description
	Enterprise Data Management In a knowledge economy, information/data is a crucial enterprise asset that has to be managed in order to securely share information within an enterprise Cloud Ecosystem. The Enterprise Data Management functions have to execute for all of the life cycle phases for all classes of data. The key Enterprise Data Management functions (refer to The Open Group White Paper: An Information Architecture Vision) are data governance, information planning and architecture, information provisioning, records and archives provisioning, and information privacy. All manner of information/data has to be managed. Data can be classified as unstructured (human-processable only, such as an image); semi-structured which is machine-readable (e.g., an e-document), or structured which is machine-processable. Information is used by business users and consists of one or more classes of data (refer to The Open Group White Paper: An Information Architecture Vision). Metadata is data about the data (e.g., creator, date/time of creation, security classification, and so on) that has to be standardized and managed within an enterprise Cloud Ecosystem. Refer to The Open Group Guide: Cloud Computing Portability and Interoperability for detailed information.
Governance Risk & Compliance	Governance Risk & Compliance encompasses, integrates, and aligns activities such as corporate governance, enterprise risk management, and corporate compliance with applicable laws and regulations. Components include compliance management (which assures compliance with all internal information security policies and standards), vendor management (to ensure that service providers and outsourcers adhere to intended and contractual information security policies applying concepts of ownership and custody), audit management (to highlight areas for improvement), IT risk management (to ensure that risks of all types are identified, understood, communicated, and either accepted, remediated, transferred, or avoided), policy management (to maintain an organizational structure and process that supports the creation, implementation, exception handling, and management of policy that represent business requirements), and technical awareness and training (to increase the ability to select and implement effective technical security mechanisms, products, process, and tools). (This description is based on the definition in TC1 – A Quick Guide to the Reference Architecture. Refer also to The Open Group White Paper: An Architectural View of Security for Cloud.)

Architecture Building Blocks (ABBs)	Description
Infrastructure Protection Services	Infrastructure Protection Services secure server, end-point, network, and application layers. This discipline uses a traditional defense-in-depth approach to make sure containers and pipes of data are healthy. The controls of Infrastructure Protection Services are usually considered as preventive technical controls such as IDS/IPS, firewall, anti-malware, white/black listing, and more. They are relatively cost-effective in defending against the majority of traditional or non-advanced attacks. (This description is based on the definition in TC1 – A Quick Guide to the Reference Architecture. Refer also to The Open Group White Paper: An Architectural View of Security for Cloud.)
Information Security	The main objective of Information Security (*aka* Information Security Management) is to implement the appropriate measurements in order to minimize or eliminate the impact that security-related threats and vulnerabilities might have on an organization. Often Information Security will address privacy and confidentiality concerns; especially in international enterprises where national legislation may differ significantly and impact the transit and storage of data/information. Information Security is reliant on cloud-consistent security labeling (e.g., security classification) and compartmentalization as necessary. This is imperative if the cloud uses information rather than network-centric security. Other controls will dictate the security during data states including matters such as encryption protocols when data is in use, in transit, or at rest (DIU, DIT, DAR). (Refer to The Open Group White Paper: An Architectural View of Security for Cloud.)
	Risk Management Risk Management starts with the categorization and costing of information and related technology assets. Subsequently, risks are identified and classified along with the resultant management decisions to accept, mitigate, transfer, or avoid them. Risks are constantly monitored and reviewed whenever there are any changes to the cloud architecture. Dashboards for security management and risk management are used to measure and report the level of effectiveness of decisions and help the organization make new decisions that will maintain and improve that effectiveness. Analysis and plans for remediating residual risks are also part of the overall risk management framework. (Refer to TC1 – A Quick Guide to the Reference Architecture.)

Architecture Building Blocks (ABBs)	Description
Policy & Standards	Security policies are part of a logical abstraction of enterprise security architecture. They are derived from risk-based business requirements and exist at a number of different levels, including information security, physical security, business continuity, infrastructure security, application security, as well as the overarching business operational risk management. Security policies are statements that capture requirements specifying what type of security and how much should be applied to protect the business. Policies typically state what should be done, while avoiding reference to particular technical solutions. Security standards are an abstraction at the component level and are needed to ensure that the many different components can be integrated into systems. Internationally recognized standards for various aspects of security from standard bodies include ISO, IETF, IEEE, ISACA, OASIS, and TCG. Direction can also be provided in the form of operational security baselines, job aid guidelines, best practices, correlation of regulatory requirements, and role-based awareness. One way to approach security policy and its implementation is to classify information and associate policies with the resulting classes of data. (Refer to TC1 – A Quick Guide to the Reference Architecture.)
Privilege Service	The Privilege Service (*aka* Privilege Management) ensures that users have the access and privileges required to execute their duties and responsibilities with Identity and Access Management (IAM) functions such as identity management, authentication services, authorization services, and privilege usage management. This security discipline enables the right individuals to access the right resources across increasingly heterogeneous technology environments and meet increasingly rigorous compliance requirements. The technical controls of the Privilege Service focus on identity provisioning, passwords, multi-factor authentication, and policy management. This security practice is a crucial undertaking for any enterprise. It is also increasingly business-aligned, and it requires business skills, not just technical expertise. (This description is based on the definition in TC1 – A Quick Guide to the Reference Architecture. Refer also to The Open Group White Paper: An Architectural View of Security for Cloud.)
Threat and Vulnerability Service	This discipline (*aka* Threat and Vulnerability Management) deals with core security, such as vulnerability management, threat management, compliance testing, and penetration testing. Vulnerability management is a complex endeavor in which enterprises track their assets, monitor and scan for known vulnerabilities, and take action by patching the software, changing configurations, or deploying other controls in an attempt to reduce the attack surface at the resource layer. Threat modeling and security testing are also part of activities in order to identify the vulnerabilities effectively. (This description is based on the definition in TC1 – A Quick Guide to the Reference Architecture. Refer also to The Open Group White Paper: An Architectural View of Security for Cloud.)

3.1.4 Performance Services

Performance Services are responsible for enforcing SLAs on Cloud Services, including measuring resource utilization, performance analysis in the cloud computing environment, and providing real-time assessment and reporting on resource/service performance.

Table 4: Performance Services ABBs of the Cloud Ecosystem Reference Model

Architecture Building Blocks (ABBs)	Description
Resource Health Monitoring	Resource Health Monitoring provides an integrated view of Cloud Resources health to achieve better performance, accountability, and business results to support cloud operational events and generate Cloud Resources performance reports. It also provides instrumentation capabilities to monitor defined SLAs.
Service Health Monitoring	Service Health Monitoring provides an integrated view of Cloud Services health to achieve better performance, accountability, and business results to support cloud operational events and generate Cloud Services performance reports. It also provides instrumentation capabilities to monitor defined SLAs.
SLA Enforcement	SLA Enforcement ensures that SLAs defined in the service contract are rigidly enforced in order to avoid any applicable penalties. Captured data related to SLAs also provide opportunities to make adjustments to contracts and agreements during the subscription renewal process.

3.1.5 Interoperability and Portability Services

Interoperability and Portability Services provide Cloud Services to achieve effective integration with all the participants of an enterprise Cloud Ecosystem.

Table 5: Interoperability and Portability Services ABBs of the Cloud Ecosystem Reference Model

Architecture Building Blocks (ABBs)	Description
Information/Data Interoperability	Information/Data Interoperability provides the Cloud Service Consumer with the ability to effectively manage the life cycle of both structured and unstructured data of an enterprise. It provides mechanisms to classify data, access policies, and information protection to adhere to compliance regulations and legislation. Information/data interoperability requires a consistent structure for behavior data interoperability (i.e., rules and data behavior). Semantically consistent information allows data to be shared and re-used across applications and enterprises boundaries. This could include the use of cloud-specific metadata-based semantic standards such as The Open Group Universal Data Element Framework (UDEF) (refer to The Open Group UDEF webinar) or the US Government National Information Exchange Model (NIEM). This would enable the information/data to be shared and re-used within an enterprise Cloud Ecosystem. Refer to The Open Group Guide: Cloud Computing Portability and Interoperability for detailed information.
Service Interoperability	Service Interoperability is the ability of Cloud Service Consumers to use their data and services across multiple Cloud Service Providers with a unified management interface (refer to NIST SP 500-292). The following highlights interoperability/portability as service model levels. Refer to The Open Group Guide: Cloud Computing Portability and Interoperability for detailed information.
	IaaS Interoperability IaaS Interoperability (*aka* System Portability – refer to NIST SP 500-292) provides a mechanism for Cloud Service Providers to provision a workload (e.g., compute) either an internal environment or onto an external Cloud Provider's environment and seamless migration of information about the service and its underlying resources.
	PaaS Interoperability The PaaS level of interoperability focuses on the ability to provide seamless coordination in the development and deployment of platform services and associated licenses. Currently there is little or no portability provided at the PaaS level.
	SaaS Interoperability Cloud Service Consumers expect to have the ability to support critical SaaS applications' features on a variety of channels (e.g., web, mobile, smart phone, etc.). Interoperability on common features is usually supported (where possible) by utilizing presentation abstraction.
Data Portability	**Data Migration** Data Migration provides an automated mechanism to transfer data from one cloud environment to another or to other computing systems.

Architecture Building Blocks (ABBs)	Description
	Data Synchronization Data Synchronization is the mechanism to ensure consistency across the Cloud Ecosystem to a single set of source data for all duplicated target data storage and *vice versa*. It ensures the continuous coherency of the data over time. It is a fundamental requirement for globally distributed applications (e.g., file synchronization between regions, and base information synchronization between catalogs). For example, a common service catalog data model that allows data synchronization capabilities between a Cloud Service Provider's service catalog and a Cloud Service Consumer's product catalog.

3.1.6 Product Catalog Services

The product catalog of the Cloud Ecosystem provides catalog information (description, type, associated base SLAs, etc.) about an enterprise's Cloud Services.

Table 6: Product Catalog Services ABBs of the Cloud Ecosystem Reference Model

Architecture Building Blocks (ABBs)	Description
Change & Configuration Services	The Change & Configuration Services ensure that the configuration of Cloud Services remains compliant with the changes in policies and compliance. It maintains an accurate configuration of Cloud Services offered in the catalog. It also ensures that the Configuration Management Database (CMDB) information is highly available, secured, and in compliance with applicable licensing terms and conditions.
Service Catalog	The Service Catalog provides flexible and easily configurable catalog information (description, type, associated base SLAs, etc.) and enables a mechanism for Cloud Service Consumers to subscribe to listed services. The information is generally collected through a self-service Cloud Service provisioning portal and allows cloud consumers to describe and manage Cloud Services easily. The service catalog includes information about the Cloud Service (pricing, payment terms and conditions, etc.), could support multiple pricing models (pay-as-you-go, tiered models, etc.), and includes technical, business, and compliance constraints. The cloud service catalog integrates with the CMDB to define and manage information about instances of catalog services and their relationship with physical and virtual infrastructure resources. The service catalog seamlessly integrates with the cloud security service and Cloud Services management tools (business and operational management tools). The service catalog could also describe the Cloud Service Provider's ability to meet a cloud performance rating (a common way to evaluate and determine competitive advantage).

3.1.7 Resource Catalog Services

The Resource Catalog Services manages the underlying Cloud Services resources of an enterprise Cloud Ecosystem.

Table 7: Resource Catalog Services ABBs of the Cloud Ecosystem Reference Model

Architecture Building Blocks (ABBs)	**Description**
Change & Configuration Service	The Change & Configuration Service for resources ensures that the configuration of Cloud Services remains compliant with the changes in policies and compliance. It maintains an accurate configuration of the Cloud Services offered in the catalog. It also ensures that CMDB information is highly available, secured, and in compliance with applicable licensing terms and conditions.
Resource Catalog	The resource catalog manages information about the resources required to support Cloud Services provisioning requests captured through the self-service Cloud Service management provisioning channel. The resource catalog also includes technical, business, and compliance constraints.

3.2 Enterprise Architecture Principles of the Cloud Ecosystem

Enterprise Architecture Principles of the Cloud Ecosystem define the underlying rules and guidelines for the use of the ABBs identified in the Cloud Ecosystem Reference Model to manage the life cycle of Cloud Services across the enterprise. These principles should be in alignment with other enterprise principles and reflect an architectural consensus across the enterprise. The principles ensure consistency and integrity of the Enterprise Architecture and form the basis for making future decisions pertinent to an enterprise’s Cloud Ecosystem.

Principle Name	**Auto-provisioned sharable system infrastructure.**
Description	The underlying computing resources of IaaS (e.g., storage, compute, and network) are shared and auto-provisioned to support an efficient system infrastructure.
Rationale	In order to meet business objectives to maximize profit, the IaaS Cloud Service Provider’s underlying computing resources serve using a multi-tenant environment. IaaS can seamlessly move workloads around to lower overhead and meet defined SLAs.

Principle Name	**Auto-provisioned sharable system infrastructure.**
Implications	IaaS should have a built-in capability of automated provisioning and dynamically move workload to meet defined SLAs. Business and service performance impact due to shared IaaS infrastructure should be well understood to avoid any undesired outcome. Cloud Service Providers should enable mechanisms to protect one tenant from other tenants. Auto-provisioning must prepare for peaks in load (e.g., higher volume of order and usage of computing resources due to advertised sale) with the use of cloud bursting. Cloud bursting is a way to address peak load by augmenting computing resources with an external IaaS provider's computing environment.

Principle Name	**Cloud solutions are designed to address performance variance.**
Description	Cloud solutions that use common and public networks, using the Internet Protocol (IP), should expect unreliable service due to performance variance, variable latency, and network failure.
Rationale	One of the essential characteristics of cloud computing is to have cloud capabilities accessed through the standard and public Internet. Cloud solutions should be designed to address unreliable IP service and variance in latency.
Implications	Cloud solutions should be designed to seamlessly handle network failure and address how to meet performance-related SLAs. Data should be well protected in all stages of data (DIU, DAR, and DIT). Built-in capabilities need to be provided to deal with communications latency variance.

Principle Name	**Automated ways to measure and optimize cloud solutions.**
Description	Cloud Services solutions should enable automated ways to measure allocation and consumption of Cloud Services and optimize the service usage by leveraging metering capability.
Rationale	In order to minimize investment on Cloud Services, Cloud Services solutions should provide real-time transparency on Cloud Services utilization to both Cloud Service Provider and Cloud Service Consumer.

Principle Name	**Automated ways to measure and optimize cloud solutions.**
Implications	Cloud Services solutions should be designed with built-in mechanisms to capture resources allocation, consumption, and produce measurements data. Provide real-time (or near real-time) assessment reports to efficiently respond to demand/usage of Cloud Services solutions. Although profiling resource usage by any cloud solution in a multi-tenant cloud environment will be challenging, it would be required to optimize the usage to ensure accurate metering. Evaluate measurements data and make any changes to optimize Cloud Services solutions.

Principle Name	**Automatic provisioning to enable horizontal scaling for distributed workload.**
Description	Cloud Service Providers seek horizontal scaling (simultaneous process of data across multiple machines) to take advantage of larger virtual machine capabilities that could be rapidly and automatically provisioned to meet the requirements of parallel processing.
Rationale	Where possible, Cloud Service Providers are looking to utilize their larger virtual machines. Comparatively, horizontal scaling allows Cloud Service Consumers to process large amounts of data efficiently with minimum investment (e.g., the use of Hadoop and MapReduce types of applications).
Implications	Cloud solutions will have to be designed specifically for loosely-coupled distributed computing with fine-grained processing which could also promote easier workload movement. Larger data sources might require partitioning into smaller sets of data sources.

Principle Name	**Loosely-coupled Cloud Services.**
Description	Ensure that SaaS, PaaS, and IaaS are loosely-coupled. For example, a Cloud Service Consumer of PaaS does not control the underlying cloud infrastructure resources (e.g., compute, storage, and network).
Rationale	Cloud Services are designed to support dynamic and scalable cloud environments.
Implications	Minimize customization of Cloud Services to effectively support a multi-tenant deployment model. Well-defined separation of concerns in a cloud environment. Figure 3 illustrates the scope of control between Cloud Service Provider and Cloud Service Consumer. For more details, refer to Section 2.7 of NIST SP 500-292.

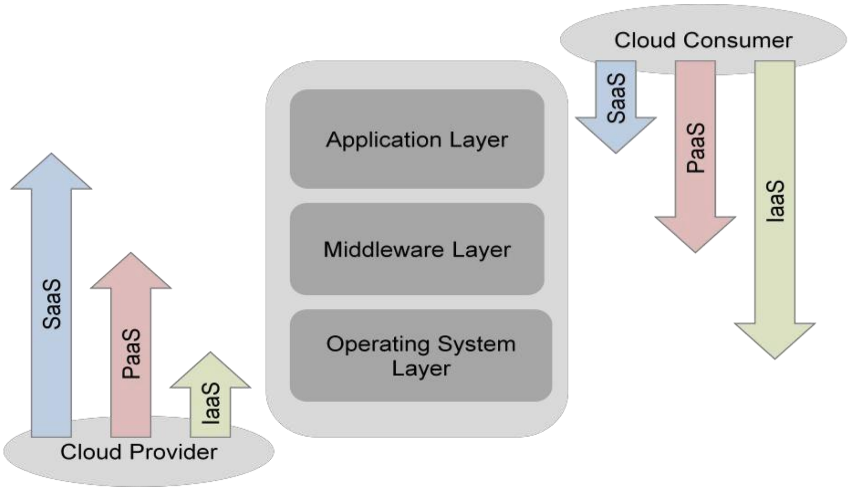

Figure 3: Scope of Control between Provider and Consumer (NIST SP 500-292)

Principle Name	**Cloud Service abstraction and control.**
Description	Ensure that Cloud Services are securely exposed with the appropriate level of abstraction and hide implementation details of a Cloud Service.
Rationale	Cloud Service abstraction provides the right separation and hides the implementation details to ensure service agility.
Implications	Ensure there is a level of abstraction that separates the concept/interface and implementation details of Cloud Services. Ensure that all essential characteristics of Cloud Services (e.g., resource pooling, broad network access, measured service, rapid provisioning, etc.) are maintained without exposing implementation details. For example, in the case of IaaS, resource abstraction components include software elements, such as hypervisors, virtual machines, virtual data storage, and other computing resource abstractions. Ensure there are appropriate controls in place to provide secure and reliable usage of underlying service resources.

Principle Name	**Multi-tenancy.**
Description	A cloud computing model must support tenant and solution isolation among multiple tenants of the cloud.
Rationale	Cloud computing stores clients' assets (information and operational processes applications) in servers distributed "who knows where", so it is critical that each client's assets are kept securely separated from the assets of other clients, irrespective of the storage media and processing resources that each client may also use in the cloud.

Principle Name	**Multi-tenancy.**
Implications	Cloud Service Providers offer assurances that they provide secure isolation between the assets of each of their clients. While this is difficult for them to evidence, their isolation control mechanisms seem to demonstrate success over this capability. SLAs may be required that guarantee separation of concerns with appropriate penalties.

4 Architectural Considerations for an Enterprise Cloud Ecosystem (Informative)

This section provides considerations that are significant in the development of an Enterprise Architecture for the Cloud Ecosystem using the Cloud Ecosystem Reference Model.

4.1 Cloud Deployment Models

A Cloud Service may be deployed on an infrastructure with one of the following deployment models.

Table 8: Cloud Deployment Models

Deployment Model	Description
Public Cloud	"A public cloud is one in which the cloud infrastructure and computing resources are made available to the general public over a public network. A public cloud is owned by an organization selling Cloud Services, and serves a diverse pool of clients." (Refer to NIST SP 500-292.)
Private Cloud	"A private cloud gives a single Cloud Service Consumer's organization the exclusive access to and usage of the infrastructure and computational resources. It may be managed either by the Cloud Service Consumer organization or by a third party, and may be hosted on the organization's premises (i.e., on-site private clouds) or outsourced to a hosting company (i.e., outsourced private clouds)." (Refer to NIST SP 500-292.)
Community Cloud	"A community cloud serves a group of Cloud Service Consumers which have shared concerns, such as mission objectives, security, privacy and compliance policy, rather than serving a single organization as does a private cloud. Similar to private clouds, a community cloud may be managed by the organizations or by a third party, and may be implemented on customer premises (i.e., on-site community cloud) or outsourced to a hosting company (i.e., outsourced community cloud)." (Refer to NIST SP 500-292.)
Hybrid Cloud	"A hybrid cloud is a composition of two or more clouds (on-site private, on-site community, off-site private, off-site community, or public) that remain as distinct entities but are bound together by standardized or proprietary technology that enables data and application portability." (Refer to NIST SP 500-292.)

4.2 Example Cloud Services

The following example Cloud Services deliver packaged capabilities to an enterprise Cloud Ecosystem. These services may be deployed on a number of environments including private and multi-tenant.

- Business Process as a Service (BPaaS) is an example service with the capability provided to manage an entire business process as a service in the cloud. Generally, the underlying capabilities of a BPaaS platform (i.e., software, technology, infrastructure resources, etc.) are owned and managed by the Cloud Service Provider. However, the Cloud Service Consumer is the source authority for information/data that traverses through the business processes.
- Information/Data as a Service (DaaS) is another example Cloud Service where Cloud Service Providers make available sets of information/data and associated metadata using one or more established standards. All other authorized services can make use of the information/data (or subsets thereof) and not worry about maintaining its quality. This class of service is especially useful for large and complex data sets such as geometrics and/or open government initiatives.

4.3 Specialized Organizational Roles

The following is a recommended list of specialized roles with some defined responsibilities (though not a comprehensive list of specialized roles) for an enterprise Cloud Ecosystem. The specialized organizational roles augment the roles defined in the Cloud Ecosystem Reference Model:

- **Cloud Service Administrator**: A person who administers cloud systems.
- **Cloud Services Strategist**: A person or strategic business unit (e.g., Cloud Services PMO) of an enterprise that develops Cloud Services strategies and provides guidance on how to transform business into using Cloud Services.
- **Cloud Service Manager**: A person who is in charge of providing guidance and direction of cloud computing efforts. This person leads a team (e.g., Cloud PMO) to ensure consistency in the cloud computing business and service delivery models of an enterprise.
- **End User**: A person who interacts with and uses a Cloud Service. End users are often unaware of how their services are provided or procured. Examples of these actors include employees, mobile users, and web users. (Refer to TC1 – Reference Architecture.)

4.4 Security Considerations

Cloud has extended enterprise boundaries and the security of enterprise information/data is one of the primary issues surrounding cloud adoption. Security boundaries are extended from a self-managed environment to an external and somewhat untrusted environment of the cloud. Some of the security considerations are:

- Ability to secure intellectual property and capital assets

- Evolve the security capabilities to support cloud deployment
- Effectively manage confidential information and apply regulatory policy requirements (records management)
- Define an approach for how to enable policy-based service delivery
- Considerations for Identity, Entitlement, and Access Management (IEM) and/or Role-Based Access Control (RBAC) for the enterprise Cloud Ecosystem

4.5 Business Considerations

Some of the strategic business objectives for consideration include:

- Allow the CIO to focus on business information and applications providing direct business value to all stakeholders, rather than supporting platform and infrastructure
- Reduce or eliminate continuously evolving IT infrastructure investments
- Efficient management of business processes in a Cloud Ecosystem
- Seamless collaboration and integration capabilities with partners, suppliers, and back-office
- Standardization of business processes for consistent and cost-effective use:
    - Standardized capabilities consumed by all applications
    - Hide implementation complexity of core business capabilities

4.5.1 Business Excellence

The following business objectives are targeted by enterprises in order to capitalize on the cloud computing IT delivery model to achieve business excellence:

- Rapid business service enablement
- Cost-effective and standardized service models:
    - Standard process, tools, and technology
- Built-in self-service accessibility capabilities
- Lower total cost of ownership

Gain higher cash flow since capital expenditures on Cloud Services are typically lower as they are based on the pay-as-you-go pricing model. At the same time, there are challenges/considerations that need to be resolved to achieve target business agility. Some of those challenges are:

- How business capabilities, both existing and new, are to be assembled quickly
- Cloud Services change management

4.5.2 Business Capability Assessment

Provide a mechanism to evaluate and address business requirements as to what needs to be processed internally and what services can be processed externally.

4.5.3 Portability and Interoperability

Portability and interoperability aspects to ensure disparate services, perhaps provided by multiple Cloud Service Providers, can seamlessly interact.

4.5.4 Contractual, Legal, and Regulatory Considerations

The enterprise Cloud Ecosystem enables consistent enforcement of various applicable regulatory, auditing, and compliance-related business requirements. The Cloud Ecosystem offers services capabilities that define, integrate, and align compliance activities of enterprise governance bodies in order to apply consistent adherence to compliance with applicable laws and regulations.

4.6 Technical Considerations

Enterprises are attempting to evolve current business solutions to take advantage of dynamic allocation of resources with Cloud Services and the use of an SOA approach to modularize business solutions including application overhaul and consolidation.

The following are some of the technical considerations to ensure that an enterprise is prepared to take advantage of the cloud.

4.6.1 Common Framework for Applications

Where appropriate, consider an application framework that enables standardized Cloud Services capabilities to create, execute, and manage enterprise cloud business solutions. A common application framework, built on the Cloud Ecosystem Reference Model, provides an effective mechanism to manage interactions and collaborations with Cloud Service Providers.

4.6.2 Robust Integration Capabilities

Ensure that the Cloud Ecosystem has a cloud connection service capability that serves as a seamless connector from one cloud environment to another (e.g., private cloud environment to external/public cloud environment). A cloud connection service ensures secure connectivity when traversing different network boundaries seamlessly, and enables performance improvement capabilities (e.g., compression).

4.6.3 Network and Bandwidth

The Enterprise Architecture of the Cloud Ecosystem requires that cloud solutions are tolerant of network failures and bandwidth inconsistency. The architecture needs to accommodate these new assumptions associated with built-in architectural enabling mechanisms to efficiently communicate/exchange information consistently in an enterprise Cloud Ecosystem.

4.6.4 Distributed Environment (Global Applications *versus* Local Applications)

The inherent capabilities of utilizing standard network access in distributed applications may impose technical constraints that will require additional capabilities (e.g., caching and continuous synchronization of information) to support expected service response time. On the other hand, local/diversified applications may require some customization/coordination of Cloud Services and therefore have low potential to replicate without alterations. In either case, it would be ideal to describe a holistic enterprise cloud architectural strategy to avoid unintentionally creating silos in the Cloud Ecosystem.

4.7 Operational Considerations

Cloud computing is extending enterprises' trust boundaries for business operations to effectively achieve targeted business objectives. In order to optimize business relationships with extended enterprises that include heterogeneous Cloud Service Providers, the enterprise Cloud Ecosystem must efficiently manage business operations with its changed nature of IT delivery. Enterprises are now responsible for brokering cloud-specific solutions of Cloud Service Providers that meet the established policies on cost-effectiveness, solution viability, and business expectations related to IT performance. For example, the ability to rapidly provision IT services without spending large amounts of resources is one of the major practices that impacts business operations of an enterprise. The following summarizes the key business operational considerations for the Cloud Ecosystem.

4.7.1 Operational Excellence

The target objectives for cloud operational excellence are to lower overall operational expenditure and operational optimization to achieve a sustainable and long-term improvement of an enterprise. Also, operational excellence effectively manages all aspects of enterprise governance that include application, data, SOA, corporate, and IT governance.

4.7.2 Cloud Services Operational Management

The enterprise must adopt an IT strategy that not only builds internal clouds but also utilizes external clouds to enhance business agility and support:

- Operational support optimization
- Fully tested operational procedures
- Automated change and configuration control

4.7.3 Workforce Management

Due to several internal and external factors, most enterprises are shrinking their IT capabilities. Enterprises would like to efficiently utilize their finite resources on innovation and engaging their strategic Cloud Services suppliers and partners to leverage available Cloud Services and expertise in order to meet business objectives. The focus of enterprises is now to train the workforce with these new realities that requires the workforce to become an IT enabler and orchestrator.

4.7.4 Problem and Error Resolution Management

The enterprise Cloud Ecosystem manages any Cloud Service-related incidents and enables an effective mechanism to perform root cause analysis, store incidents-related information for further analysis, and provide an effective service to evolve Cloud Services so future incidents can be prevented.

4.7.5 Service-Level Agreements (SLAs)

The enterprise Cloud Ecosystem provides the capabilities to meet expected Service-Level Agreements (SLAs). For example, it provides a mechanism to seamlessly handle network failure and address performance-related SLAs. While engaging Cloud Service Providers, the enterprise must carefully negotiate SLAs to ensure that its requirements are explicit and fairly managed. The Cloud Ecosystem will provide a mechanism that provides opportunities/insights in real-time to make adjustments to SLAs with Cloud Service Providers during their active relationship period.

4.7.6 Licensing and Contract Management

In order to reduce IT service costs, enterprises require efficient enablement of Cloud Services. Cloud Service Providers provide many options to optimize licenses and contracts needs associated with their Cloud Services offerings along with an expedited auto-provisioning process and flexibility to adjust Cloud Services to meet immediate business requirements.

4.7.7 Cloud Service Subscription and Life Cycle Management

The externalization of IT is the movement of IT resources from direct enterprise control and ownership to one or more external service providers. This requires new operational capabilities to build relationships with external Cloud Service Providers to expedite Cloud Services provisioning to meet business needs, within effective pricing parameters. Cloud Service Providers will provide effective Cloud Services management through such capabilities as a self-service, quickly provisioned, show back-based IT consumption model.

4.7.8 Cloud In/Exit/Migration Strategy

As enterprise boundaries continue to disappear, their ability to rapidly provision IT services without large capital expenditure is appealing to budget-minded executives. IT organizations are taking an “adopt and go” strategy to satisfy internal customer IT consumption requirements. For example, many IT organizations are utilizing Cloud Service Providers with effective life-cycle management (i.e., in/exit/migration of services) to support non-critical IT services (e.g., development and test applications). This requires an effective strategy to engage Cloud Service Providers in enabling cloud solutions, shifting Cloud Services from one Cloud Service Provider to another, and discontinuing Cloud Services of Cloud Service Providers when required.

4.7.9 Capacity and Services Monitoring

The enterprise Cloud Ecosystem shall consider providing an integrated monitoring view and performance reporting capabilities in order to achieve better performance, accountability, and business results from its Cloud Services. The Cloud Ecosystem shall enable a real-time and efficient allocation of underlying resource workloads in order to provide optimal use of running Cloud Services.

5 Using the Cloud Ecosystem Reference Model with the TOGAF Standard (Informative)

5.1 Introduction

This chapter describes how to develop, manage, and govern an Enterprise Architecture of a fictitious organization named “CloudEcoSource” with use of the Cloud Ecosystem Reference Model and the TOGAF standard. It describes an approach for each phase of the TOGAF Architecture Development Method (ADM) and what the architect should consider when looking to apply the TOGAF ADM to an enterprise Cloud Ecosystem. This informative case study describes a generic approach to develop an Enterprise Architecture by utilizing Architecture Building Blocks (ABBs) identified in the Cloud Ecosystem Reference Model. The standard defines an approach to identify Solution Building Blocks (SBBs) to address the architectural capabilities of ABBs. For example, the following describes the relation of ABBs and SBBs for rapid provisioning and data protection in an enterprise Cloud Ecosystem:

- An SBB for rapid provisioning can be provided by any of the participants of an enterprise Cloud Ecosystem delivering the Cloud Service (e.g., Cloud Service Provider, Cloud Service Broker, etc.). An ABB for these capabilities is, however, also part of the architecture of the consuming enterprise, because the architecture requirement for rapid provisioning will remain even if another participating entity in the enterprise Cloud Ecosystem provides the SBB.
- A data protection ABB should also appear in every applicable participant’s architecture. From the perspective of the customer enterprise, each instantiation (SBB) of that building block is another participant with which there is a relevant relationship as part of the customer’s Cloud Ecosystem. This is because security policies applicable to the customer’s data need to be carried out consistently across all parties handling that data, regardless of how the building block is actually implemented.

5.1.1 CloudEcoSource Background

In order to illustrate how the TOGAF standard can be applied for the Cloud Ecosystem, a fictitious organization named “CloudEcoSource” with three separate initiatives will be referenced for each phase of the TOGAF ADM.

Besides having a strong IT function in the organization, CloudEcoSource has engaged multiple external Cloud Service Providers for its heterogeneous cloud infrastructure platform and software services to support its business needs. The organization intends to use the TOGAF standard for Enterprise Architecture practices to manage its Cloud Services as well. CloudEcoSource has currently three distinct cloud-specific initiatives that have the characteristics of IaaS, PaaS, and SaaS for cloud. This section will describe how CloudEcoSource plans to use the TOGAF standard to create and evolve an Enterprise

Architecture for the Cloud Ecosystem. The following is a brief description of the cloud-specific initiatives of CloudEcoSource:

- **IaaS initiative**: Infrastructure modernization and consolidation

  An IaaS-focused initiative of CloudEcoSource with the expectations on how to transform and regulate dynamic resources consumption in a multi-tenant infrastructure environment with effective management of privacy of its tenants (i.e., enterprise customers).

- **PaaS initiative**: Rapid application development platform

  A PaaS-focused initiative to identify and describe architectural capabilities of a platform for CloudEcoSource business solutions. The instances of the platforms could be deployed and operated either solely by an enterprise or by participating entities of the Cloud Ecosystem.

- **SaaS initiative**: Enhanced collaborations among multiple service providers

  A SaaS-focused initiative where CloudEcoSource is assembling business capabilities for business collaborations that extend the organization's traditional enterprise application boundaries with extended users (both internal and external to the organization).

5.2 Preliminary Phase

The TOGAF Preliminary Phase is about defining "where, what, why, who, and how we do architecture" in the enterprise concerned. It does the preparation and establishes the architecture framework needed for new Enterprise Architecture work. The TOGAF standard provides for incremental architecture development. Each cycle through Phases A to H creates an incremental addition to the Enterprise Architecture. (The cycles typically overlap, with Phases A to F of each new cycle being carried out in parallel with Phase G: Implementation Governance of the previous cycle.)

The Preliminary Phase does what is needed before the cycles can start. It is usually carried out when the TOGAF framework is first adopted by a particular architecture team for a particular enterprise. Its activities may be revisited as needed for subsequent architecture engagements.

The Preliminary Phase is where the architect adopts the principles of the Cloud Ecosystem, and organizational change flexibility. This affects two other outputs of the phase: the governance and support strategy, and the content of the initial Architecture Repository. It focuses on the following aspects to ensure that the organization's architectural model has the support of necessary business and IT capabilities for the use of the organization's Cloud Ecosystem:

- Describe the business mission, goals, and objectives to ensure that Architecture Principles are in alignment with them.
- Describe and ensure that there is a process to document business requirements and constraints (both internal and external) that will impact the Cloud Ecosystem.
- Ensure that the organization model for Enterprise Architecture and the ADM are in alignment with the business goals and objectives of the Cloud Ecosystem.

- Confirm that the architecture governance structure and guidelines will be able to provide support for all aspects of the organization's Cloud Ecosystem.
- Prepare to create a request for Cloud Ecosystem architectural work to get formal approval in Phase A.

5.2.1 Architecture Principles

Architecture Principles are a set of principles that relate to architecture work. They reflect a level of consensus across the enterprise, and embody the spirit and thinking of existing enterprise principles. Architecture Principles govern the architecture process, affecting the development, maintenance, and use of the Enterprise Architecture.

The Preliminary Phase defines the Architecture Principles that will form part of the constraints on any architecture work undertaken in the enterprise. They are typically developed by the lead Enterprise Architect, in conjunction with key stakeholders, and are approved by the Architecture Board. They are included in the tailored architecture framework, which is an output of the Preliminary Phase.

An enterprise participating in the Cloud Ecosystem will in general have an established set of Architecture Principles. These should be examined in the context of the Cloud Ecosystem for completeness and applicability. It is possible to identify several scenarios that could apply:

- Existing principles, which fit poorly, if at all, with cloud. This can happen when a principle dates from an earlier period, when cloud in its current form did not exist. Should we keep the principle as-is and accept the consequences, even if it means little or no cloud? Can it be amended? In this case we need to look at the underlying Business Principle and evaluate whether the Architecture Principle can be phrased differently. It is possible that we may come to the conclusion that the principle is no longer valid.
- Principles which are clearly still relevant but need to be expressed differently. This too may require revisiting the underlying Business Principle.
- Existing principles whose implications need to be given particular attention in the cloud context.
- New principles which are needed to address the specific challenges of the Cloud Ecosystem.

The Enterprise Architecture Principles of the Cloud Ecosystem defined in Section 3.2 can be listed with the Motivation Extension viewpoint of the ArchiMate standard. Figure 4 illustrates the viewpoint of an enterprise's Cloud Ecosystem.

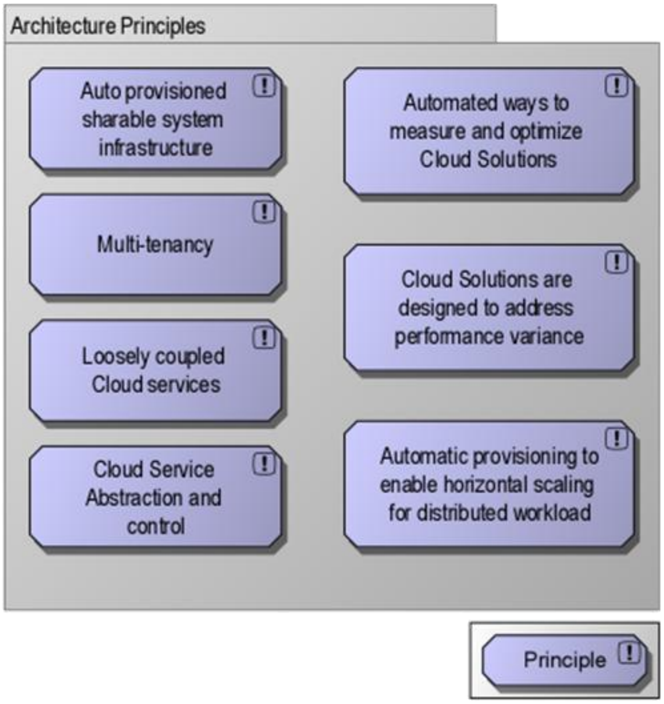
Architecture Principles
Auto provisioned sharable system infrastructure
Automated ways to measure and optimize Cloud Solutions
Multi-tenancy
Cloud Solutions are designed to address performance variance
Loosely coupled Cloud services
Cloud Service Abstraction and control
Automatic provisioning to enable horizontal scaling for distributed workload
Principle

Figure 4: Enterprise Cloud Ecosystem Architecture Principles

The rest of this section describes the additional steps taken in the Preliminary Phase to achieve the overall goals of the architectural effort outlined for CloudEcoSource.

5.2.2 Define Governance Approach

The Cloud Ecosystem can leverage and extend the TOGAF Architecture Governance Framework to manage its cloud architectural activities and Cloud Service Providers as one of the participants within the Cloud Ecosystem as illustrated below. In addition, the established architecture governance board of CloudEcoSource will govern the project.

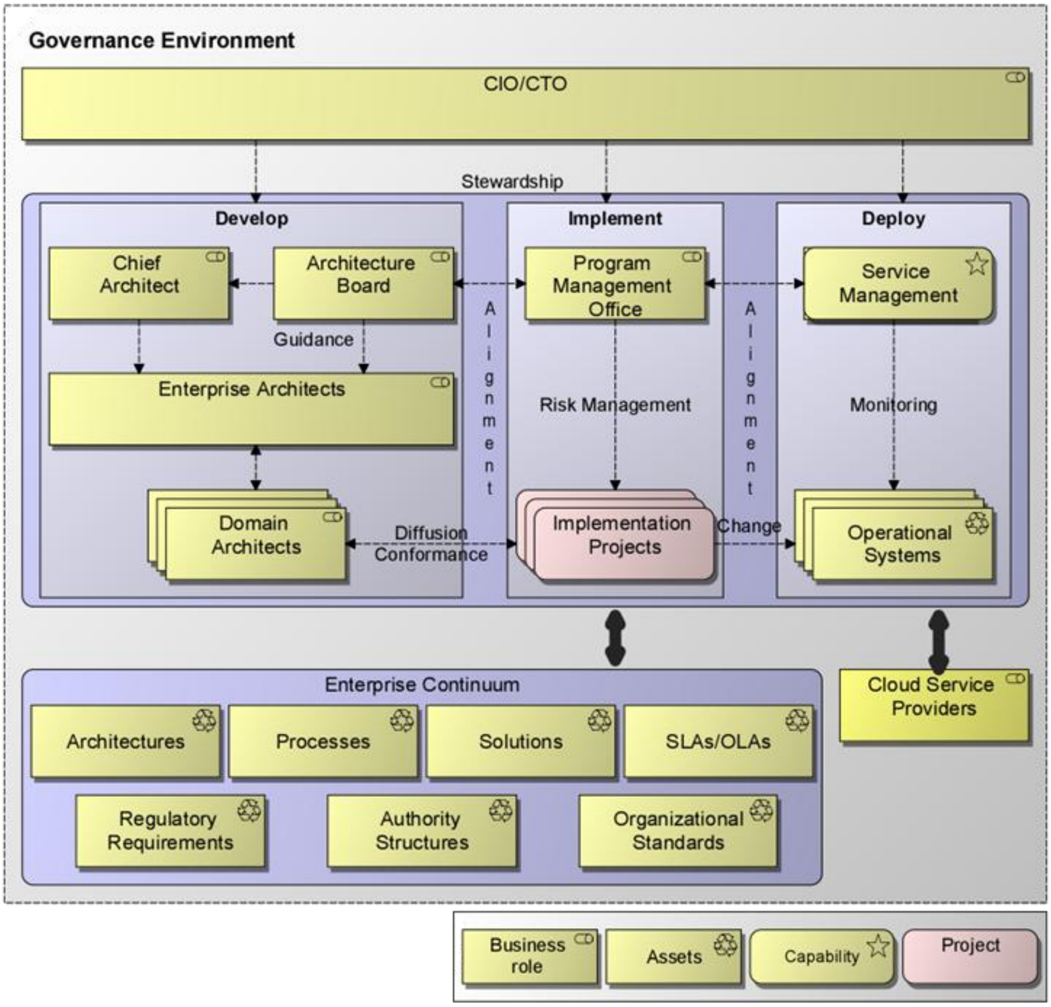

Figure 5: EA Governance Structure of CloudEcoSource – An Illustration

5.2.3 Organizational Implications

In order to effectively manage the CloudEcoSource Cloud Ecosystem, the management has determined that it will be ideal to augment the current structure with the recommended organizational roles defined in Section 4.3.

5.3 Phase A: Architecture Vision

The Architecture Vision phase focuses on addressing the changing business requirements from both internal and external stakeholders and envisions a mechanism to meet those requirements in an optimal way. It focuses on the following to ensure that necessary adjustments to current business and IT capabilities are addressed, thus enabling an efficient use of the Cloud Ecosystem of an organization:

- First and foremost, secure the organization's top management support as well as commitment from all impacted stakeholders.

- Ensure that the impact to all stakeholders' interests is understood and agreed by relevant stakeholders.
- Validate the business mission, goals, and objectives to ensure that Architecture Principles are in alignment with them.
- Establish Key Performance Indicators (KPIs) for the Cloud Ecosystem to validate and align the Enterprise Architecture of an organization.
- Describe and ensure that there is a process to document business requirements and constraints (both internal and external) that will impact the Cloud Ecosystem.
- Ensure that the organization model for Enterprise Architecture and the ADM are in alignment with the business goals and objectives of the Cloud Ecosystem.
- Ensure that existing architecture governance will effectively utilize the Cloud Ecosystem and provide guidance to address gaps and constraints.
- Obtain formal approval for the architecture work of the Cloud Ecosystem.

The rest of this section describes the steps taken in Phase A to achieve the overall goals of the architectural effort outlined for CloudEcoSource.

5.3.1 Establish the Architecture Project

CloudEcoSource followed its corporate policies and procedures to ensure that its cloud initiatives have been recognized and endorsed by the appropriate management as a planned cloud architectural activity within the Cloud Ecosystem.

5.3.2 Identify Stakeholders, Concerns, and Business Requirements

In order to help us finalize the business requirements, expectations, and scope of the initiatives, we should identify the key stakeholders of CloudEcoSource. The following table shows stakeholder concerns, their classifications (with expectations), and mapping to architectural output to be developed to satisfy and communicate their concerns.

Table 9: Stakeholder Map of CloudEcoSource – An Illustration

Stakeholder	**Key Concerns**	**Class**	**Architectural Viewpoint/Output (Catalogs, Matrices, and Diagrams)**
Corporate	High-level business drivers, goals, and objectives	Key Players	Organization Decomposition diagram Business Footprint diagram Business Goals to Cloud Services Mapping diagram
Program Management Office (PMO)	Business portfolio, product catalog, functional prioritization, funding	Keep Informed	Business Footprint diagram Functional decomposition diagram Portfolio catalog

Stakeholder	Key Concerns	Class	Architectural Viewpoint/Output (Catalogs, Matrices, and Diagrams)
Cloud Business Support	Service agreements, compliance, service demand, audit and reports	Key Players	Service-Level Agreements (SLAs) Actor/Role matrix Compliance and Reporting
Cloud Operations Support	Information assurance, service life cycle, capacity and performance, service resources	Key Players	Service Life Cycle diagram Information/Data Security diagram SLA Compliance reports Cloud Service Capacity Planning

Different stakeholders, playing different roles, also have different concerns (stakeholder viewpoints) which are the key drivers for the acceptance of the architecture program. Concerns are key drivers of the stakeholders, which, from their perspective, are decisive for the acceptance of the architecture program. There must be an inventory of all stakeholders and their concerns in the Architecture Vision phase.

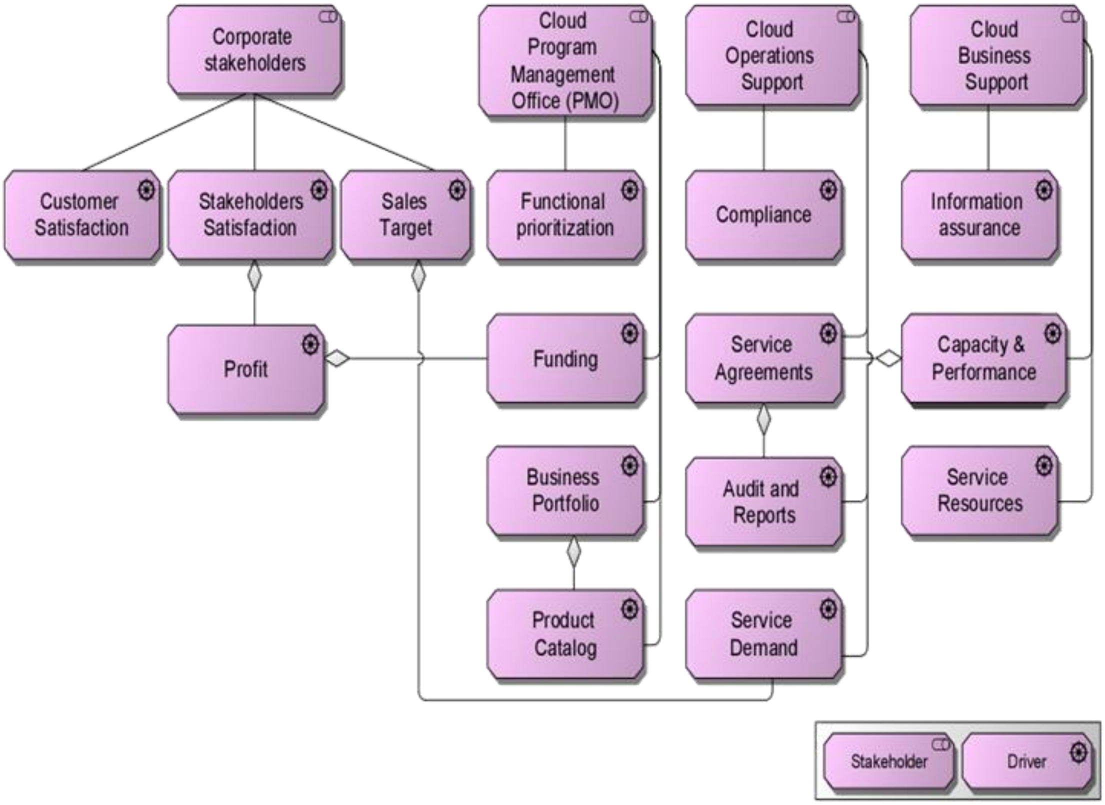

Figure 6: Stakeholder Concerns Viewpoint of CloudEcoSource – An Illustration

Then these concerns must be related to the goals of the future architecture. This can be achieved using the Goal Refinement viewpoint (as proposed in the Motivation Extension) and instantiated for a subset of CloudEcoSource.

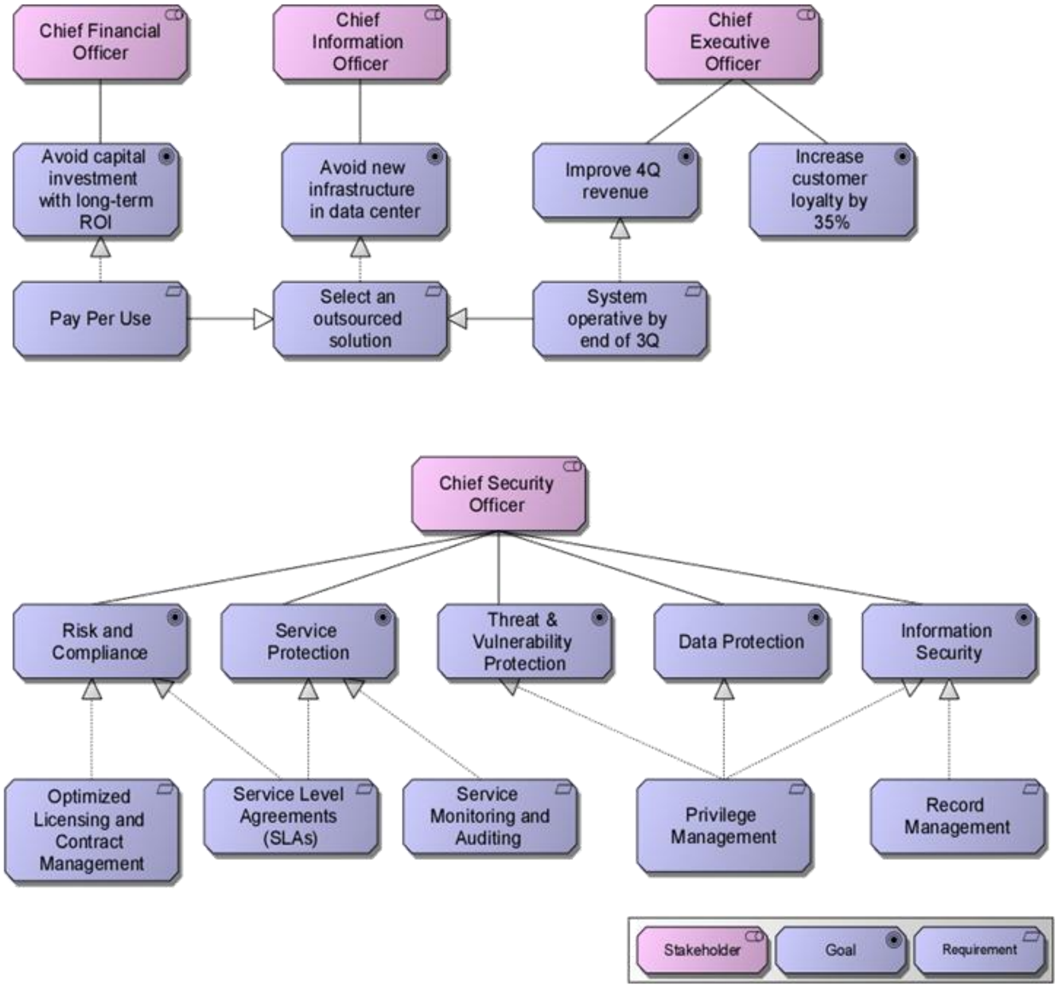
Chief Financial Officer
Chief Information Officer
Chief Executive Officer
Avoid capital investment with long-term ROI
Avoid new infrastructure in data center
Improve 4Q revenue
Increase customer loyalty by 35%
Pay Per Use
Select an outsourced solution
System operative by end of 3Q
Chief Security Officer
Risk and Compliance
Service Protection
Threat & Vulnerability Protection
Data Protection
Information Security
Optimized Licensing and Contract Management
Service Level Agreements (SLAs)
Service Monitoring and Auditing
Privilege Management
Record Management
Stakeholder
Goal
Requirement

Figure 7: Goal Refinement Viewpoint of CloudEcoSource – An Illustration

5.3.3 Confirm and Elaborate Business Goals, Business Drivers, and Constraints

Once the business goals and strategic drivers of the organization are to be confirmed by key stakeholders, we should capture the applicable business, technical, and operational constraints of CloudEcoSource. These are essential items to ensure management endorsement for the cloud initiatives. For example, constraints pertaining to security, privacy, and confidentiality of information have to be clearly understood especially in the context of the CloudEcoSource Cloud Ecosystem where national security and privacy legislation differ. Addressing these constraints may well have a major architectural impact.

In order to highlight the capability evalation process, let’s consider that stakeholders of CloudEcoSource expect to improve existing Customer Relations Management (CRM) capabilities to reduce the number of complaints filed by its customers.

5.3.4 Evaluate Business Capabilities

CloudEcoSource business, technical, and operational capabilities related to the Cloud Ecosystem (see Chapter 4) are currently immature. Figure 8 illustrates one of the possible ways to highlight the target business capabilities of CloudEcoSource to support the value chain targeted to achieve business agility.

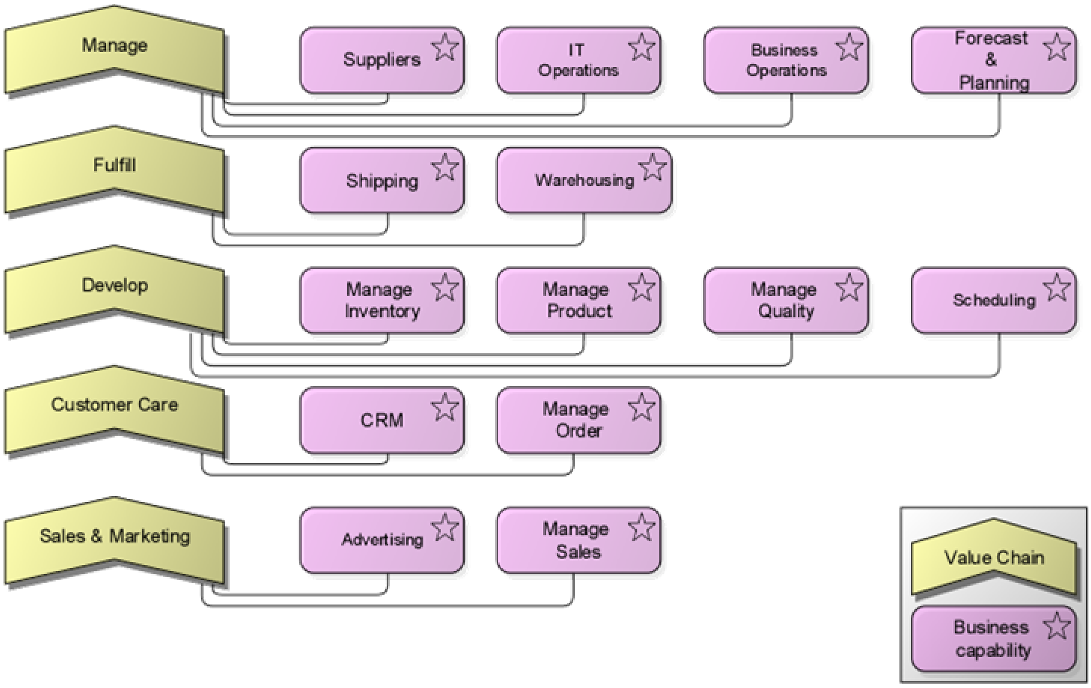

Figure 8: Target Business Capabilities of CloudEcoSource – An Illustration

Once the capabilities are defined, the possible implications for the CRM capability, for example, can be assessed and visualized with the stakeholder view. The results of the assessment are documented in a Capability Assessment (refer to the TOGAF 9.1 Specification, Part IV, Section 36.2.10).

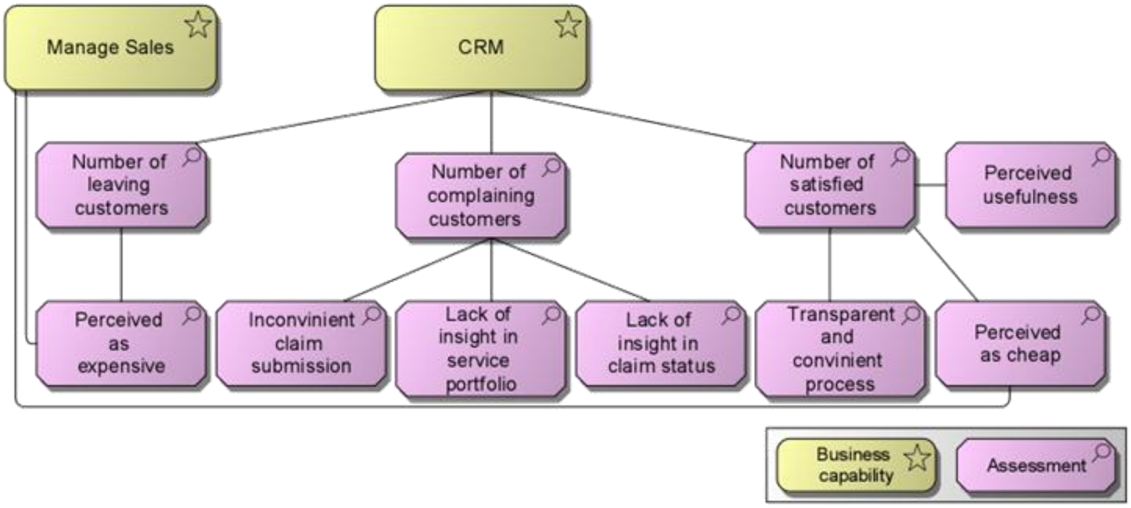
Manage Sales
CRM
Number of leaving customers
Number of complaining customers
Number of satisfied customers
Perceived usefulness
Perceived as expensive
Inconvinient claim submission
Lack of insight in service portfolio
Lack of insight in claim status
Transparent and convinient process
Perceived as cheap
Business capability
Assessment

Figure 9: CRM and Manage Sales Capabilities Assessment View of CloudEcoSource – An Illustration

5.3.5 Assess Readiness for Business Transformation

Table 10 illustrates the result of the CloudEcoSource readiness assessment to perform architecture work of cloud initiatives for effective enablement of the organization's Cloud Ecosystem.

Table 10: Business Transformation Readiness Assessment – An Illustration

Assessment ID	Readiness Factor	Priority (Low/Med/High)	Readiness Status (Low/Fair/Acceptable /Good/High)	Transformation Assessment (Difficulty Level: Low/Med/High)
1	Business needs	High	High	Low
2	Financial support	High	Fair	Low
3	Sponsorship support	High	Good	Low
4	Business readiness	High	Good	High
5	IT readiness	High	Acceptable	High
6	Operational readiness	High	Low	Med
7	Governance readiness	Med	Fair	High

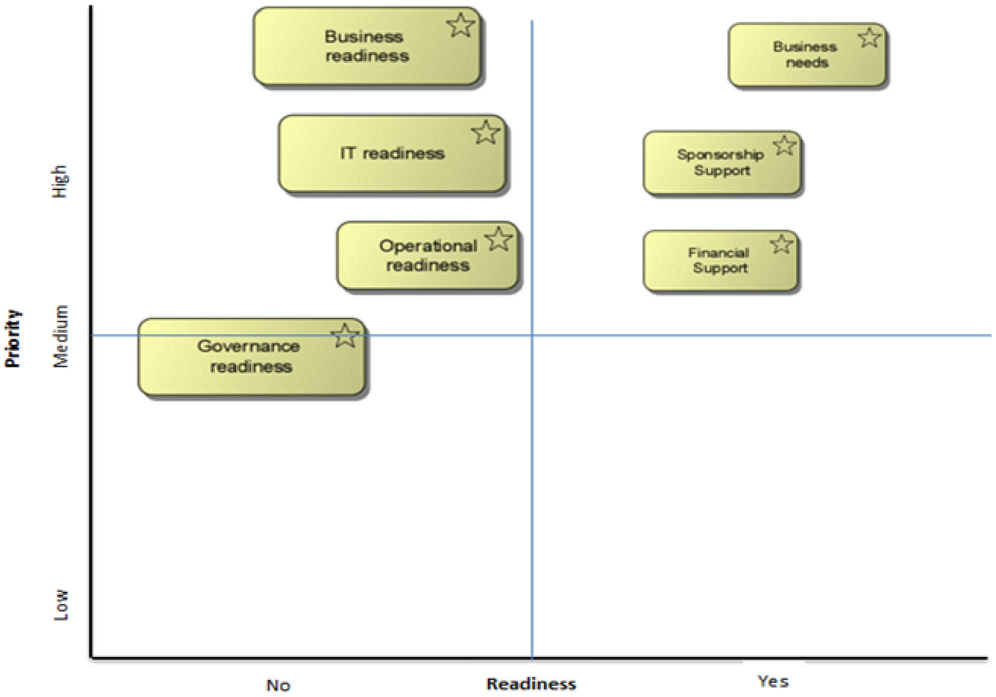

Figure 10: Business Transformation Readiness Assessment Matrix of CloudEcoSource – An Illustration

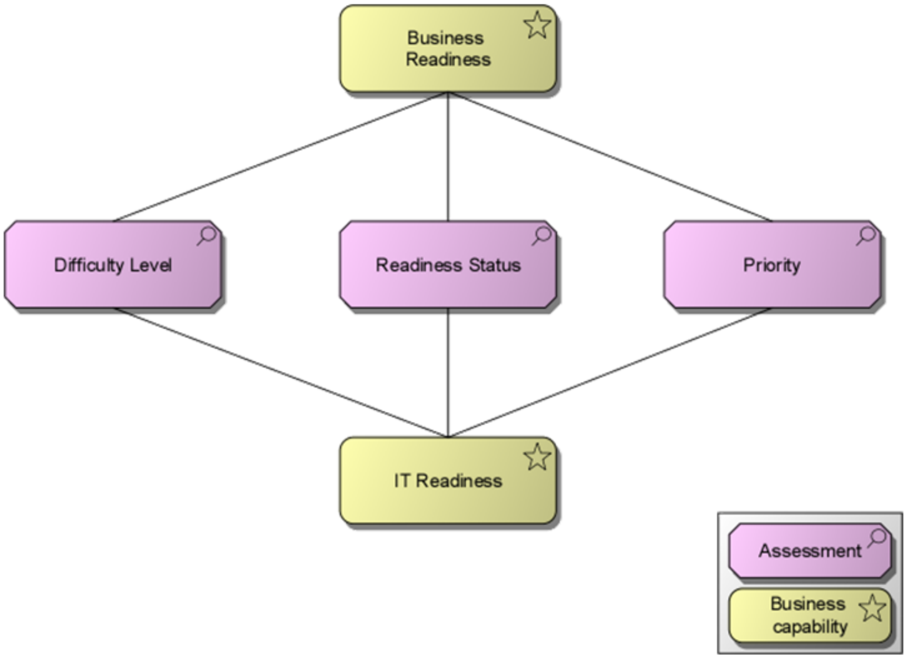

Figure 11: Readiness Factors Assessment of CloudEcoSource – An Illustration

5.3.6 Define Scope

CloudEcoSource developed a high-level strategic architecture that gives management and other stakeholders an overview of enterprise perspectives on the Cloud Ecosystem and the ways it will support business objectives. The scope also identifies the impacted segments (e.g., procurement, infrastructure, application platform, and solutions) and how to use the cloud Program Management Office (PMO) to manage the Cloud Services portfolio to ensure effective execution of architectural activities.

5.3.7 Confirm and Elaborate Architecture Principles, including Business Principles

The architecture team of CloudEcoSource confirmed that the Architecture Principles defined in the Preliminary Phase are in alignment with the enterprise principles, goals, and objectives and have been endorsed by the architecture governance board.

5.3.8 Develop Architecture Vision

The Architecture Vision of CloudEcoSource is to provide a Cloud Ecosystem that will support heterogeneous Cloud Service Providers in order to meet the objectives of its stakeholders. The architecture will enable a mechanism to effectively address all Cloud Service models (i.e., infrastructure, platform, and software) to minimize costs and to achieve business agility. Figure 12 illustrates a conceptual view of the Target Architecture of CloudEcoSource. It is based on the stakeholder concerns, business capability requirements, scope, constraints, and principles outlined for the CloudEcoSource Cloud Ecosystem.

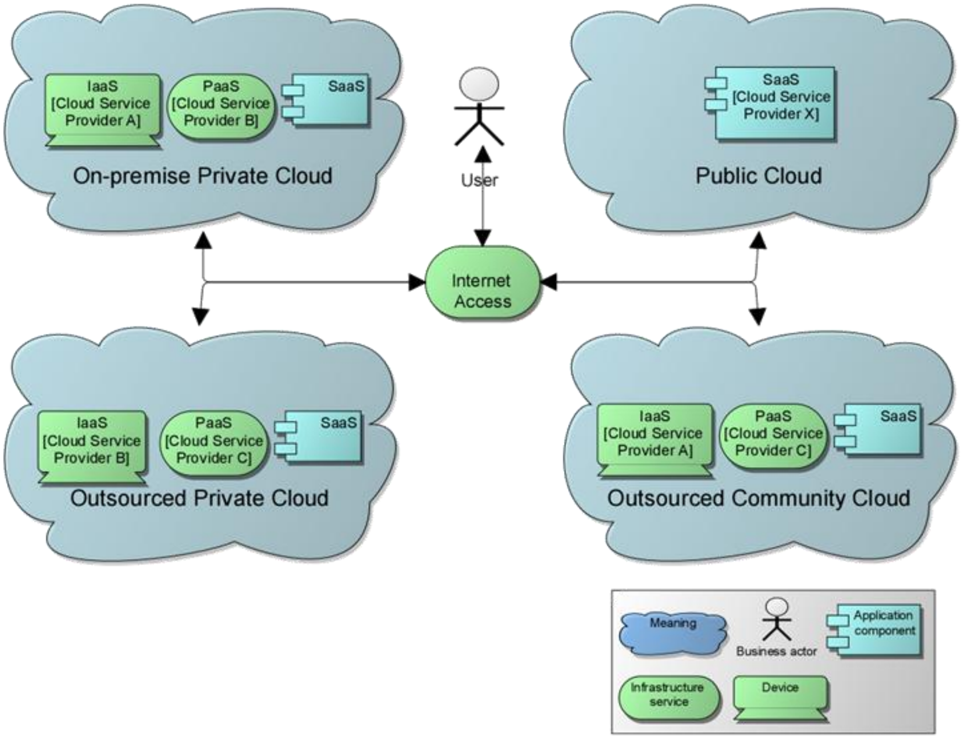
IaaS [Cloud Service Provider A]
PaaS [Cloud Service Provider B]
SaaS
On-premise Private Cloud
User
SaaS [Cloud Service Provider X]
Public Cloud
Internet Access
IaaS [Cloud Service Provider B]
PaaS [Cloud Service Provider C]
SaaS
Outsourced Private Cloud
IaaS [Cloud Service Provider A]
PaaS [Cloud Service Provider C]
SaaS
Outsourced Community Cloud
Meaning
Business actor
Application component
Infrastructure service
Device

Figure 12: Target Architecture of CloudEcoSource – An Illustration

5.3.9 Define the Target Architecture Value Propositions and KPIs

In order to track performance and to ensure that there are mechanisms in place to measure the architecture work of CloudEcoSource, the following performance measurements are defined:

- Procurement of Cloud Services will be at least 20% cheaper than the development cost.
- The operational cost of Cloud Services will be at most 85% of the current operational cost.
- Any request instigated by a user will provide a response within three seconds.

5.3.10 Develop Statement of Architecture Work; Secure Approval

The Architecture Statement of Work is defined to capture the architecture approach and impact to all stakeholders of CloudEcoSource. It contained a roadmap and communications plan to ensure that all stakeholders are aware of the progress of the cloud initiatives. The Architecture Statement of Work has captured risks classification and assigned a risk mitigation strategy.

It has now been approved by the sponsor and all applicable signing authorities to proceed with the architecture work.

5.4 Phase B: Business Architecture

The Business Architecture describes the business values of the Cloud Ecosystem to the key stakeholders of an organization and ensures that the business strategy, organization’s structure, governance, business process information, as well as interactions between these concepts are well defined. One of the objectives of the Business Architecture is to establish a mechanism that allows the organization to quickly deliver business value to its customers. Organizations have to maintain business structure to enable business functionality to achieve business agility. Business structure not only describes products and services that an organization provides, but also describes functions, processes, and their inter-relationships. Organizations using Cloud Services might have extended business structures due to business services provided not only by internal units, but also by external organizational units.

The Business Architecture describes relationships between different instances of Cloud Service models to ensure that organizations have consistent and coherent cloud-enabled business capabilities. Cloud Services provided by external service providers are transforming business processes and require new approaches to manage the impact on the organization’s functions and its IT environment. The life cycle management of Cloud Services requires constant check to ensure that business objectives are met with efficient and effective business risk management. Organizations might have to transform and evolve existing business processes and practices for efficient IT management. To achieve business agility, the organizations need to formulate strategy and address Cloud Services-related business objectives to enable efficient IT management by:

- Adopting Cloud Services as part of the enterprise strategy to transform business and IT functions

- Establishing an effective mechanism for Cloud Services management that allows existing business processes to integrate cloud sourcing practices and guidelines
- Evolving existing business processes to incorporate a business-driven approach to enable business process redesign that uses new capabilities to create optimal business solutions in order to achieve target objectives – this needs to be accomplished in an environment that is friendly to use
- Assessing business capabilities and realizing that Cloud Services will require new organizational roles (e.g., Cloud Service Broker, Cloud Strategist) to efficiently manage the cloud environment that generally extends traditional organizational boundaries with the use of external Cloud Service Providers

Figure 13 outlines the expected input and output of the Business Architecture phase from a Cloud Ecosystem perspective:

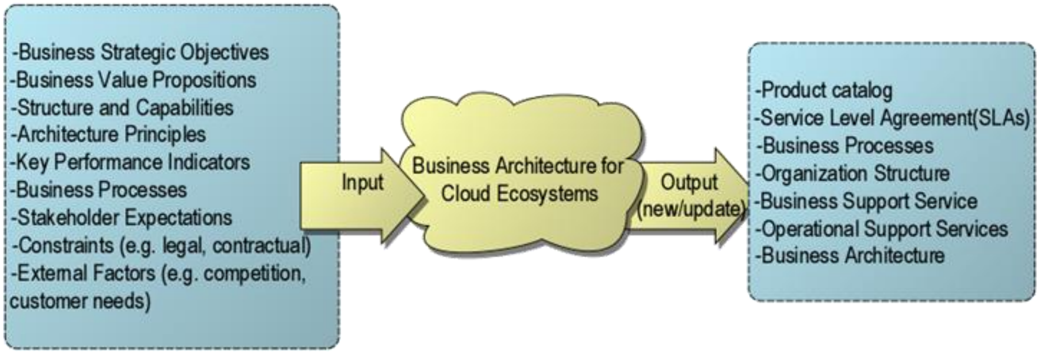
-Business Strategic Objectives
-Business Value Propositions
-Structure and Capabilities
-Architecture Principles
-Key Performance Indicators
-Business Processes
-Stakeholder Expectations
-Constraints (e.g. legal, contractual)
-External Factors (e.g. competition, customer needs)
Input
Business Architecture for Cloud Ecosystems
Output (new/update)
-Product catalog
-Service Level Agreement(SLAs)
-Business Processes
-Organization Structure
-Business Support Service
-Operational Support Services
-Business Architecture

Figure 13: Business Architecture – An Enterprise Ecosystem Perspective

Organizations have to build consistent and integrated business capabilities portfolios that are internally developed or procured from external Cloud Service Providers. The key aspects of the Business Architecture for the Cloud Ecosystem are to not only describe business processes, actors, roles, and collaborations, but also to depict the coherent relationships between Cloud Services in respect to their deployment models. The business-focused approach of the TOGAF ADM will be used to ensure that the organization's business objectives of the Cloud Ecosystem support all stakeholders. A comprehensive Business Architecture not only provides and supports the recommended deliverables for the Business Architecture, but also specifies the extended business boundaries, roles, products, and services for the Cloud Ecosystem. The following recommended deliverables are to capture all relevant aspects of the Cloud Ecosystem:

- **Organization/Role/Location catalog**: Describes a definitive listing of all actors/participants that interact with the Cloud Ecosystem.
- **Organization Structure diagram**: Highlights the extended organizational boundaries.
- **Functional Decomposition diagram**: Describes business processes, Cloud Services functions, and their inter-relationships.
- **Business Footprint diagram**: Captures the relationships between business goals, functions, and how these functions map to services provided by the Cloud Ecosystem.

- **Information Flows** that capture the information needs within and between business processes and organizational elements.
- **Conceptual Information/Data model** that describes the high-level information elements (subjects, entities, attributes, and values) used by an enterprise.
- **Conceptual Metadata model** that describes the data needed to manage, use, and share the data.

The Business Architecture for CloudEcoSource describes the Cloud Services strategy with functional, information, and services deployment aspects to achieve the organization's required business agility. This will enable CloudEcoSource to execute evolving business needs at an acceptable cost, time, and quality with minimum risks. To sustain the business strategic objectives described above, initiatives need to be placed in the appropriate architectural context to develop a business portfolio that gets translated into concrete projects and criteria to measure success in executing those initiatives. One of the key deliverables in the Business Architecture is to ensure that business requirements effectively translate into the Target Business Architecture of CloudEcoSource.

In order to develop relevant architectural viewpoints to describe how stakeholder concerns are addressed, we will use value stream mapping and describe the relationships between the key business participants of CloudEcoSource. In addition, we should identify key business metrics to ensure the viability of cloud solutions. Once key participants for the Cloud Ecosystem are identified, a Functional Decomposition diagram and a Business Footprint diagram will be used to describe and capture their inter-relationships.

The rest of this section describes the steps taken in Phase B to achieve the overall goals of the architectural effort outlined for CloudEcoSource.

5.4.1 Select Reference Models, Viewpoints, and Tools

Use the Cloud Ecosystem Reference Model described in Chapter 3 as a foundation to determine viewpoints, to capture functional activities within CloudEcoSource. The Business Support Service and Operational Support Service viewpoints will demonstrate various stakeholder concerns and informational behaviors of the enterprise. Also, to measure the progress towards strategic objectives and to communicate that progress, Business Support Services will be associated with KPIs relative to the business functions of CloudEcoSource. These business functions are associated with standardized processes to translate business strategic objectives into operations. The service product catalog will manage required business building blocks and their relationships with external Cloud Service Providers.

The Functional Decomposition diagram will capture various business functional capabilities and their relationships. Also capturing reference models from external Cloud Service Providers will help to describe the impact on the organizational roles and responsibilities. Focus will not only identify and describe functional boundaries, but associated metrics for measurement.

5.4.2 Develop Baseline Business Architecture Description

Use the models identified in Section 5.4.1 as a guideline for creating new architecture content to describe the Baseline Architecture.

5.4.3 Develop Target Business Architecture Description

Where new architecture models need to be developed to satisfy stakeholder concerns, use the models identified in Section 5.4.1 and the Baseline Architecture created above as a guideline for creating new architecture content to describe the Target Architecture.

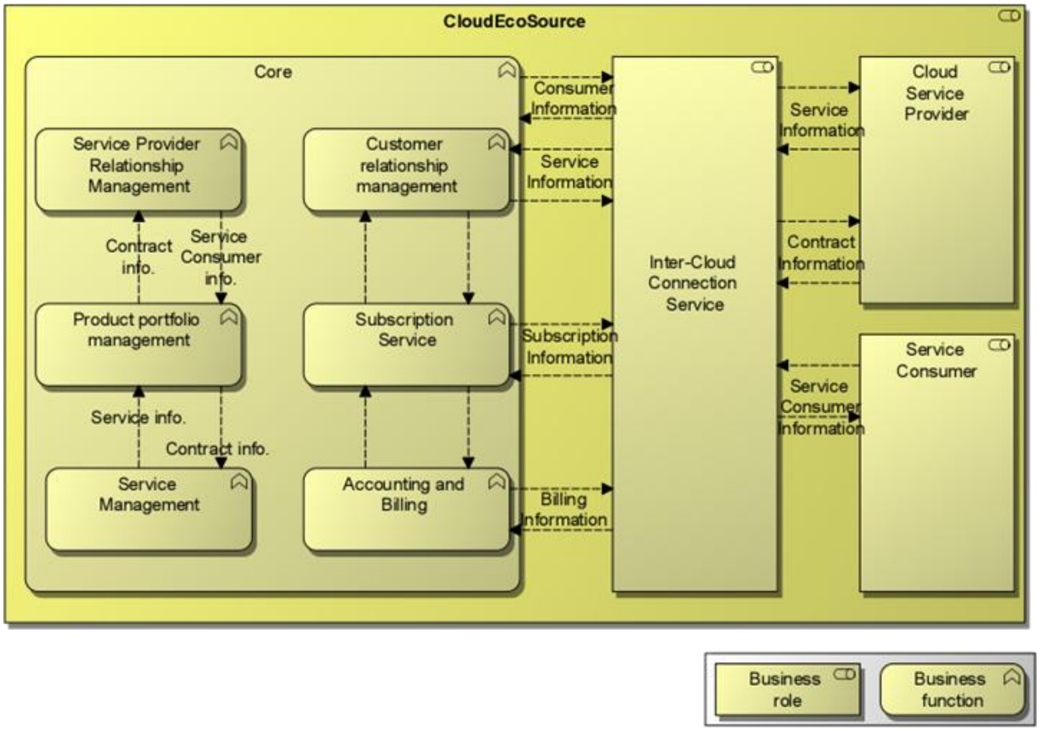

Figure 14: Business Communication of CloudEcoSource – An Illustration

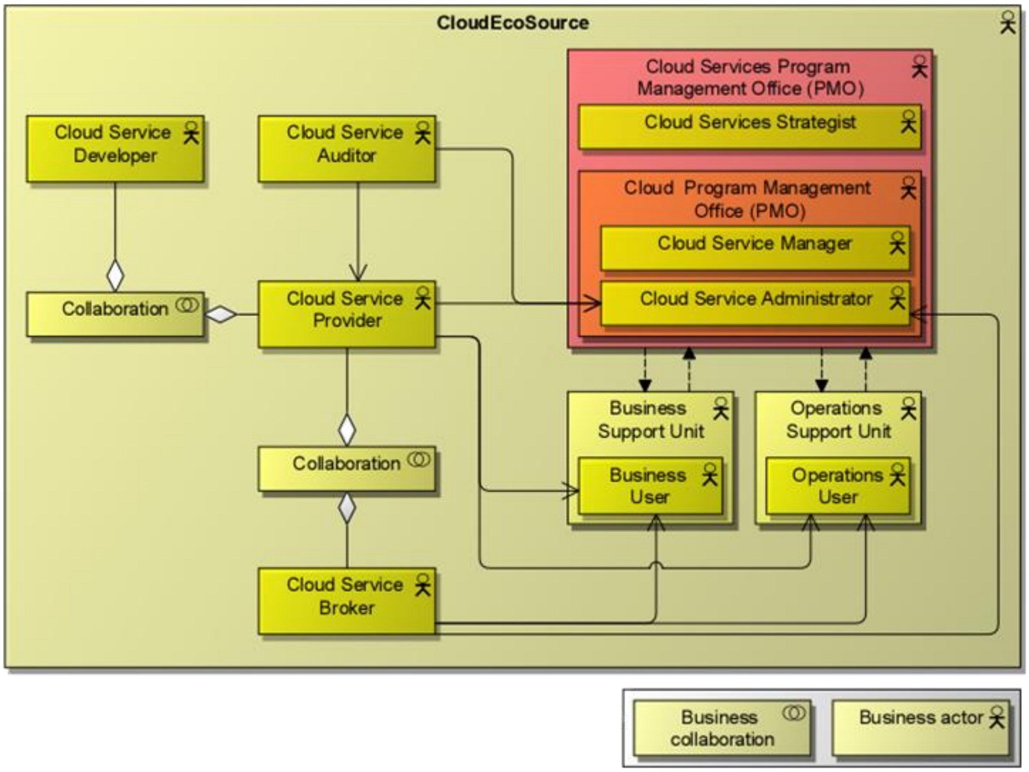

Figure 15: Actor Collaboration Diagram – An Illustration

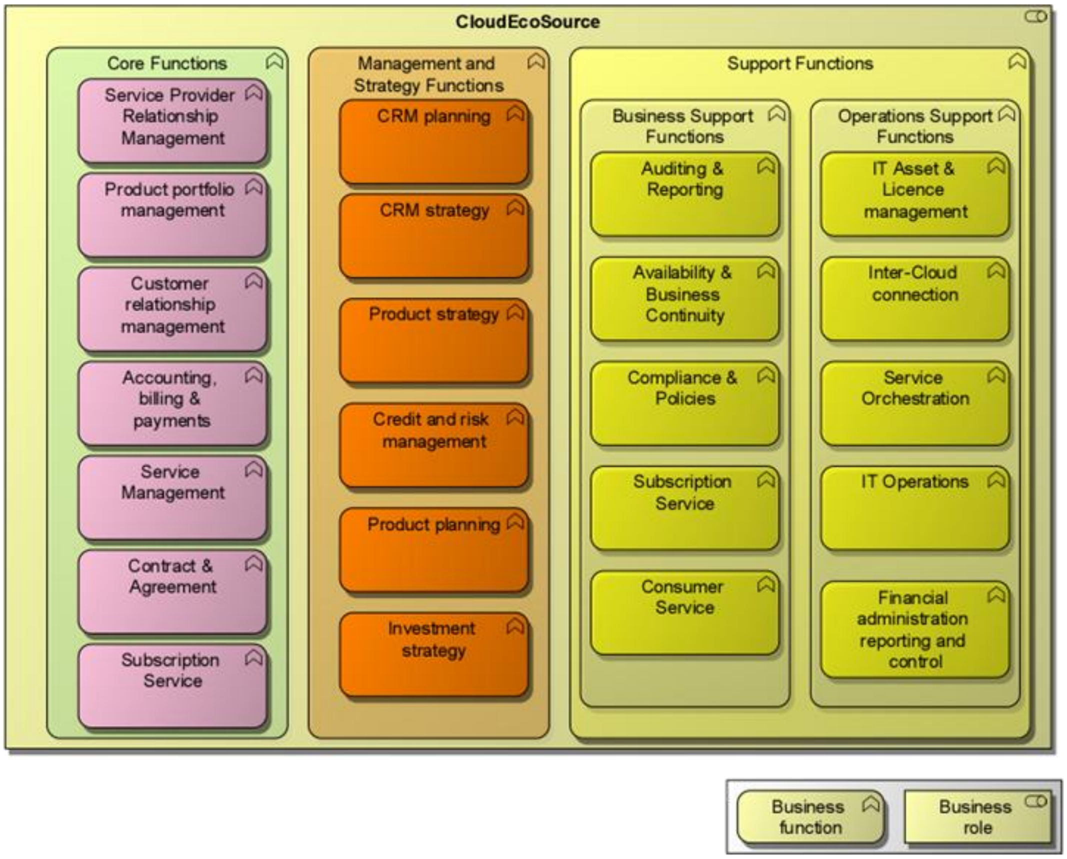
CloudEcoSource
Core Functions
Service Provider Relationship Management
Product portfolio management
Customer relationship management
Accounting, billing & payments
Service Management
Contract & Agreement
Subscription Service
Management and Strategy Functions
CRM planning
CRM strategy
Product strategy
Credit and risk management
Product planning
Investment strategy
Support Functions
Business Support Functions
Auditing & Reporting
Availability & Business Continuity
Compliance & Policies
Subscription Service
Consumer Service
Operations Support Functions
IT Asset & Licence management
Inter-Cloud connection
Service Orchestration
IT Operations
Financial administration reporting and control
Business function
Business role

Figure 16: Functional Decomposition Diagram – An Illustration

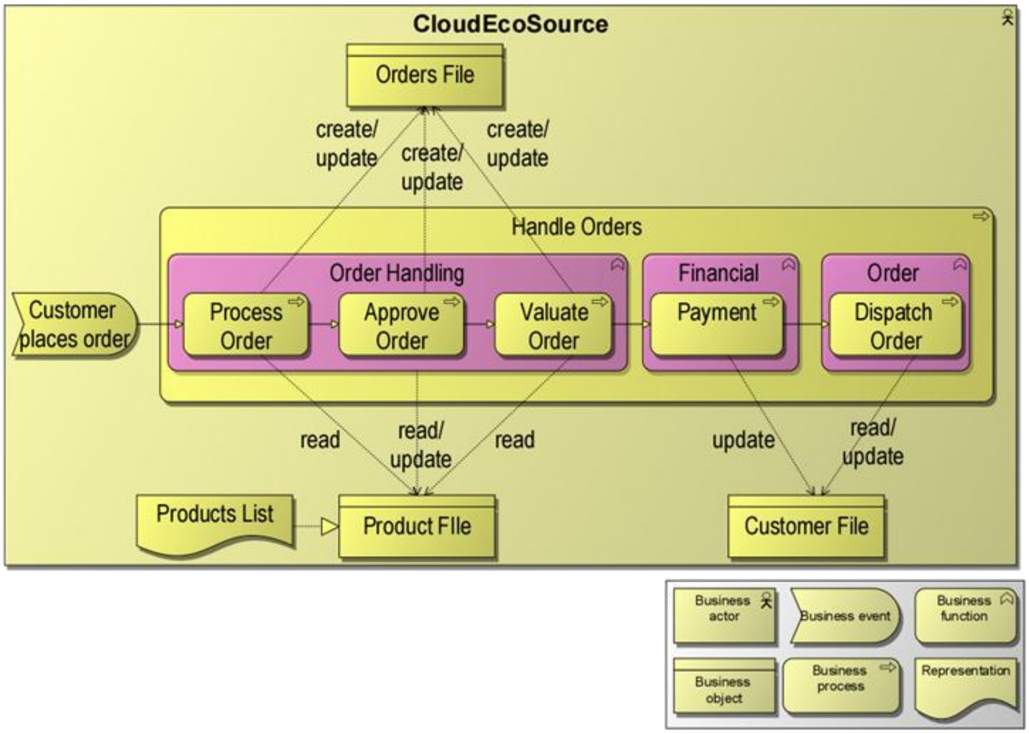

Figure 17: Business Functions/Processes Relationship – An Illustration

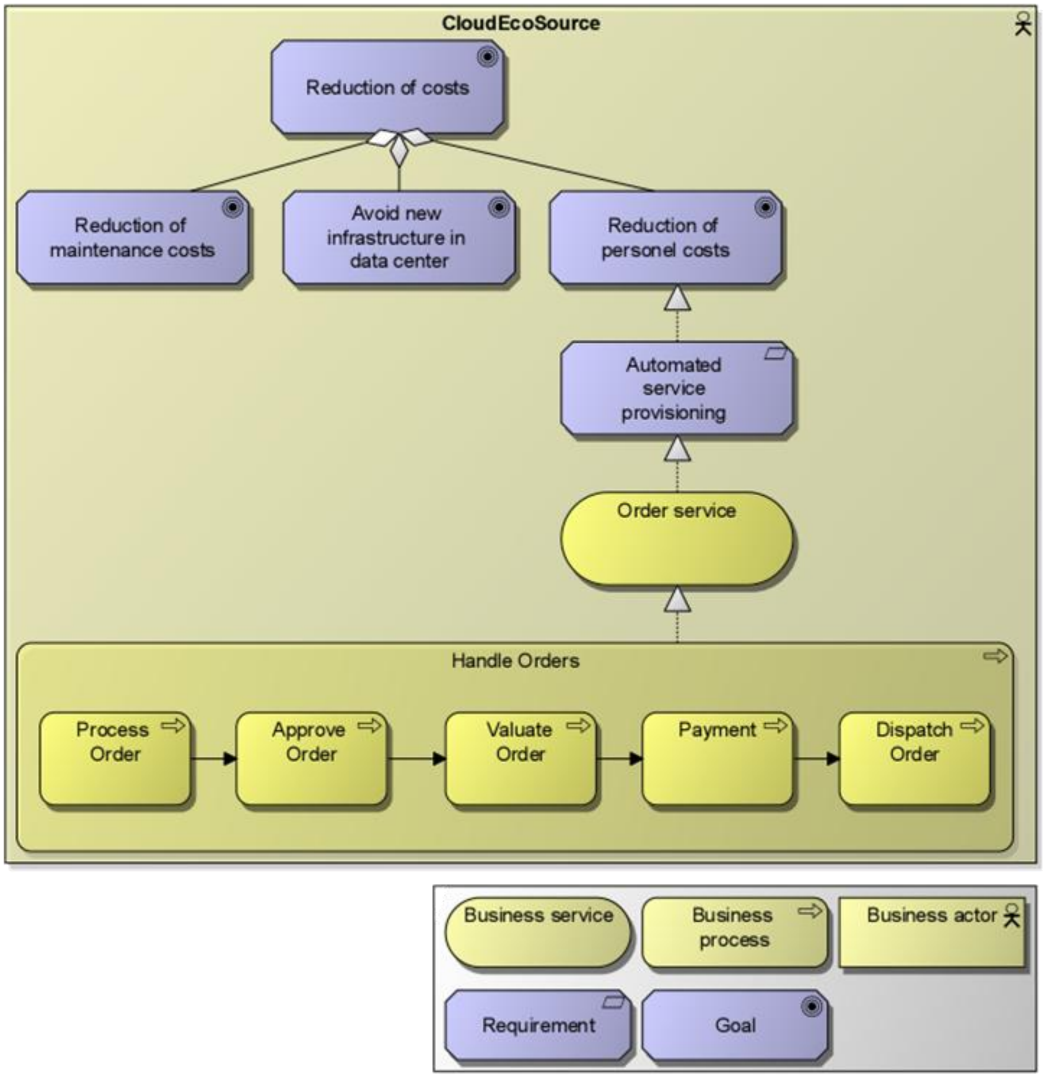

Figure 18: Requirements, Goals, and Process Relationship View – An Illustration

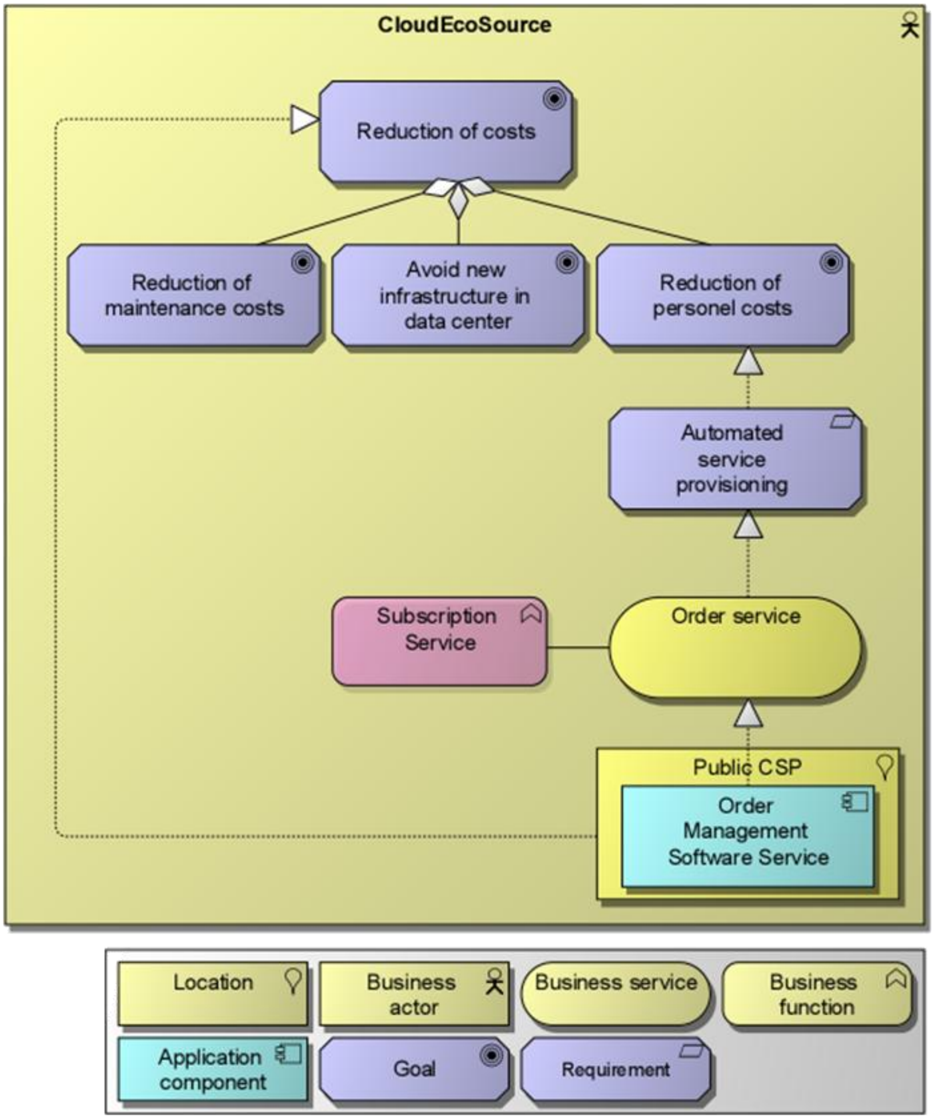

Figure 19: Business Footprint Diagram – An Illustration

5.4.4 Perform Gap Analysis

Verify the architecture models of CloudEcoSource and its Cloud Service Providers to ensure consistency and accuracy. Perform a trade-off analysis to resolve conflicts (if any) among the different views. Validate that the architecture and models support the principles, objectives, and constraints of the enterprise and test architecture models for completeness.

Identify gaps between the Baseline and Target Architecture.

CloudEcoSource has not performed Business Architecture work related to the Cloud Ecosystem earlier by engaging external Cloud Service Providers. Any new business processes or impact on existing business processes need to have the approval of key stakeholders. This includes training IT personnel to effectively manage Cloud Service Providers, and establishing a mechanism to determine which business functions and data are good candidates for public/private/hybrid clouds.

5.4.5 Define Candidate Roadmap Components

Following creation of a Baseline Architecture, a Target Architecture, and developing gap analysis results, a Business Roadmap is required to prioritize activities over the coming phases. CloudEcoSource has prioritized Cloud Services related to IaaS, PaaS, and SaaS services to ensure all stakeholder concerns are addressed. The initial Business Roadmap will be used as raw material to support cross-service models (i.e., IaaS, PaaS, and SaaS) roadmap within the Opportunities & Solutions phase.

5.4.6 Resolve Impacts Across the Architecture Landscape

Once the Business Architecture is finalized, it is necessary to understand any wider impacts or implications not only from existing internal architecture work, but services provided by Cloud Service Providers. Identify any services that could be leveraged from Cloud Service Providers in the CloudEcoSource Cloud Ecosystem. Envision the impact of Cloud Services provided by Cloud Service Providers and/or developed internally (both current and planned) on the Cloud Ecosystem.

Also, in order to effectively engage external Cloud Service Providers, CloudEcoSource must negotiate SLAs (e.g., price, liability, and service support and termination agreements) to ensure that its business and technical requirements and risks are fairly balanced with Cloud Service Providers.

5.4.7 Conduct Formal Stakeholder Review

Check the original motivation for the Cloud Ecosystem architecture and the Statement of Architecture Work against the proposed Business Architecture, asking if it is fit for the purpose of supporting subsequent work in the other architecture domains. Adjustments should be made in order to ensure that the proposed Business Architecture supports all stakeholder concerns.

5.4.8 Finalize the Business Architecture

Engaging Cloud System Providers in a Cloud Ecosystem will impact the working practices of an enterprise. CloudEcoSource will have to make adjustments to current practices, roles, and carefully analyze the impact of selected building blocks on the overall architecture of the Cloud Ecosystem. Re-using services in the form of building blocks as much as possible with captured rationale about decisions in the architecture documentation assists in architectural decisions in the future. All architectural decisions related to building blocks should be captured in the Architecture Repository along with clear traceability to business requirements. All gap analysis results and decisions to address those gaps should also be captured in the Architecture Repository.

5.4.9 Update Architecture Definition Document

In order to get a buy-in from all stakeholders, the Architecture Definition Document is updated. Prepare the business sections of the Architecture Definition Document providing a high-level description of the people and locations involved with key business functions and how a management footprint shall enforce standards, rules, and guidelines impacting the CloudEcoSource Cloud Ecosystem. The business section of the Architecture Definition Document also provides details on how relationships with Cloud Service Providers will have an impact on the skill matrix and working practices of CloudEcoSource.

5.5 Phase C: Information Systems Architecture

The objectives of Phase C of the TOGAF ADM are to develop Target Architectures for both the application and data (in either order) of an architecture project. This section describes the Data Architecture for a Cloud Ecosystem.

The Data Architecture requires a comprehensive assessment of an enterprise's information and underlying data. This phase will extend the conceptual work completed in the earlier phases of the ADM. A structured and comprehensive approach to enterprise information/data management enables the effective use of data to capitalize on its competitive advantages.

The enterprise information model for a Cloud Ecosystem will facilitate a common understanding of the corporate structured and unstructured data and will serve as a basis for the Target Data Architecture. The model facilitates unified access across all types of enterprise data, consistently applies applicable business rules, and accelerates Cloud Services development. Data quality should be well defined and captured in the metadata for all data assets of an enterprise (refer to The Open Group White Paper: An Information Architecture Vision). These metadata attributes will dictate what technology constraints (e.g., caching, partitioning, and failover), service qualities (e.g., availability, performance, scalability), and service delivery concepts (e.g., DaaS) will be used within an enterprise Cloud Ecosystem. Data quality also drives the service levels requirements of Cloud Services.

The information security service ABB defines and manages the requisite security classifications, compartments, and legislative constraints on the use of the information within an enterprise Cloud Ecosystem. It is also critical to use the metadata to define access policies to support granular data access for individual, role-based, and governance-based security access controls.

Where applicable, architecture practitioners should consider including the following in order to complete the Data Architecture for an enterprise Cloud Ecosystem:

- Practitioners should identify data migration to cloud requirements, with governance for data quality, and to ensure that an enterprise-wide common data definition is established by defining a system of records for enterprise data.

- Architecting data for cloud also utilizes various data caching techniques aimed at improving data availability, performance, and scalability. The Cloud Ecosystem requires that cloud solutions are tolerant of network failures and data consistency. The Data Architecture might need to accommodate new assumptions that data consistency is generally sacrificed over data availability and requires an enabling mechanism (e.g., data partitioning) to relay/expose consistent data via cloud solutions.

- The Data Architecture for CloudEcoSource describes the Cloud Services strategy to address the distributed nature of CloudEcoSource data resources. The architecture provides a flexible data integration mechanism and ensures that data in the cloud is appropriately shared and maintained.

- Address big data and social networking data by utilizing semantic techniques to convey the intent of data during information exchange. This requires the treatment of data as information assets associated with appropriate categorization, quality, and their potential use in the Cloud Ecosystem. Within an enterprise Cloud Ecosystem, data categorization integrates disparate data to serve as common business objectives and make them securely available as information assets rapidly and efficiently.

The rest of this section describes the steps taken in Phase C to achieve the overall goals of the architectural effort outlined for CloudEcoSource.

5.5.1 Select Reference Models, Viewpoints, and Tools

Use the enterprise Cloud Ecosystem Reference Model described in Chapter 3 as a foundation to determine viewpoints to address various stakeholder concerns and to capture functional activities within CloudEcoSource. The Cloud Ecosystem requires addressing various regulatory, auditing, and compliance business requirements and selecting relevant Data Architecture viewpoints that will enable the architect to demonstrate how the stakeholder concerns are being addressed in the Data Architecture.

Determine appropriate tools, techniques, and modeling processes to create and manage data views to address all stakeholder concerns. Leveraging Cloud Services from heterogeneous Cloud Service Providers requires a consolidated view of the semantically consistent data inventory to reduce any possible overlaps and identify gaps in data relationships. Elaborated views to address all stakeholder concerns help achieve business objectives. The data used within and across the business processes of CloudEcoSource must be cataloged as the basis for further documentation. This catalog includes both structured data and unstructured content. Using conceptual data models to document data taxonomies will create consistent views and describe how data is created, distributed, migrated, secured, and archived in the CloudEcoSource Cloud Ecosystem.

5.5.2 Develop Baseline Data Architecture Description

In order to develop the Target Data Architecture of CloudEcoSource, and assess the current state, develop cross-reference information entities in the Baseline Data Architecture to promote consistency, re-use, and avoid redundancy. The Baseline Architecture can use existing data models to understand existing data sources and then add any needed extensions for cloud into the baseline models. Otherwise, use the guidelines identified in Section 5.5.1 for creating a new Baseline Data Architecture that clearly identifies a system of records and Data Architecture building blocks that enable secure sharing of information on the cloud.

5.5.3 Develop Target Data Architecture Description

Sharing data in a cloud is considered a paradigm shift and the Target Data Architecture should address the structural and operational changes for the Cloud Ecosystem.

Develop a target description for the Data Architecture, to the extent necessary to support the Architecture Vision and Target Business Architecture. Ensure that non-functional data requirements are incorporated in the Target Data Architecture and translated into SLAs. For example, some critical non-functional requirements in the cloud are:

- Data security measuring criteria (e.g., privacy, confidentiality, data obfuscation, etc.)

- Data availability and tolerance threshold on data loss
- Data reliability
- Volume of data

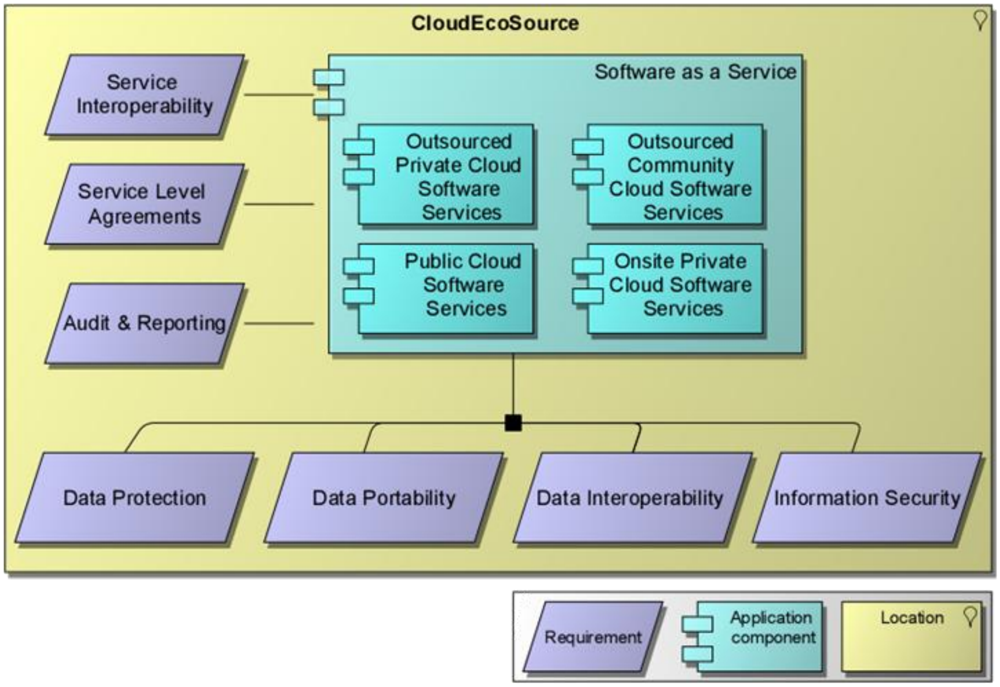

Figure 20: SaaS and Data Requirements – An Illustration

Where new architecture models need to be developed to satisfy stakeholder concerns, use the models identified within Section 5.5.1 as a guideline for creating new architecture content to describe the Target Architecture.

5.5.4 Perform Gap Analysis

The purpose of gap analysis is to attain business and IT objectives and validate that architecture models support established principles and guidelines to support expected data consistency and accuracy. If required, develop several alternatives, with analysis of the work and trade-offs associated with each alternative to achieve the stakeholder objectives. Also provide a mechanism to address any implications of closing the identified Data Architecture-related gaps in the current organizational context to effectively achieve the Target Data Architecture. Ensure that there are effective data governance policies and that compliance procedures are established for the CloudEcoSource Cloud Ecosystem.

5.5.5 Define Candidate Roadmap Components

Define the Data Architecture Roadmap based on the Baseline and Target Architecture gaps in order to prioritize other architectural activities. The defined candidate roadmap will also be utilized in the Opportunities & Solutions phase to create a consolidated/integrated Architecture Roadmap for the CloudEcoSource Cloud Ecosystem.

5.5.6 Resolve Impacts Across the Architecture Landscape

It is necessary to resolve the impact of the cloud Data Architecture on architectures of the CloudEcoSource Cloud Ecosystem. The Cloud Ecosystem provides an efficient underlying mechanism for the delivery of on-demand compute capacity. The infrastructure services are highly variable in nature (i.e., elastic) and the Data Architecture must assume and plan for the inconsistent failure of any component (i.e., infrastructure, platform, software components) in order to provide efficient and effective mechanisms for the business solutions of the Cloud Ecosystem.

An additional challenge is the need to integrate data with various cloud deployment scenarios of the CloudEcoSource Cloud Ecosystem. Some capabilities to address these are provided at SaaS and PaaS level and will have impact not only on the Data Architecture but on the entire architecture landscape of CloudEcoSource.

5.5.7 Conduct Formal Stakeholder Review

Check the original motivation for the Cloud Ecosystem architecture and the Statement of Architecture Work against the proposed Data Architecture. Determine whether it is fit for the purpose of supporting subsequent work in the other architecture domains. Adjustments to architectures should be made in order to ensure that the proposed Data Architecture supports all stakeholder concerns. Identify any impact or constraint on the Application and Technology Architecture of the CloudEcoSource Cloud Ecosystem.

5.5.8 Finalize the Data Architecture

Finalize all work on the Data Architecture and conduct a final check to ensure that all stakeholder concerns are addressed. Ensure that the ABBs of the Data Architecture support the business requirements and don't impact adversely on the CloudEcoSource Cloud Ecosystem.

5.5.9 Create Architecture Definition Document

Create Data Architecture sections of the Architecture Definition Document describing data logical models. Highlight how the Data Architecture addresses any data interoperability and data security requirement with rationale for building block decisions in the Architecture Definition Document. Route the document for review by relevant stakeholders, and incorporate feedback.

5.6 Phase D: Technology Architecture

In order to realize a Technology Architecture that provides a flexible and adaptable technology infrastructure for the Cloud Ecosystem, enterprises will have to carefully align short-term and long-term business objectives with a modular set of technology services to support information systems services. By incorporating the concerns of the stakeholders, these technology services enable the functioning of explicit and comprehensive capabilities that address the identified technical services gaps in the enterprise Cloud Ecosystem. New technical services and their underlying technology building blocks need to be defined and detailed to ensure that all applicable technical considerations (some of them are outlined in Section 4.6) are considered and incorporated into the Technology Architecture. To determine whether these capabilities are to be built within the enterprise or utilize Cloud Service Provider services, trade-off analyses need to be performed to identify, evaluate, and address the impact on the Cloud Ecosystem of any new technology services introduced/modified/eliminated. Required architectural viewpoints should be created to demonstrate how stakeholder concerns relating to technology are addressed.

Architecture practitioners should consider including the following as part of the activities/deliverables for both the Baseline and Target Technology Architecture in order to complete Phase D:

- Determine the overall Technology Architecture approach and determine any cloud-specific technology resources required (e.g., matrices, diagrams, patterns, etc.) for the Cloud Ecosystem. For example, it would be beneficial to have cloud product/technology metrics to highlight relationships that could be used for technology assessment.
- Technology capabilities and their decomposition showing the technology required for the Cloud Ecosystem in order to realize a particular Cloud Service (i.e., IaaS, PaaS, and SaaS). The technology deployment model (e.g., on-site/outsourced) will have implications on supporting expected non-functional requirements that are generally described and measured by SLAs of the Cloud Ecosystem. SLAs define measurements for services performance, availability, maintainability, and supportability aspects of Cloud Services. Also, services in the Cloud Ecosystem may have impact when inter-service communications over various network boundaries are utilized.
- Architectural capabilities to support essential cloud characteristics (e.g., resource pooling, rapid elasticity, measured services, etc.) and handle their impact on the architecture by providing technology management capabilities that allow self-service administration within a context of participants (e.g., consumers or providers) of the enterprise Cloud Ecosystem.
- Interactions of technology capabilities and their relationships to information systems ABBs of the enterprise Cloud Ecosystem.
- Applicable view of environments (e.g., development, test, rroduction) outlining physical deployment locations (public/private/hybrid/community) in the context of the enterprise Cloud Ecosystem. These technology views describe interactions of architectural capabilities and relationships to enable multi-tenant environments.
- Security: The Technology Architecture must include applicable security implications for utilizing Cloud Service Providers in the enterprise Cloud Ecosystem. This includes different levels of security controls that are required to support variations of cloud deployment models and impact on the workload processing and network/communications capabilities of the enterprise Cloud Ecosystem.
- Portability and Interoperability: The Technology Architecture must enable mechanisms to support data portability and service interoperability in order to effectively communicate between multiple cloud environments with minimum impact to the service availability of the Cloud Ecosystem. Standardized information exchange mechanisms will effectively allow Cloud Service Consumers to utilize multiple Cloud Service Providers and the efficient migration of data and services of the Cloud Ecosystem when required.

The Technology Architecture of the Cloud Ecosystem describes the technology services strategy to address the Cloud Ecosystem’s technical services requirements. The architecture realizes both the logical and physical technical aspects of the infrastructure, platform, and software services capabilities of the Cloud Ecosystem in order to support business objectives. The architecture will provide guidance in establishing ideal SBBs of the Cloud Ecosystem in the later phases of the ADM. Understanding the existing Technology Architecture and assessment of its features and functionality will identify technology gaps.

The Technology Architecture for the Cloud Ecosystem will enable comprehensive technical services for the Cloud Ecosystem where each tenant has mechanisms to effectively control demand and manage the life cycle of services.

The rest of this section describes the steps taken in Phase D to achieve the overall goals of the architectural effort outlined for CloudEcoSource.

5.6.1 Select Reference Models, Viewpoints, and Tools

Review and validate the set of Technology Principles. These will normally form part of an overarching set of Architecture Principles with alignment to the enterprise principles that include Cloud Ecosystem principles as described in the Preliminary Phase (see Section 5.2.1). Guidelines for developing and applying Technology Principles are established that promote ubiquitous access and self-service administration of technology services. This will ensure that all essential characteristics necessary for the Cloud Ecosystem are supported in the technology services.

Select relevant Technology Architecture resources (reference models, viewpoints, matrices, diagrams, patterns, etc.) from the Architecture Repository, on the basis of the business drivers, stakeholders, and their concerns.

Identify requirements for appropriate tools and techniques to be used to support the infrastructure, platform, and software services of the Cloud Ecosystem. These technical requirements will set the foundations for viewpoints required for the Cloud Ecosystem and to demonstrate how the stakeholder concerns are being addressed in the Technology Architecture. For example, the Technology Architecture will have to support viewpoints to demonstrate essential cloud capabilities for:

- Real-time allocation of computing resources to Cloud Services in order to provide required elasticity and scalability capabilities
- Automatically adjust computing resources between various Cloud Services instances and processing requirements in order to achieve targeted performance measurements
- Tenant-based resources usage tracking and billing based on Cloud Services consumption
- Technical capabilities to securely interoperate and port workloads of the Cloud Ecosystem

5.6.2 Develop Baseline Technology Architecture Description

In order to support the Target Technology Architecture and to address stakeholder concerns, a baseline description of the existing technology capabilities will have to be assessed through developing the Baseline Technology Architecture. The scope and level of detail to be defined will depend on the extent to which existing technology components are likely to be carried over into the Target Technology Architecture, and on whether architectural descriptions exist.

Identify the relevant Technology Architecture building blocks and existing cloud-enabled technology services. Evaluate associated assumptions about security and interoperability, by drawing on any artifacts held in the Architecture Repository. If nothing exists within the Architecture Repository, define technology capabilities for each application in line with the product catalog and associated entry in the Technology Portfolio catalog. The Technology Portfolio catalog maintains a list of all technology services and associated information of the Cloud Ecosystem.

5.6.3 Develop Target Technology Architecture Description

Develop a target description for the Technology Architecture to support the Architecture Vision and how the Technology Architecture will address stakeholder concerns. Describe the value of Cloud Services to stakeholders (e.g., consumers and external parties involved) by showing the technology composition of each Cloud Service and associated contract(s) and agreement(s). The scope and level of details will depend on the use of existing Cloud Services and if relevant architectural descriptions exist in the Architecture Repository.

The Technology Architecture practitioners may add additional technology requirements to address the architectural needs identified in earlier phases in order to describe a broad and comprehensive Target Architecture for the Cloud Ecosystem.

The Target Technology Architecture of CloudEcoSource describes how software, platform, and infrastructure services are used to support cloud business solution requirements, their usage, and relationships. This provides an overall perspective on technical dependencies to enable an effective Cloud Ecosystem. The architecture describes SLAs that measure the effectiveness of the overall Cloud Ecosystem architecture, evaluates compliance with business policies, and enables practitioners to select the right ABBs by conducting a quick trade-off/fit-for-purpose analysis. The CloudEcoSource architects decided to use all available Cloud Service models to deliver their Cloud Services. The following view of the Target Technology Architecture highlights the seamless use of Cloud Services provided by Cloud Service Providers (depicted with CSP-*) and their use to deploy cloud solutions on the CloudEcoSource Cloud Ecosystem:

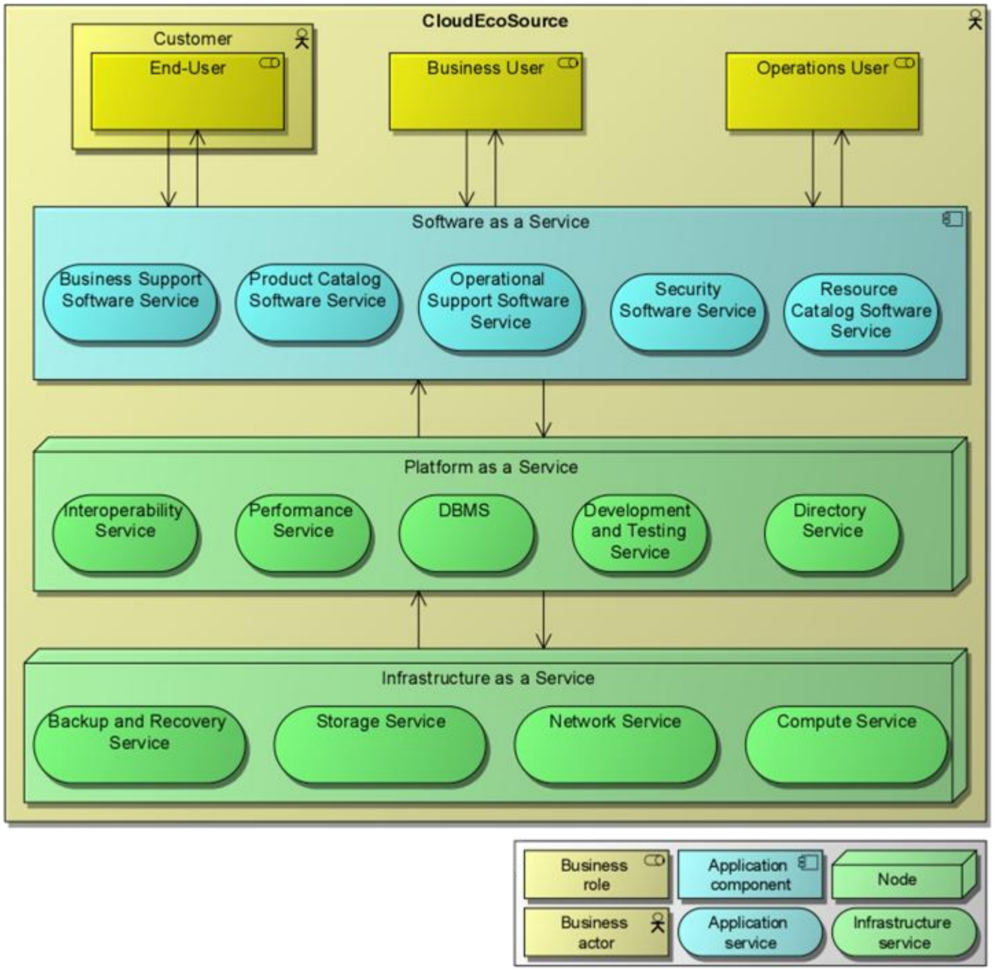

Figure 21: Technology Architecture Viewpoint of CloudEcoSource – An Illustration

5.6.4 Perform Gap Analysis

The purpose of gap analysis is to attain the business and IT objectives of the Cloud Ecosystem and validate that architecture models support established principles and guidelines to support the expected technology consistency and accuracy. If required, develop several alternatives, with analysis of the work and trade-offs associated with each alternative to achieve stakeholder objectives. Also provide a mechanism to address any implications of closing the identified Technology Architecture-related gaps in the current organizational context to effectively achieve the Target Technology Architecture. Ensure that there are effective data governance policies and compliance procedures established for the CloudEcoSource Cloud Ecosystem.

5.6.5 Define Candidate Roadmap Components

Define the Technology Architecture Roadmap based on the gap analysis in order to prioritize other architectural activities. The defined candidate roadmap will also be utilized in the Opportunities & Solutions phase to create a consolidated/integrated Architecture Roadmap for the CloudEcoSource Cloud Ecosystem.

5.6.6 Resolve Impacts Across the Architecture Landscape

It is necessary to resolve any impact of the Cloud Technology Architecture on architectures of the Cloud Ecosystem. The Cloud Ecosystem Technology Architecture capabilities shall enable an efficient underlying mechanism to deliver on-demand Cloud Services. Analyze the artifacts to identify:

- Does this Technology Architecture create an impact on any pre-existing architectures and are associated assumptions still valid for the Cloud Ecosystem?
- Have recent changes been made that impact the Technology Architecture of the Cloud Ecosystem? The changes may include any outsourced/built-in Cloud Services, impact of new applicable business policies, and technology advancements.
- Identify any opportunities to standardize technology of the Cloud Ecosystem and analyze the impact to stakeholders.

5.6.7 Conduct Formal Stakeholder Review

Check the original motivation for the Cloud Ecosystem architecture and the Statement of Architecture Work against the proposed Technology Architecture. Determine whether it is fit-for-purpose. Adjustments to architectures should be made in order to ensure that the proposed Technology Architecture supports all stakeholder concerns. Identify any impact or constraint on the Application and Data Architecture of the CloudEcoSource Cloud Ecosystem and refine the proposed Technology Architecture if necessary.

5.6.8 Finalize the Technology Architecture

Finalize all work on the Technology Architecture and conduct a final check to ensure that all stakeholder concerns are addressed. Ensure that ABBs of the Technology Architecture support the business requirements, consistent with the defined business policies, and don’t impact adversely the functional effectiveness of the CloudEcoSource Cloud Ecosystem.

5.6.9 Create Architecture Definition Document

Create the Technology Architecture sections of the Architecture Definition Document describing technology logical models. Highlight how the Technology Architecture addresses the business requirements and policies with rationale for building block decisions in the Architecture Definition Document. Route the document for review by relevant stakeholders, and incorporate received feedback to determine whether review of the document is once again required.

5.7 Phase E: Opportunities and Solutions

Phase E concentrates on how to deliver the architecture. It takes into account the complete set of gaps between the Target and Baseline Architectures in all architecture domains, and logically groups changes into work packages within the enterprise’s portfolios. This is an effort to build a best-fit roadmap that is based upon the stakeholder requirements, the enterprise’s business transformation readiness, identified opportunities and solutions, and identified implementation constraints. The key is to focus on the final target while realizing incremental business value.

The emphasis of Phase E is on the approach to deliver the Target Architecture and starts the transformation of the ABBs from Phases B to D into SBBs. The Cloud Ecosystem architecture implementation considers the different types of cloud deployment model in addition to the on-premises extension to the Cloud Ecosystem. It may also consider new implementation(s) on the Cloud Ecosystem.

The project life cycle in the Cloud Ecosystem is drastically reduced due to the cloud computing capability of services that can be rapidly assembled through IaaS, PaaS, and SaaS. Phase E identifies the process to deliver the Target Architecture through projects, programs, or portfolios.

The traditional gap analysis between the current ABB and target ABB is not directly relevant since it is an infrastructure replacement. In the Cloud Ecosystem the Target Architecture consists of services of ABBs.

From the Architecture Vision phase it is essential to define the Target Architecture in terms of services components. Overall Phase E output will be candidate work packages, which would become Architecture Roadmap components and incremental delivery though the Transition Architecture through Phase F.

Phase E considers architecture reference materials of the Cloud Ecosystem. The Cloud Ecosystem needs to be monitored as it evolves with new standards and new capabilities of Cloud Services that are offered by the vendors on a regular basis.

At this juncture the implementation issues such as financial, technical, and contractual need to be considered.

The implementation model and type depends on some of the following considerations:

- Time to market
- Legacy applications dependency and phasing out
- Cost *versus* risk
- Capability of the organization
- Cloud readiness

The objectives of Phase E are to review the target business objectives and capabilities, consolidate the gaps from Phases B to D, and then organize groups of building blocks to address these capabilities. Additional tasks may include:

- Confirm the enterprise's capability for undergoing change
- Derive a series of Transition Architectures that deliver continuous business value through the exploitation of opportunities to realize the building blocks
- Generate and gain consensus on an outline Implementation and Migration Strategy

The rest of this section describes the steps taken in Phase E to achieve the overall goals of the architectural effort outlined for CloudEcoSource.

5.7.1 Determine/Confirm Key Corporate Change Attributes

The main objective of this step is to analyze the business culture, abilities, and skill sets for effective implementation of the Enterprise Architecture. An enterprise adoption of the Cloud Ecosystem brings its own advantages and challenges. The key advantage is the rapid assembly of applications services. Also, the services may be consumed based on pay per usage, reducing capital expenditures.

The challenges are to build confidence about the new deployment model that is not located on the premises.

Creation of an Implementation Factor Assessment and Deduction matrix serves as a repository for helping make architecture implementation migration decisions. The step also includes assessments of the transition capabilities of the organizations involved considering the culture and abilities (to adopt emerging technology). It also provides for assessments of the enterprise and IT organization skill sets (cloud computing).

Table 11: Implementation Factor Assessment and Deduction Matrix – An Illustration

Factor	Description	Deduction
Change in application implementation	Application implementation on cloud rather than on-premises	• Business to be aware of the new model • Compliance/governance to be modified for moving business services to the cloud • Essential skills training
SaaS to address business need	Business application assembled from SaaS to fulfil business requirements	• Capability to provide identity management, access control, and customize services • Business units deploying their own applications due to low cost and ease of deployment thereby introducing security holes
Scalability and elasticity	Applications able to scale and shrink as per the demand	• Skills to design applications to take advantage of scalability on-demand
Application integration	Integration of application services on the cloud and on-premises	• Skills to do integration with on-premises and legacy enterprise applications with the cloud
Enterprise data segregated into cloud silos	Each SaaS utilized creates its own data	• Integration challenges • Extract transform load data from various services • Data integration and replication solutions
Business functions and data	Traditional business functions and data reside locally on premises	• Establish a mechanism to determine the business functions and data that can be hosted in public/private/hybrid

5.7.2 Determine Business Constraints for Implementation

The business drivers that triggered the adoption of the enterprise-based on the Cloud Ecosystem need be reviewed. The initial factors to consider may be a business-driven adoption of technology to reduce cost, automate processes, shorten time-to-market, improve competitiveness, etc.

IT systems in large enterprises may have evolved over the last two or three decades. A revisit of Phases B to D may be required, as there may be other services and the need to convert manual processes to automated processes.

Educating the business users to use business process management tools gives more control to the business users to manage the business with less dependency on IT. There may be also constraints such as time-to-market, cost, skills, etc.

The Enterprise Architecture maturity assessment is reviewed, to identify whether they are able to meet the targeted maturity.

5.7.3 Review and Consolidate Gap Analysis Results from Phases B to D

An enterprise adopting the Cloud Ecosystem brings its own challenges due to the business services consumed from different vendors. The gaps identified in Phases B to D need to be assessed and analyzed for potential implications due to the change in application deployment model from package/bespoke solution to a Cloud Services model.

Consideration must be given to the dependencies of applications in the Cloud Ecosystem as they span across the on-premises deployment model and cloud deployment model. Also there may be inter-dependencies with Cloud Services consumed from different Cloud Service Providers.

Table 12: Consolidated Gaps, Solutions, and Dependencies Matrix of CloudEcoSource – An Illustration

Architecture	Gap	Potential Solutions	Dependencies
Business	Organization has not performed Business Architecture work related to the Cloud Ecosystem earlier by engaging external Cloud Service Providers.	New business processes or impact on existing business processes need to have key stakeholders' approval.	
Business	Business Agility	Business process assembled through services.	Existing business process integration
Data	Data consistency and accuracy implications of data in different SaaS/PaaS providers.	Ensure that there are effective data governance policies and the compliance procedures are established for the CloudEcoSource Cloud Ecosystem.	

Architecture	Gap	Potential Solutions	Dependencies
Technology	To support expected technology consistency and accuracy.	To have an effective technology stack validation and selection process.	

5.7.4 Review Consolidated Requirements across Related Business Functions

To assess the requirements, gaps, solutions, and factors to identify a minimal set of requirements whose integration into work packages would lead to a more efficient and effective implementation of the Target Architecture.

To identify the shared services that can be utilized across the enterprise through provision of shared resources.

5.7.5 Consolidate and Reconcile Interoperability Requirements

In the Cloud Ecosystem, interoperability requirements are a critical success factor, as business services are provided by one or more Cloud Service Provider.

Based on the solution, the services can be consumed either from an information system deployed on a PaaS or business services from a SaaS. The interoperability between PaaS and SaaS needs to be considered. See The Open Group Guide: Cloud Computing Portability and Interoperability for detailed information.

In addition to interoperability, the APIs provided by the cloud vendors need consideration as potential factors accounting for services consumption and future extension.

5.7.6 Refine and Validate Dependencies

Dependencies are identified. These provide constraints in determining the sequencing of the Implementation and Migration Plan. The key dependencies usually are existing implementations of business services and information systems or changes to them. In the Cloud Ecosystem it is very important to understand the dependencies as the implementation duration is greatly reduced due to rapid infrastructure provisioning and business service availability with SaaS.

Dependencies assist in sequencing the efforts required, grouping the related projects, identifying milestones and logical/actual delivery points, and in planning the project duration.

Determining the dependencies becomes a critical key factor for migration planning in the Cloud Ecosystem, especially as more vendors are involved.

5.7.7 Confirm Readiness and Risk for Business Transformation

The Business Transformation Readiness Assessment previously conducted in Phase A is reviewed to determine its impact on the Architecture Roadmap and the Implementation and Migration Strategy.

Risks associated with transformation are identified, classified, and mitigation planned and documented as Cloud Ecosystem risks are very different from traditional on-premises technology projects risks.

The Architecture Roadmap, focused on the cloud deployment model, has the capability of rapid provisioning of the services. The solutions are to be thoroughly analyzed to find the dependencies between the services.

5.7.8 Formulate Implementation and Migration Strategy

The overall strategic implementation direction that guides the Transition Architecture(s) are considered based on:

- **Greenfield**: A completely new implementation of the Cloud Ecosystem.
- **Revolutionary**: A radical change moving the on-premises deployment model to the Cloud Ecosystem.
- **Evolutionary**: A strategy of convergence, such as parallel running or a phased approach to introduce new capabilities such as a hybrid model of extending the on-premises capability with the Cloud Ecosystem.

5.7.9 Identify and Group Major Work Packages

Key stakeholders, planners, and the Enterprise Architects need to assess the missing business capabilities identified in the Architecture Vision and Target Architecture gap analyses.

In the Cloud Ecosystem the information system will be moved from on-premises to the cloud based on the Migration Strategy as Greenfield, Revolutionary, or Evolutionary. Group the work packages to suit the Migration Strategy.

5.7.10 Identify Transition Architectures

Where the scope of change to implement the Target Architecture requires an incremental approach, then one or more Transition Architectures may be necessary.

In the Cloud Ecosystem the type of services based on IaaS, PaaS, or SaaS will determine the number, type, and duration of Transition Architectures. Also the Migration Strategy as Greenfield, Revolutionary, or Evolutionary becomes a determining factor.

5.7.11 Create the Architecture Roadmap & Implementation and Migration Plan

The Architecture Roadmap is consolidated from the work packages and Transition Architecture that describes the timeline of the progression from the Baseline Architecture to the Target Architecture. The identified Transition Architectures and work packages should have a clear set of outcomes.

To create a roadmap for delivery of services based on cloud solutions:

- Revisit the initial implementation planning.

- Identify the major implementation projects that can be implemented on the Cloud Ecosystem.
- Decide on approach:
  - Make *versus* buy *versus* re-use through services and shared services
  - COTS services for cloud and on-premise application
- Assess priorities of business services that can be migrated to the Cloud Ecosystem based on business readiness and business user acceptance.
- Identify dependencies of services within services between cloud and on-premises.
- Develop an impact analysis on the existing IT systems.
- Group projects into Transition Architectures.

The Implementation and Migration Plan demonstrates the activity necessary to realize the Architecture Roadmap based on the Cloud Ecosystem. The projects and resource requirements consider the Cloud Ecosystem in addition to the on-premises application. The application implementation needs to consider the priority of the services based on the business requirement identified earlier.

Finally, update the Architecture Vision, Architecture Definition Document, and Architecture Requirements Specification with any additional relevant outcomes from this phase.

5.8 Phase F: Migration Planning

Migration Planning assumes a very important role in successful cloud adoption. The migration projects will have to be sorted according to the Cloud Vision of the organization, the Cloud Transformation Roadmap, the benefits to the organization, the mutual dependencies among projects, and, finally, the financial feasibility.

The Cloud Vision of the organization should be analyzed and the drivers for the projects to move to the cloud should be understood. The key business drivers could be:

- Providing agility
- Making the organization future-ready
- Cost optimization by bringing elasticity in the solution
- Exposing a re-usable solution to a wider audience

The rest of this section describes the steps taken in Phase F to achieve the overall goals of the architectural effort outlined for CloudEcoSource. Each of the steps below is taken in cooperation with the appropriate project/program office.

5.8.1 Prioritize and Create a Migration Roadmap

Prioritize the cloud migration projects by assessing the migration benefits, project internal upgrade plans, mutual dependencies among projects, and financial feasibility. Create a Cloud Migration Roadmap based on the priority determined above. Derive a migration schedule based on the roadmap and individual project timelines and distinct milestones.

5.8.2 Determine Resource Requirement and Cloud Infrastructure Provider

Determine the resources required for each of the projects. Determine the SLAs and elasticity requirements for the migration projects. Choose the Cloud Infrastructure Provider – whether this provider should be the organization itself, building a private cloud environment, or whether the organization would manage a private cloud in a third-party provider environment. In case of a private cloud within the organization boundary, determine whether it will be on-premise or near-premise (a physical establishment separated by geographical boundary but part of the organization's physical infrastructure). Understand the infrastructure available to support the cloud project. Discuss the migration projects and corresponding SLAs and elasticity requirements with the Cloud Infrastructure Provider.

5.8.3 Determine the Cost/Benefit

Assess the funding required and the benefit that the organization would achieve if migration is performed. Chart the projects to visualize the cost/risk *versus* the benefits. Request the funding from the appropriate funding authority.

5.8.4 Determine the Risks

Assess the overall risk of migration to the cloud. Assess the risk of individual projects and identify the high-risk projects.

5.8.5 Create a Cloud Migration Roadmap

Create a roadmap based on the outcome from the above steps and approvals obtained from the funding authority. Create a Cloud Migration Roadmap with distinct milestones.

5.8.6 Create Detailed Implementation Plan

Working closely with the appropriate PMO, assist in the creation of a Detailed Implementation Plan based on the preliminary Migration Roadmap and individual project timelines (developed in Phase E).

5.8.7 Create Formal Migration Contract

Create a formal contract with the Cloud Infrastructure Provider with a detailed description of SLA requirements, elasticity requirements, subscription process, and fees. The final Migration Roadmap and Detailed Implementation Plan should also be part of the contract.

5.9 Phase G: Implementation Governance

Implementation Governance focuses on making sure that implementation projects conform to the agreed Cloud Ecosystem Target Architecture(s). This must not be seen as a silo'ed effort but as an aligned activity that supports an organization's corporate, IT, and architecture governance.

Conformance is achieved through the proactive execution of an architecture compliance process. Rather than executing a compliance check at the end of the implementation, compliance is performed throughout the implementation at agreed compliance gates.

The rest of this section describes the steps taken in Phase G to achieve the overall goals of the architectural effort outlined for CloudEcoSource.

5.9.1 Confirm Scope and Priorities for Deployment with Development Management

The CloudEcoSource governance body decides on the scope and priorities of the Implementation Governance activities. This includes reviewing project and architecture artifacts, deployment challenges, and newly identified/updated CloudEcoSource Cloud Ecosystem SBBs being cataloged and marked for development.

5.9.2 Identify Deployment Resources and Skills

CloudEcoSource cloud implementation resources have to be made aware and educated on the architecture compliance process. In turn, this details the expectations of the implementation resources regardless of the method they utilize to implement the project.

5.9.3 Guide Development of Solutions Deployment

The goals, objectives, and plans for each CloudEcoSource implementation project are reviewed and conformance recommendations are made.

5.9.4 Perform Enterprise Architecture Compliance Reviews

The architecture compliance process is proactively executed where individual CloudEcoSource implementation projects are reviewed to make sure that they comply with the defined and agreed architecture, stated business objectives, and the overall cloud strategy.

5.9.5 Implement Business and IT Operations

Utilizing DevOps (Development Operations), CloudEcoSource leverages a strong collaborative relationship between the implementation teams and IT operations, which assists in decreasing the time, and lowering the risk in deploying the implementation projects.

5.9.6 Perform Post-Implementation Review and Close the Implementation

Once the implementations have been deployed to the Cloud Ecosystem they are reviewed and the results are then published.

5.10 Phase H: Architecture Change Management

The Architecture Change Management process ensures that the deployed architecture delivers maximum business value during its life cycle and that the architecture achieves its original target business value. This requires constant architecture assessment to ensure a well-managed architecture life cycle of the Cloud Ecosystem. It also ensures that the architecture capabilities have the flexibility to address ongoing changes in business and technology.

In order to ensure that the architecture continuously achieves its target business objectives and to avoid any business disruption, the Architecture Change Management process evaluates and evolves the Enterprise Architecture to appropriately address both internal and external factors to improve overall business performance. The following is a list of factors that need to be frequently assessed and appropriately addressed during the life cycle of the Enterprise Architecture:

- Incremental improvements to architectural capabilities that are critical to the enterprise's business processes transformation through automation
- New performance improvement opportunities that enable efficient operational decision-making activities to enhance customers' (both internal and external) experience
- Business requirements to create/change how customers, partners, and suppliers interact with the Enterprise Architecture capabilities to enhance Enterprise Architecture value proposition and business operations
- Ensure that service contracts with Cloud Service Providers have adequate provisions that allow enterprises to enable a change/exit/migration strategy without negatively impacting the Cloud Service delivery
- Perform routine risk assessments for the enterprise on Cloud Service Providers and the utilization of Cloud Services; the assessments must reflect the changing landscape with possible timely adjustments to enable efficient use of the enterprise's Cloud Ecosystem

The rest of this section describes the steps taken in Phase H to achieve the overall goals of the architectural effort outlined for CloudEcoSource.

5.10.1 Establish the Value Realization Process

In order to achieve business agility, CloudEcoSource must establish a cloud-first business policy to realize benefits and exploit its enterprise Cloud Ecosystem capabilities. This might require changes to organizational processes, performance matrices, and culture. Investments may be necessary to deliver the capabilities of the Cloud Ecosystem and to ensure that clear guidelines are established for the business value realization process. Establish benchmarks to assess the overall costs, service levels, and maturity level of business capabilities enabled by the enterprise Cloud Ecosystem.

CloudEcoSource needs to develop a catalog of IT services in order to track performance and costs associated with each service on its capabilities, usage, and the potential roles of Cloud Service Providers.

5.10.2 Deploy Monitoring Tools

CloudEcoSource established a cloud compliance process at the PMO level. The Cloud PMO identifies services and application re-use potential, establishes and shares change management best practices on service optimization and utilization of services provided by Cloud Service Providers, and tracks benefits realization by deploying monitoring capabilities. These monitoring capabilities provide critical information to assess the impact of business and technology changes on the enterprise Cloud Ecosystem. Having capabilities to track business performance, Quality of Service (QoS), and maturity assessments of services, CloudEcoSource has efficient operating models to better assess the overall viability (both internal and external Cloud Services capabilities) of the enterprise Cloud Ecosystem.

5.10.3 Manage Risks

Establish routine risk management to evaluate performance, financial position, and leadership of existing and potential Cloud Service Providers for the enterprise Cloud Ecosystem. Manage Enterprise Architecture risks and proactively adjust any Cloud Service Provider engagement in order to avoid any business disruption.

5.10.4 Provide Analysis for Architecture Change Management

Use the deployed monitoring capabilities for analysis and proactively identify business performance benchmarks for routine maturity assessments of the Cloud Ecosystem. Analyze Cloud Services maturity indicators to identify opportunities for improvement in the business capabilities of the enterprise Cloud Ecosystem. Ensure that any change requests to business capabilities adhere to established Enterprise Architecture governance guidelines, policies, and processes.

5.10.5 Develop Change Requirements to Meet Performance Targets

The change requests to the business capabilities of the Cloud Ecosystem must meet the performance targets for CloudEcoSource. Ensure that there is a clear understanding of current and future capabilities of Cloud Services and change requirements have a viable roadmap to deliver the required business capabilities (whether to build internally and/or use services provided by Cloud Service Providers).

5.10.6 Manage the Governance Process

CloudEcoSource must utilize the established governance process to evolve the enterprise Cloud Ecosystem in order to reduce the number of exceptions to the process. Any new/changed service must be in compliance with the Cloud Ecosystem Reference Model in order to minimize the exceptions to the Enterprise Architecture. The governance body of CloudEcoSource meets regularly to decide on ways to handle identified architectural changes to the enterprise Cloud Ecosystem.

The effectiveness of the governance process must be assessed periodically and applicable refinements made to the process.

5.10.7 Activate the Process to Implement Change

Activate the change process as described in the overall architecture governance process. The changes will be documented in the Architecture Definition Document and will describe the business performance objectives. The document describes how architecture change addresses new business requirements and policies.

Route the document for review by relevant stakeholders, incorporate received feedback, and determine whether review of the document is once again required. Once architecture change is approved and finalized, upload the documents in the Architecture Repository.

5.11 Requirements Management

Requirements Management is a process that is triggered by some organizational change that needs to be addressed (refer to Iacob et al.: Delivering EA with TOGAF and ArchiMate). It is a dynamic process in which the Enterprise Architecture requirements together with the subsequent changes are identified, stored, and used by the relevant ADM phases. As changes in requirements occur they may require iteration of the ADM. The focus of the Requirements Management process is to manage the requirements across the ADM rather than addressing and prioritizing the requirements (this is done within the relevant phase of the ADM) – refer to the TOGAF 9.1 Specification.

When a new architectural problem is assigned to the architecture team, the first task is to analyze the problem based on goals and requirements. This can be done with the Motivation Extension of the ArchiMate standard. The goals and requirements help to identify which combination of products, services, processes, and applications are needed to solve the problem and translate them into Enterprise Architecture models. If there are still unclear issues, the architecture team must repeat this process in order to refine and realize the elements of the architecture (refer to Iacob et al.: Delivering EA with TOGAF and ArchiMate).

5.11.1 Requirements Management and CloudEcoSource

The first step in the process of developing an Enterprise Architecture for the Cloud Ecosystem is to identify the architectural requirements. In order to identify and understand the requirements, the organization has to conduct need assessment and requirement analysis. The information can be gathered from the related stakeholders, cloud vendors, and cloud computing experts. A workshop (potentially using a business scenario) will be useful to identify the services that the organization needs and also the details of each service. More useful sources to elicit cloud-specific requirements are the cloud computing building blocks, service delivery models, deployment models, enabling technologies, and the essential characteristics of cloud computing. Advocate interviews can be the primary source of data collection to do requirements analysis. Below is a list of the cloud-specific requirements of CloudEcoSource.

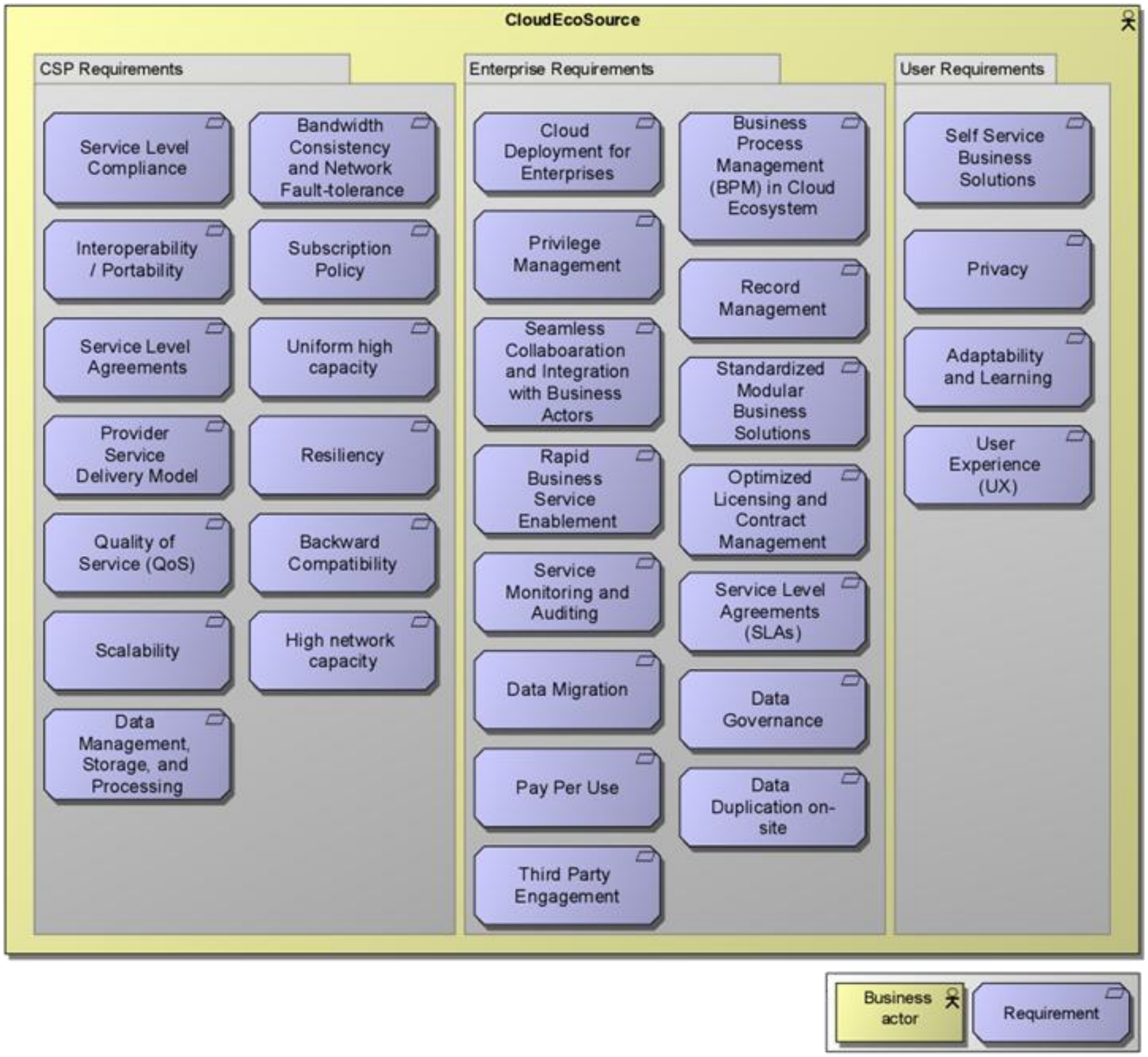
CloudEcoSource
CSP Requirements
Service Level Compliance
Bandwidth Consistency and Network Fault-tolerance
Interoperability / Portability
Subscription Policy
Service Level Agreements
Uniform high capacity
Provider Service Delivery Model
Resiliency
Quality of Service (QoS)
Backward Compatibility
Scalability
High network capacity
Data Management, Storage, and Processing
Enterprise Requirements
Cloud Deployment for Enterprises
Business Process Management (BPM) in Cloud Ecosystem
Privilege Management
Record Management
Seamless Collaboaration and Integration with Business Actors
Standardized Modular Business Solutions
Rapid Business Service Enablement
Optimized Licensing and Contract Management
Service Monitoring and Auditing
Service Level Agreements (SLAs)
Data Migration
Data Governance
Pay Per Use
Data Duplication on-site
Third Party Engagement
User Requirements
Self Service Business Solutions
Privacy
Adaptability and Learning
User Experience (UX)
Business actor
Requirement

Figure 22: CloudEcoSource Requirements – An Illustration

Acronyms

ABB	Architecture Building Block
ADM	(TOGAF) Architecture Development Method
BPaaS	Business Process as a Service
CMDB	Configuration Management Database
COTS	Commercial Off-The-Shelf
DaaS	Data as a Service
DAR	Data at Rest
DevOps	Development Operations
DIT	Data In Transit
DIU	Data In Use
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IEM	Identity, Entitlement, and Access Management
KPI	Key Performance Indicator
NIEM	(US Government) National Information Exchange Model
PaaS	Platform as a Service
PMO	Program Management Office
QoS	Quality of Service
RBAC	Role-Based Access Control
SaaS	Software as a Service
SBB	Solution Building Block
SLA	Service-Level Agreement
SOA	Service-Oriented Architecture

Index