Part III

Cloud Frameworks and Technologies

7

Cloud Reference Frameworks

Kapil Bakshi[1] and Larry Beser[2]

[1] *Cisco Systems Inc.*
[2] *HP Enterprise Services*

7.1 Introduction

Cloud reference frameworks are important tools for enabling meaningful dialogs when comparing cloud technical architectures, for informing business stakeholders evaluating cloud services, and providing for a common cloud taxonomy across organizational boundaries. Reference frameworks are composed of a variety of reference architectures and reference models, which collectively describe all of the relevant aspects in a context that can then be applied to particular stakeholder viewpoints and interests.

The majority of this chapter describes commonly discussed cloud and related reference frameworks. These frameworks most commonly arise from standards bodies, consortiums, and forums where the need for common ground generally overrides proprietary interests. As a result, any particular reference framework embodies the perspectives and interests of the organization from which it emerged, such as a security or any other architectural view.

Systemic interoperability, being a critical factor for market success in general, is enabled through the development and adoption of reference frameworks. By leveraging each framework's architectural view in the context of any particular initiative, business outcomes are more clearly mapped to enabling technologies, which lowers risk while enhancing investment return.

Encyclopedia of Cloud Computing, First Edition. Edited by San Murugesan and Irena Bojanova.

7.2 Review of Common Cloud Reference Frameworks

7.2.1 NIST Cloud Reference Framework

The National Institute of Standards and Technology (NIST) promotes the US economy and public welfare by providing technical leadership for the measurement and standards infrastructure. The Institute has published a reference architecture document for cloud computing to foster adoption of cloud computing, and its implementation depends upon a variety of technical and nontechnical factors. This document was published in the form of Special Publication 500-292 (Liu *et al*., 2011). Titled *NIST Cloud Computing Reference Architecture (RA) and Taxonomy,* this document explains the components and offerings of cloud computing. The NIST Cloud RA is a vendor-neutral architecture and provides flexibility for innovation within the framework. The NIST Cloud RA is presented in two parts:

- a complete overview of the actors and their roles;
- the necessary architectural components for managing and providing cloud services such as service deployment, service orchestration, cloud service management, security, and privacy.

The NIST cloud-computing reference architecture defines five major actors:

- A cloud consumer represents a person or organization that uses the service from a cloud provider via a business relationship. A cloud consumer uses the appropriate service based on a service catalog and a service contract with the cloud provider.
- A cloud provider acquires and manages the computing infrastructure and cloud software that provides the services and makes arrangements to deliver the cloud services to the cloud consumers through network access. The types of services can be infrastructure as a service (IaaS), software as a service (SaaS), and platform as a service (PaaS).
- A cloud carrier provides network connectivity and transport of cloud services from cloud providers to cloud consumers.
- A cloud auditor conducts independent assessments of cloud services, information system operations, performance, and security of the cloud implementation.
- A cloud broker manages the usage, performance, and delivery of cloud services, and negotiates relationships between cloud providers and cloud consumers. They can provide intermediation, aggregation, and arbitrage functions.

A cloud provider's activities can be described in five major areas, as shown in Figure 7.1: service deployment, service orchestration, cloud service management, security, and privacy. Service deployment models include public cloud, private cloud, community cloud, or hybrid cloud. The differences between these service models are based on how cloud resources are provided to a cloud consumer.

Service orchestration is the process of composing system components, like hardware and software resources, in an abstracted fashion, to support the cloud providers for the creation of a service.

Cloud service management includes service-related functions (business support, provisioning/configuration, and portability/interoperability) for services consumed by cloud consumers. Business support can include customer care, contractual issues, inventory management, accounting/billing, reporting/auditing, and pricing management. Provisioning/configuration consists of resource provisioning, monitoring and reporting, SLA, and metering management. Cloud service management may also include mechanisms to support data portability, service interoperability, and system portability.

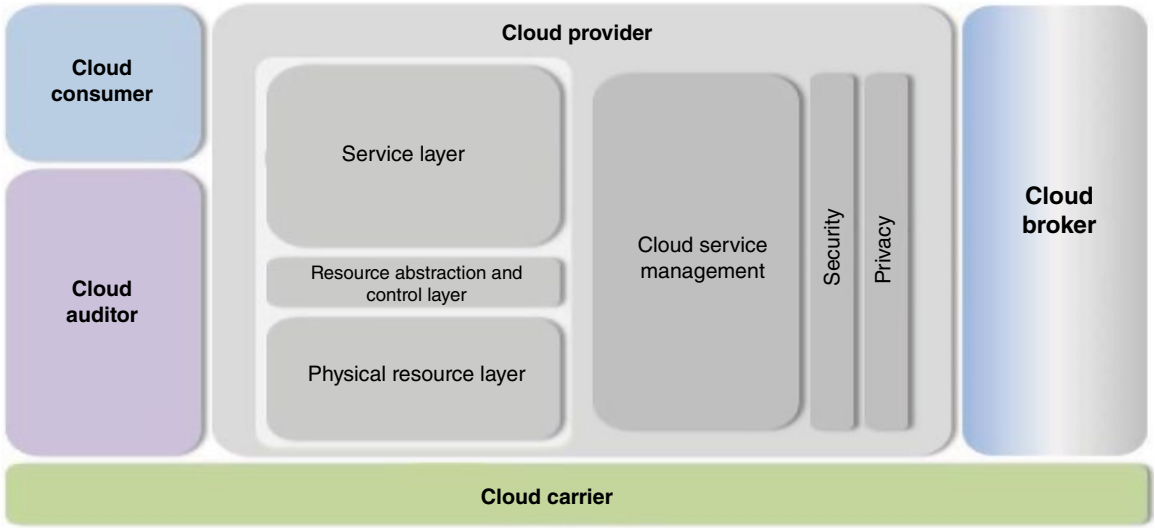

Figure 7.1 *NIST cloud reference architecture. Source: Liu et al. (2011)*

The NIST Cloud RA makes security a concern of cloud providers, consumers, and other parties. Cloud-based systems address security requirements such as authentication, authorization, availability, confidentiality, identity management, integrity, audit, security monitoring, incident response, and security policy management. With regard to privacy aspects of RA, personal information (PI) and personally identifiable information (PII) should be protected and processed appropriately by the cloud providers.

Key Takeaway

This framework enables use case and scenario planning methods by providing major actor and service constructs for cloud.

7.2.2 IETF (Draft) Cloud Reference Framework

This section discusses the Cloud Reference Framework submitted to Internet Engineering Task Force (IETF) as a draft. The IETF is an open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and operations. The IETF-proposed draft cloud reference framework describes different layers for interoperability, integration, and operations of virtualized applications (Figure 7.2). The IETF draft reference framework provides standardization of cloud functional elements and the interfaces between the functions.

The cloud reference framework consists of the following horizontal layers:

- user/customer side services/functions and resources layer (USL);
- access delivery layer (ADL);
- cloud service layer (CSL);
- resource control (composition and orchestration) layer (RCL);

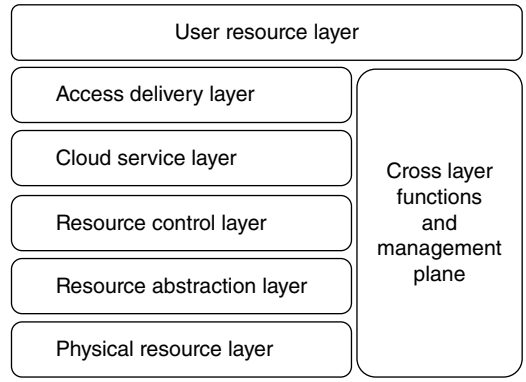

Figure 7.2 *IEFT cloud reference architecture. Source: Khasnabish et al., 2013*

- resource abstraction and virtualization layer (RAVL);
- physical resource layer (PRL).

The vertical cross-layer cloud management functions perform the following:

- configuration management;
- services registry and discovery;
- monitoring with logging, accounting, and auditing;
- service-level agreement (SLA) management;
- security services and infrastructure management.

The cloud reference framework also describes Intercloud. Intercloud provides a capability to enable portability and interoperability of independent cloud domains, and cloud provisioning and operation services.

The USL functions include access to information and identity tasks in the cloud, including visualization and administrative management functions.

The ADL hosts infrastructure components to deliver cloud-based services to customers and their access by end users. The ADL may include endpoint functions such as user portal and service gateways, like distributed cache and content delivery network (CDN) gateways. The Intercloud functions of the ADL include Intercloud infrastructure to support cloud federation, federated identity, cloud services registry/discovery, and cloud brokering functions.

The cloud service layer provides functionality for the three cloud services models, namely, IaaS, PaaS, and SaaS. The CSL develops these services based on the basic technical resources of CPU, memory, hard-disk space, and bandwidth.

The resource control layer manages and integrates the virtual resources to the upper layers and provides the ability to create efficient, secure, and reliable services. Additionally, the RCL layer has the following responsibilities:

- resources composition and orchestration;
- resource schedule control;
- Intercloud resource control;
- resource availability control;
- resource security management;
- services lifecycle management.

The RAVL provides the abstraction of the physical resources to the higher layers. The abstracted physical resources are abstracted first, next they are composed by the cloud management software (at composition and abstraction layers), and finally they are deployed as virtual resources on the virtualized physical resources. The function of the RAVL is to convert physical resources into a virtual resources pool. As part of the RAVL, the networking (resources) layer converts network capabilities and capacities (such as bandwidth, ports, etc.) into a set of resource pools, which can be leveraged by the upper layers. The resource pools include virtual switch, virtual router, virtual firewall, virtual network interface, virtual network link, and virtual private network (VPN) resources.

The PRL consists of resources like CPU, memory, hard disk, network interface card (NIC), and network ports.

As noted, in addition to the above-mentioned layers, this framework also provides vertical functions that run across all of those layers. The functions provided by the vertical layer are cloud management plane, cloud configuration management, cloud service registry/repository, cloud monitoring, accounting, and audit management, cloud SLA management, and cloud security services management.

Key Takeaway

This framework provides the essential architecture building blocks for engaging cloud networking and associated communications services.

7.2.3 Cloud Security Alliance: Cloud Reference Model

The Cloud Security Alliance (CSA) is a nonprofit organization that promotes research into best practices for securing cloud computing and the ability of cloud technologies to secure other forms of computing. The CSA has developed a cloud reference model, coupled with a security and compliance model (Figure 7.3).

The CSA's Cloud Reference Model has IaaS as the foundation of all cloud services, with PaaS building upon IaaS, and SaaS in turn building upon PaaS. As a result, in addition to capability inheritance, information security issues and risk are also inherited.

Infrastructure as a service includes the infrastructure resource stack, including facilities, hardware platforms, abstraction, and connectivity functions. It provides the capability to abstract resources, as well as to deliver physical and logical connectivity to those resources. IaaS provides a set of Application Programming Interfaces (APIs), which allows management and other interaction with the infrastructure.

Platform as a service provides a layer of integration with application development frameworks, middleware capabilities, and functions such as database, messaging, and queuing. These services allow developers to build applications on the platform with programming languages and tools.

Software as a service builds upon the underlying IaaS and PaaS stacks and provides a self-contained operating environment that is used to deliver the entire software user experience, including the content, its presentation, the application, and management capabilities. Based on IaaS, SaaS, or PaaS, consumers can leverage their content and metadata to develop and deploy applications.

The security and compliance models portray cloud service mapping, which can be compared against a catalog of security controls to determine which controls exist and which do not — as provided by the consumer, the cloud service provider, or a third party (Figure 7.3). The security stack addresses several layers including physical, compute and storage, trusted computing, network, management, information, and applications. The security stack can in turn be compared to a compliance framework or set of requirements such as PCI, DSS, HIPPA, or FedRAMP.

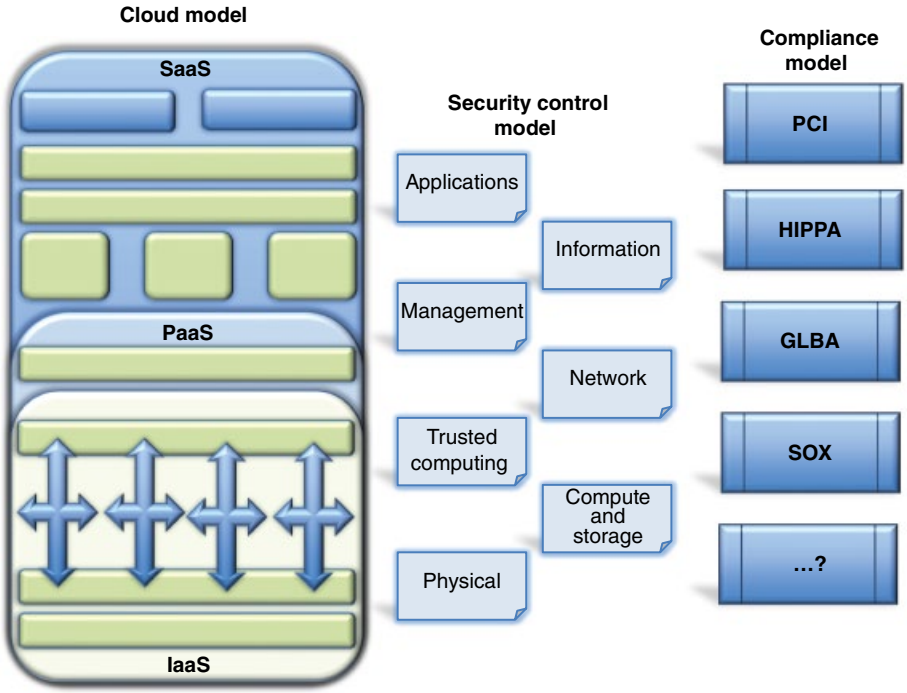

Figure 7.3 *CSA cloud, security, and compliance reference model. Source: Archer et al. (2011)*

The CSA also has 13 other domains, which highlight strategic and tactical security within a cloud environment and can be applied to any combination of cloud service and deployment models. The domains are divided into two broad categories: governance and operations. The governance domains are broad and address strategic and policy issues, while the operational domains focus on more tactical security concerns and implementation within the architecture.

The governance domain consists of:

- governance and enterprise risk management;
- legal issues, including contracts and electronic discovery;
- compliance and audit;
- information management and data security;
- portability and interoperability.

The operational domain focuses on:

- business continuity and disaster recovery;
- datacenter operations;
- incident response, notification, and remediation;
- application security;
- encryption and key management
- Identity and access management;
- virtualization;
- security as a service.

Key Takeaway

This reference model provides the essential architectural building blocks for engaging security and compliance for cloud initiatives.

7.2.4 Distributed Management Task Force Common Information Model

Founded in 1992, the Distributed Management Task Force, Inc. (DMTF) focuses on collaboration and the development of systems management standards, as well as their validation, promotion, and adoption in IT organizations. Its standards provide common management infrastructure components for instrumentation, control, and communication in a platform-independent and technology-neutral way.

Initially developed in 1997, their Common Information Model (CIM) provides a common definition of management information for systems, networks, applications, and services, and allows for vendor extensions. The CIM's common definitions enable vendors to exchange semantically rich management information between systems throughout the network. As a conceptual information model not bound to a particular implementation, CIM allows for the interchange of management information between management systems and applications in a vendor-neutral fashion. This can be either "agent to manager" or "manager to manager" communications that provides for distributed system management. There are two parts to CIM: the CIM specification and the CIM schema.

The CIM specification describes the language, naming, and Meta schema, and mapping techniques to other management models such as simple network management protocol (SNMP), management information bases (MIBs), distributed management task force (DMTF), and management information formats (MIFs). The Meta schema is a formal definition of the model. It defines the terms used to express the model and their usage and semantics. The elements of the Meta schema are classes, properties, and methods. The Meta schema also supports indications and associations as types of classes and references as types of properties.

The CIM schema provides the actual model descriptions. The CIM schema supplies a set of classes with properties and associations that provide a well-understood conceptual framework within which it is possible to organize the available information about the managed environment (DMTF Architecture Working Group, 2012).

The CIM schema itself is structured into three distinct layers:

- The Core schema is an information model that captures notions that are applicable to all areas of management.
- Common schemas are information models that capture notions that are common to particular management areas, but independent of a particular technology or implementation. The common areas are systems, devices, networks, applications, metrics, databases, the physical environment, event definition and handling, management of a CIM infrastructure (the interoperability model), users and security, policy and trouble ticketing/knowledge exchange (the support model). These models define classes addressing each of the management areas in a vendor-neutral manner.
- Extension schemas represent organizational or vendor-specific extensions of the common schema. These schemas can be specific to environments, such as operating systems (for example, UNIX or Microsoft Windows). Extension schema fall into two categories, technology-specific areas such UNIX98 or product-specific areas that are unique to a particular product such as Windows.

The formal definition of the CIM schema is expressed in a managed object file (MOF) which is an ASCII or UNICODE file that can be used as input into an MOF editor, parser, or compiler for use in an application. The unified modeling language (UML) is used to visually portray the structure of the CIM schema.

Key Takeaway

The DMTF CIM provides essential architecture building blocks for engaging cloud management systems and related interoperability concerns

7.2.5 ISO/IEC Distributed Application Platforms and Services (DAPS)

The International Organization for Standardization (ISO) is the world's largest developer of voluntary international standards. Founded in 1947, they have published more than 19 500 International Standards covering almost all aspects of technology and business. JTC 1/SC38 consists of three working groups: Web services, service oriented architecture (SOA), and cloud computing. JTC 1/SC38 also includes a study group on cloud computing whose goals include providing a taxonomy, terminology, and value proposition for cloud computing.

The working group on cloud computing was established in February 2012. It is committed to usage scenarios and use cases as an analysis tool to identify specific characteristics and requirements of cloud computing. The relationship between usage scenarios and use cases is illustrated in Figure 7.4. Standard templates are provided as well to facilitate the methodology.

Among the major scenarios covered are high level scenarios (including provisioning methods such as IaaS, PaaS, and "generic"), cloud delivery scenarios (such as PaaS-based CRM), business support, migration, portability, interoperability, mobility, and cloud computing for the public sector.

The working group's collection of use case scenarios and use cases provide a real-life method to identify where standards are or can be applied to cloud reference architectures and help quantify what gaps may exist. This method also enables relevant stakeholders to be identified and their collaboration to occur in context.

As of 2013, ISO/IEC JTC 1/SC 38 has eight published standards and five standards are under development in DAPS. The cloud computing standards focused on by the working group include standards that define cloud computing vocabulary and reference architecture, including general concepts and characteristics of

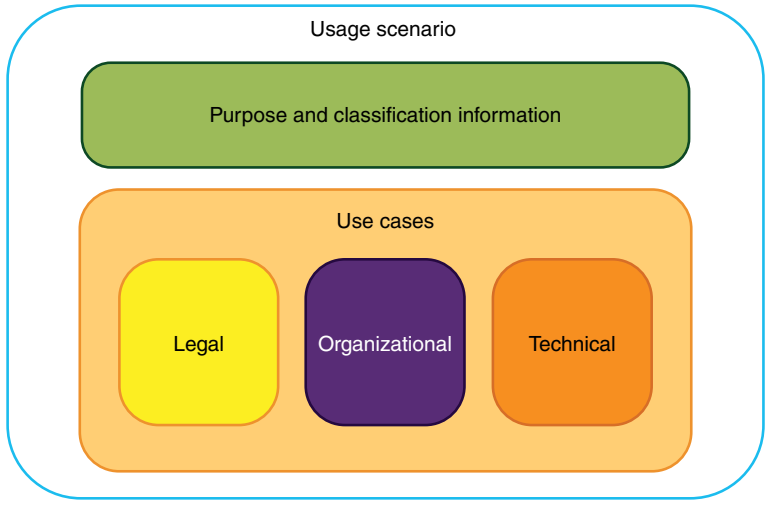

Figure 7.4 *Usage scenarios and use cases. Source: ISO/IEC JTC 1/SC 38/WG 3 (2013)*

cloud computing, types of cloud computing, components of cloud computing, and cloud computing roles and actors (ISO/IEC JTC 1/SC 38/WG 3, 2013). Primary goals of the working group standards activity include interoperability and enabling future standards work.

Key Takeaway

This standard provides reference examples and exposes methods and techniques for decomposing business requirements in use case and scenario planning efforts, primarily toward application and systems interoperability.

7.2.6 Open Grid Forum Open Cloud Computing Interface (OCCI)

The Open Grid Forum (OGF) is a community of users, developers, and vendors leading the global standardization effort for distributed computing (including clusters, grids, and clouds). The OGF community consists of thousands of individuals in industry and research, representing over 400 organizations in more than 50 countries. It is an open community committed to driving the rapid evolution and adoption of applied distributed computing.

The purpose of the Open Cloud Computing Interface Working Group (OCCI-WG) is the creation of practical solutions that interface with cloud infrastructures offered as a service. They focused initially on solutions that covered the provisioning, monitoring, and definition of Cloud Infrastructure Services (IaaS). The current release of the Open Cloud Computing Interface is suitable to serve many other models in addition to IaaS, including PaaS, and SaaS.

The OCCI goals are interoperability, portability, and integration in a vendor-neutral context with minimal cost. The current specification consists of three documents. This specification describes version 1.1 of OCCI. Future releases of OCCI may include additional rendering and extension specifications. The documents of the current OCCI specification suite are:

- OCCI Core: describes the formal definition of the OCCI core model.
- OCCI HTTP Rendering: defines how to interact with the OCCI core model using the RESTful OCCI API. The document defines how the OCCI core model can be communicated and thus serialized using the HTTP protocol.
- OCCI Infrastructure: contains the definition of the OCCI Infrastructure extension for the IaaS domain. The document defines additional resource types, their attributes, and the actions that can be taken on each resource type.

By focusing on the delivery of API specifications for the remote management of cloud infrastructures, the work enables the development of vendor-neutral interoperable tools. Their scope is the high-level functionality required for lifecycle management of virtual machines or workloads running on virtualization technology supporting service elasticity. The API work is supported by use cases that provide context and applicability of the API in lifecycle management. Reference implementations are specifically excluded, as are details relating to supporting infrastructure design (such as storage and network hardware configuration).

Key Takeaway

The OGF OCCI provides essential architecture building blocks for engaging cloud infrastructure analysis and design from an interoperability perspective.

7.2.7 Open Security Architecture (OSA) Secure Architecture Models

Open Security Architecture (OSA) is a not-for-profit-organization supported by volunteers for the benefit of the security community. The OSA is divided into three categories: the Control Catalog, the Pattern Landscape, and the Threat Catalog. The OSA provides a single, consistent, clearly defined control catalog intended to simplify requirements from numerous standards, governance frameworks, legislation, and regulations.

Patterns show the best practice set of controls that should be specified for a given situation, consisting of security architectures that address specific security problems. Applying OSA patterns in your work gives you a fast start, improves the quality of the solution you deploy, and reduces overall effort (Figure 7.5).

The Control Catalog, based on NIST 800-53 (2006), provides details for all controls required to create a security solution. Controls are mapped against other standards, regulations, legislation, and governance standards. To ensure consistency between patterns and application of controls, the OSA has defined "actors" for the use cases. OSA actors are prototypical business roles which can be used singly or in combination, depending on the intent of the use case.

The OSA Threat Catalog is a list of generic risks that need to be taken into account when rating the applicability of a control to a given pattern. For the classification of top-level threats, the OSA proposes to categorize the threat space into sub-spaces according to a model of three orthogonal dimensions labeled motivation, localization, and agent. The threat agent is the actor that imposes the threat on a specific asset. Threat agents can be human, technological, or *force majeure* (environmental).

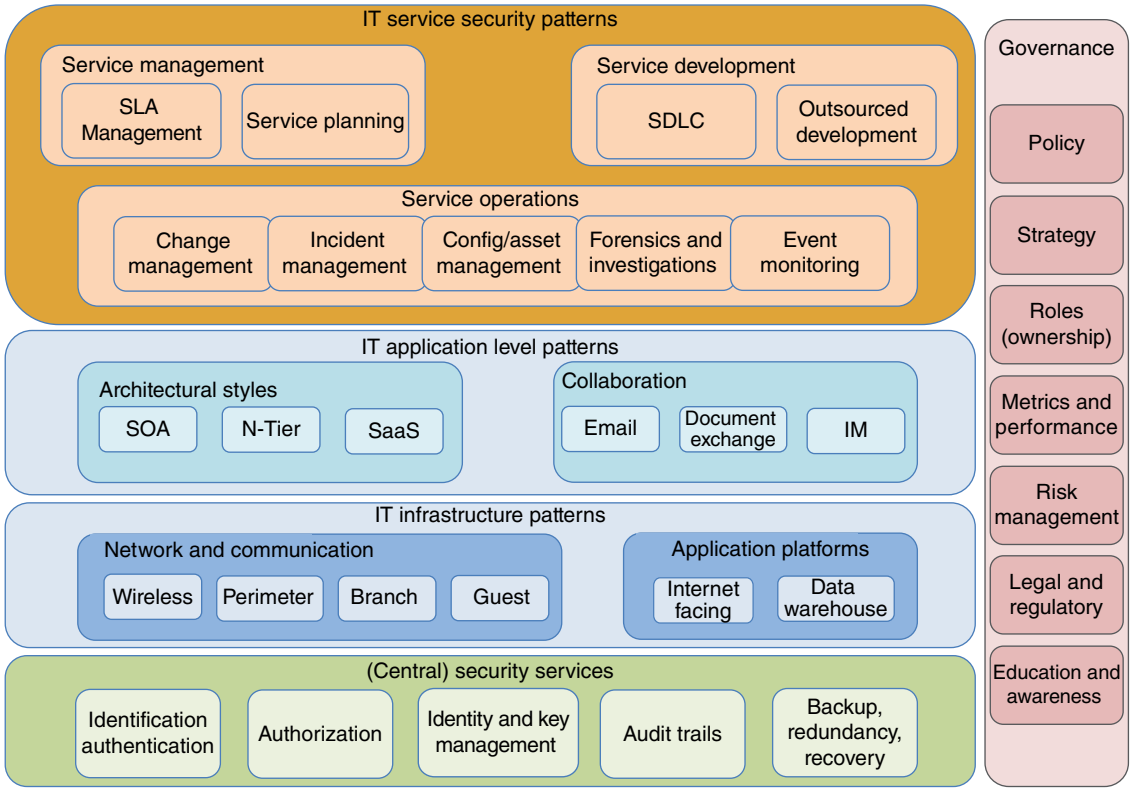

Figure 7.5 *OSA pattern landscape. Source: Phaedrus and Tobias (n.d.)*

The Cloud Computing Pattern published by the OSA illustrates the application of controls, actors, and threats in the construction of a cloud security reference pattern. The pattern enables the evaluation of a given cloud solution according to its function and capabilities in a vendor-agnostic fashion.

Key Takeaway

The OSA secure architecture model provides essential architecture building blocks for engaging cloud security and compliance. It also offers guidance in the application of the architecture building blocks to use case and scenario planning efforts for cloud security and compliance perspectives.

7.2.8 Organization for the Advancement of Structured Information Standards

The Organization for the Advancement of Structured Information Standards (OASIS) is a nonprofit consortium that drives the development, convergence, and adoption of open standards for the global information society. OASIS promotes industry consensus and produces worldwide standards for security, cloud computing, SOA, Web services, the smart grid, electronic publishing, emergency management, and other areas.

OASIS cloud-related standards include:

- AMQP: advanced message queuing protocol offers organizations an easier, more secure approach to passing real-time data streams and business transactions. By enabling a commoditized, multi-vendor ecosystem, AMQP creates opportunities to transform the way business is done over the Internet and in the cloud.
- IDCloud: identity in the cloud identifies gaps in existing identity management standards for the cloud and the need for profiles to achieve interoperability within current standards. IDCloud performs risk and threat analyses on collected use cases and produces guidelines for mitigating vulnerabilities.
- OData: Open Data is a REST-based protocol that simplifies the sharing of data across applications for reuse in the enterprise, cloud, and mobile devices. OData enables information to be accessed from a variety of sources including relational databases, file systems, content management systems, and traditional web sites.
- SAML: security assertion markup language provides a framework for communicating user authentication, entitlement, and attribute data between online partners.
- SOA-RM: SOA reference model defines the foundation upon which specific SOA concrete architectures can be built.
- TOSCA: topology and orchestration specification for cloud applications enhances the portability of cloud applications and the IT services that comprise them. TOSCA enables the interoperable description of application and infrastructure cloud services, the relationships between parts of the service, and the operational behavior of these services, independent of the supplier that creates the service, the particular cloud provider, or hosting technology. TOSCA facilitates higher levels of cloud service and solution portability without lock in.

OASIS perspectives on cloud generally are in data/messaging or security contexts. They are included in the category of "open standard" bodies promoting interoperability and ease of management in heterogeneous environments. The OASIS Cloud Application Management for Platforms (CAMP) technical committee advances an interoperable protocol that cloud implementers can use to package and deploy their applications. CAMP defines interfaces for self-service provisioning, monitoring, and control. Common CAMP-use cases include moving premise applications to the cloud (private or public), and redeploying applications across cloud platforms from multiple vendors.

Key Takeaway

The OASIS cloud-related standards provides essential architecture building blocks for engaging cloud service design and cloud service interoperability initiatives

7.2.9 SNIA Cloud Data Management Interface Standard

The Storage Networking Industry Association (SNIA) is an association of producers and consumers of storage networking specifications and standards. It works towards its goal "to promote acceptance, deployment, and confidence in storage-related architectures, systems, services, and technologies, across IT and business communities" by forming and sponsoring technical work groups for storage networking standards and specifications.

The Cloud Data Management Interface (CDMI) is a SNIA standard that specifies a protocol for self-provisioning, administering, and accessing cloud storage. With help of the CDMI, the clients can discover cloud storage capabilities and leverage the CDMI to manage data and containers. In addition, metadata can be set on containers and their contained data elements through CDMI. The CDMI can be used for administrative and management applications to manage containers, accounts, security access, monitoring/billing information, and storage that is accessible by other protocols. The CDMI exposes the capabilities of the underlying storage and data services to potential clients. Figure 7.6 portrays a cloud reference model.

The cloud storage reference model includes functions and layers that enable clients to discover the capabilities available in the cloud storage, manage containers and the data that is placed in them; and allow metadata to be associated with containers and the objects they contain. This is portrayed in above three layers of the model. CDMI defines RESTful HTTP operations for the above functions.

The CDMI defines the functions to manage the data and as a way to store and retrieve the data. The means by which the storage and retrieval of data is achieved is termed a data path. Hence, CDMI specifies both a data path and a control path interface.

The container metadata layer is used to configure and expose the data requirements of the storage provided through the storage protocol (e.g., block protocol or file protocol). For example, for the underlying file system for a block protocol (e.g., iSCSI), the CDMI container provides a useful abstraction for representing the data system metadata.

The SNIA's CDMI is based on an object model with categorized data, container, domain, queue, and capability objects. The CDMI defines two namespaces that can be used to access stored objects: a flat-object ID namespace and a hierarchical path-based namespace. Objects are created by ID by performing HTTP commands against a special URI.

The CDMI uses many different types of metadata: HTTP metadata, data system metadata, user metadata, and storage system metadata. HTTP metadata is metadata that is related to the use of the HTTP protocol (e.g., content length, content type). The CDMI data system metadata, user metadata, and storage system metadata are defined in the form of name-value pairs. Data-system metadata are metadata that are specified by a CDMI client and are a component of objects. Data-system metadata abstractly specify the data requirements associated with data services that are deployed in the cloud storage system.

Key Takeaway

This cloud interface standard provides essential architecture building blocks for engaging cloud storage design and infrastructure integration.

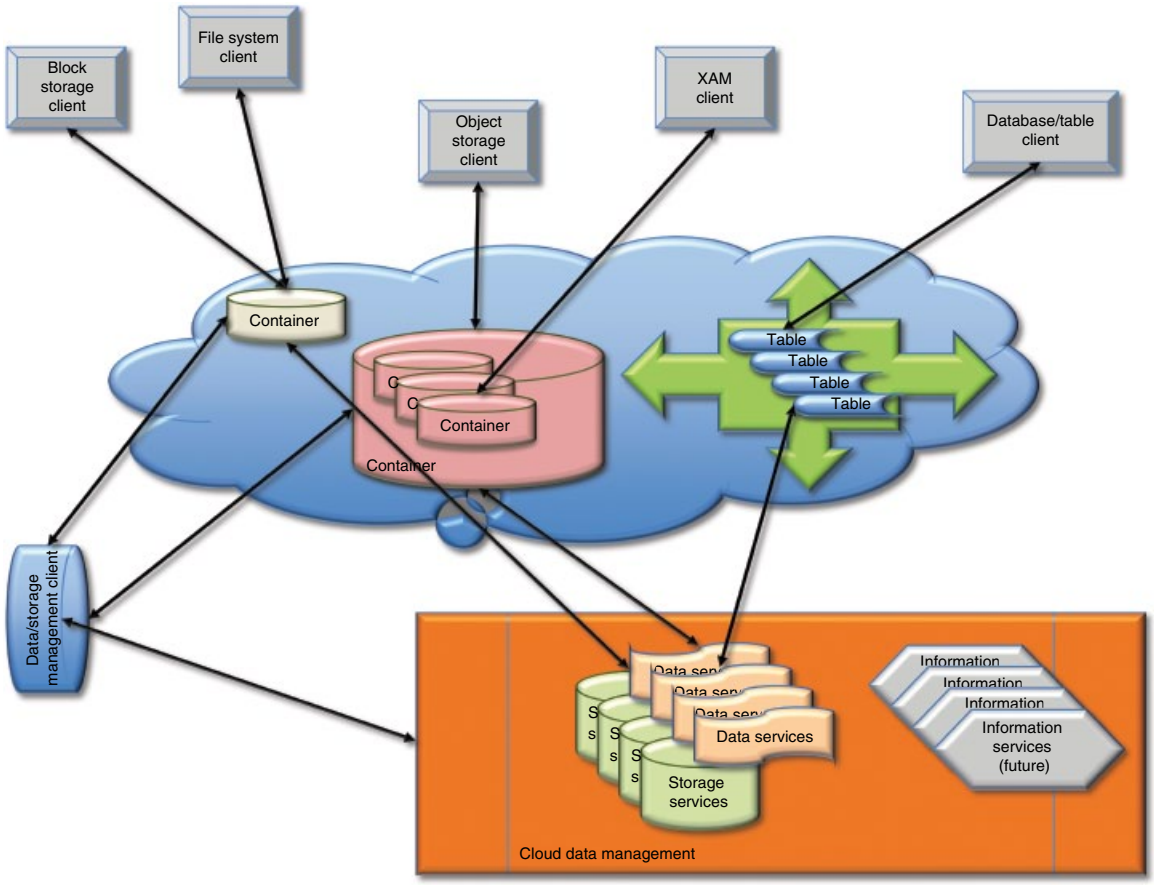

Figure 7.6 *Cloud storage reference model. Source: Bairavasundaram (2012)*

7.2.10 The European Telecommunications Standards Institute Cloud Standard

The European Telecommunications Standards Institute (ETSI) produces globally applicable standards for information and communications technologies (ICT), including fixed, mobile, radio, converged, broadcast, and Internet technologies. Their work in cloud is an extension of an earlier focus on grid computing. The ETSI has four published standards for cloud focused on standardization, interoperability testing, and service-level agreements. The ETSI working programs include security, interoperability, connected things, wireless systems, fixed networks, content delivery, and public safety.

The latest published cloud standard from ETSI (ETSI TS 103 142 Test Descriptions for Cloud Interoperability) describes the testing requirements and scenarios for interoperability as defined by another standards group, the OCCI from the Open Grid Forum. This illustrates the interlocking interests of the many open standards groups and how they collaborate to drive agnostic interoperable solutions.

In order to unleash the potential of cloud computing, the European Commission (EC) published a Communication on Cloud Computing, released on September 27, 2012, identifying cutting through the jungle of standards as one of the key actions to foster mass adoption of cloud computing. The ETSI was requested by the EC to coordinate with stakeholders in the cloud standards ecosystems and devise standards

and roadmaps in support of EU policy in critical areas such as security, interoperability, data portability, and reversibility. The first meetings were held in Cannes in December 2012.

Related to cloud standards projects at ETSI are those addressing "connected things" (ETSI, 2013). An ever increasing number of everyday machines and objects are now embedded with sensors or actuators and have the ability to communicate over the Internet. These "smart" objects can sense and even influence the real world. Collectively, they make up what is known as the "Internet of Things" (IoT). The IoT draws together various technologies including radio frequency identification (RFID), wireless sensor networks (WSNs), and machine-to-machine (M2M) service platforms. The ETSI is addressing the issues raised by connecting potentially billions of these "smart objects" into a communications network by developing the standards for data security, data management, data transport, and data processing. This will ensure interoperable and cost-effective solutions, open up opportunities in new areas such as e-health and smart metering, and allow the market to reach its full potential.

Key Takeaway

The ETSI cloud standards outline architecture building blocks for engaging cloud networking and communications interoperability.

7.2.11 The Open Group Cloud Model

The Open Group (TOG) is a vendor and technology-neutral industry consortium that provides innovation and research, standards and certification development on topics of IT Architecture. It is currently developing several related cloud-reference models, namely Cloud Computing Reference Architecture, the Cloud Ecosystem Reference Model, and the Distributed Computing Reference Model. This section will discuss details of the published Distributed Computing Reference Model (DCRM) (Figure 7.7).

The DCRM contains several components that are focused on the interfaces between the components. The DCRM is leveraged in the context of portability and interoperability of cloud reference architecture. The management systems and marketplaces are particular kinds of components, shown separately because of their particular relationships to platforms and infrastructure.

The application data, applications, platforms, and infrastructure stack can be applied to enterprise systems, cloud systems, and user devices. In cloud systems, applications may be exposed as software as a service (SaaS), platforms may be exposed as platform as a service (PaaS), and infrastructure may be exposed as infrastructure as a service (IaaS).

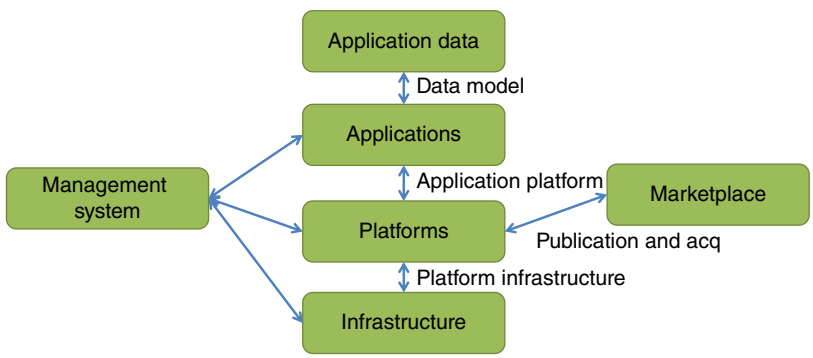

Figure 7.7 *Distributed computing reference model. Source: Bakshi and Skilton (2013)*

In the DCRM, an application can have several facets – a cloud SaaS service, enterprise application service, composition of cloud and enterprise application services, an application program running on a server, and/or application mobile device. They can also be SOA style – applications consisting of collections of services. These may be explicitly programmed as service compositions; for instance, using the OASIS standard Web services business process execution language (WS-BPEL). Applications interfaces include application data through data models, through application-application interfaces, and through application-platform interfaces (APIs).

An application platform consists of the hardware and software components that provide the services used to support applications. It exposes an application platform interface to applications. In the DCRM, a platform may be a PaaS service, where interfaces could be application-platform interfaces, platform-platform interfaces, infrastructure through platform-infrastructure interfaces, management systems through platform management interfaces, or marketplaces through publication and acquisition interfaces. Platforms are used by developers to develop applications and other programs and by systems managers to run and configure applications, either through management systems or directly.

In the DCRM, infrastructure includes cloud IaaS services, hardware in servers, PCs and mobile devices, and virtualized hardware resources in enterprise systems. A cloud infrastructure service makes hardware components available as cloud resources, generally through a virtualization layer. The functional interface in this case supports the loading and execution of machine images. The management interface enables the hardware resources to be provisioned and configured, and enables machine images to be deployed on them. Infrastructure interfaces to platforms through platform-infrastructure interfaces; management systems through infrastructure management interfaces.

Management systems are components to manage cloud and enterprise IT resources. Management systems interface with applications through APIs, platforms through platform management interfaces, and infrastructure through infrastructure management interfaces. Management systems are used by systems managers to manage applications, platforms, and infrastructure.

A cloud marketplace enables cloud providers to make their products available and enables cloud consumers to choose and obtain the products that meet their requirements. The products may be services, machine images, applications, or other cloud-related products. They can have associated descriptions, prices, terms of use, and so forth, so that consumers can select them and contract for their use. Marketplaces interface with platforms through product publication and acquisition interfaces.

Key Takeaway

This reference model provides essential architecture building blocks for engaging cloud portability and cloud interoperability perspectives and offers guidance in the application of the architecture's building blocks to use case and scenario planning efforts for cloud portability and cloud interoperability initiatives.

7.3 Conclusion

Cloud reference frameworks are a critical tool for architecting, engineering, and standard setting in any major cloud initiative. Today's most influential groups are promoting "open" standards as a rule, which recognize the various requirements for heterogeneous ecosystems. They provide the mechanism for introducing transformational change, while still supporting legacy systems.

Collaboration across the groups is a part of the "Open" movement, wherein each group's interest/focus is applied in the context of one or several other reference frameworks using scenarios and use cases. In this

fashion, reference frameworks constitute the common taxonomy and architectural landscape for cloud and its evolution.

Essential to the success of a cloud effort is the appropriate application of a framework to one's own business environment, business requirements, and technical capabilities. Each framework presented in this chapter has a particular focus and use as described in its key takeaway. By aligning a framework with the actual work at hand, the architecture and engineering efforts become better informed and better integrated. This reduces overall risk and works to ensure anticipated business outcomes.

References

Archer, J., Boehme, A., Cullinane, A., *et al*.(2011) *Security Guidance for Critical Areas of Focus in Cloud Computing. Cloud Security Alliance (CSA)*, https://cloudsecurityalliance.org/download/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v3/ (accessed November 29, 2015).

Bairavasundaram, L., Baker, S., Carlson. M., *et al*. (2012) *SNIA Cloud Data Management Interface v1.0.2, Technical Position*, http://snia.org/sites/default/files/CDMI%20v1.0.2.pdf (accessed November 29, 2015).

Bakshi, K. and Skilton, M. (2013) *Guide: Cloud Computing Portability and Interoperability*, Berkshire, United Kingdom, http://www.opengroup.org/cloud/cloud/cloud_iop/index.htm (accessed December 4, 2015).

DMTF Architecture Working Group (2012) *Common Information Model (CIM) Metamodel Version 3.0.0* (Document Number: DSP0004, December 13).

ETSI (2013) *Building The Future, ETSI Work Programme 2013–2014*, http://www.etsi.org/images/files/WorkProgramme/etsi-work-programme-2013-2014.pdf (accessed November 29, 2015).

Khasnabish, B., Ma, S., So, N., *et al*. (2013) IETF Cloud Reference Framework. IETF Fremont, California. http://datatracker.ietf.org/doc/draft-khasnabish-cloud-reference-framework/?include_text=1.

Liu, F., Tong, J., Mao, J., *et al*. (2011) *NIST Cloud Computing Reference Architecture*. Special Publication 500-295, ITL NIST, Gaithersburg, MD, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505 (accessed November 29, 2015).

ISO/IEC JTC 1/SC 38/WG 3 (2013) *Methodology and Guidelines for Cloud Computing Usage Scenario and Use Case Analysis*, International Standards Organization, Geneva.

Phaedrus, R. and Tobias, S. (n.d.) *Open Security Architecture. Release 08.02*,
http://www.opensecurityarchitecture.org/cms/library/patternlandscape/251-pattern-cloud-computing (accessed December 4, 2015).