1  **NIST**

2  **National Institute of
Standards and Technology**
U.S. Department of Commerce

3

4  _____

5  # NIST Cloud Computing

6  # Security Reference Architecture

7  _____

8

9

10

11
12  *NIST Cloud Computing Security Working Group*
13  *NIST Cloud Computing Program*
14  *Information Technology Laboratory*

15

16

17

18

19  **NIST** **National Institute of Standards and Technology** • U.S. Department of Commerce

20    This page left intentionally blank

21

# Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This document reports on ITL's research, guidance, and outreach efforts in Information Technology and its collaborative activities with industry, government, and academic organizations.

# Acknowledgements

---

[1] "Contributors" are members of the NCC SWG who dedicated substantial time on a regular basis to research and development in support of this document.

Ken E. **Stavinoha**, PhD., Cisco Systems
Steven **Woodward**, Cloud Perspectives

OTHER ACTIVE MEMBERS:
   Richard J **Blake**, General Services Administration
   Ron **Martin**, Open Security Exchange
   Sundararajan **Ramanathan**, Capgemini

**NOTE**: All views expressed in this document by our contributors are their personal opinions and not those of the organizations with which they are affiliated.

# Table of Contents

## List of Figures

## List of Tables

## EXECUTIVE SUMMARY

The National Institute of Standards and Technology (NIST), along with other agencies, was tasked by the U.S. Chief Information Officer with specific activities aimed at accelerating the adoption of cloud computing [11]. These include the delivery of a US Government Cloud Computing Technology Roadmap and the creation of other NIST Special Publications (NIST SPs) that address the definitions, security aspects, and reference architecture of Cloud Computing. In furtherance of its statutory responsibilities, NIST has developed a series of Special Publications aimed at accelerating the Cloud Computing adoption by Federal agencies:

- NIST SP 500-291: *Cloud Computing Standards Roadmap*

- NIST SP 500-292: *NIST Cloud Computing Reference Architecture*

- NIST SP 500-293: *US Government Cloud Computing Technology Roadmap Volume 1, High-Priority requirements to Further USG Agency Cloud Computing Adoption*

- NIST SP 500-293: *US Government Cloud Computing Technology Roadmap Volume II,* Useful Information for Cloud Adopters (Draft)

- NIST SP 500-293: *US Government Cloud Computing Technology Roadmap Volume III, Technical Considerations for USG Cloud Computing Deployment Decisions* (Draft)

- NIST SP 800-144: *Guidelines on Security and Privacy in Public Cloud Computing*,

- NIST SP 800-145: *The NIST Definition of Cloud Computing*

- NIST SP 800-146: *Cloud Computing Synopsis and Recommendations* (Draft)

This document was developed as part of a collective effort by the NIST Cloud Computing Public Security Working Group in response to the priority action plans for the early USG cloud computing adoption identified in NIST SP 500-293: *US Government Cloud Computing Technology Roadmap Volume 1, High-Priority Requirements to Further USG Agency Cloud Computing Adoption.* NIST SP 500-293 highlights concerns around the protection and control of cloud Consumer data. This document introduces the NIST Cloud Computing Security Reference Architecture (NCC-SRA or, for the sake of brevity, SRA), providing a comprehensive formal model to serve as security overlay to the architecture described in NIST SP 500-292: *NIST Cloud Computing Reference Architecture.* This document also describes a methodology for applying a Cloud-adapted Risk Management Framework (CRMF) using the formal model and an associated set of *Security Components* (derived from the capabilities identified in the Cloud Security Alliance's Trusted Cloud Initiative – Reference Architecture [TCI-RA]) to orchestrate a secure cloud Ecosystem by applying the Risk Management Framework described in NIST SP 800-37 (Rev. 1): *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.*

The study upon which the NCC-SRA is based collected, aggregated, and validated data for a Public cloud, considering all three cloud service models – Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) – and all cloud Actors (i.e., Consumer, Provider, Broker, Carrier, and Auditor).While this document focuses on a Public cloud deployment model because it best supports illustrative examples of all of the NCC-SRA Security Components

and security considerations, the NCC-SRA (the formal model, the set of Security Components and the methodology for applying the CRMF) is agnostic with respect to cloud deployment model, and its methodology can easily be applied to Private, Community, or Hybrid clouds.

The NCC-SRA introduces a risk-based approach to determine each cloud Actor's responsibility for implementing specific controls throughout the life cycle of the cloud Ecosystem. Specifically, for each instance of the cloud Ecosystem, the security components are analyzed to identify the level of involvement of each cloud Actor in implementing those components. The ultimate objective of this document is to demystify the process of describing, identifying, categorizing, analyzing, and selecting cloud-based services for the cloud Consumer seeking to determine which cloud service offering most effectively addresses their cloud computing requirement(s) and supports their business and mission-critical processes and services in the most secure and efficient manner.

# 1 INTRODUCTION

The National Institute of Standards and Technology (NIST) has been tasked by the U.S. Chief Information Officer to provide technical leadership for US government (USG) agency efforts related to the adoption and development of cloud computing standards [11]. The goal is to accelerate the Federal government's adoption of *secure* and effective cloud computing solutions to reduce costs and improve services. The NIST strategy consists of two parts: (1) build a USG Cloud Computing Technology Roadmap that focuses on the highest priority USG cloud computing security, interoperability, and portability requirements; and (2) lead efforts to develop standards and guidelines in close consultation and collaboration with standards bodies, the private sector, and other stakeholders.

The NIST Cloud Computing Security Working group was created to achieve broad collaboration between Federal and private stakeholders in efforts to address the security-related concerns expressed by Federal managers. One of the tasks of the NIST Cloud Computing Working Group is to design a Cloud Computing Security Reference Architecture that supplements SP 500-292: *NIST Cloud Computing Reference Architecture (RA)* with a formal model and identifies the core set of *Security Components* recommended for building a successful and secure cloud computing Ecosystem. The document provides for an understanding of the security interdependencies of cloud services, Actors, and requirements that USG agency technical planning and implementation teams and agency procurement offices should identify and address in order to acquire cloud services with security levels that meets agency needs.

## 1.1 AUDIENCE

This document is designed to serve as a guide for USG agency technical planning and implementation teams. The intended audience for this document includes the following categories of individuals:

- System managers, executives, and information officers making decisions about cloud computing initiatives;
- Security professionals, including security officers, security administrators, auditors, and others with responsibility for information technology security;
- Information technology program managers concerned with security measures for cloud computing;
- Procurement officers responsible for acquisition of cloud computing resources and/or resources for cloud computing projects; and
- Users of Public cloud computing services.

The document presumes that readers possess a fundamental understanding of the NIST Risk Management Framework (RMF) described in NIST SP 800-37 (Rev. 1), risk-based assessment for IT systems, and cloud computing. Because of the evolving nature of security considerations in a

cloud computing environment, readers are encouraged to take advantage of the other resources referenced in this document, the majority of which are available on-line.

## 1.2  OBJECTIVES

In contrast, a primary focus of the cloud computing model is on the economic benefits of shared use that can provide higher-quality and faster services at a lower cost to users.  In the traditional, enterprise IT service delivery model, there is a significant emphasis on procuring, maintaining, and operating the necessary hardware and related infrastructure to support a given service. However, the migration of an agency's operations to a cloud computing environment does not inherently provide for the same level of security and compliance with USG mandates that were achieved in the traditional IT model.  A Consumer's ability to comply with any business, regulatory, operational, or security requirements in a cloud computing environment is a direct result of the service and deployment model adopted by the agency, the cloud architecture, and the deployment and management of the resources in the cloud environment.

Understanding the relationships and interdependencies between the different cloud computing deployment models and service models is critical to understanding the security risks involved in cloud computing. The differences in methods and responsibilities for securing different combinations of service and deployment models present a significant challenge for Consumers who need to perform a thorough risk assessment and accurately identify the security controls necessary to preserve the security level of their environment, operations, and data after migrating to the cloud.

The purpose of this document is to define a NIST Cloud Computing Security Reference Architecture (NCC-SRA) – a framework that:

- identifies a core set of Security Components that can be implemented in a Cloud Ecosystem to secure the environment, the operations, and the data migrated to the cloud;
- provides, for each Cloud Actor, the core set of Security Components that fall under their responsibilities depending on the deployment and service models;
- defines a security-centric formal architectural model that adds a security layer to the current NIST SP 500-292: *NIST Cloud Computing Reference Architecture*; and
- provides several approaches for analyzing the collected and aggregated data.

The document concludes with an illustrative example of securely orchestrating a Cloud Ecosystem for a Unified Messaging System (UMS) migrated to a Public Software as a Service (SaaS) cloud by introducing a Security Index System (SIS) for the confidentiality, integrity, and availability of each component in the process of prioritizing the implementation of the core set of Security Components.

The NCC-SRA is intended to be an elastic, dynamic framework that is layered over the NIST Reference Architecture and takes into account:

- The cloud computing service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS);

- The cloud deployment models: Public, Private, Community, and Hybrid;[2]
- The NIST RA's defined Actors: Consumer, Provider, Broker, Carrier, and Auditor.

The five Actors are the collaborating parties engaged in building a fully functional and secure cloud Ecosystem. The cloud Consumer performs a security and risk assessment for each use case of data migrated to the cloud. By electing the cloud deployment model and the service model, the Consumer identifies the cloud Ecosystem model and the corresponding instance of the NCC-SRA model that best suits its needs in terms of functionality, cost, and security capabilities.

The information provided in this document is presented in a manner that is familiar to Federal stakeholders (i.e., referencing NIST SP 800-37 (Rev. 1): *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, and NIST SP 800-53 (Rev. 4): *Security and Privacy Controls for Federal Information Systems and Organizations*) and to private sector organizations that offer cloud services (i.e., leveraging the Cloud Security Alliance's Trusted Cloud Initiative – Reference Architecture [CSA TCI-RA]).[3] In addition, this document supports a consistent, repeatable process for selecting and implementing the appropriate Security Components for different combinations of cloud service models and deployment methods, which can help agencies, avoid duplication of efforts and reduce costs.

The NCC-SRA document is not a comprehensive guide to security requirements for all possible instances of cloud type, data, and service model. Rather, the NIST document aims to identify only a core set of Security Components that should be implemented by each Cloud *Actor* defined in the NIST RA specification.

1.3    **SCOPE**

This document describes the components of the NCC-SRA, specifically:

- A formal model;

- A set of Security Components that leverages the CSA TCI-RA; and

---

[2] See NIST SP 800-145: *The NIST Definition of Cloud Computing* for detailed explanations of service and deployment models [14]. The illustrative examples in this document assume a Public cloud, but the framework described can be used for Private, Community, and Hybrid clouds as well.

[3] Available at https://research.cloudsecurityalliance.org/tci/

- A methodology for applying, from the Consumer's perspective, a Cloud-adapted Risk Management Framework (CRMF) for securing a cloud-based service. The CRMF is derived from the NIST Risk Management Framework as described in NIST SP 800-37 (Rev. 1): *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.*

This document collects, aggregates, and validates data for a Public cloud deployment model, with all three service models (SaaS, PaaS, and IaaS) and all cloud Actors. This focus on a Public cloud deployment model is for purposes of example only as it best supports illustrative examples of all of the NCC-SRA Security Components and security considerations. The NCC-SRA (the formal model, the set of Security Components, and the methodology for applying CRMF) is agnostic with respect to cloud deployment model, and its methodology can easily be applied to data and operations hosted in Public, Private, Community, or Hybrid clouds.

## 1.4   STRUCTURE OF THE DOCUMENT

This document is organized into four sections supported by six annexes that present the reader with a logical (and, when necessary, step-by-step) methodology for evaluating cloud-based services using a Risk Management Framework (RMF) approach.

**Section 2** presents a comprehensive overview of the NCC-SRA, of the RMF as outlined in NIST SP 800-37 (Rev. 1): *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, and the assumptions and clarifications regarding the responsibilities and roles of cloud Actors for the purposes of this document.

**Section 3** outlines the data analysis methodology used to populate the responsibility matrix (shown in **Annex D**), which assigns accountability for implementing each Security Component to a particular Actor or set of Actors for a Public cloud in all three service models. The core set of Security Components is derived from the Cloud Security Alliance's TCI-RA. This section also discusses data collection, aggregation, and validation as initial steps in the data analysis methodology, and maps the derived Security Components from the matrix to the NIST SP 800-53 (Rev. 4): *Security and Privacy Controls for Federal Information Systems and Organizations* security control families. The data analysis methodology is completed by illustrating the generation of a heat map with a cloud Actor-centric view (e.g. Consumer, Provider) based upon the data aggregated for a Public cloud and all service models (IaaS, PaaS, and SaaS). The Heat map highlights the level of control exerted by each of the cloud Actors.

**Section 4** introduces the NIST Security Architecture formal model and discusses the *Architectural Components* of the model for each cloud Actor.

**Section 5** describes the orchestration of a secure cloud Ecosystem as defined by interactions between the cloud Actors for implementing and integrating the Security Components. To better illustrate the interactions among cloud Actors and their roles and responsibilities in orchestrating a

cloud Ecosystem, the section provides a use case example – a generic USG agency service migrated to the cloud – and highlights the necessary steps to secure the cloud Ecosystem and to determine the high-level cloud architecture that meets the cloud Consumer's security requirements. This section concludes with the negotiation of the contractual terms and agreements in Service Level Agreements (SLAs).

**Annex A** depicts the core set of Security Components and how to use it for a particular cloud deployment model (Public cloud in this case), described in detail in **Sec. 5**.

**Annex B** depicts how the Security Components are mapped or paired to the NIST SP 800-53 (Rev. 4): *Minimum Security Requirements for Federal Information and Information Systems* security control families using the color code presented in **Table 3**.

**Annex C** is the Generic Heat Map of cloud Actor responsibilities for implementing Security Components and associated security controls in a cloud Ecosystem.

**Annex D** presents the Data Aggregation table, which indicates the shared responsibility of cloud Actors to apply Security Components and control measures to varying degrees (i.e., least responsible, solely responsible, shared responsibility) at the Service-based Ecosystem level.

**Annex E** presents a matrix that maps the high-level security components, and with them the NIST SP 800-53 (Rev. 4): *Security and Privacy Controls for Federal Information Systems and Organizations* security control families, to the Architectural Components and Sub-Components defined for each cloud Actor.

**Annex F** presents the Security Index System (SIS) for the Confidentiality, Integrity, and Availability (C/I/A) security triad and the Aggregated Security Index System (ASIS) used to prioritize the Security Components for the Unified Messaging System (UMS) use case. The SIS example given in this document is merely illustrative: it should not be considered guidance for any UMS migration to the cloud.

## 1.5 USING THE DOCUMENT

Federal agencies may use the information presented in this document to help them follow the steps presented below when migrating a service to the cloud.

- **Describe** the service that should be migrated to the cloud
- **Identify** the necessary capabilities of the service
- **Categorize** the Information System to determine the impact levels and the Security Components and associated security control baselines (three sets of baseline controls corresponding to low-impact, moderate-impact, and high-impact information systems).

Baseline controls are chosen based on the security category and associated impact level of information systems determined in accordance with Federal Information Processing Standard (FIPS) 199: *Standards for Security Categorization of Federal Information and Information Systems* and FIPS 200: *Minimum Security Requirements for Federal Information and Information Systems*, respectively [16][17].

- **Analyze and select** the most appropriate instance of a cloud Ecosystem by identifying the cloud composite architecture, such as the cloud deployment and service models:
  - o Public IaaS, Public PaaS, Public SaaS;
  - o Private IaaS, Private PaaS, Private SaaS;
  - o Hybrid IaaS, Hybrid PaaS, Hybrid SaaS;
  - o Community IaaS, Community PaaS, and Community SaaS.
- **Identify** the cloud Actors involved in orchestrating the Cloud Ecosystem (e.g., type of Provider and Broker)
- **Tailor** the baseline Security Components to fulfill the security requirements for the particular use case (i.e., system migrated to the cloud) by:
  - o Identifying and customizing the core set of Security Components to the assessed impact level of the system migrated to the cloud by applying a SIS as described in **Sec. 5.2.2.1**;
  - o Identifying the NIST SP 800-53 (Rev. 4): *Security and Privacy Controls for Federal Information Systems and Organizations* security controls necessary for each Security Component;
  - o Applying scoping considerations to the remaining baseline Security Components and associated controls;
  - o Identifying, when necessary, additional compensating Security Components and security controls;
  - o Assigning specific values to organization-defined security parameters via explicit assignment and selection statements;
  - o Supplementing baselines with additional Security Components and control enhancements, if needed; and
  - o Providing additional specification information for Security Components implementation.

**Sec. 5.2** provides a more concrete example of how a new cloud Ecosystem for a UMS can be orchestrated by leveraging the information presented in this document.

## 2  BACKGROUND

This document presents the NIST Cloud Computing Security Reference Architecture formal model derived from NIST SP 500-292: *NIST Cloud Computing Reference Architecture*, an associated set of Security Components derived from the CSA TCI-RA, and a methodology for using the formal model and the security components to orchestrate a secure cloud Ecosystem.

### 2.1   REVIEW OF THE FEDERAL CLOUD COMPUTING STRATEGY

In the *Federal Cloud Computing Strategy* published in 2011, U.S. Chief Information Officer Vivek Kundra advises that Federal agencies "should make risk-based decisions which carefully consider the readiness of commercial or government providers to fulfill their Federal needs.  These can be wide-ranging, but likely will include: security requirements, service and marketplace characteristics, application readiness, government readiness, and program's stage in the technology lifecycle" [12].

The approach to securing a cloud Ecosystem is intrinsically related to the cloud computing service model (SaaS, PaaS, or IaaS) and to the deployment model (Public, Private, Hybrid, or Community) that best fits the Consumer's business missions and security requirements.  As previously stated, for each use case of data migrated to the cloud, it is necessary for the Consumer to evaluate the particular security requirements in the specific cloud architectural context, and to map them to proper security controls and practices in technical, operational, and management classes.  Even though the Cloud Security Reference Architecture inherits a rich body of knowledge of general network security and information security, both in theory and in practice, it also addresses the cloud-specific security requirements triggered by characteristics unique to the cloud, such as:

- Broad network access,
- Decreased visibility and control by consumers,
- Dynamic system boundaries and comingled roles/responsibilities between consumer and provider,
- Multi-tenancy,
- Data residency,
- Measured service, and
- Significant increase in scale (on demand), dynamics (elasticity, cost optimization), and complexity (automation, virtualization).

The above-listed cloud computing characteristics often present an agency with security risks that are different from those in traditional information technology solutions.  To preserve the pre-migration security level of their data once it has been moved to the Cloud, agencies need the ability to identify all cloud-specific risk-adjusted security controls or components in advance and request from the cloud Providers through contractual means and SLAs that all Security Components are identified and controls fully and accurately implemented.

## 2.2 APPROACH

**Figure 1** below depicts the NCC-SRA approach described in detail in this document.
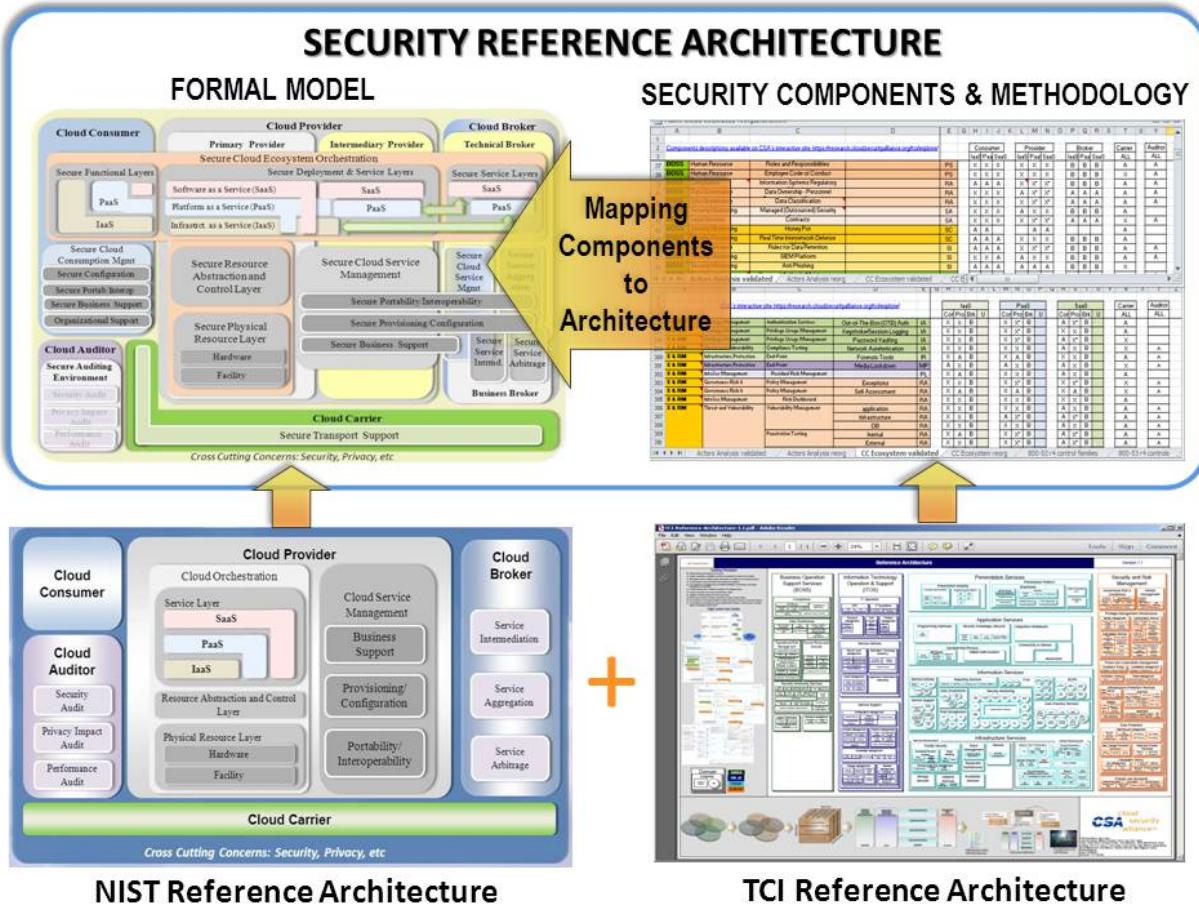


**Figure 1:** NIST Cloud Computing Security Reference Architecture Approach

The NCC-SRA is based on a three-dimensional approach using the following constructs:

- The three types of service models defined in the NIST RA: IaaS, PaaS, and SaaS;
- The four types of deployment models defined in the NIST RA: Public, Private, Hybrid, and Community; and
- The five Actors defined in the NIST RA: Provider, Consumer, Broker, Carrier and Auditor.

All of the aforementioned constructs are defined in **Sec. 2.4**.

As introduced in **Fig. 1** above, the NCC-SRA provides a formal model, a set of Security Components, and a methodology for using this information to orchestrate a secure cloud Ecosystem. The NCC-SRA formal model was derived from the NIST SP 500-292: *NIST Cloud Computing Reference Architecture*, and is described in detail in **Sec. 3**.

The NCC-SRA also provides a set of Security Components deemed important in securing the data and operations of a Cloud Computing Ecosystem. In defining this set, the document leverages the CSA TCI-RA shown in **Annex A**. The set of Security Components and guidance on how to use them for a particular cloud model is introduced in detail in **Sec. 3**.

The NCC-SRA is presented using a cloud Ecosystem that can be constructed employing all possible combinations of the four deployment models with the three service models. These combinations result in the following twelve instances of cloud architectures:

- Public IaaS, Public PaaS, Public SaaS;
- Private IaaS, Private PaaS, Private SaaS;
- Hybrid IaaS, Hybrid PaaS, Hybrid SaaS;
- Community IaaS, Community PaaS, and Community SaaS.

The NCC-SRA (the formal model, the set of Security Components and the methodology for applying cloud-adapted Risk Management Framework) is agnostic with respect to cloud deployment model, and its methodology can easily be applied to data pertaining to Private, Community, or Hybrid clouds. For purposes of example, this document describes the approach using a Public cloud deployment model because it best supports illustrative examples of all of the NCC-SRA Security Components and security considerations.

The NCC-SRA introduces a risk-based approach to determine each cloud Actor's responsibility for implementing specific controls throughout the life cycle of the cloud Ecosystem. Specifically, for each instance of the cloud Ecosystem, the Security Components are analyzed to identify the level of involvement of each cloud Actor in implementing those components. The ultimate objective of this document is to demystify the process of describing, identifying, categorizing, analyzing, and selecting cloud-based services for the cloud Consumer seeking to determine which cloud service offering most effectively addresses their cloud computing requirement(s) and supports their business and mission-critical processes and services in the most secure and efficient manner.

**Figure 2,** below provides a graphical representation of the NCC-SRA three-dimensional approach that leads to the twelve cloud instances for which data is collected, aggregated, and analyzed for each cloud type.
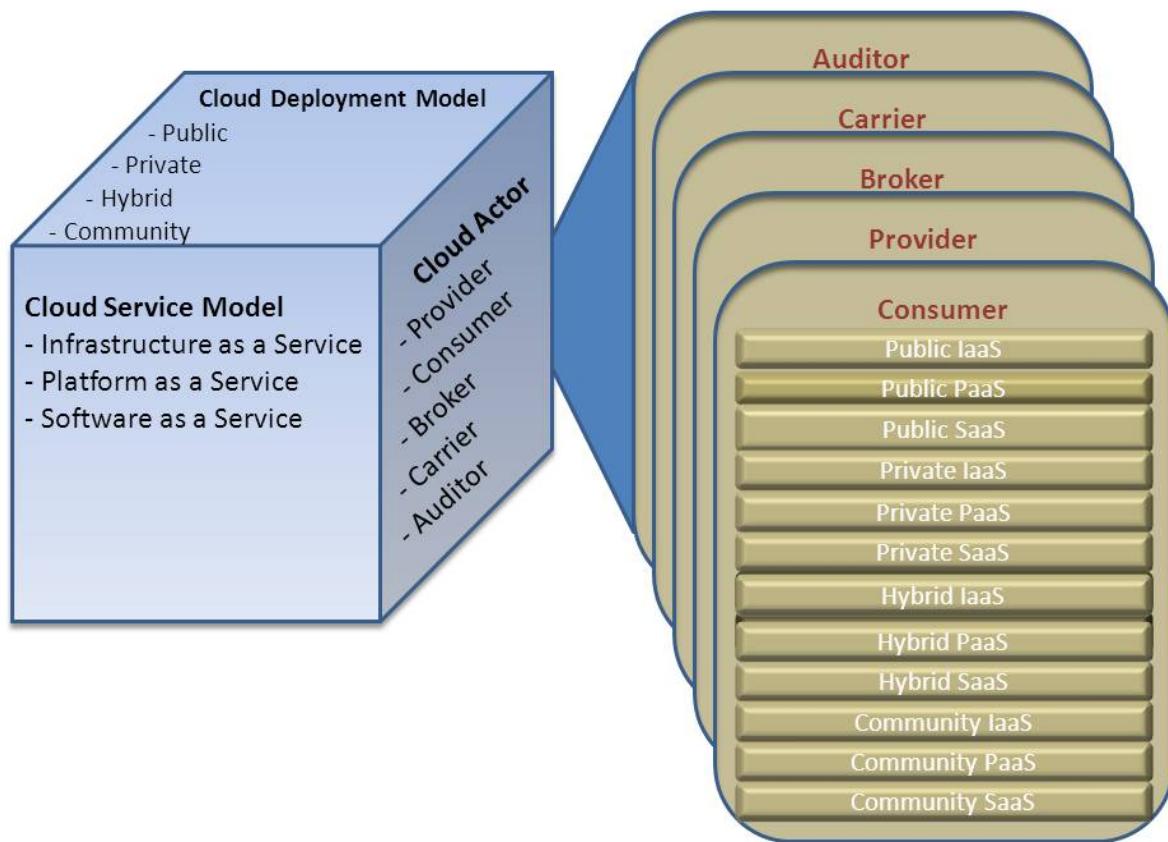
**Figure 2: Security Reference Architecture Constructs and Instances**

For each instance of the cloud Ecosystem, the Security Components are analyzed to identify the level of involvement of each cloud Actor in implementing the core set of Security Components.

Collected data for each instance are then validated and aggregated to illustrate the core set of Security Components from (1) the cloud Actor perspective, highlighting the way in which responsibilities change with the service model or (2) from the cloud Ecosystem perspective, highlighting the shifting of responsibilities among cloud Actors. Detailed information can be found in the sections to follow, starting with **Sec. 4**.

By providing in this document a common core set of Security Components for each instance of the cloud Ecosystem, and by defining a formal model agnostic of the deployment mode or service model with a set of *Architectural Components* to which the Security Components are mapped, the SRA is intended to aid an organization that elects to migrate services to the Cloud in architecting and securing their cloud Ecosystem and identifying each cloud Actor's responsibilities in implementing the necessary Security Components and associated security controls.

## 2.3 **RISK MANAGEMENT**

All Federal information systems must undergo an Assessment and Authorization (A&A) process to determine whether they comply with FISMA and Office of Management and Budget (OMB) Circular A-130, Section 8b (3), *Securing Agency Information Systems* requirements in addition to any other applicable requirements [6][18].  FISMA and OMB Circular A-130 also require any entities operating systems on behalf of the Federal government – including cloud Providers – to meet the same security and privacy requirements as Federal agencies.  Security and privacy requirements for cloud Providers, including the security and privacy controls for information systems processing, storing, or transmitting Federal information, are expressed in appropriate contracts or other formal agreements using the RMF and associated NIST security standards, special publications, and guidelines.

NIST SP 500-293 (Vol. 1): *U.S Government Cloud Computing Technology Roadmap* identifies in Requirement 2 "the need to demonstrate that the required level of protection of Federal data can be provided in the cloud environment in order to inspire confidence and trust to a level where security is not perceived to be an impediment to the adoption of cloud computing."  The document also emphasizes that the "cloud Provider and the cloud Consumer have differing degrees of control over the computing resources in a cloud system." Therefore the implementation of the security requirements becomes a shared or split responsibility among cloud Actors [1].

The assurance or confidence that the risk presented by using cloud services is at an acceptable level depends on the trust that the organization places in the external cloud Provider and Broker, when involved in the orchestration of the cloud Ecosystem.

This Risk Management process ensures that issues are identified and mitigated early in the investment cycle with routine and periodic reviews.  In addition, the CIO Council maintains a library[4] of helpful online documentation for agencies, including a best practices guide for Creating Effective Cloud Computing Contracts for the Federal Government.

### 2.3.1    THE RISK MANAGEMENT FRAMEWORK

The Risk Management Framework (or RMF), illustrated in **Fig. 3** below, provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle.  For each identified Step, there is at least one standard that provides guidance: these are also identified in the graphic.

---

[4]   https://cio.gov/resources/document-library/
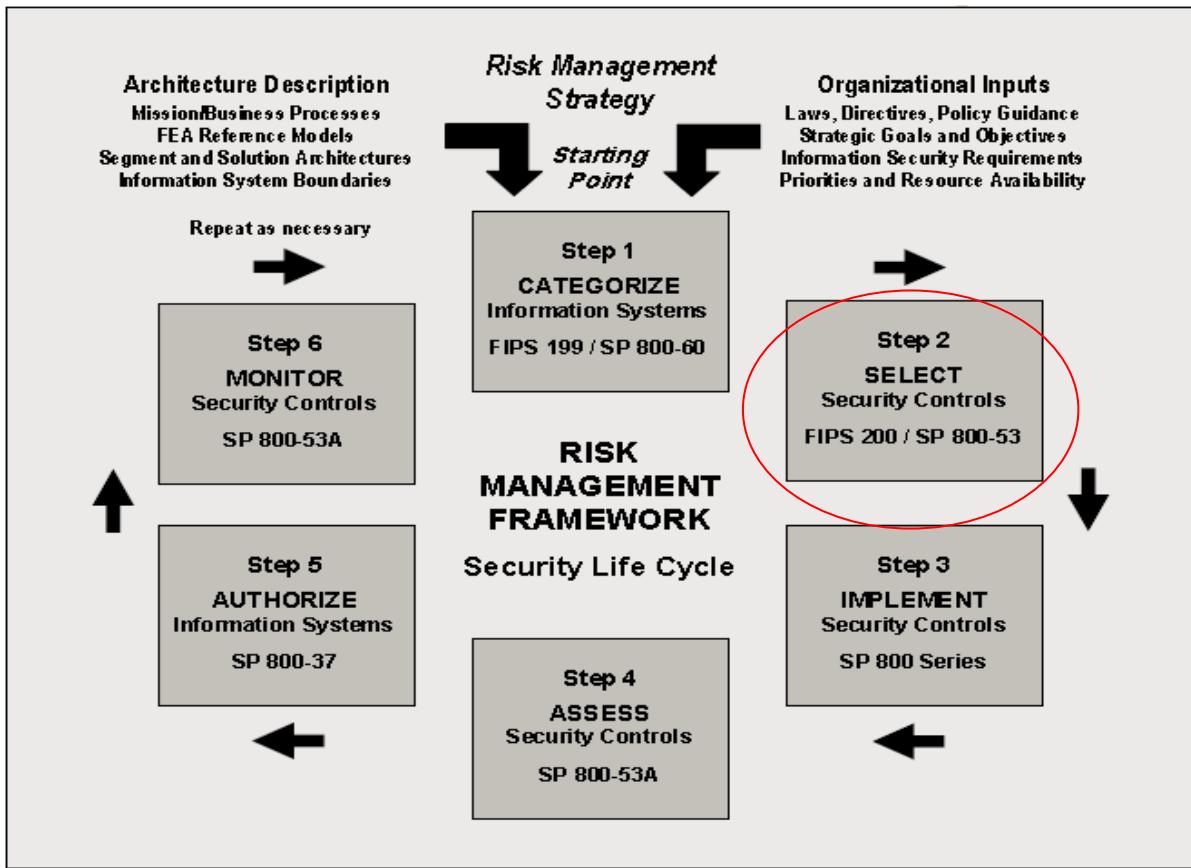
**Figure 3:** Risk Management Framework (NIST Special Publication 800-37 Rev 1.)

The RMF is also consistent with the National Strategy for Trusted Identities in Cyberspace (NSTIC) Identity Ecosystem as it develops. This Identity Ecosystem is intended to provide a user-centric online environment, with a set of technologies, policies, and agreed-upon standards for cloud-based transactions, ranging from anonymous to fully authenticated and authorized. The NSTIC program is actively working across industry, academia, and government to raise the level of trust associated with identities involved in online transactions. Solutions developed through the NSTIC effort may also strengthen a Cloud Ecosystem by addressing certain authentication, authorization, and privacy issues in the Cloud.

The six main steps in the NIST Risk Management Framework as described in NIST SP 800-37 (Rev. 1): Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach are:

**Step 1: Categorize** the information system and the information processed, stored, and transmitted by that system based on an impact analysis. FIPS 199: Standards for Security Categorization of Federal Information and Information Systems provides security categorization guidance for non-

national security systems. NIST SP 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories provides implementation guidance on the assignment of security categories to information and information systems. CNSSI 1253: Security Categorization and Control Selection for National Security Systems provides similar guidance for national security systems.

The RMF categorization step, including consideration of legislation, policies, directives, regulations, standards, and organizational mission/business/operational requirements, facilitates the identification of security requirements.

**Step 2: Select** an initial set of baseline security controls for the information system based on the security categorization, tailoring, and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions. FIPS 200: Minimum Security Requirements for Federal Information and Information Systems provides the minimum required (i.e., baseline) security controls for low-, moderate-, and high-security systems. NIST SP 800-53 (Rev. 4): Minimum Security Requirements for Federal Information and Information Systems provides security control selection guidance for non-national security systems. CNSSI 1253: Security Categorization and Control Selection for National Security Systems provides similar guidance for national security systems.

**Step 3: Implemen**t the security controls and describe how the controls are employed within the information system and its operating environment. NIST SP 800-70 (Rev. 2): National Checklist Program for IT Products—Guidelines for Checklist Users and Developers provides guidance for the users and developers of security configuration checklists.

**Step 4: Assess** the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. NIST SP 800-53A (Rev. 1): Guide for Assessing the Security Controls in Federal Information Systems and Organizations provides security control assessment procedures for security controls defined in NIST SP 800-53 (Rev. 4): Minimum Security Requirements for Federal Information and Information Systems.

**Step 5: Authorize** information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable. NIST SP 800-37 (Rev. 1): Guide for Applying the Risk Management Framework to Federal Information Systems provides guidance on authorizing an information system to operate.

**Step 6: Monitor** the security controls in the information system on an ongoing basis, including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials. NIST SP 800-37 (Rev. 1): Guide for Applying the

[Risk Management Framework to Federal Information Systems](#) provides guidance on monitoring the security controls in the environment of operation, the ongoing risk determination and acceptance, and the approved information system authorization to operate status.  [NIST SP 800-53A (Rev. 1): Guide for Assessing the Security Controls in Federal Information Systems and Organizations](#) provides continuous monitoring guidance for the security controls defined in [NIST SP 800-53 (Rev. 4): Minimum Security Requirements for Federal Information and Information Systems](#).

The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations.  While the framework is flexible and easily adaptable in most cases, it assumes a traditional IT environment, and requires some customization to address the unique characteristics of cloud-based services.  The "Cloud-adapted RMF," or CRMF, which closely parallels the original RMF, highlights the following six steps:

**Step 1**: **Categorize** the information system or service migrated to the cloud, and the information processed, stored, and transmitted by that system based on an impact analysis.  This step is very similar to the traditional Step 1 of the RMF, as described above.

**Step 2**: **Identify** security requirements for the information system or service migrated to the cloud, and perform a risk assessment – including a Confidentiality, Integrity, and Availability (C/I/A) analysis – to identify the Security Components that are appropriate for the system. Select the baseline Security Controls.

**Step 3**: **Select** the cloud Ecosystem architecture that best fits the analysis performed in Step 2 for the information system or service migrated to the cloud.

**Step 4**: **Assess** Service Provider(s) based on their Authorization-To-Operate (ATO). Identify the Security Controls needed for the cloud-based information system or service already implemented by the cloud Provider, and negotiate the implementation of the additional Security Components and Controls identified as necessary for this system or service. When applicable, identify the Security Controls that remain within the cloud Consumer's responsibility, and implement them.

**Step 5**: **Authorize** the use of the selected cloud Provider (and cloud Broker, when applicable) for hosting the cloud-based information system or service. Negotiate a Service Agreement (SA) and SLA that reflects the negotiation performed in Step 4.

**Step 6**: **Monitor** the cloud Provider (and the cloud Broker when applicable) to ensure that all SA and SLA terms are met and that the cloud-based information system maintains the necessary security posture. Directly monitor the Security Components and associated Controls under the cloud Consumer's direct responsibility.

The NCC-SRA provides the most comprehensive support for Step 2. This approach will enable agencies to systematically identify their common, hybrid, and system-specific security controls and other security requirements to procurement officials, Cloud Brokers, Providers, and Carriers. This document also provides information regarding each cloud Actor's responsibilities, for each cloud deployment model and service model, in applying each identified Security Component as outlined in this document. Our approach of leveraging the TCI-RA capabilities for defining a core set of Security Components that is then used to perform a risk assessment and to identify the Security Index values for the C/I/A triad prior to selecting the NIST SP 800-53 (Rev. 4): *Minimum Security Requirements for Federal Information and Information Systems* security controls appropriate for the system might appear, at first, convoluted or unjustified. However, by centering the system's analysis and the risk assessment on the cloud capabilities and the core set of Security Components, the approach provides a mechanism for prioritizing the implementation of the security controls based upon the results of the C/I/A analysis.

For example, a Consumer planning the migration of their particular agency's data to a Public IaaS cloud may, upon completion of the risk assessment analysis, follow the steps presented in **Sec. 5** to identify the Security Components that must be implemented to secure their data. This is accomplished by leveraging the Security Components identified in this document for a Public IaaS cloud. The set of Security Components would be a union of the sets assigned in this document to each cloud Actor for the cloud instance of interest (see **Annex A**), augmented, as needed, with additional Security Components and controls for the particular data and/or application(s) migrated to the cloud.

### 2.3.2   MANAGING THE RISK INHERENT IN CLOUD SERVICES

Starting with June 6, 2014, USG agencies are required to accept only cloud Providers that have been assessed and authorized through the Federal Risk and Authorization Management Program (FedRAMP) and have received a FedRAMP Provisional ATO issued by the Joint Authorization Board (JAB) [5]. FedRAMP is a government-wide program that provides a standard framework for assessing and authorizing cloud service vendor using a standardized approach to security assessment, authorization, and continuous monitoring, similar to the A&A process used to assess Federal agencies for compliance with applicable mandates. The purpose of this process is to assess whether a cloud vendor adheres to the minimum mandated security requirements for Federal

---

[5]   It is important to note that Federal Agencies can grant a FedRAMP ATOs directly as long as they use a FedRAMP security package. When using the services of a third-party, independent Assessor (3PAO) accredited by FedRAMP to A&A, the Agency may submit the A&A package to JAB to obtain a FedRAMP Provisional Authorization. FedRAMP will maintain a secure repository of all assessed and authorized cloud service providers, clearly listing if a security package was assessed by FedRAMP JAB or a Federal Agency. When a Federal Agency leverages a FedRAMP Provisional ATO, the Agency remains responsible to review the package and to issue their internal ATO prior to using the provider's services. See http://www.gsa.gov/portal/category/102999 for more information.

agencies and implements the identified security controls for low- and moderate-impact systems as described in FIPS 199: *Standards for Security Categorization of Federal Information and Information Systems* and FIPS 200: *Minimum Security Requirements for Federal Information and Information Systems* [16][17].

FedRAMP authorizes third parties to conduct these assessments, which are conducted against criteria for baseline and specifically-defined security controls defined in NIST SP 800-53 (Rev. 4): *Security and Privacy Controls for Federal Information Systems and Organizations*. FedRAMP's set of security controls are also aligned with NIST SP 800-37: *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. FedRAMP itself issues ATO to Providers once the assessment has been completed. Cloud Consumers may consider the ATO proof of proper implementation of the security controls assessed by FedRAMP, and negotiate only the implementation of the additional Security Components that are deemed necessary for the specific cloud-based service.

FedRAMP maintains an online site with requirements, templates, and supporting materials for agencies and cloud vendors at http://www.FedRAMP.gov.

Federal agencies are responsible and accountable for the information security risk incurred by the use of information system services offered by external suppliers, including cloud Providers and cloud Brokers. The CRMF provides a structured, yet flexible approach for managing the portion of risk resulting from the incorporation of cloud-based information systems into the mission and business processes of the organization. Consumers can require cloud Providers to implement all steps in the RMF process. The only exception is the security authorization step, as that remains an inherent Federal responsibility that is directly linked to the management of risk related to the use of cloud services.

The CRMF can be used to address the security risks associated with cloud systems by incorporating it into the terms and conditions of the contracts with external cloud Providers and cloud Brokers. Performance aspects of these terms and conditions are also incorporated into the SLA, which is an intrinsic part of the SA between the cloud Consumer and cloud Provider and/or Broker. Contractual terms should include, for example, guarantees of the Consumer's timely access to or Provider's timely delivery of cloud audit logs, continuous monitoring logs, and any user access logs. More information will be provided in **Sec. 5.2.4** of this document.

Based upon the deployment model and the service type elected, the agency would retain and take it upon themselves to implement the set of the Security Components identified for the Consumer, augmented with the supplemental set specific to the Consumer's use case. For example, the agency may require in the SLA (and other appropriate contractual documents) that a Public IaaS Provider implement the associated Security Components identified in the NCC-SRA, augmented with use-case specific supplemental Security Components and controls.

USG cloud Consumers should also require cloud Providers and Brokers to present appropriate evidence that demonstrates their compliance with the RMF in protecting Federal information. It is important to emphasize that, while the six steps of the CRMF listed in **Sec. 2.3.1** cover the entire Life Cycle of cloud-based information systems, this document is primarily focused on Step 2 and only provides pointers for the other steps.

## 2.4    ASSUMPTIONS, CLARIFICATIONS AND DEFINITIONS

This section clarifies the roles and responsibilities of the cloud Actors described in NIST SP 500-292: *NIST Cloud Computing Reference Architecture*, and lists the assumptions made regarding their core operational responsibilities with associated security requirements.

### 2.4.1    CLOUD COMPUTING SERVICE AND DEPLOYMENT MODELS

The definitions of service models and deployment models below come from NIST SP 800-145: *The NIST Definition of Cloud Computing* [14].

#### 2.4.1.1 SERVICE MODELS

*Service models* describe, broadly, what type of service the cloud provides to Consumers: an application, a programming platform, or raw computing resources. In the cloud computing Ecosystem, the cloud Consumer has three different service models to choose from: SaaS, PaaS, and IaaS.

**Figure 4** below presents some examples of cloud services available to a cloud Consumer (For more details, see NIST SP 500-292: *NIST Cloud Computing Reference Architecture*, **Appendix B**).

In an IaaS deployment, the capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

In a PaaS deployment, the capability provided to the Consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming, libraries, services, and tools supported by the Provider. The 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 configuration settings for the application-hosting environment.
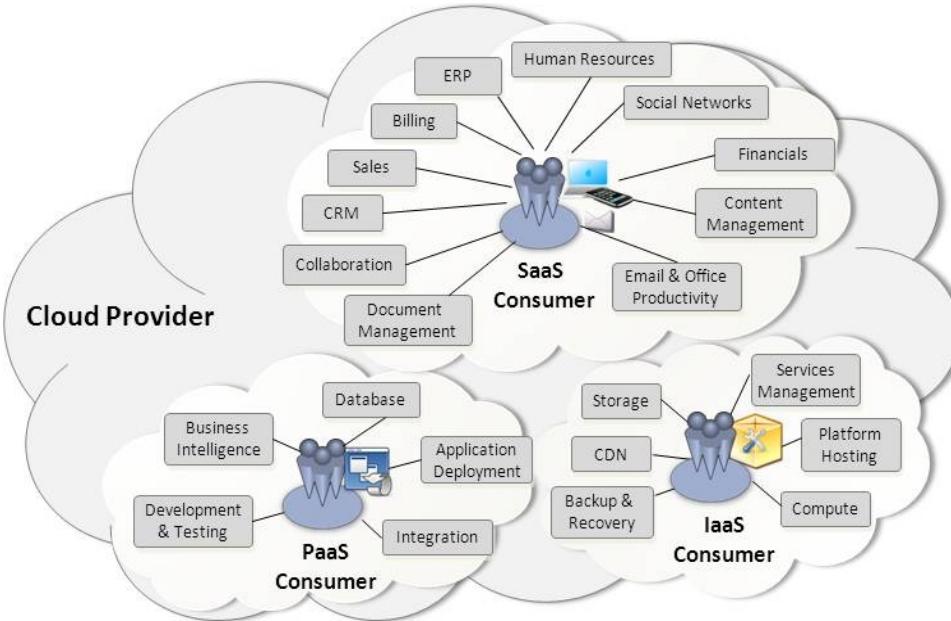
**Figure 4: Example of Services Available to a Cloud Consumer (NIST SP 500-292)**

In a SaaS deployment, the capability provided to the Consumer is to use the Provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The 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.

**2.4.1.2** DEPLOYMENT MODELS

*Deployment models* describe the relationship between the cloud Provider and cloud Consumer(s) – for example, the Consumer may be one of many entities using a Provider's cloud service, it may have sole access to a particular service, or it may own and operate its own cloud. There are four cloud deployment models: Public, Private, Community, and Hybrid.

In a *Public* cloud, the cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

In a *Private* cloud, the cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple Consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

In a *Community* cloud, the cloud infrastructure is provisioned for exclusive use by a specific community of Consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

In a *Hybrid* cloud, the cloud infrastructure is a composite of two or more distinct cloud infrastructures (Private, Community, or Public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

### 2.4.2 CLOUD ECOSYSTEM

When cloud services are procured by Federal agencies (acting in the role of Consumer), it is the cloud Consumer's responsibility to determine the set of Security Components and associated controls required to protect data migrated to the cloud and to determine and/or approve the manner in which selected Components and controls are implemented. If the Consumer cannot directly implement selected security controls, then the responsibility for implementation is shared with other Actors in the Ecosystem, most notably the cloud Provider and cloud Broker. While the responsibility for implementation may not rest solely with the Consumer, it is ultimately the Consumer's responsibility to specify what controls must be put in place and to provide oversight and accountability for the security of the cloud Ecosystem.
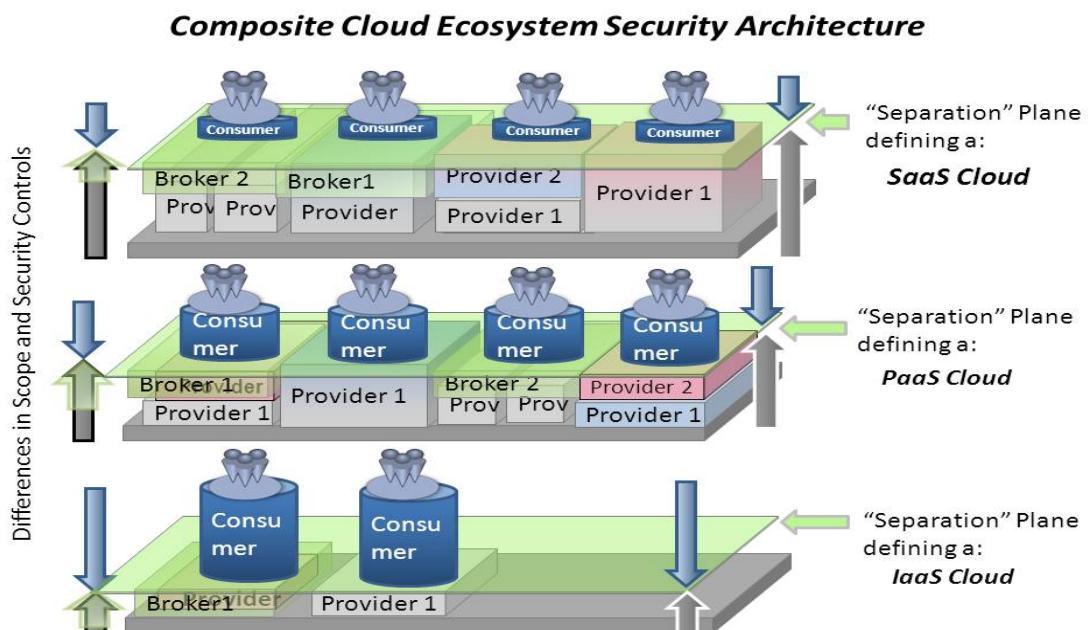


**Figure 5:** Composite Cloud Ecosystem Security Architecture

**Figure 5** presents an illustration of a composite cloud Ecosystem Security Architecture that graphically depicts the cloud Actors involved in orchestrating a cloud Ecosystem. The graphic also presents different possible compositions for each cloud service model.

The diagram illustrates the two types of Providers and two types of Brokers based on the roles played by these cloud Actors in the cloud orchestration. The role of transporting data within the cloud is assigned by NIST SP 500-292: *NIST Cloud Computing Reference Architecture* to the cloud Provider, leaving the cloud Carrier with the role and responsibility of securely transporting the data in transit between the end-user and the Cloud. Additional assumptions and clarifications are provided in the following sub-sections for each cloud Actor.

It is important to note that the cloud Carrier involved in the cloud Ecosystem is not represented in the diagram because the service provided by the Carrier (i.e., data transport) can be accomplished using different vehicles from dedicated communication channels to the open Internet that involve multiple Internet Service Providers and the backbone network operators. This complexity makes it difficult to illustrate the cloud Carrier in the composite cloud Ecosystem architecture in a single location in the diagram, or using only one graphical form, without misleading the audience or misrepresenting the cloud Carrier's role. However, it is important to highlight that the cloud Carrier role is critical to the functioning of the cloud Ecosystem. In a cloud Ecosystem that serves the needs of USG organizations, it is the Consumer's (i.e., agency's) responsibility to identify, based upon the risk analysis performed, the full set of security controls that must be mandated and implemented to secure the operations and data migrated to the cloud, and implement those security controls that fall directly under its area of responsibility. It is also the Consumer's responsibility to determine/identify the subset of security controls that fall under Broker, Carrier and Provider responsibilities, based on the type of cloud Ecosystem used. The union of all subsets of security controls must result in a combined set that can fully secure the cloud Ecosystem.

It is the responsibility of all cloud Actors involved in orchestrating a cloud Ecosystem, and in providing technical services, to ensure they address the cloud Consumers' areas of concern regarding:

- Risk Management
  - Risk Analysis
  - Risk Assessments
  - Vulnerability Assessments
  - Incident Reporting and Response
- Business Continuity
  - Disaster recovery plans
  - Restoration plan incorporating and quantifying the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for services
- Physical Security
  - Physical and Environmental Security Policy

- o Contingency Plan
- o Emergency Response Plan
- o Facility Layout
- o Security Infrastructure
- o Human Resources
- o Environmental Security
- o Visual inspection of the facility
- User Account Termination Procedures
- Compliance with National and International/Industry Standards on Security
- Transparent view of the security posture of the cloud Providers, Brokers, and Carriers.

### 2.4.3 CLOUD CONSUMER

A Cloud Consumer is the entity that maintains a business relationship with, and uses services from, cloud Providers, cloud Brokers, and cloud Carriers.

A cloud Consumer browses the service catalog from a cloud Provider or cloud Broker, requests the appropriate service(s), and sets up service contracts with the cloud Provider (either directly or through a cloud Broker) before effectively using the service. The Consumer may set up Carrier services separately, or use the Carrier services integrated into the offering of the cloud Provider/Broker.

The cloud Consumer may be billed for the service provisioned, and needs to arrange payments accordingly. Cloud Consumers use SLAs to specify the technical performance requirements that must be fulfilled by a cloud Provider and/or cloud Broker.

As previously described, if the cloud Consumer is a USG agency, it is ultimately accountable for the security of data and/or applications held by the cloud Provider on the Consumer's behalf. The migration of any operations to the Cloud does not void the mandate of compliance with FISMA and OMB directives. Therefore, it behooves any USG agency using cloud services to identify the set of security controls required to protect its assets in the cloud. The security controls should then be implemented by the cloud Consumer, cloud Provider, cloud Carrier, and cloud Broker as applicable. Any cloud Provider, Carrier, or Broker handling Federal information or operating information systems on behalf of the Federal government must meet the same security requirements as the source Federal agency. The security requirements also apply to external subsystems storing, processing, or transmitting Federal information and any services provided by, or associated with, the subsystem.

### 2.4.4 CLOUD PROVIDER

A cloud Provider is the entity responsible for making a service available to cloud Consumers (either directly or indirectly via a Broker). A cloud Provider acquires and manages the computing

infrastructure required for providing the services, runs the cloud software that provides the services (at least for SaaS and PaaS service deployments), and makes arrangements to deliver the cloud services to the cloud Consumers through network access.

A cloud Provider's activities can be sorted into five major categories:

- Service deployment
- Service orchestration
- Service management
- Security
- Privacy

From a strictly technical perspective, Providers could offer their services directly to Consumers or to Technical Brokers that extend or enhance the Provider's services by adding an additional layer of functionality in a transparent way (see **Sec. 2.4.5** for more information).  **Figure 5** above depicts the two major types of Providers, discussed below:

1. Primary Provider (labeled "Provider 1" in the Cloud Composite Architecture); and
2. Intermediary Provider (labeled "Provider 2" in the Cloud Composite Architecture).

### 2.4.4.1 PRIMARY CLOUD PROVIDER EXAMPLE

A Primary Provider offers services hosted on infrastructure that it owns.  It may make these services available to Consumers through a third party (such as a Broker or Intermediary Provider), but the defining characteristic of a Primary Provider is that it does not source its service offerings from other Providers.

### 2.4.4.2 INTERMEDIARY CLOUD PROVIDER EXAMPLE

An Intermediary Provider has the capability to interact with other cloud Providers without offering visibility or transparency into the Primary Provider(s).  An Intermediary Provider uses services offered by a Primary Provider(s) as invisible components of its own service, which it presents to the customer as an integrated offering (as shown in the simple illustrated example provided by **Fig. 6** below).  From a security perspective, all security services and components required of a Primary Provider are also required of an Intermediary Provider.
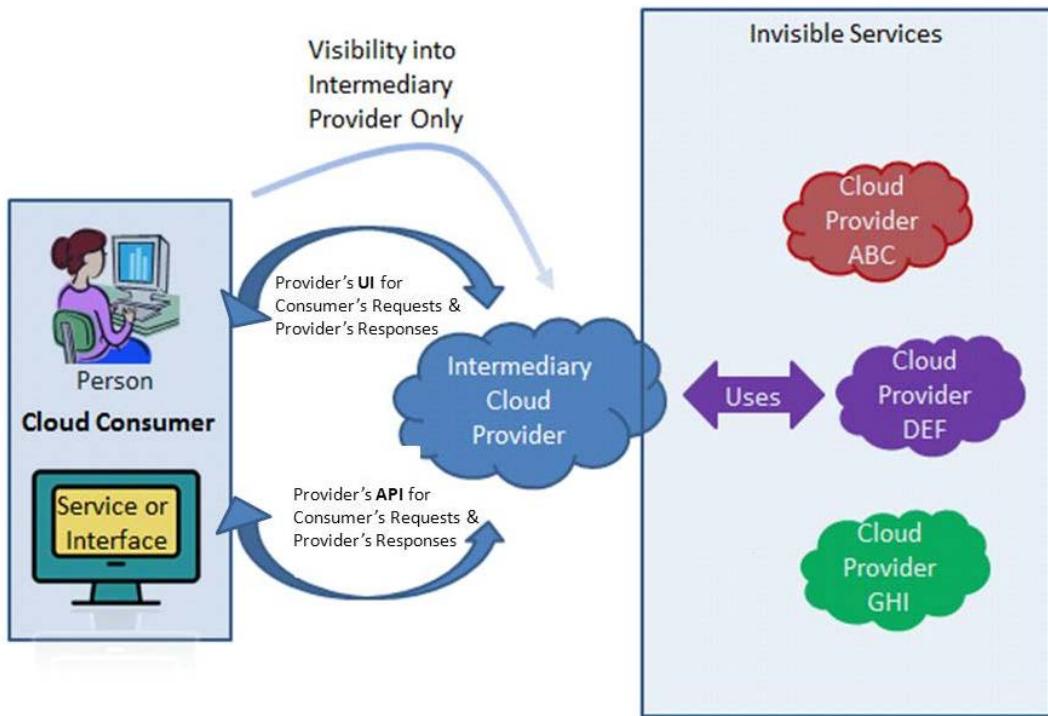
**Figure 6:** Intermediary Cloud Provider Example

### 2.4.5 CLOUD BROKER

NIST SP 500-292: *NIST Cloud Computing Reference Architecture* defines a cloud Broker as an entity that manages the use, performance and delivery of cloud services, and negotiates relationships between cloud Providers and cloud Consumers [13].

The purpose of this section is to elaborate on the description of the cloud Broker provided in NIST SP 500-292: *NIST Cloud Computing Reference Architecture*, to provide a better description of the roles and types of services that a cloud Broker may offer to cloud Consumers, and to emphasize the differences between a cloud Broker and a cloud Provider.

As cloud computing evolves, the integration of cloud services may be too complex for cloud Consumers to manage alone. In such cases, a cloud Consumer may request cloud services from a cloud Broker, instead of contacting a cloud Provider directly. Cloud Brokers provide a single point of entry to manage multiple cloud services. The two key defining features of a cloud Broker, distinct from an Intermediary Provider, are the ability to offer a single consistent interface (for business or technical purposes) to multiple differing Providers, and the *transparent visibility* the Broker allows into who is providing the services in the background – recall from **Sec. 2.4.4.2** that Intermediary Providers do not offer such transparency.

It is important to note that in the majority of the graphical representations of a cloud Broker, the transparency shown in the images does not imply a cloud Broker is modifying the functional layers provided by a cloud Provider. Rather, such transparency indicates that the cloud Broker, in addition to providing extra functionality, allows the cloud Consumer to have a particular level of visibility into and information about the cloud Provider services. Also, when necessary, the Broker facilitates direct communication with the Provider in the orchestration of the cloud Ecosystem and during operational processes. Herein, this is referred to as the "*transparent visibility* into the primary service Providers," as noted above.

In general, cloud Brokers provide services in three categories [13]:

- **Aggregation:** A cloud Broker combines and integrates multiple services into one or more new services. The Broker provides data integration and ensures the security of data in transition between the cloud Consumer and multiple cloud Providers.
- **Arbitrage:** Service arbitrage is similar to service aggregation, except that the services being aggregated are not fixed. Service arbitrage means a Broker has the flexibility to choose services from multiple Providers, depending upon the characteristics of the data or the context of the service.
- **Intermediation:** A cloud Broker enhances a given service by improving some specific capability and providing value-added services to cloud Consumers. The improvement can be managing access to cloud services, identity management, performance reporting, enhanced security, etc.

### 2.4.5.1 DIFFERENTIATING BUSINESS AND TECHNICAL BROKER SERVICES

An organization that acts as a cloud Broker may provide one or both of the following services:

- Business and relationship support services (business support such as billing and contractual intermediation, arbitrage and aggregation);
- Technical support service (service aggregation, arbitrage, and technical intermediation), with a key focus on handling interoperability issues among multiple cloud Providers.

A Business Broker only provides business and relationship services, and does not have any contact with the cloud Consumer's data, operations, or artifacts (e.g., images, volumes, firewalls) in the cloud. Conversely, a Technical Broker *does* interact with a Consumer's assets: the Technical Broker aggregates services from multiple cloud Providers and adds a layer of technical functionality by addressing single-point-of-entry and interoperability issues. These Broker roles are not mutually exclusive. For example, a given entity might serve as a Business Broker in one context, a Technical Broker in another, and both in a third context.

Both types of Brokers always allow the cloud Consumer a particular level of transparency into the identity of the target cloud Providers. In **Figure 5,** there is a particular emphasis on the different levels of transparency and aggregation possible through a cloud Technical Broker (Broker 2) and Intermediary Provider.

**Figure 7** below shows a simple example of cloud brokerage. Depending upon the Broker services rendered, the brokerage can be business-oriented, technically oriented, or a combination of the two. Note that two key characteristics of brokerage – aggregation and providing transparent visibility into the cloud Providers – are fulfilled.

A cloud Business Broker could also offer value-added intermediation services such as: service catalogue lookups, subscription handling, customer relation management, unified billing, etc.
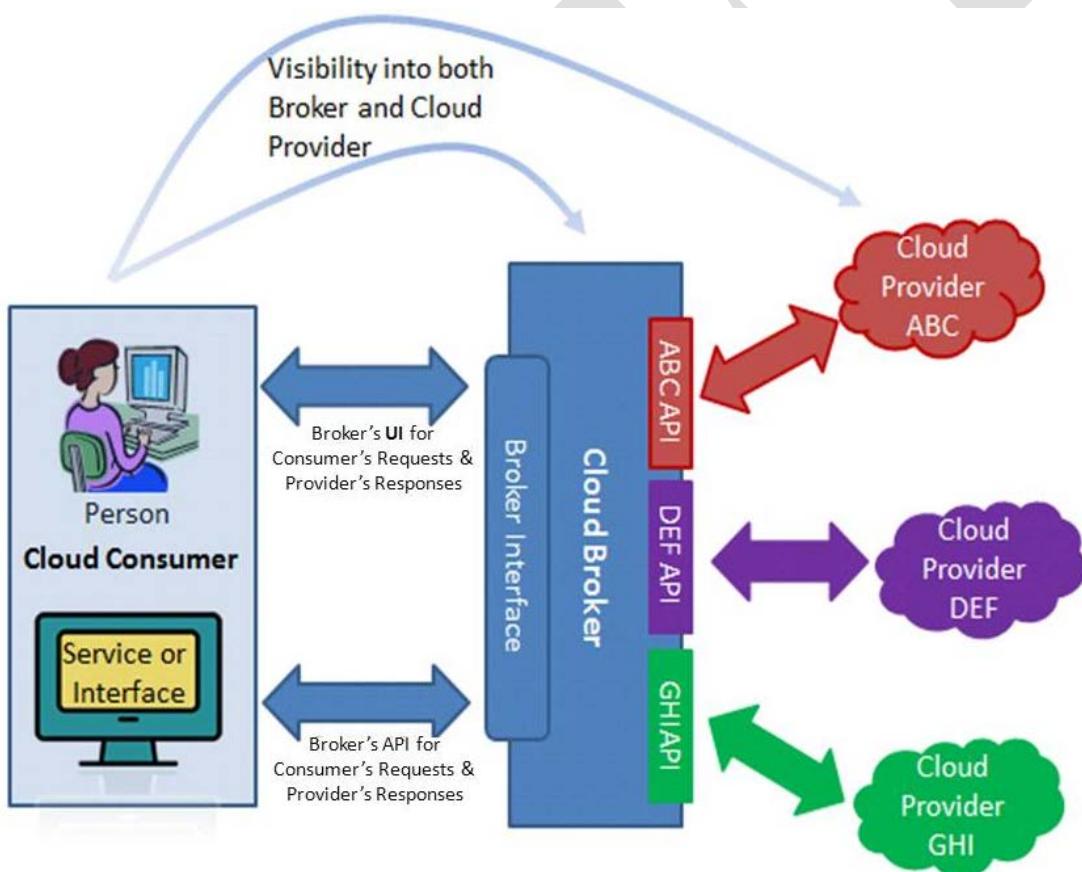


**Figure 7:** Cloud Broker Example

A cloud Technical Broker could offer cross-provider technical services such as orchestration, load management and cloud-bursting, integrated identity and authorization management, security brokerage and integrated security management, metrics retrieval, cost and usage reporting, etc.

### 2.4.6 CLOUD CARRIER

A cloud Carrier acts as an intermediary that provides connectivity and transport of cloud services between cloud Consumers and cloud Providers through network, telecommunications, and other access devices. For example, cloud Consumers can obtain cloud services through networked devices, such as computers, laptops, mobile phones, mobile Internet devices (MIDs), etc. The distribution of cloud services is normally provided by network and telecommunication Carriers or a transport agent: a transport agent refers to a business organization that provides physical transport of storage media such as high-capacity hard drives. Note that a cloud Provider will set up SLAs with a cloud Carrier to provide a level of service consistent with the levels established in SLAs offered to cloud Consumers. The Provider may require the cloud Carrier to provide dedicated and secure connections between it and its Consumer(s).

The security concerns of the Carrier role include consideration for the exposures and threats that would be present in the transmission of data to and from a cloud structure. Due to the evolutionary nature of the Internet and the development over time of new methods for signal transmission, there are inherent vulnerabilities in the channels that transmit data to and from cloud structures. Security breaches at juncture and insertion points present a challenging security problem for Carriers in both cloud and non-cloud transmissions. For these reasons, the Carrier is responsible for maintaining security control points that span the systems they manage, as well as security testing, risk management, and preventative tasks that would be expected to reduce vulnerabilities in transmission channels. Carriers can offer dedicated lines of communication between endpoints, including interstate and international dedicated lines.

The security responsibilities of the cloud Carrier – unlike those of other roles in the cloud Ecosystem – are always the same, regardless of the cloud service of deployment model.

### 2.4.7 CLOUD AUDITOR

A cloud Auditor is a party that can conduct an independent assessment of cloud services, with the intent to express an opinion thereon. A cloud Auditor can evaluate the services provided by a cloud Provider in terms of security controls, privacy impact, performance, etc. Audits can be used to verify conformance to standards (set forth in mandates, the service contract, industry best practices, or other sources) through review of objective evidence.

Security controls are the management, operational, and technical safeguards or countermeasures employed within an organizational information system to protect the C/I/A of the system and its information. A cloud Auditor can make an assessment of the security controls in the information system, in accordance with generally accepted auditing standards, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to the security requirements for the system. The security auditing should also include the verification of compliance with regulation and security policy. For example, an Auditor can be

tasked with ensuring that the correct policies are applied to data retention according to relevant rules for the applicable jurisdictions providing legislative and regulatory data compliance oversight. The Auditor may ensure that fixed content has not been modified and that the legal and business data archival requirements have been satisfied.

The NCC-SRA document acknowledges the importance of the auditing process, the complexity of an audit, and the wide variation among the audited targets. However, the document limits its analysis of the Auditor – from a security perspective – to its responsibilities for security components designed to protect the data accessed and collected during an audit, the evaluation process, and the report findings.

The underlying service model used by the systems being audited plays a secondary role from the viewpoint of the cloud Auditor. What is relevant is that the Security Components available and accessible to the Auditor enable the collection of objective evidence from the responsible parties required for the audit. It is assumed that an Auditor would also have some persistent and sensitive information regarding their client files as well, and that their report findings are stored in the cloud. Therefore, the Auditor will need to be cognizant of the Security Components available to support this function by using widely accepted industry best practices, such as those addressed in GAO-12-331G Government Auditing Standards.

### 2.4.8   BUSINESS MODELS AND NIST REFERENCE ARCHITECTURE

The NIST RA and the overarching Security Reference Architecture provides a flexible formal model in terms of the cloud Actors that allows vendors of different cloud services to easily map their business model to the NIST architecture. The key concept that supports this flexibility is the fact that an organization that offers cloud services may engage in different business functionalities with different partners and customers, taking on different roles and assuming different cloud Actors' responsibilities. These functionalities can be thought of as a separate cloud Ecosystem with its own context – based on service, contractual, technical, and other characteristics – and the particular role of the organization depends upon this context. This means that a given organization can be a Provider of some cloud services to a particular cloud Consumer and at the same time serve as a Broker of other or of a subset of services to another Consumer.

Consider the relationships of the entities in **Figure 8** below – three agencies and two cloud service vendors. Agency 1 uses the PaaS cloud services from Vendor A, while implementing in house their end-users' business management. In this business relationship, Agency 1 is a Consumer of the PaaS cloud services offered by Vendor A as a Primary Provider. Agency 2 also uses the PaaS cloud services offered by Vendor A. In this case, Vendor A also implements the business management functions (authorization contract management) of Agency 2's end-users. Agency 2 is a Consumer of the cloud services offered by Vendor A as a Primary Provider. It is important to note that Vendor A, in its role of cloud Provider, offers different cloud service packages to different Consumers. In the last scenario depicted in **Figure 8** below, Agency 3 consumes Vendor B's SaaS cloud services

while it contracts with Vendor A the business management functions of its end-users. In this business scenario, a particular level of trust must exist or be established between Vendor B and Vendor A. In this case, Agency 3 is a Consumer of SaaS cloud services offered by Vendor B as a Provider while Vendor A is a Broker for Agency 3, since it is providing value-added business management functionality.
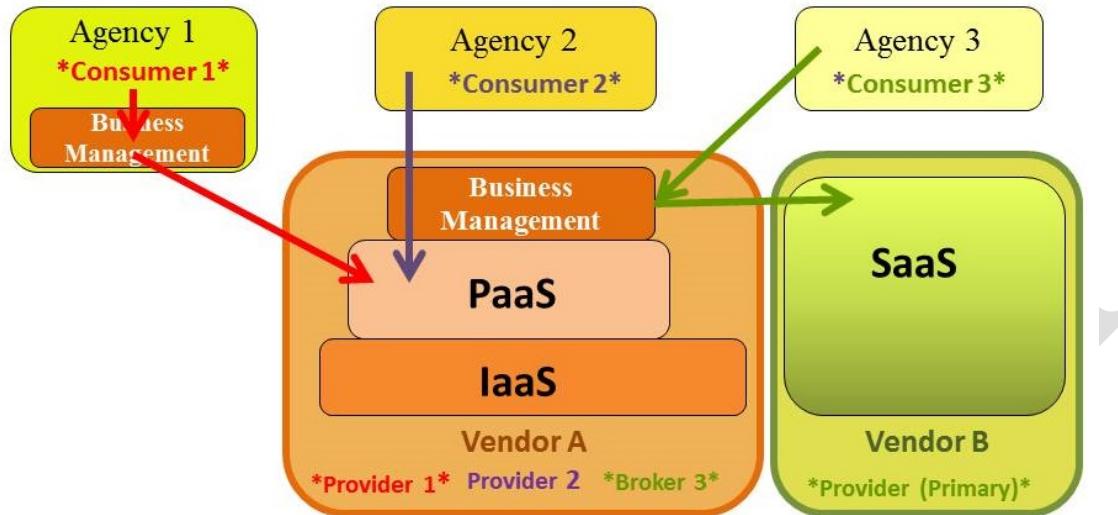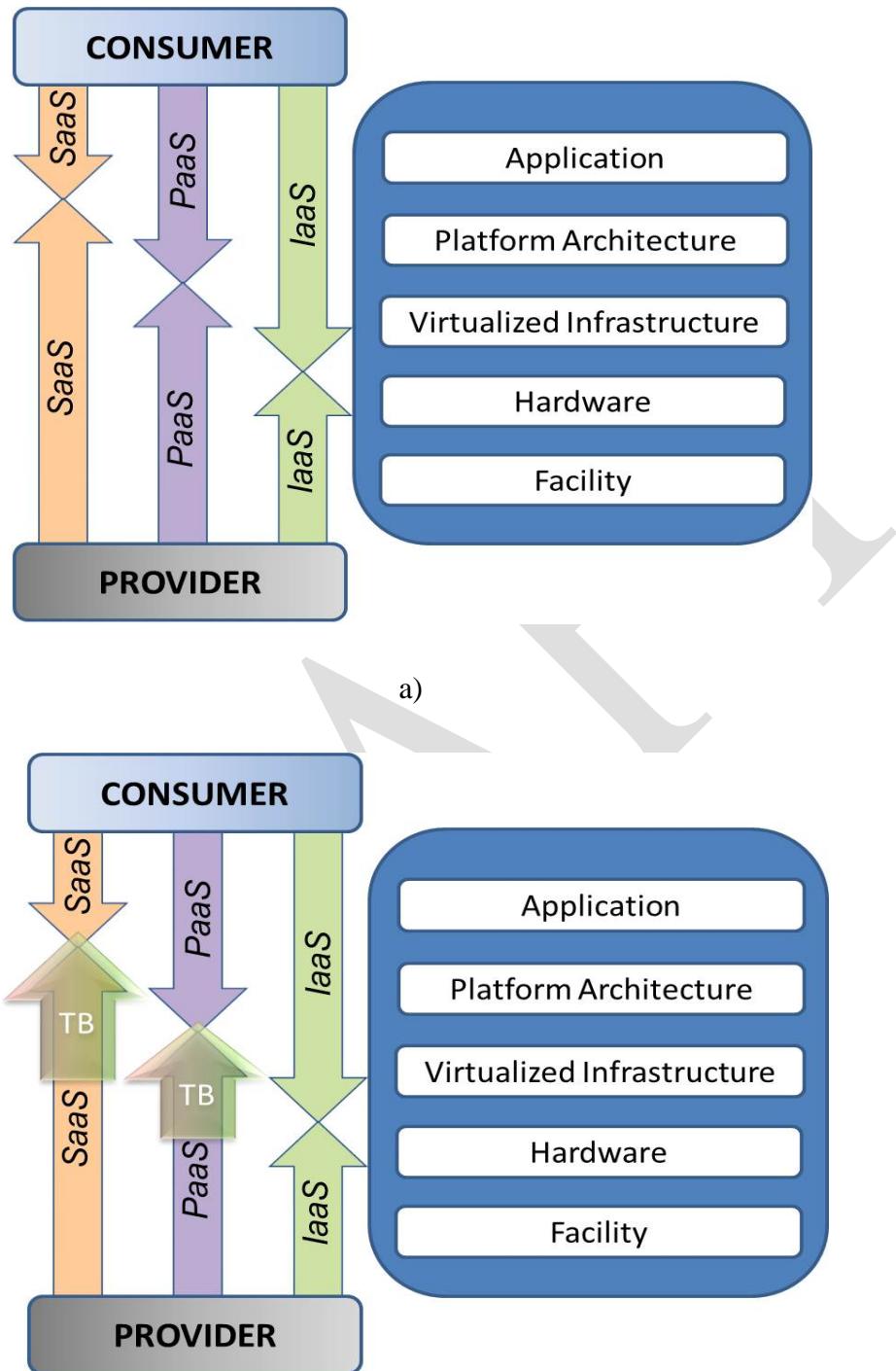


**Figure 8: Business Models vs. NIST Reference Architecture**

In sum, it is important to keep in mind that the NIST RA and NCC-SRA do not constitute a comprehensive, one-to-one translation of all organizations' business models, but rather allow for flexible mapping of the business models employed by all cloud service vendors. The architecture described in these two documents defines cloud Actors based upon the roles they play in relation to their business partners and customers in the context of cloud services.

### 2.4.9 SECURITY CONSERVATION PRINCIPLE

The core concept of the Security Conservation Principle is that, for a particular service migrated to the cloud, the full set of necessary Security Components and controls that must be implemented to secure the cloud Ecosystem is always the same; however, the division of responsibility for those Components and controls changes based upon the characteristics of the cloud, particularly the service deployment. **Figure 9** below depicts the *Security Conservation Principle* for the cloud Ecosystem.

a)



**Legend:** TB = cloud Technical Broker

b)

**Figure 9: Security Conservation Principle (based on graphic from NIST SP 800-144)**

For the sake of brevity, diagram a) in **Figure 9** identifies only the major cloud Actors: Consumer and Provider. The diagram highlights the shifting of the responsibility for implementing particular Security Components between the Consumer and Provider, depending upon the cloud service deployment model. Essentially, the level of responsibility for either Actor correlates to the Actor's level of control over certain "layers" of the cloud. In a SaaS cloud, where the Consumer controls only the application layer, the Provider assumes most of the responsibility for Security Components. Conversely, in an IaaS cloud – where the Consumer may control everything except the hardware the service runs on and the facility in which that hardware is kept – the Consumer assumes most of the responsibility for Security Components.

Since a Technical Broker may be involved in a cloud Ecosystem providing additional functionality – and with that, adequate embedded security and privacy – diagram b) in **Figure 9** illustrates the same concept with generic technical Broker functionality added.

# 3 SECURITY REFERENCE ARCHITECTURE: DATA ANALYSIS METHODOLOGY

This Security Reference Architecture leverages the Trusted Cloud Initiative – Reference Architecture[6] shown in **Annex A**. To accomplish this, the team that authored this document extracted all of the capabilities described in the TCI-RA while preserving the path to the three root-domains (Business Operation Support Service [BOSS], Information Technology Operation Support [ITOS], and Security and Risk Management [S&RM]) and generated a total set of 346 Security Components. An example of the resulting data collection form can be seen in **Table 1** below.

**Table 1: SRA Data Collection Form with the Set of Security Components**

| High-level component (L1) | Mid-level component (L2) | Low-level component (L3) | Basic-level component (L4) | Cloud Consumer | Cloud Provider | Cloud Broker | Cloud Carrier | Cloud Auditor |
|---|---|---|---|---|---|---|---|---|
| Business Operations Support | Security Monitoring Services | Branding Protection | | | | | | |
| | | Anti Phishing | | | | | | |
| | | Real Time Internetwork Defense (SCAP) | | | | | | |
| | | User Behaviors and Profile Patterns | | | | | | |
| | Legal Services | Contracts | | | | | | |
| | | E-Discovery | | | | | | |
| | | Incident Response Legal Preparation | | | | | | |
| | Internal Investigations | Forensic Analysis | | | | | | |
| | | e-Mail Journaling | | | | | | |
| ...ration & Support (ITOS) | IT Operations | DRP | Plan Management | | | | | |
| | | | Test Management | | | | | |
| | | IT Governance | Architecture | | | | | |
| | | | Standards and | | | | | |
| | | Resource Management | Segregation of duties | | | | | |
| | | | Contractors | | | | | |
| | | PMO | Program Mngmt | | | | | |
| | | | Project Mngmt | | | | | |
| | | | Remediation | | | | | |

---

[6] See https://research.cloudsecurityalliance.org/tci/explore/

For a particular deployment model (Public cloud in the example presented in this document), the collected data was aggregated, validated, and processed as part of the data analysis methodology presented in the next section.

<h2>3.1    DATA COLLECTION</h2>

The data collection effort was focused on populating the NCC-SRA formal model by assessing the applicability of each Security Component for a given cloud instance. Accordingly, each blank cell under each cloud Actor heading (note the Cloud Consumer, Cloud Provider, etc. columns in **Table 1**) was marked with one of the following:

- "X" to indicate that the Security Component should be implemented by the Actor to secure the Consumer's applications and data in the Cloud.

- "A" to indicate that the Security Component should be implemented internally, independent of the Consumer's data, for administrative or best-practice reasons.

- "B," specific to Business Brokers only, to indicate a Security Component that is implemented to secure the cloud computing business-oriented service. The marking also emphasizes that the Business Broker only provides business and relationship services, and does not have any contact with the cloud Consumer's data migrated to the cloud.

- A blank cell indicates that the Security Component cannot be implemented by the particular cloud Actor or is not necessary in securing the cloud Ecosystem.

In the process of collecting data, the definitions provided by CSA for the capabilities identified in the TCI-RA were used to better determine the applicability of the Security Component to the given cloud instance for each cloud Actor.

The purpose of the markings is to provide cloud Consumers with a reference they can use to identify the Security Components that are applicable for a particular cloud service model. The markings also indicate which Actor(s) in the cloud Ecosystem – Consumer, Provider, or Broker, in most cases – is responsible for a particular Security Component based on the use case or type of cloud service offered.[7] As indicated by the data sets, there are areas in which the responsibility for a particular Security Component may reside with multiple cloud Actors depending on the specifics of the Component and the particular use case.

It is important to distinguish between responsibility for identifying and setting Security Components requirements and responsibility for their implementation. The cloud Consumer is always

---

[7] Many of the Security Components are common and should be considered by all cloud Actors (organizations) for implementation in their internal operations as well as in cloud-based service offering operations.

accountable for ensuring that all appropriate provisions for an effective security control environment are identified and implementation requirements are in place. This accountability cannot be relinquished.
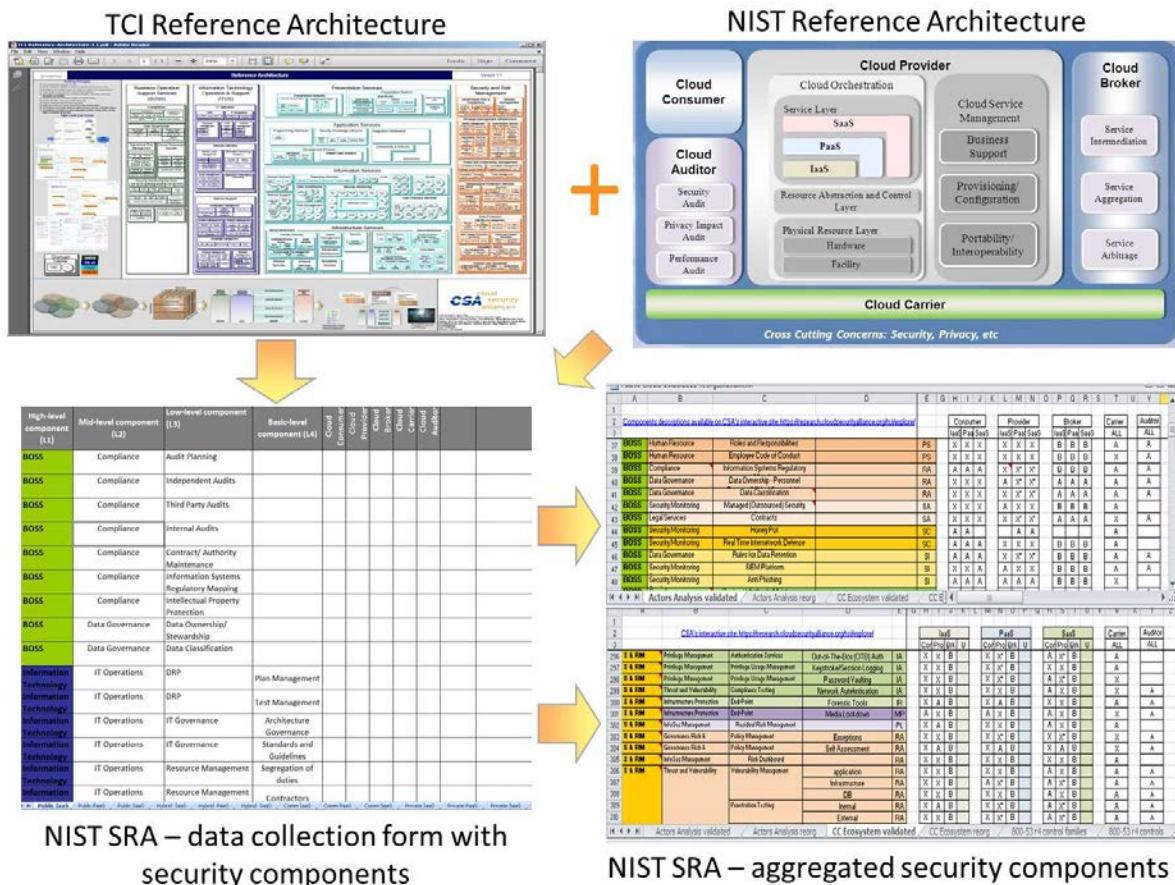
For some Security Components in certain cloud service models, the cloud Consumer is both accountable and responsible for implementation. For example, "Security Monitoring - End-point Monitoring" is a Security Component that, regardless of the service model, can only be implemented by the Consumer.

Even when responsibility for implementation is outsourced to another cloud Actor, if a Security Component is applicable, the Consumer remains accountable for identifying that Security Component and for requiring implementation through contractual means. For example, "Data Governance – Secure Disposal of Data" is a Security Component that the Consumer may be able to implement for a IaaS cloud service model but needs to be implemented by Provider(s) for all other service models. The Consumer needs to ensure through contractual means that the Component is properly implemented by the Provider(s) of the cloud services.

## 3.2    DATA AGGREGATION AND VALIDATION

The data collected for a Public cloud (as described in **Sec. 3.1**) is aggregated for all cloud Actors in a service-centric way, to facilitate data validation using the Security Conservation Principle defined above in **Sec. 2.4.9**. The same data was then also aggregated for all cloud service models in an Actor-centric way to allow for a better understanding of the dynamics as the responsibilities for implementing the full set of Security Components shift among cloud Actors with changes in the service model (SaaS, PaaS, IaaS).

**Figure 10** captures graphically the derivation of the Security Components, the data collection process, and the two types of data aggregation used to analyze the set of Security Components for each cloud service model (i.e., SaaS, PaaS, IaaS).

**Figure 10:** Security Components Overview

The first type of data aggregation applied to each deployment model is cloud Actor-centric. For each cloud Actor, the data collected for the core set of Security Components for each service type (IaaS, PaaS, and SaaS) is gathered on one matrix in adjacent columns (for an example of a Public cloud deployment model, see **Annex D 11.1**) to highlight the level of control the cloud Actor has over the implementation of each Security Component and how this level increases or diminishes depending upon the service model.

The second type of data aggregation applied to each deployment model is cloud Ecosystem-centric. For each type of service, the data collected for the core set of Security Components for each Actor is gathered on one matrix in adjacent columns (for an example of a Public cloud deployment model, see **Annex D 11.2**) to highlight the shared responsibilities among Actors involved in constructing and securing the cloud Ecosystem for implementing the identified Security Components. This type of aggregation also highlights the Security Conservation Principle described in **Sec. 2.4.9**.

The accuracy of the data collected for each cloud deployment mode was verified and data was validated in both aggregation scenarios by ensuring that:

1. In the Actor-centric aggregation type, the cloud Consumer's responsibility for implementing Security Components is higher for an IaaS service deployment and decreases for a PaaS service deployment, reaching minimum for a SaaS service deployment. Conversely, the combined responsibility for the cloud Provider and Technical Broker increases significantly from an IaaS service deployment to a PaaS deployment to a SaaS deployment, where it reaches the maximum.
2. In the Ecosystem-centric aggregation type, the cumulative set of Security Components implemented by all Actors involved in the cloud Ecosystem remains the same regardless of the service deployment (IaaS, PaaS, or SaaS).

It is important to note that based on NIST SP 500-292: *NIST Cloud Computing Reference Architecture* definitions of the cloud Carrier, the data collected for this Actor and its security responsibilities do not vary with the cloud deployment or service model. This is due to the Carrier's unique role of securing the data in transit between the Consumer and the cloud. All other transport roles and responsibilities within the cloud are attributed to the cloud Provider.

The data collected for and responsibilities attributed to the cloud Auditor also do not change with the cloud deployment or service model, since the NCC-SRA only addresses the core set of Security Components necessary to be implemented to secure the Actor's auditing environment.

## 3.3  DERIVING THE SECURITY RESPONSIBILITIES FOR THE INTERMEDIARY PROVIDER AND TECHNICAL BROKER

The overall core set of Security Components that a Technical Broker or an Intermediary Provider should analyze and implement (in addition to the baseline set of Security Components all cloud Actors should implement) to secure the cloud Ecosystem were determined using the following steps:

1. Identify the "floor" or lowest service layer of the Technical Broker or Intermediary Provider (e.g., "Infrastructure" layer if the Broker builds its services supplementing an IaaS Provider);
2. Identify the "ceiling" or highest service layer of the Technical Broker or Intermediary Provider (e.g., "Platform" layer if the Broker offers PaaS services);
3. Extract from the data sets provided in **Annex D** the Primary Provider set of Security Components corresponding to the [floor]aaS and the one corresponding to the [ceiling]aaS
4. Perform a logical subtraction of the [floor]aaS from the [ceiling]aaS.

**Figure 11** below illustrates the approach described above.

$$SC(IP \mid TB)_{XaaS} = SC(PP)_{XaaS} - SC(PP)_{YaaS}$$

*Example:*

a) $SC(IP)_{SaaS} = SC(PP)_{SaaS} - SC(PP)_{PaaS}$ , where "XaaS" = "SaaS", "YaaS" = "PaaS"
b) $SC(TB)_{PaaS} = SC(PP)_{PaaS} - SC(PP)_{IaaS}$, where "XaaS" = "PaaS", "YaaS" = "IaaS"

<u>*Legend:*</u>
*SC – set of Security Components*
*PP – Primary Provider*
*IP – Intermediary Provider*
*TB – Technical Broker*
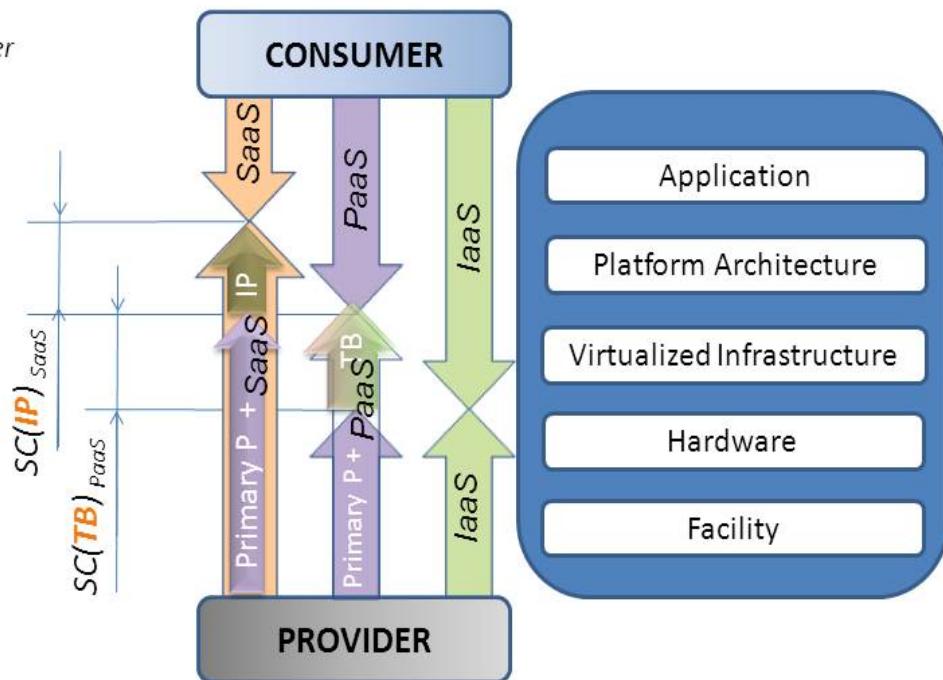


**Figure 11: Security Components for Technical Broker & Intermediary Provider**

## 3.4  MAPPING SECURITY COMPONENTS TO SECURITY CONTROL FAMILIES

NIST SP 500-293 Vol. 2 (Draft): *US Government Cloud Computing Technology Roadmap Volume II: Useful Information for Cloud Adopters* identifies the need for clarification of security control roles and responsibilities as a challenging security requirement.  To address this issue, this document maps the Security Components identified in the Security Reference Architecture to the NIST SP 800-53 (Rev. 4): *Security and Privacy Controls for Federal Information Systems and Organizations* security control families.  This mapping is necessary to set a common ground for government cloud Consumers and cloud Providers and Brokers in the private sector.

This section outlines the process used to map the Security Components to the security control families of NIST SP 800-53 (Rev. 4): *Minimum Security Requirements for Federal Information and Information Systems*.  The mapping or assignment of the Security Components to one of the

eighteen families of security controls identified in NIST SP 800-53 Rev. 4 was accomplished by sorting each Component into the "best fit" security control family. It is important to note that this mapping is not based upon particular security controls defined in NIST SP 800-53 Rev. 4, since each Security Component may be associated with multiple 800-53 security controls that often belong to different control families.

In the data collection forms presented in **Sec. 3**, the NCC-SRA Security Components preserved the three root-domains and service layers identified by the TCI-RA capabilities (see also **Table 2** below).

**Table 2: TCI Reference Architecture - Domains and Service Layer**

| DOMAINS | SERVICE LAYERS |
|---------|----------------|
| Business Operations Support Services (BOSS) | Infrastructure Services |
| Information Technology Operations and Support (ITOS) | Information Services |
| Security and Risk Management (S&RM) | Application Services |
| | Presentation Services |

The eighteen security control families identified in NIST SP 800-53 Rev. 4 are listed in **Table 3** below. **Annex B** depicts the mapping of the Security Components to the NIST 800-53 security control families using the color code presented in **Table 3**.

**Table 3: NIST SP 800-53 Rev. 4 Control Families - Assigned Color Codes**

| ID | Color Code | Family Name | ID | Color Code | Family Name |
|----|-----------|-------------|----|-----------|-------------|
| AC | | Access Control | MP | | Media Protection |
| AT | | Awareness and Training | PE | | Physical and Environmental Protection |
| AU | | Audit and Accountability | PL | | Planning |
| CA | | Security Assessment and Authorization | PS | | Personnel Security |
| CM | | Configuration Management | RA | | Risk Assessment |
| CP | | Contingency Planning | SA | | System and Services Acquisition |
| IA | | Identification and Authentication | SC | | System and Communications Protection |
| IR | | Incident Response | SI | | System and Information Integrity |
| MA | | Maintenance | PM | | Program Management |

Cloud Consumers can quickly identify Security Component/security control family pairs by consulting the color codes diagram in **Annex B**. For example, a large number of Presentation Layer – Presentation Modality and Security and Risk Management Infrastructure – Infrastructure Protection Security Components are mapped to the access control (AC) family and therefore coded to the shade of blue shown on **Table 3** in the top left-hand corner.

## 3.5     EMPIRICAL DATA ANALYSIS AND THE GENERIC HEAT MAP

When the Consumer migrates a service to the Cloud, (e.g., to a Public cloud), the Consumer may review and customize the data set presented in this document for their particular use case. The customized Ecosystem-centric aggregated data of all three types of services (IaaS, PaaS, and SaaS) for the cloud deployment model that best fits the Consumer's needs (e.g., **Annex D 11.2** for a Public cloud data set) can be used to generate an overall heat map that identifies, in a unified view, the Security Components that require special attention for a particular cloud deployment model, regardless of the service model elected by the Consumer.

Even though Consumers remain responsible for identifying all Security Components and controls that need to be implemented to secure their application or service migrated to the cloud, they can use such a heat map as a means for visualizing the distribution of responsibilities for implementing these Security Components between Consumers and Providers and/or Brokers. Consumers can use the heat map to identify the Security Components that, for a particular deployment mode and regardless of the service model, fall under the Provider(s) and/or Broker's responsibility for implementation as opposed to the Security Components that fall under their own responsibility.

| | |
|---|---|
| [AX AX AX] => 3.0 | The vector is: AX AX AX -> 3 |
| [XX AX AX] => 2.5 | The vector has (2) AX + (1) XX -> 2.5 |
| [XA AX AX] => 2.0<br>[XX XX AX] => 2.0 | The vector has (2) AX or (1) AX+(2) XX -> 2 |
| [XA XX AX] => 1.5<br>[XX XX XX] => 1.5 | The vector has (1) AX + (1) XX or (3) XX ->1.5 |
| [XA XA AX] => 1.0<br>[XA XX XX] => 1.0 | The vector has (1) AX or (2) XX -> 1 |
| [XA XA XX] => 0.5 | The vector has (1) XX -> 0.5 |
| [XA XA XA] => 0.0 | The vector is: XA XA XA -> 0 |
| AA AA AA => admin only | The vector is: AA AA AA |
| Null cells | The vector has empty cells |
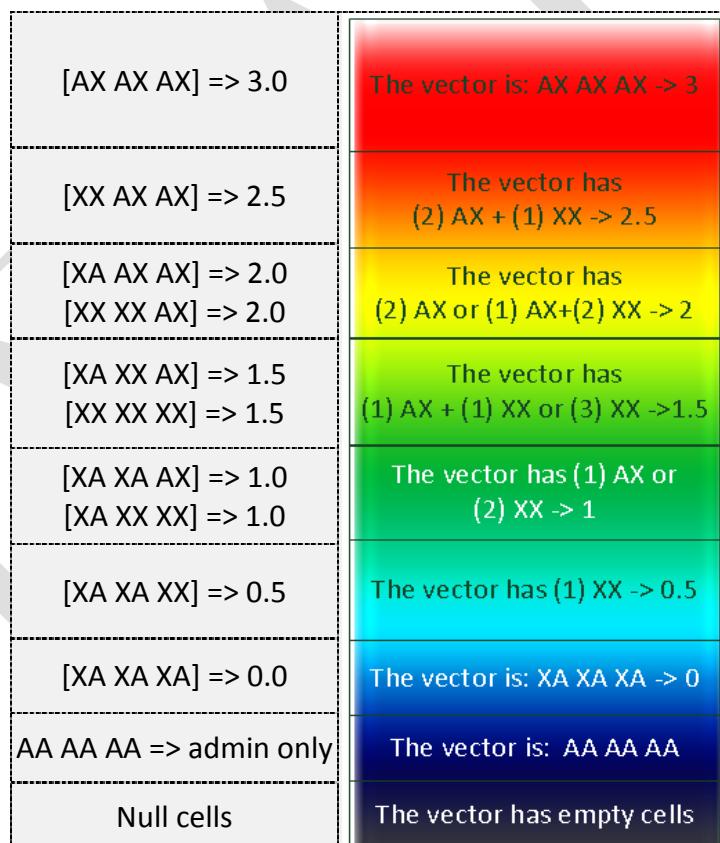
**Figure 12: Legend of the Generic Heat Map**

The heat map represents in "hot" colors the Security Components where the cloud Consumer loses the ability to implement and manage the Security Component and associated security controls. The "warm" colors are used to represent the Security Components where both Consumer and Provider share responsibility (depending on the service type). The "cool" colors represent the Security Components where the Consumer keeps control of (and is responsible for) implementing the security mechanisms in the cloud Ecosystem. The Heat Map can then be used to identify those Security Components (i.e., the "hot" and "warm" components) and the security controls that need to be specified in SLAs and contracts with cloud Providers, Brokers and Carriers. The legend for the colors used in the Heat Map is shown in **Fig. 12** above.

To generate a heat map for a particular cloud deployment model (e.g., Public cloud), the data for the Consumer and the Provider is extracted from each row of the Ecosystem-centric data form (e.g., **Annex D** for a Public cloud), for all three service models (see the columns labeled IaaS, PaaS, and SaaS in **Table 4** below). The data is then formatted as a vector.

**Table 4: Security Component - Vector Generation**

| Domain | High-level Security Component | Mid-level Security Component | Low-level Security Component | 800-53 Family | IaaS | | | PaaS | | | SaaS | | | ALL | ALL |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Consumer | Provider | Broker | Consumer | Provider | Broker | Consumer | Provider | Broker | Carrier | Auditor |
| BOSS | Compliance | Contract/ Authority Maintenance | | PM | X | A | B | X | A | B | A | X | B | X | A |

EXTRACTED VECTOR:     [X A,      X A,      A X]

The definitions of the designations "X," "A," and "B," are provided in section 3.1 above. As applied here, if the Consumer has an X for a Security Component and the Provider has an A, then this combination is interpreted as a case where the Consumer has the most responsibility for implementing the controls associated with this Security Component. If both the Consumer and the Provider have an X, it means that both Actors share the responsibility to implement that particular Component for the service type being discussed. However, if the Provider has an X while the Consumer has an A for a Security Component, it means that the Provider is fully responsible for implementing the security controls associated with the Security Component, for securing the data migrated to the cloud.

In the example in **Table 4** above, the vector (**X**A, **X**A, **A**X) shown means that for this Security Component, the Consumer has an "X" for IaaS, "X" for PaaS, and "A" for SaaS, meaning that it is the Consumer's responsibility to implement that Component in an IaaS or PaaS cloud and that the

Security Component can only be implemented by the Provider for SaaS. When using a SaaS cloud, the Consumer can at most implement this Security Component for internal administrative functions. The same vector (X**A,** X**A,** A**X**), indicates that the cloud Provider has an "A" for IaaS, "A" for PaaS, and "X" for SaaS respectively, meaning that, for an IaaS or PaaS cloud, the Security Component can only be implemented internally by the Provider for its own administrative reasons and not to secure a Consumer's data or services, while the Provider is solely responsible for that same Security Component in a SaaS cloud.

The next step after extracting the vectors is to quantify their components, in terms of how much control a Consumer is transferring to the Provider. This means assigning numerical values to each of the components of the vector, according to how much control the Consumer has over the implementation of a particular Security Component. Specifically, the components are assigned the following numerical values from 0 to 1, based on requirements for negotiation and SLA specification between Consumer and Provider: XA = 0, XX = 0.5 and AX = 1. XA = 0 means the Consumer has full control over the implementation of the Security Component, and AX = 1 means the Consumer needs to negotiate with the Provider requirements for the implementation of the Security Component to ensure the Consumers accountability needs are met. The "least responsibility" vector (AA AA AA) and the vector derived from empty cells do not have any numerical values assigned to them since they represent a Security Component implemented for administrative functions that reside with the respective system owners and are independent of the Consumer's application(s) or service(s) migrated to the cloud. For each vector the numerical values of each component are added to determine the overall numerical value of the vector that is then represented in the Heat Map using the legend presented in **Fig. 11**, providing a visual indicator of which Security Components can be handled by the Consumer and which ones need to be addressed in contracts with Providers and/or Brokers.

A generic heat map generated using the data aggregated for a Public cloud following the approach described above is provided in **Annex C** as an example. Similar heat maps can be generated for all other types of clouds based on similar data collected, aggregated and validated (e.g., Private, Hybrid, etc.)

# 4   SECURITY REFERENCE ARCHITECTURE: FORMAL MODEL

## 4.1   OVERVIEW OF THE FORMAL MODEL

The Cloud Computing Security Reference Architecture formal model is derived from the NIST Reference Architecture (NIST RA) described in NIST SP 500-292: *NIST Cloud Computing Reference Architecture*, which is illustrated in **Fig. 13** below with the latest updates included. The SRA formal model indicates that each of the Architectural Components identified in the NIST RA should be secured by implementing the appropriate SRA Security Components and associated NIST SP 800-53 (Rev. 4): *Security and Privacy Controls for Federal Information Systems and Organizations* security controls, as necessary. It is important to reiterate that even though the SRA only maps the Security Components to NIST SP 800-53 Rev. 4 security control families in this document, the final goal for a cloud Consumer is to identify the precise set of security controls that best address the security needs and FISMA compliance for their specific cloud computing use case.
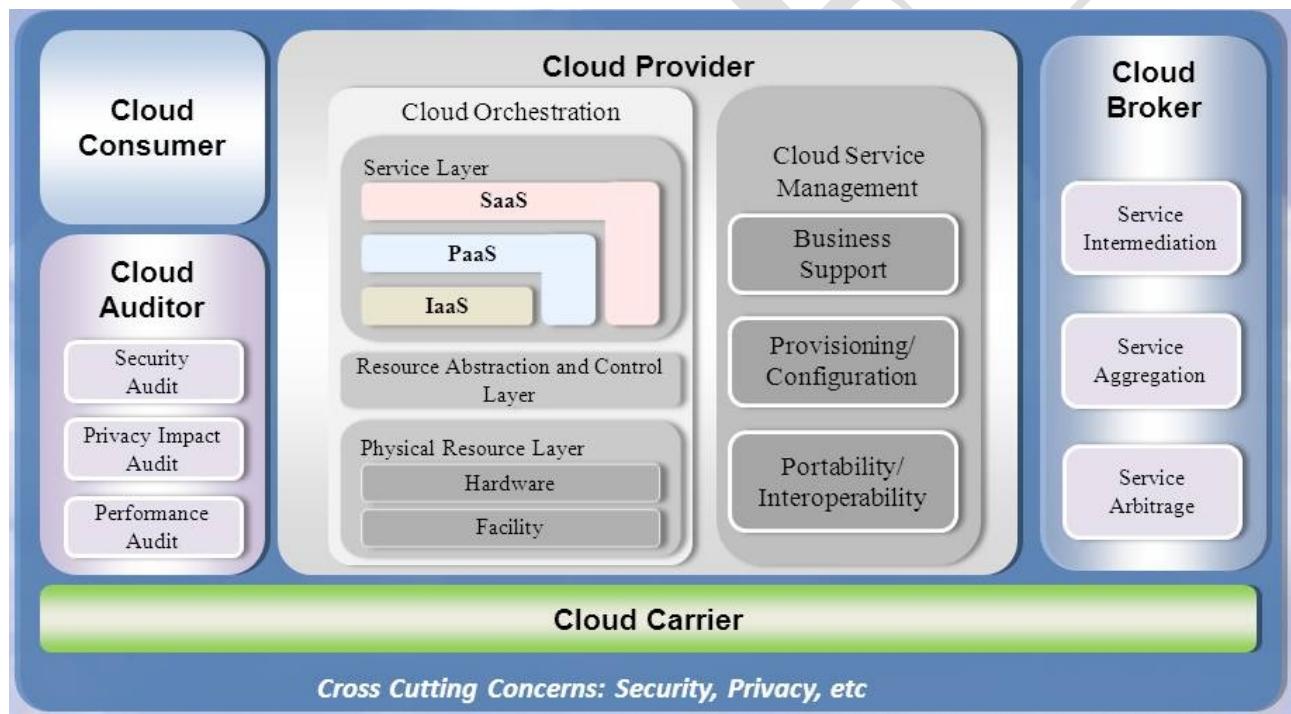


**Figure 13:** NIST Cloud Computing Reference Architecture (updated)

The SRA formal model presented in **Fig. 13** below depicts, in a layered representation, the cloud Actors on the background and the security Architectural Components defined for each Actor in the foreground. The Architectural Components and Sub-Components are stretched across multiple Actors when different Actors could perform similar or identical functions. For example, "Secure Provisioning and Configuration" is an Architectural Sub-Component indicating a service both Providers and Technical Brokers could implement as part of "Secure Cloud Service Management."

Additionally, the Technical Broker could offer "Secure Service Aggregation" to its customers. The technical configuration and provisioning aspects associated with the aggregation are represented in the diagram by stretching the "Secure Provisioning and Configuration" Architectural Sub-Component across the graphical representation of the "Secure Service Aggregation" Architectural Component. It is also important to note that the Consumer could implement "Secure Configuration" as part of "Secure Cloud Consumption Management" when needed to complement the services offered by the Provider and/or Technical Broker.
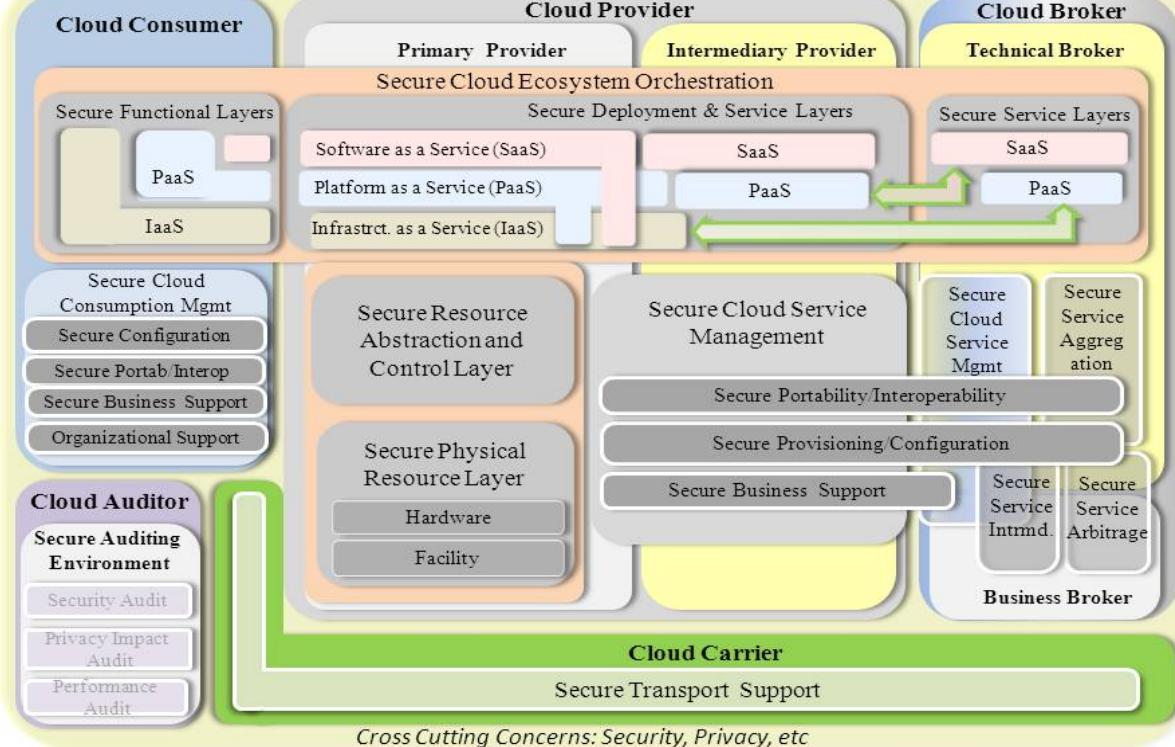


**Figure 14: Formal Model - Security Reference Architecture**

The hierarchical list of all Architectural Components and Sub-Components is as follows:

**Cloud Consumer**

- Secure Cloud Consumption Management
    - Secure Configuration
    - Secure Portability and Interoperability
    - Secure Business Support
    - Secure Organizational Support

- Secure Cloud Ecosystem Orchestration
- Secure Functional Layers

**Cloud Provider**

- Secure Cloud Service Management
    - Secure Provisioning and Configuration
    - Secure Portability and Interoperability
    - Secure Business Support
- Secure Cloud Ecosystem Orchestration
    - Secure Physical Resource Layer (Hardware & Facility) – only for a Primary Provider
    - Secure Resource Abstraction and Control Layer (Hardware & Facility) – only for a Primary Provider
    - Secure Deployment & Service Layers

**Cloud Carrier**

- Secure Transport Support

**Cloud Auditor**

- Secure Auditing Environment

**Cloud Broker**

- Secure Cloud Service Management
    - Secure Provisioning and Configuration – only for a Technical Broker
    - Secure Portability and Interoperability – only for a Technical Broker
    - Secure Business Support
- Secure Cloud Ecosystem Orchestration – only for a Technical Broker
    - Secure Service Layers
- Secure Service Aggregation
    - Secure Provisioning and Configuration (technical aspects of aggregation) – only for a Technical Broker
    - Secure Portability and Interoperability (technical aspects of aggregation) – only for a Technical Broker
- Secure Service Intermediation
    - Secure Provisioning and Configuration
- Secure Service Arbitrage
    - Secure Provisioning and Configuration

The Architectural Components and Sub-Components are introduced and discussed for each cloud Actor in the subsections below.

**Annex B** of this document presents a matrix that maps the high-level Security Components, and with them the NIST SP 800-53 (Rev. 4): *Minimum Security Requirements for Federal Information and Information Systems* security control families, to the Architectural Components and Sub-Components defined for each cloud Actor.

For instance, the "Policy and Standards – Role-based Awareness" Security Component is mapped to the Consumer's "Secure Cloud Consumption Management" Architectural Component, in particular the "Secure Consumption/Configuration" Architectural Sub-Components,  indicating that the Consumer is required to address the secure processes and policies.

## 4.2 CONSUMER - ARCHITECTURAL COMPONENTS

NIST SP 500-292: *NIST Cloud Computing Reference Architecture* identifies the Provider's and Broker's services based on the areas in which the cloud Actors conduct their activities. Our document leverages the services described for each Actor in NIST SP 500-292 to define the Architectural Components of the NCC-SRA. Since NIST RA lacks an introduction to and analysis of the Consumer's responsibilities and functions, our document contains the first introduction and description of the Consumer's Architectural Components. These Components are derived from the Consumer's responsibilities and functions in orchestrating a cloud Ecosystem and have no equivalent components in the NIST RA. The Consumer's Architectural Components complement the Provider's and Broker's Architectural Components as derived from the NIST RA.

**Figure 15** below highlights the cloud Consumer Actor on the SRA formal model diagram.

The Consumer's Architectural Components are:
- Secure Cloud Consumption Management
    - Secure Configuration
    - Secure Portability/Interoperability
    - Secure Business Support
    - Secure Organizational Support
- Secure Cloud Ecosystem Orchestration
    - Functional layer
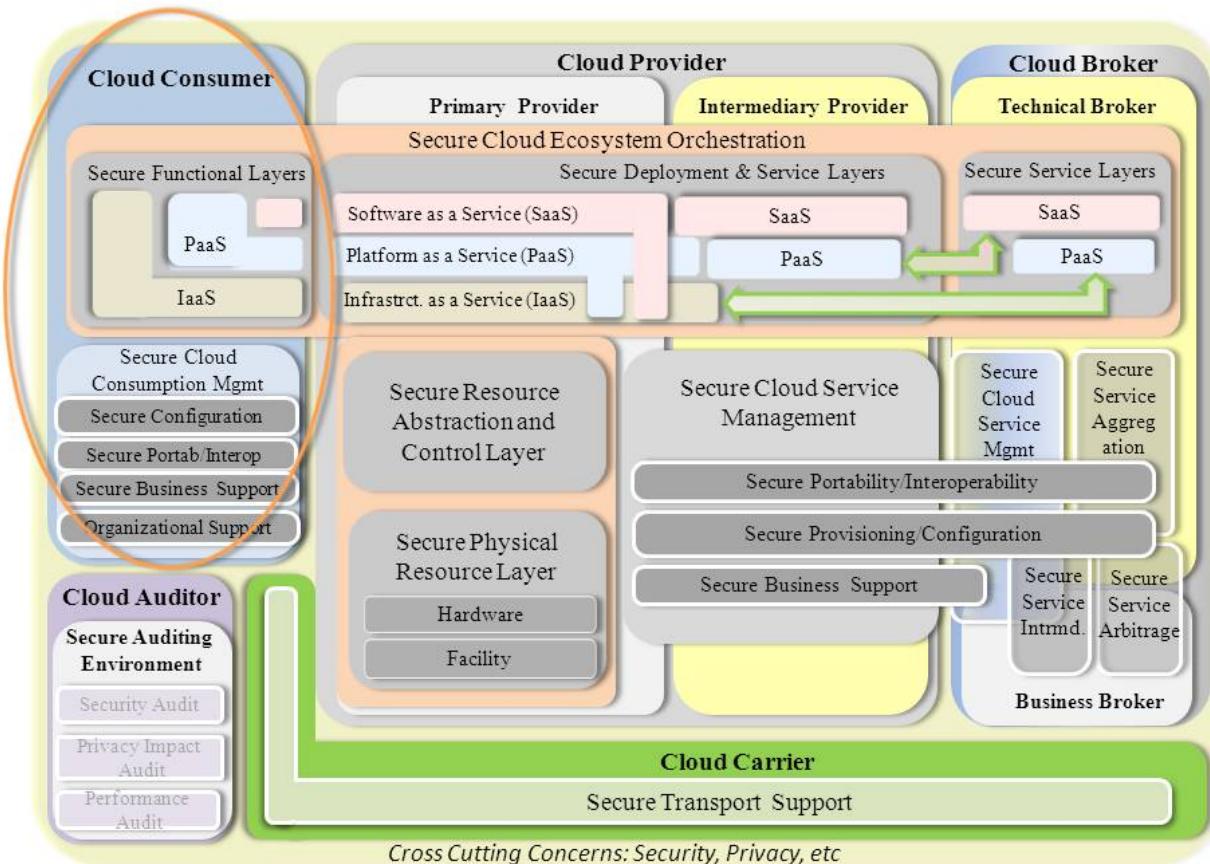
**Figure 15:** SRA – Cloud Consumer

The following subsections discuss each of the cloud Consumer's Architectural Components.

### 4.2.1 SECURE CLOUD CONSUMPTION MANAGEMENT

The *Secure Cloud Consumption Management* Architectural Component includes all of the functions that are necessary for the management and operations of the service used by the cloud Consumers. The *Secure Cloud Consumption Management* component can be described from the perspective of:

- Secure business support requirements;
- Secure provisioning and configuration requirements;
- Secure portability and interoperability requirements; and
- Secure organizational support (including organization processes, policies and procedures).

These lead to the following main Architectural Sub-Components:

- Secure Business Support (B)
- Secure Configuration (C)
- Secure Portability/Interoperability (I)
- Secure Organizational Support (O)

These four Architectural Sub-Components are discussed in detail later in this section.

One of the challenges cloud Consumers face when moving applications and data to the cloud is ensuring that the NIST RMF (or the CRMF) is applied properly and the near real-time management and ongoing information system authorization meets the agency's needs through a robust *continuous monitoring* process (see NIST SP 800-37 [Rev. 1]: *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* for more details). The responsibility for performing continuous monitoring activities is shared among Actors involved in the cloud Ecosystem. Without shared agreements and a well-structured, cost-effective automation process that ensures that the effectiveness of the security controls can be measured in near real-time, continuous monitoring of security controls is difficult to implement.

One possible solution that can support the continuous monitoring process and ensure that the proper mechanisms are in place is the adoption of standards such as the Security Content Automation Protocol (SCAP).[8] For example, Operating System (OS) images used by a cloud Provider can introduce risks to cloud Consumers and their organizations when using pre-owned virtual machines where the OS images were uploaded with built-in Trojans. Malicious conversion of the cloud services into "bot-net-in-a-box" or spam servers can wreak havoc on operations. By using standards such as SCAP, cloud Actors can collaborate on checking security policy compliance, identifying vulnerabilities in OS images, and measuring deviations from required configuration settings. Additionally, cloud Consumers can gain measurable data to map to high-level NIST SP 800-53 (Rev. 4): *Minimum Security Requirements for Federal Information and Information Systems* requirements and to gain necessary information to make cost-effective, risk-based decisions with regards to the organizational information systems operating in a cloud Ecosystem.

**Annex E** presents all the high-level SRA Security Components and their mapping to each of the Architectural Components and Sub-Components defined for a cloud Consumer, next to similar mappings for Provider, Broker, Carrier, and Auditor.

---

[8] NIST maintains a list of SCAP-validated products at: http://nvd.nist.gov/scapproducts.cfm.

The cloud Consumer's *Secure Business Support* Architectural Component includes services used to run business operations, including:

- Managing business relationships with the other cloud Actors (Provider, Broker, Carrier and Auditor), providing points-of-contact in accordance with security best practices such as authenticating and authorizing interactions between Actors.
- Following up business issues and addressing cloud-related problems with the other cloud Actors in accordance with security best practices involving secure business process and continuity of operations.
- Managing service contracts, including setting up, negotiating, and closing/terminating contracts to ensure security concerns are addressed to satisfy mandates.
- Procuring services only after security concerns have been addressed.
- Managing payment and invoices management to ensure no fraudulent payments are processed and online security best practices are followed.

The Secure Business Support Architectural Component also includes capabilities such as identity provisioning and credential management to the organization's employees and contractors through access control policies, business continuity plans, and various productivity tracking mechanisms for use by the Consumer. These are the services that enable the secure daily operations of a business in a cloud environment.

**Annex E** provides the high-level SRA Security Components mapped to the Architectural Components of a cloud Consumer. The Secure Business Support Architectural Component is coded "B" under the "Consumer" section of the table.

The cloud Consumer *Secure Configuration* Architectural Component includes any capabilities, tools, or policies that ensure the secure configuration of cloud resources and compliance with the applicable security standards, specifications, and mandates (e.g., NIST SP 800-53 [Rev. 4]: *Minimum Security Requirements for Federal Information and Information Systems*, NIST SP 800-37 [Rev. 1]: *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, FIPS 199: *Standards for Security Categorization of Federal Information and Information Systems*) as well as requirements set forth in the SLA. Criteria for securely configuring cloud resources may also include proprietary measures that have been set forth between the cloud Consumer and cloud Provider.

Securely managing the configuration of a Consumer's cloud resources should address the following areas:

- *Rapid provisioning:* automatically deploying cloud systems based on the requested service/resources/capabilities. Securely managing rapid provisioning means, for example, ensuring that the requests are from an authenticated and authorized source.

- *Resource changing:* adjusting configuration/resource assignment for repairs, upgrades, and joining new nodes into the cloud. Securely managing resource changing means, for example, that requests for change in resources and changes in any configuration of resources are received from an authenticated and authorized source.

- *Monitoring and reporting:* discovering and monitoring virtual resources, monitoring cloud operations and events, and generating security reports. Performance reports in the context of security such as excessive use of resources compared to normal use.

- *Metering:* providing a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, active user accounts). Securely managing metering means that cloud Providers implement specific internal controls to ensure that storage can be encrypted, processing can be sandboxed, abnormal bandwidth usage can be reported, and user account management is in compliance with security policies of the consumer.

- *Service Level Agreement Management:* encompassing the SLA contract definitions (basic schema with the Quality of Service parameters), SLA monitoring, and SLA enforcement according to defined policies. In the context of secure configuration, the SLAs will need to provide ample visibility in order to ensure compliance with secure configuration management mandates as defined in NIST SP 800-53 (Rev. 4): *Minimum Security Requirements for Federal Information and Information Systems*.

**Annex E** provides the high-level SRA Security Components mapped to the Architectural Components of a cloud Consumer. The Secure Configuration Architectural Component is coded "C" under the "Consumer" section of the table.

### 4.2.1.3 SECURE PORTABILITY AND INTEROPERABILITY

The cloud Consumer's *Secure Portability and Interoperability* Architectural Sub-Component ensures that data and applications can be moved securely to multiple cloud Ecosystems while the risk mitigation measures in place are commensurate with the data security and privacy requirements and necessary level of protection. The Security Components mapped to this architectural subcomponent provide increased flexibility for data and/or applications transferred to different cloud Providers or technical Brokers.

Providers should offer Consumers a mechanism to interoperate their data and applications among multiple cloud Ecosystems through a secure and unified management interface. Requirements for secure portability and interoperability vary based on cloud service model adopted. Providers and Brokers should keep system maintenance time and disruptions (i.e., downtime) at an acceptable minimum level defined in the SLAs.

**Annex E** provides the high-level SRA Security Components mapped to the Architectural Components of a cloud Consumer. The Secure Portability/Interoperability Architectural Component is coded "I" under the "Consumer" section of the table.

The *Secure Organizational Support* Architectural Sub-Component covers policies, procedures, and processes provided by the organization in support of the overall cloud *Secure Consumption Management*.

Therefore, as the table in **Annex E** illustrates for a cloud Consumer, the Security Components mapped to the Organizational Support Architectural Sub-Component include (but are not limited to): Compliance Management; Audit Management under Governance Risk & Compliance; Technical Security Standards; Best Practice & Regulatory Correlation; and Information Security Policies under Policies and Standards.

**Annex E** provides the high-level SRA Security Components mapped to the Architectural Components of a cloud Consumer. The Secure Organizational Support Architectural Component is coded "O" under the "Consumer" section of the table.

NIST SP 500-292: *NIST Cloud Computing Reference Architecture* describes *Service Orchestration* as the composition of system components that support the cloud Provider's activities in arrangement, coordination, and management of computing resources, in order to provide secure cloud services to cloud Consumers.

As emphasized earlier in this document, *Secure Ecosystem Orchestration* is a process that requires various levels of secure participation from all cloud Actors – Consumer, Provider, Broker, and Carrier as necessary – with different degrees of involvement based upon the cloud service and deployment models.

The NCC-SRA expands on the generic stack diagram (depicted in **Fig. 15** above) of the composition that underlies the provisioning of cloud services (the three-layer model representing the three types of system components cloud Providers need to compose to deliver their services). In addition, the SRA extrapolates the cloud Provider's *Service Layer* to construct a *Secure Service Layer* Architectural Sub-Component for the Provider and Technical Broker, and the *Secure Functional Layer* Architectural Sub-Component for the Consumer (see **Fig. 16** below). The Secure Functional/Service Layer Architectural Sub-Components depict the participation of these cloud Actors in orchestrating the cloud Ecosystem and providing the necessary functionality based upon the Cloud's architecture and service model.
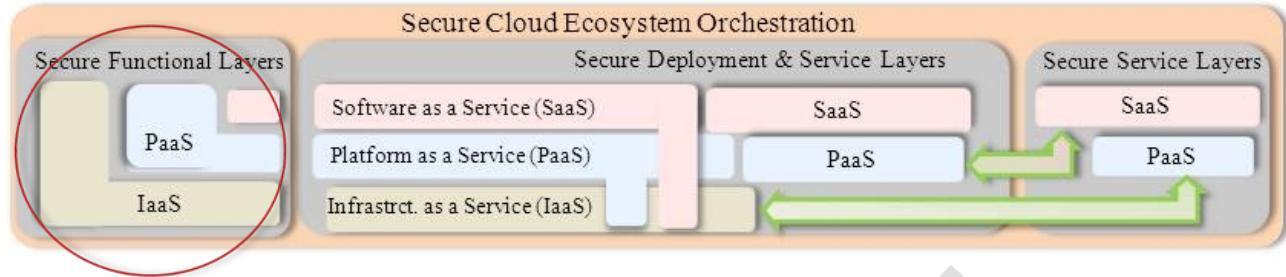
**Figure 16:** Secure Cloud Ecosystem Orchestration

A cloud Consumer may only secure its interface to the cloud service and the functional layers above this interface in the functionality stack. The interface to the cloud service can be at the IaaS, PaaS, or SaaS level, depending on the cloud model adopted. A cloud Consumer can only rely on the cloud Provider or Technical Broker to secure the service layers below this service interface.

**4.2.2.1** SECURE FUNCTIONAL LAYER

The set of Security Components a cloud Consumer implements to secure the cloud Functional Layer depends upon the particular cloud service model used. It is intrinsically correlated with the sets of Security Components implemented by the other cloud Actors involved in the cloud Ecosystem. The Secure Functional Layer Architectural Sub-Components for the Consumer are graphically represented in **Fig. 17**, below.
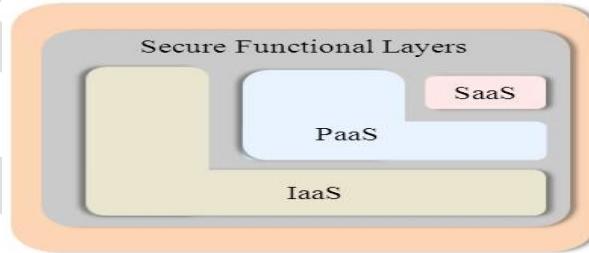


**Figure 17:** Secure Functional Layers

In a SaaS cloud Ecosystem, a cloud Consumer has only limited administrative control of the applications used – in other words, minimal control of the cloud and its Security Components.

In a PaaS cloud Ecosystem, a cloud Consumer has control over the applications and possibly some control over the hosting environment settings, but has limited or limited access to the infrastructure underlying the platform, such as the network, servers, OS, or storage media.

In an IaaS cloud Ecosystem, a cloud Consumer uses the provisioned infrastructure and computing resources, such as a virtual computer, for its fundamental computing needs. In this type of Ecosystem the Consumer has access to more fundamental forms of computing resources and also

Page 61

has more control over the software components in an application stack, including the OS and network.

For example, in an IaaS cloud Ecosystem, a Consumer may implement the Infrastructure Protection Service – Endpoint Firewall for all service models. However, a cloud Consumer would be unable to implement the Infrastructure Protection Service – Server Firewall Security Component for a PaaS or SaaS cloud. Instead, the cloud Consumer needs to rely on the cloud Provider's Server Firewall services, and therefore should make sure the desired level of protection is clearly stipulated in the SLA.

**Annex E** provides the high-level SRA Security Components mapped to the Architectural Components of a cloud Consumer. The Secure Functional Layer Architectural Sub-Component is coded "L" under the "Consumer" section of the table.

## 4.3    PROVIDER – ARCHITECTURAL COMPONENTS

NIST SP 500-292: *NIST Cloud Computing Reference Architecture* identifies the RA's Architectural Components based upon the areas in which a cloud Provider conducts its activities, as follows: service deployment, service orchestration, cloud service management, security, and privacy. Since security, privacy, data content management, and SLAs are cross-cutting concerns, the Security Reference Architecture formal model (**Fig. 14**) interlaces the Provider's security activities at all levels across all the Provider's areas of responsibility, embedding the security in all Architectural Components pertaining to the cloud Provider. Additionally, the cloud deployment is depicted in the NCC-SRA as part of the cloud Ecosystem orchestration, being directly correlated with the services offered by a cloud Provider. Therefore, the NCC-SRA formal model defines, for a cloud Provider, the following Architectural Components and Sub-Components:

- Secure Cloud Ecosystem Orchestration
    - Secure Deployment & Service Layers (L)
    - Secure Resource Abstraction and Control Layer (Hardware & Facility) – applicable only to a Primary Provider (R)
    - Secure Physical Resource Layer (Hardware & Facility) – applicable only to a Primary Provider (P)
- Secure Cloud Service Management
    - Secure Provisioning and Configuration (C)
    - Secure Portability and Interoperability (I)
    - Secure Business Support (B)

**Figure 18** below highlights the cloud Provider in the NCC-SRA formal model diagram, emphasizing the two types of Providers (Primary and Intermediary), and graphically represents the Architectural Components pertaining to each of them.
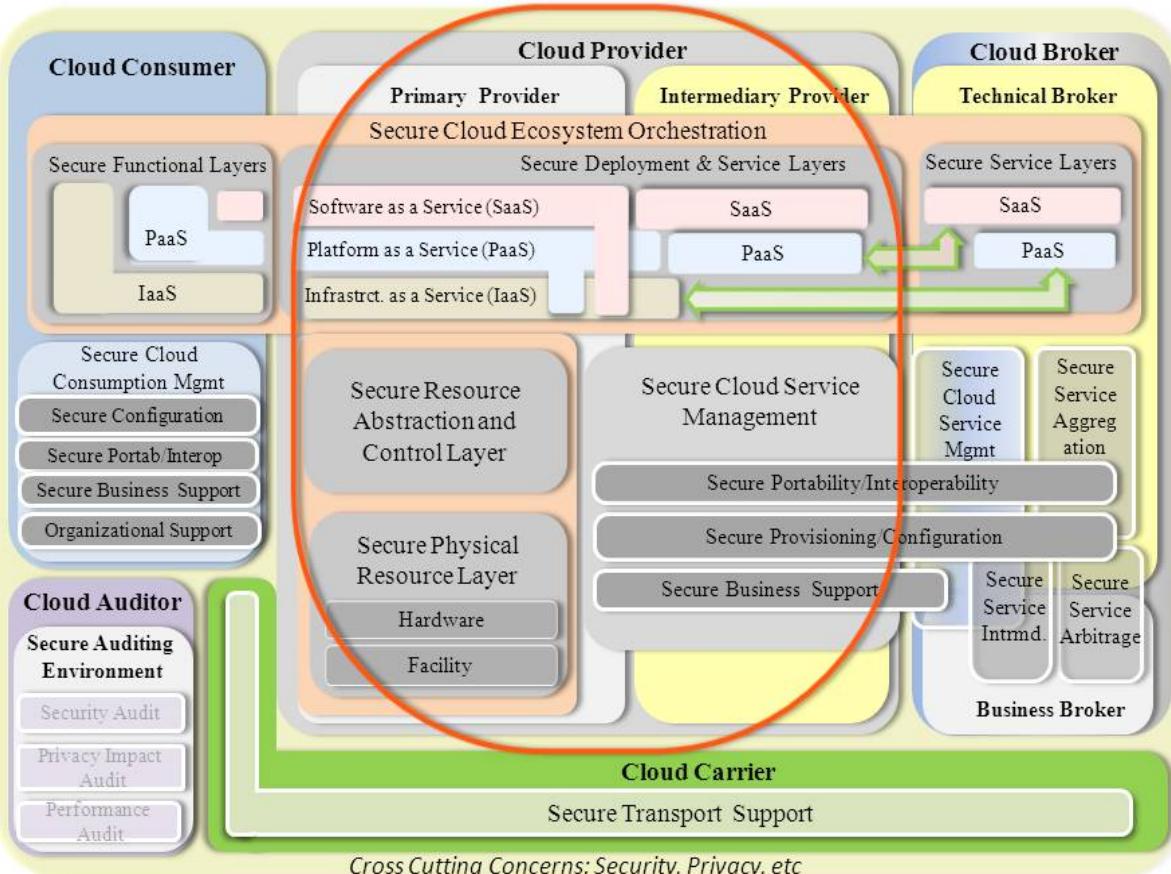
**Figure 18:** SRA – Cloud Provider

A primary Provider may deliver services to a cloud Consumer directly, through a Technical Broker, or through partnering with an Intermediary Provider. An Intermediary Provider delivers services to the cloud Consumer by integrating services provided by one or more Primary Providers. There is often a chain of dependency among multiple cloud Providers, and it is often hidden from the cloud Consumer. To the cloud Consumer, a Primary Provider and an Intermediary Provider deliver services in exactly the same fashion. An Intermediary Provider is responsible for the same Security Components and controls as a Primary Provider, and needs to coordinate among multiple Providers in order to implement the required Security Components and controls.

### 4.3.1 SECURE CLOUD ECOSYSTEM ORCHESTRATION

NIST SP 500-292: *NIST Cloud Computing Reference Architecture* describes *Service Orchestration* as the composition of system components that support the cloud Provider's activities in

arrangement, coordination and management of computing resources in order to provide cloud services to cloud Consumers.

The document identifies a three-layer model (as seen in **Fig. 18**) that represents the three types of system components cloud Providers need to compose to deliver their services. The three layers are:

1. The *service layer* that represents the three models of service a Provider can offer – SaaS, PaaS, and IaaS.
2. The *resource abstraction and control layer* that contains the system components a cloud Provider uses to provide and manage access to the physical computing resources through software abstraction.
3. The *physical resource layer* that includes all of the physical computing resources such as hardware resources (CPU and memory), networking equipment and software (routers, firewalls, switches, network links and interfaces), storage components (hard disks), and any other physical computing infrastructure elements.

**Figure 19** below expands upon the NIST RA diagram in **Fig. 13**. It identifies the Architectural Component for Provider-based Secure Cloud Service Orchestration for Providers as *Secure Cloud Ecosystem Orchestration*. This Architectural Component has similar generic stack composition that underlines the provisioning of cloud services for Providers:

- Secure Deployment and Service Layer (L)
- Secure Resource Abstraction and Control Layer (R)
- Secure Physical Resource Layer (P)

All three layers are discussed in more detail in the next three subsections.
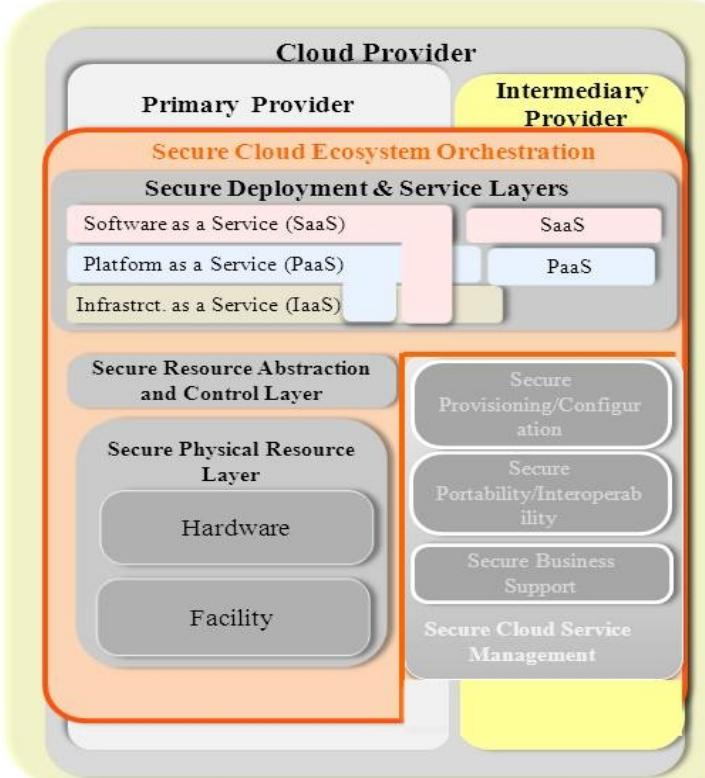
**Figure 19:** Secure Service Orchestration – Stack Diagram

SECURE DEPLOYMENT AND SERVICE LAYER

The set of Security Components a cloud Provider can implement to secure the Service Layer depends upon the particular type of cloud service offered (i.e., SaaS, PaaS, or IaaS) and the cloud deployment model (e.g., Public, Private). For each of the twelve instances of cloud Ecosystems, the set of Security Components a Provider is responsible for implementing is intrinsically correlated with the sets of Security Components implemented by the other cloud Actors involved in the cloud Ecosystem.
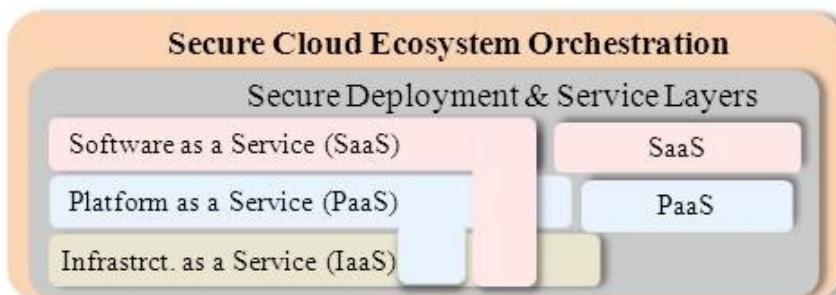


**Figure 20:** Secure Deployment and Service Layers

In an IaaS cloud Ecosystem, a cloud Provider owns and maintains the physical computing resources underlying the service, including the servers, networks, storage, and hosting infrastructure. The cloud Provider runs the cloud software necessary to make computing resources available to the IaaS cloud Consumers through a set of service interfaces and computing resource abstractions, such as virtual machines and virtual network interfaces. Regardless of the cloud Ecosystem offered, a cloud Provider always has control over the physical hardware and cloud software that makes the provisioning of these infrastructure services possible (e.g., the physical servers, network equipment, storage devices, host OS, and hypervisors for virtualization).

In a PaaS cloud Ecosystem, a cloud Provider manages the computing infrastructure for the platform and runs the cloud software that provides the components of the platform, such as the runtime software execution stack, databases, and other middleware components. A cloud Provider offering PaaS cloud Ecosystems also typically provides tools for the cloud Consumer's development, deployment, and management processes related to their services in the cloud. Such tools could be integrated development environments (IDEs), development versions of cloud software, software development kits (SDKs), or deployment and management tools.

For a SaaS cloud Ecosystem, the cloud Provider deploys, configures, maintains, and updates the operation of the software applications on the cloud infrastructure so that the services are provisioned at the expected service levels to cloud Consumers. The Provider of SaaS cloud Ecosystems assumes most of the responsibilities involved in managing and controlling the cloud applications and infrastructure.

**Annex E** provides the high-level SRA Security Components mapped to the Architectural Components of a cloud Provider. The Secure Service Layer Architectural Component is coded "L" under the "Provider" section of the table.

**4.3.1.2** SECURE RESOURCE ABSTRACTION AND CONTROL LAYER

The *Secure Resource Abstraction and Control Layer* is the Architectural Component that contains the Security Components a cloud Provider would implement to provide and manage secure access to its physical computing resources through software abstraction. Examples of resource abstraction components include software elements such as hypervisors, virtual machines, and virtual data storage. The resource abstraction components need to ensure efficient, secure, and reliable usage of the underlying physical resources. While virtual machine technology is commonly used at this layer, other means of providing the necessary software abstractions are also possible. The control aspect of this layer refers to the securing software components that are responsible for resource allocation, access control, and usage monitoring. This is the software framework that ties together the numerous underlying physical resources and their software abstractions to enable resource pooling, dynamic allocation, and measured services.
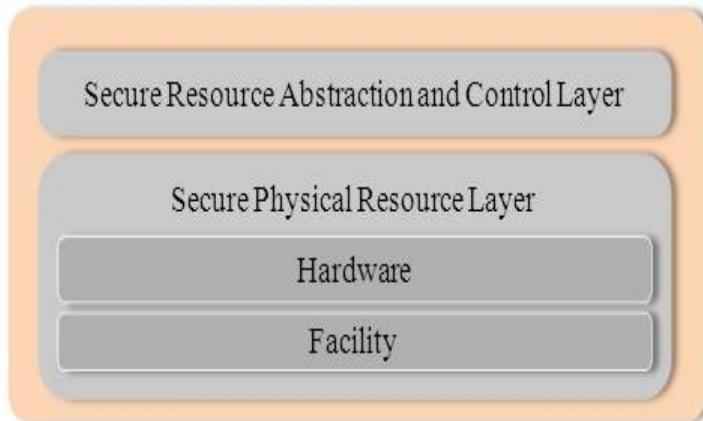
**Figure 21:** Secure Resource Abstraction and Physical Resource Layers

**Figure 21** above expands upon the NIST RA shown in **Fig. 13**. It identifies a generic stack of the composition that underlines the Secure Resource Abstraction and Control Layer – the Architectural Sub-Component discussed in this subsection – staked over the *Secure Physical Resource Layer,* discussed in the next subsection.

A cloud Provider should implement appropriate security mechanisms to ensure that only authorized users have access to systems, services, and data, and that one user or tenant cannot access the information of another tenant without proper permissions. The system should separate user-related functionality (including user interface services) from the system management functionality and should not expose the information system management-related functionality to non-privileged users. Security functions should be isolated from non-security functions and may be implemented as a layered structure, ensuring minimal interactions between layers and independence of the lower layers' functionality from the functionality of upper layers.

Applying the CRMF on behalf of a USG cloud Consumer and providing continuous monitoring is a responsibility shared among all cloud Actors involved in the cloud Ecosystem. Cloud Providers should implement well-structured, cost-effective automation processes for continuous monitoring of security controls to ensure their effectiveness and to provide near real-time measurements of security parameters in support of a risk-based decision process with regards to the organizational information systems operating in a cloud Ecosystem. As discussed earlier in **Sec. 4.2.1**, one possible solution that can support the continuous monitoring process and that would ensure proper security mechanisms are in place is the adoption of standards such as SCAP.

**Annex E** provides the high-level SRA Security Components mapped to the Architectural Components of a cloud Provider. The Secure Resource Abstraction and Control Layer Architectural Component is coded "R" under the "Provider" section of the table.

### 4.3.1.3 SECURE PHYSICAL RESOURCE LAYER

The *Secure Physical Resource Layer* (shown in **Fig. 21**) is an architectural subcomponent that contains the Security Components needed to secure physical computing resources. This layer includes hardware resources, such as computers (CPU and memory), networks (routers, firewalls, switches, network links, and interfaces), storage components (hard disks), and other physical computing infrastructure elements. It also includes facility resources, such as heating, ventilation and air conditioning (HVAC), power, communications, and other aspects of the physical plant.

**Annex E** provides the high-level SRA Security Components mapped to the Architectural Components of a cloud Provider. The Secure Physical Resource Layer Architectural Component is coded "P" under the "Provider" section of the table.

### 4.3.2 SECURE CLOUD SERVICE MANAGEMENT

NIST SP 500-292: *Cloud Computing Reference Architecture* describes cloud *Service Management* as the Architectural Component that includes all of the service-related functions necessary for the management and operation of those services offered to cloud Consumers. Cloud Service Management can be described from the perspective of:

- Provisioning and configuration requirements;
- Portability and interoperability requirements; and
- Business support requirements.

**Figure 22** below expands upon the NIST RA diagram shown in **Fig. 13**. It identifies the *Secure Cloud Services Management* Architectural Component of the SRA formal model, with similar generic stack composition that underlines the provisioning of cloud management. As the image depicts by stretching the graphical representation of the Architectural Component over both types of cloud Providers, secure cloud management is a service that both Primary and Intermediary Providers offer.
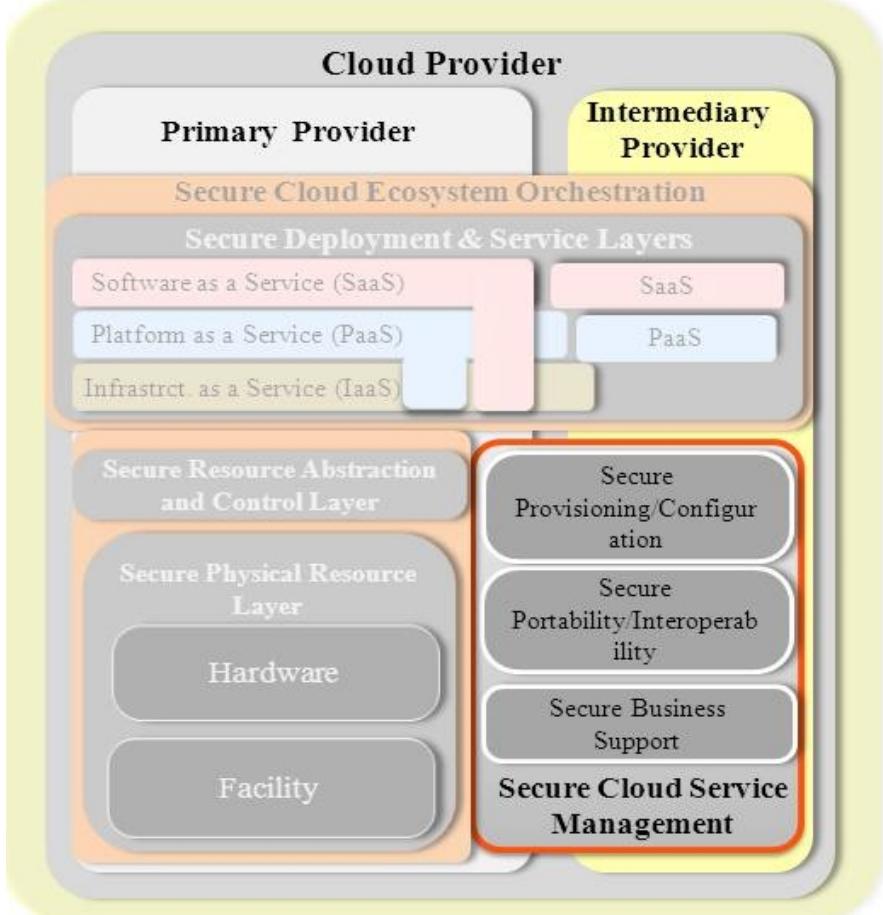
**Figure 22:** Secure Cloud Service Management – Stack Diagram

Moreover, different perspectives of the overall Secure Cloud Service Management can be supported and implemented by either a cloud Provider or a cloud Broker, depending upon the structure of each cloud Ecosystem. These services are supplemented by the cloud Consumer's *Secure Cloud Consumption Management*, discussed in **Sec. 4.2.1**.

The following sub-sections focus on the Architectural Sub-Components corresponding to the Secure Service Management activities offered by Primary and Intermediary Providers.

**4.3.2.1** SECURE PROVISIONING AND CONFIGURATION

The *Secure Provisioning and Configuration* Architectural Sub-Component includes all Security Components (such as capabilities, tools, or policies) that ensure the secure configuration and provisioning of cloud resources, with particular focus on compliance with the applicable security standards, specifications, and regulations. Criteria for securely configuring cloud resources may

also include proprietary measures that have been set forth between the cloud Consumer and cloud Provider in SLAs.

Securely managing the cloud resources configuration and provisioning should address, but not be limited to, the following areas:

- *Rapid provisioning:* Automatically deploying, in a secure manner, cloud systems based on the requested service, resources, or capabilities. Since availability of services is intrinsically correlated with the secure, rapid provisioning of cloud capability based on varying needs and demand levels, measures need to be taken to ensure that the deployment mechanisms and availability of new resources and capability are not subject to denial of service (DoS) attacks[9].

- *Resource changing:* Adjusting configuration/resource assignment for repairs, upgrades, and joining new nodes into the cloud based upon new and updated security configuration policies and requirements.

- *Monitoring and Reporting:* Discovering and monitoring virtual resources, monitoring cloud operations and events, and generating security reports that include abnormal performance measures. Reporting should provide enough visibility – preferably in an automated way – to support the Consumer's continuous monitoring requirements.

- *Metering:* Providing a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, active user accounts). Metering

---

[9] A Denial of Service (DoS) attack or Distributed Denial of Service (DDoS) attack can jeopardize the cloud service by saturating the limited network bandwidth and interrupting the configuration/routing information. A DoS or DDoS attack can also cause the computing platform to slow down responses to legitimate requests because it is overloaded with non-legitimate traffic. Since cloud computing provides the ability to rapidly provision computing resources and to detect possible bandwidth saturation by constantly probing the cloud applications, cloud availability, and capability to provide on-demand services (SaaS, PaaS, IaaS) can be disturbed by DoS or DDoS attacks. When bandwidth degradation is detected, the cloud Provider monitoring agent performs application migration – which may temporarily stop the services – to relocate the current application to another subnet. Malicious, excessive requests for cloud capabilities (services, bandwidth, and CPU time) can exhaust resources and impair the quality of service provided. For example, flooding is one kind of DoS attack that saturates computing resources and also interrupts the configuration/routing information. In cloud computing, there are two basic types of flooding attacks identified by Xiao Z. & Xiao Y. (2012) [19]:

- Direct DOS – the attacking target is determined, and the availability of the targeted cloud service is fully lost due to the attack.

- Indirect DOS – the attack is twofold: 1) all services hosted in the same physical machine with the target victim will be affected; and 2) the attack is initiated without a specific target.

capability needs to be protected from tampering.  Sufficient evidence of these protections will support Consumers in their efforts to meet monitoring requirements and mandates.

- *SLA management:* Encompassing the SLA contract definition (basic schema with the Quality of Service parameters), SLA monitoring, and SLA enforcement according to defined security policies.

**Annex E** provides the high-level NCC-SRA Security Components mapped to the Architectural Components of a cloud Provider.  The Secure Provisioning and Configuration Sub-Component is coded "P" under the "Provider" section of the table.

## 4.3.2.2  SECURE PORTABILITY AND INTEROPERABILITY

The *Secure Portability and Interoperability* Architectural Sub-Component for cloud Providers ensures that data and applications can be moved securely to multiple cloud Ecosystems, as established by cloud Consumer security requirements.  System maintenance time and disruptions (i.e., downtime) should be kept at an acceptable minimum level established in the SLA.  Providers should offer Consumers a mechanism to interoperate their data and applications along multiple cloud Ecosystems through a secure and unified management interface.

Requirements for secure portability and interoperability vary based on the cloud service model. For example, SaaS cloud Ecosystems may require data integration between multiple applications running in different clouds, whereas IaaS cloud Ecosystems require the ability to migrate the data and applications onto new clouds while ensuring the applications remain operational.  The first example may be as simple as performing data extractions and backing up data in a standard format.  The second example may require first capturing virtual machine images and then migrating them to one or more new cloud Providers who may use different virtualization technologies.

Configurations based upon the security policies of the Consumer as defined in the SLAs will also need to be preserved.  After migration, any provider-specific extensions to the virtual machine images need to be removed or recorded.  Cloud Providers need to understand and ensure portability and interoperability requirements set by cloud Consumers and meet them without raising any security concerns by implementing a rigorous process that maintains the operational status of all security controls during migration.

**Annex E** provides the high-level SRA Security Components mapped to the Architectural Components of a cloud Provider.  The Secure Portability and Interoperability Sub-Component is coded "I" under the "Provider" section of the table.

*Secure Business Support* entails the set of business-related services dealing with the Provider's Customers and supporting security processes. This Architectural Sub-Component includes the Security Components used to run client-facing business operations that support the Provider's role of enabling business support to cloud Consumers, cloud Brokers, and other cloud Providers involved in the orchestration of the cloud Ecosystem in a secure manner.

An Intermediary Provider needs to ensure that downstream Providers adequately implement the Security Components and controls that fall under their responsibility, and that risks and liability are appropriately addressed.

All Primary and Intermediary Providers in a cloud Ecosystem share all business support responsibilities, once those responsibilities have been identified and captured in the contracts with the cloud Consumer. Some of the Providers' business support responsibilities include:

- *Customer management*: Manage customer accounts, open/close/terminate accounts, manage user profiles, manage customer relationships by providing points-of-contact and resolving customer issues based upon security policies of the Consumer.
- *Contract management:* Manage service contracts, including setup, negotiation, and close/termination, to include supplying information that supports the Consumer's security auditing and reporting requirements.
- *Inventory Management:* Set up and manage service catalogs, etc. in a secure manner.
- *Accounting and Billing:* Manage customer billing information, send billing statements, process received payments, and track invoices to ensure that any fraudulent activities are identified, tracked, and corrected efficiently.
- *Reporting and Auditing:* Monitor end-users' operations, generate reports to support the Consumer's security auditing and monitoring requirements.
- *Pricing and Rating:* Evaluate cloud services and determine prices, handle promotions and pricing rules based on an end-user's profile without violating Consumer protections as afforded to them by the law.

**Annex E** provides the high-level SRA Security Components mapped to the Architectural Components of a cloud Provider. The Secure Business Support Sub-Component is coded "B" under the "Provider" section of the table.


## 4.4    BROKER – ARCHITECTURAL COMPONENTS

**Section 2.4.5** clarifies the role of the cloud Broker defined in NIST SP 500-292: *NIST Cloud Computing Reference Architecture*. The cloud Broker is defined as an entity that manages the use,

performance and delivery of cloud services, and negotiates relationships between cloud Providers and cloud Consumers.

**Figure 23** below highlights the cloud Broker in the Secure Reference Architecture formal model diagram, emphasizing the two types of Brokers (Technical and Business), and graphically representing the Architectural Components pertaining to them.
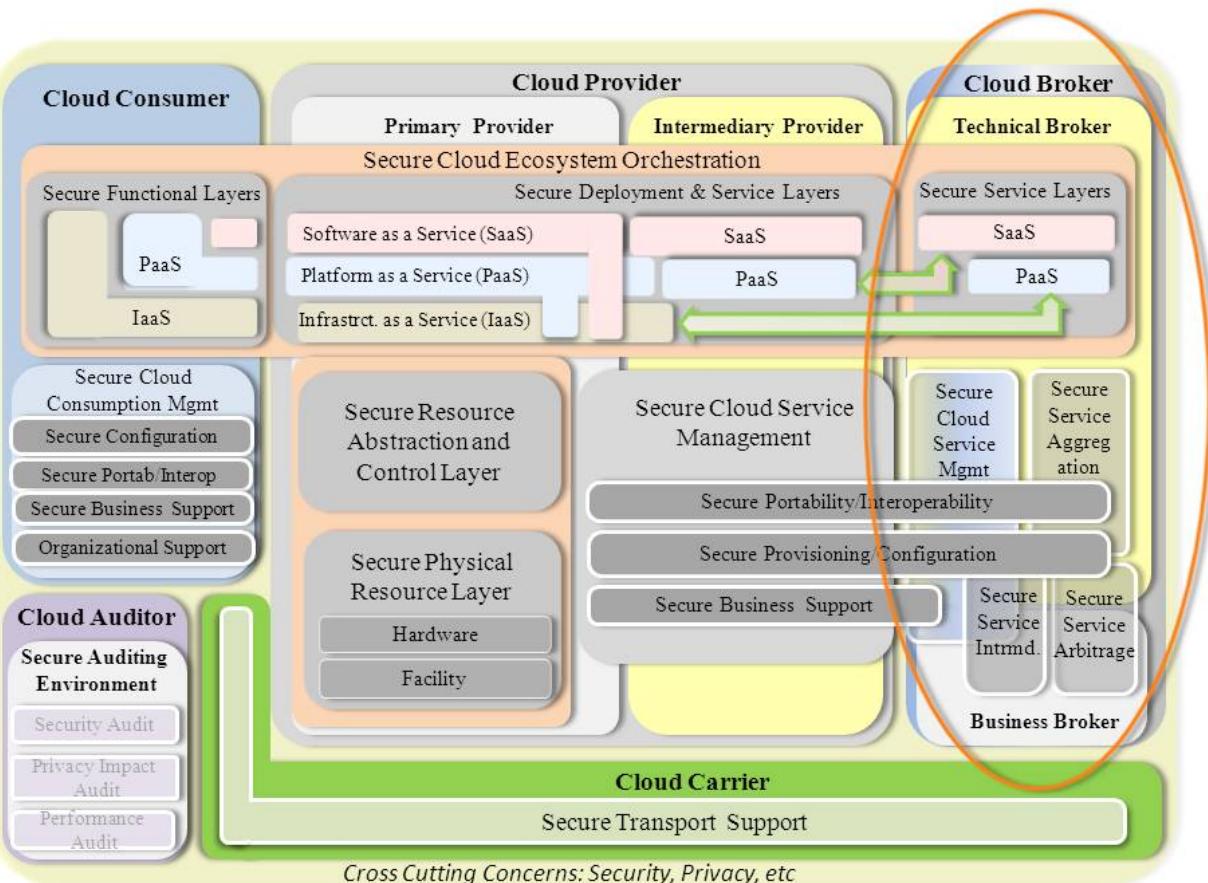


**Figure 23:** SRA – Cloud Broker

In general, a cloud Broker renders some combination of services that can be divided into five Architectural Component categories: Secure Service Aggregation, Secure Service Arbitrage, Secure Service Intermediation, Secure Cloud Service Management, and Secure Cloud Ecosystem Orchestration.  Four of those services correspond to the four Broker services identified in NIST SP 500-292: *NIST Cloud Computing Reference Architecture*, while the fifth one corresponds to the Broker's responsibility to secure the functionality of the offered service as part of the cloud Ecosystem orchestration.  Detailed definitions of these five Architectural Components are listed below:

Page 73

- *Secure Service Aggregation*: This Architectural Component includes the Security Components that support the fusion and integration of multiple isolated services into one or more new services. The cloud Broker provides data integration and ensures the secure movement of data between the cloud Consumer and multiple cloud Providers based upon the security policies of the Consumer. *Secure Service Aggregation* can be described from the perspective of the:
    - o portability and interoperability technical requirements; and
    - o provisioning and configuration technical requirements.
- *Secure Service Arbitrage*: This Architectural Component is similar to the *Secure Service Aggregation* component, except that the services being aggregated are not fixed. Service arbitrage means a cloud Broker has the flexibility to choose services from multiple Providers. The cloud Broker can, for example, use a credit-scoring service to measure and select a cloud Provider with the best score.
- *Secure Service Intermediation*: This Architectural Component includes the Security Components that facilitate the enhancement of a given service by allowing the cloud Broker to improve some specific capability and offer value-added services to cloud Consumers, while ensuring the security policies of the Consumer are maintained. The improvement can be managing access to cloud services, identity management, performance reporting, enhanced security, etc.
- *Secure Cloud Service Management:* This Architectural Component includes all Security Components that support the management of all service-related functions (technical and business) that are necessary for the operations of the services offered by the cloud Broker. Secure Cloud Service Management can be described from the perspective of the:
    - o business support requirements;
    - o provisioning and configuration business requirements; and
    - o portability and interoperability business requirements.

- *Secure Cloud Ecosystem Orchestration*: This Architectural Component includes all Security Components that a Technical Broker needs to implement to secure the functionality implemented and the additional services offered based upon the cloud deployment model (e.g., Private, Public) and service model (SaaS, PaaS, or IaaS).
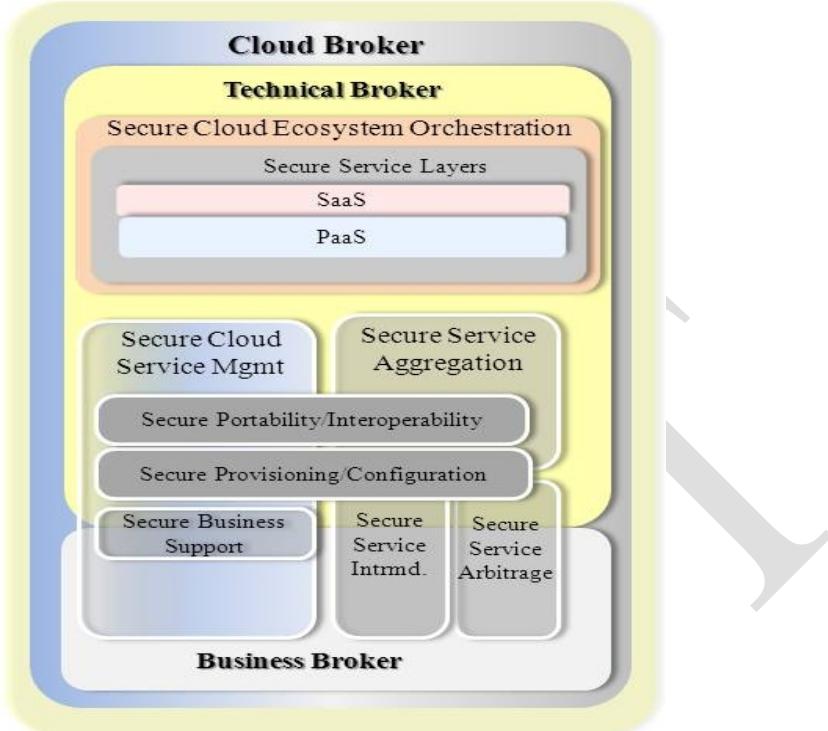
**Figure 24:** Cloud Broker – Architectural Components

The set of Security Components a Technical Broker could implement to protect the Consumer's data migrated to the cloud is, in practice, identical to the set of Security Components an Intermediary Provider that offers homologous services should implement. Additional information on how to extract the Technical Broker's set of Security Components is detailed in **Sec. 4.4.1**.

The shared responsibility of cloud actors to apply Security Components and control measures to varying degrees (least responsible to solely responsible to shared responsibility) is depicted in the Service-Based Ecosystem-Level Aggregation Data table in **Annex D**. Each cloud Actor, striving for unity of effort, provides an ecosystem of Security Components which augment and reinforce each other to protect the Consumer's data and operations in the Cloud.

### 4.4.1   TECHNICAL BROKER

**Figure 11** of this document depicts the Technical Broker having responsibilities similar to those of an Intermediary Provider in terms of securing cloud services with respect to the *Secure Cloud Ecosystem Orchestration* and the *Secure Cloud Service Management* Architectural Components.

As emphasized earlier in **Sec. 2.4.5.1**, a Technical Broker interacts with the Consumer's operational processes, cloud artifacts, and/or consumer data by aggregating services from multiple cloud Providers and adding a layer of technical functionality by addressing single-point-of-entry and

interoperability issues. In the SRA formal model the Architectural Components for the Broker in general and for the Technical Broker in particular are designed in such a way as to emphasize all major roles the Actor has. For example, the Secure Portability/Interoperability Architectural Sub-Component extends over Secure Service Management and Secure Service Aggregation (see **Fig. 24**) to indicate that for a Broker there are two aspects of this activity: a business/management aspect under Secure Service Management and a technical aspect under Secure Service Aggregation. Since an Intermediary Provider does not aggregate services but rather embeds services offered by a Primary Provider, the business and technical aspects of the activity cannot be separately identified. However, the overall set of Security Components that secure homologous services provided by a Technical Broker or an Intermediary Provider are the same.

**Figure 25** presents a generic stack diagram of the composition that underlies the Technical Broker's cloud services.
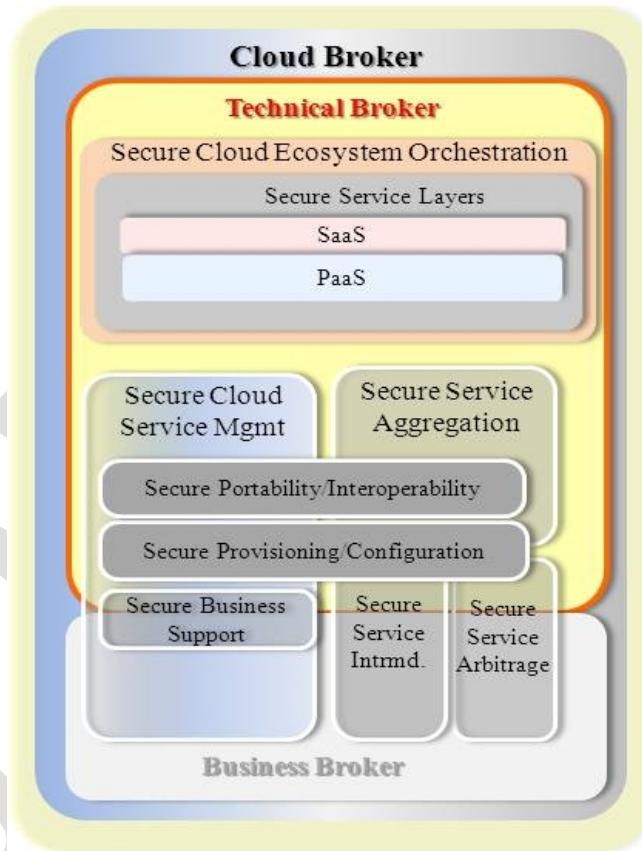


**Figure 25:** Technical Broker – Architectural Components

The diagram depicts the *Secure Cloud Ecosystem Orchestration* in addition to the four transparent Architectural Components that represent the four types of activities a cloud Technical Broker may perform to deliver their services. The overall set of Architectural Components and their Sub-Components is:

- Secure Cloud Ecosystem Orchestration
  - Secure Service Layer (technical aspects) (L)
- Secure Service Aggregation
  - Secure Provisioning/Configuration (technical aspects) (aC)
  - Secure Portability/Interoperability (technical aspects) (aI)
- Secure Service Management
  - Secure Portability/Interoperability (management aspects) (I)
  - Secure Provisioning/Configuration (management aspects) (C)
  - Secure Business Support (B)
- Secure Service Intermediation
  - Secure Provisioning/Configuration (technical aspects) (aC)
- Secure Service Arbitrage
  - Secure Provisioning/Configuration (technical aspects) (aC)

### 4.4.2  BUSINESS BROKER

**Section 2.4.5.1** described the Business Broker as a provider of business and relationship support services (arbitrage and business intermediation). In contrast to a Technical Broker, a Business Broker does not have any contact with the Consumer's data, operational processes, or artifacts (such as images, volumes, or firewalls) in the cloud.
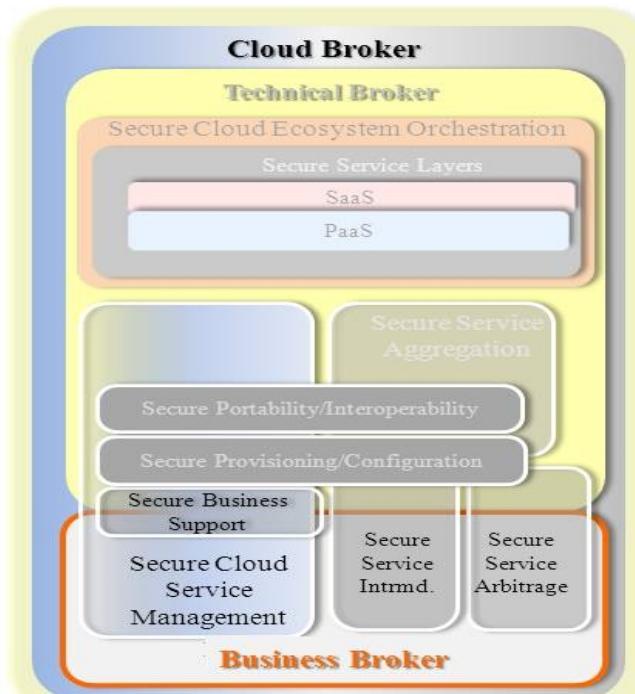


**Figure 26:** Business Broker – Architectural Components

Page 77

**Figure 26** above depicts the Business Broker role in providing security services within the NCC-SRA.

The diagram illustrates the three *transparent* Architectural Components that represent the three types of activities a Business Broker may perform to deliver their services. The graphical transparency depicts the operational transparency into the cloud Providers a cloud Broker is required to ensure for Consumers. The Architectural Components and their Sub-Components are:

- Secure Service Management
  - Secure Business Support (B)
- Secure Service Intermediation
  - Secure Provisioning/Configuration (business aspects) (C)
- Secure Service Arbitrage
  - Secure Provisioning/Configuration (business aspects) (C)

For the sake of brevity, the following section discusses the Architectural Components for both types of cloud Brokers, noting that the specific Architectural Components for each type of cloud Broker are identified above in this section and in **Sec. 4.4.1**.

### 4.4.3 SECURE CLOUD ECOSYSTEM ORCHESTRATION

The set of Security Components a cloud Broker can implement to secure the *Cloud Ecosystem Orchestration* Architectural Component depends upon the particular type of cloud service offered and the cloud deployment model. The set of Security Components a Broker is responsible to implement is intrinsically correlated with the sets of Security Components implemented by the other cloud Actors involved in the construct of the cloud Ecosystem.

**Figure 27** below expands upon the NIST RA diagram shown in **Fig. 13**. It identifies the same generic stack of the composition that underlines the provisioning of cloud services, emphasizing the core sets of security components for a cloud Broker involved in Secure Cloud Ecosystem Orchestration.
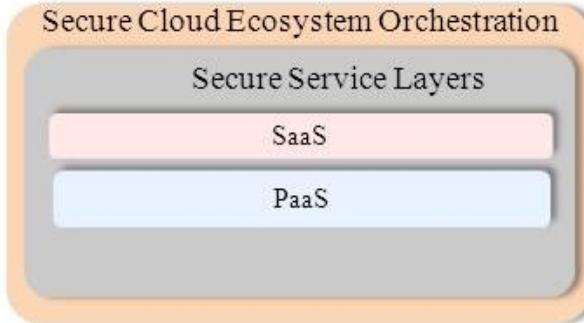


**Figure 27:** Secure Cloud Ecosystem Orchestration – Broker Stack Diagram

The diagram depicts the cloud Broker services at the Platform service layer or the Software service layer, built upon IaaS or PaaS cloud Providers respectively. A more detailed discussion on the *Secure Service Layers* is provided below.

### 4.4.3.1 SECURE SERVICE LAYERS

The set of Security Components a cloud Broker can implement to secure the Service Layer depends upon the particular type of service offered (e.g., PaaS or SaaS). It is possible to aggregate SaaS applications on PaaS components offered by multiple Providers, or to aggregate PaaS components built on Providers' IaaS components. However, this is not a necessity and the dependencies are optional. Each of the services can stand independently and may be offered separately. The security requirements for the technical Broker implementing additional functionality layers depend on the type of cloud service layers utilized.

For a SaaS cloud Ecosystem, a cloud Technical Broker could aggregate services offered by multiple Providers and could configure, maintain, and update the operation of the software applications deployed on those aggregated services so that they would be provisioned to cloud Consumers at the expected service levels and meet all identified security requirements. The technical Brokers offering SaaS cloud Ecosystems assume most of the responsibilities for managing and controlling the applications securely.

For a PaaS cloud Ecosystem, a cloud Technical Broker could securely aggregate services offered by multiple Providers and offer tools for the cloud Consumer's development, deployment, and management processes of their services in the cloud. Such tools could be IDEs, development versions of cloud software, SDKs, or deployment and management tools. The Broker could also offer tools and processes that secure such aggregation.

A Technical Broker does not participate in implementing Security Components and controls for the Resource Abstraction and Control Layer or the Physical Resource Layer.

**Annex E** provides the high-level SRA Security Components mapped to the Architectural Components of a cloud Broker. The Secure Service Layer Sub-Component is coded "L" under the "Broker" section of the table.

### 4.4.4   SECURE SERVICE AGGREGATION

A cloud Broker combines and integrates multiple services into one or more new services. The Broker provides data integration and ensures the secure movement of data between the cloud Consumer and multiple cloud Providers.

The *Secure Service Aggregation* Architectural Component addresses the Technical Broker's responsibilities to ensure that all data, including service requests and responses to and from cloud Providers, maintain the required levels of C/I/A. This Component also addresses the Broker's responsibility to ensure that appropriate levels of availability (for the Consumer to underlying Providers) are met, as per the Consumer's security requirements stated in the contract and SLA. As a service aggregator, the Technical Broker only supports the Consumer's data in transit: therefore the security requirements of data at rest are not within the scope of a technical Broker offering aggregation.

The set of Security Components covered by the Broker's Secure Service Aggregation Architectural Component is similar to the set of components an Intermediary Provider offering similar services would need to implement (see **Sec. 4.3**). The technical differences consist of the transparency offered by the cloud Broker into the underlying Providers. Reports, dashboards, and all plans should expose information on the actual underlying Providers, which is not necessarily the case with an Intermediary Provider.

The Technical Broker, positioned between cloud Consumers and multiple aggregated cloud Providers, should offer security services in both directions of the functional stack – upwards towards cloud Consumers and downwards towards the underlying cloud Providers. Correspondingly, all reports and plans should consider the Broker-Consumer interface and the Broker-Provider(s) interface.

Two Architectural Sub-Components are associated with Secure Service Aggregation:

- Secure Provisioning and Configuration
- Secure Portability and Interoperability

For a Technical Broker, the security requirements for provisioning and configuring particular functionality offered to cloud Consumers are in principle similar to the security requirements a cloud Provider has for securing equivalent functionality. The same applies to security requirements intended to ensure secure portability and interoperability (see **Sec. 4.3.2.1** and **Sec. 4.3.2.2** for additional information).

**Annex E** provides the high-level SRA Security Components mapped to the Architectural Components of a cloud Provider. The *Secure Service Aggregation* Architectural Component is basically comprised of the sum of Secure Provisioning and Configuration ("aC") mapping and Secure Portability and Interoperability ("aI") under the "Broker" section of the table.

**4.4.5**    SECURE CLOUD SERVICE MANAGEMENT

NIST SP 500-292: *NIST Cloud Computing Reference Architecture* describes cloud *Service Management* as the Architectural Component that includes all of the service-related functions that

are necessary for the management and operation of those services required by or proposed to cloud Consumers.  Cloud Service Management can be described from the perspective of:

- provisioning and configuration requirements;
- portability and interoperability requirements; and
- business support requirements.

**Figure 28** below expands upon the NIST RA diagram shown in **Fig. 13**.  It identifies a generic stack of the composition that underlines the provisioning of cloud Services Management, emphasizing the core sets of security aspects of the cloud management.

Different aspects of the overall Secure Cloud Service Management can be supported and implemented by either a cloud Provider or by a cloud Broker, depending upon the structure of each cloud Ecosystem.  These Architectural Components are supplemented by the cloud Consumer's Secure Cloud Consumption Management Architectural Component.



**Figure 28:** Secure Cloud Service Management – Broker Stack Diagram

*The Secure Cloud Service Management Architectural* Component has the following Architectural Sub-Components derived from the types of activities listed above that pertain to the management of cloud services:

- Secure Portability and Interoperability (I);
- Secure Provisioning and Configuration (C); and
- Secure Business Support (B).

**4.4.5.1** SECURE PORTABILITY AND INTEROPERABILITY

The *Secure Portability and Interoperability* Architectural Sub-Component for cloud Brokers ensures that data and applications can be moved securely between multiple cloud Ecosystems as required by the Cloud Consumer.  Brokers should keep system maintenance time and disruptions (i.e., downtime) at an acceptable minimum level defined in the SLAs.  They should also offer

Consumers a mechanism to interoperate their data and applications among multiple cloud Ecosystems through a secure and unified management interface. Requirements for secure portability and interoperability vary based on the cloud service model adopted.

**Annex E** provides the high-level SRA Security Components mapped to the Architectural Components of a cloud Broker. The Secure Portability/Interoperability Architectural Sub-Component is coded "I" under the "Broker" section of the table.

## 4.4.5.2 SECURE PROVISIONING AND CONFIGURATION

The *Secure Provisioning and Configuration* Architectural Sub-Component includes all Security Components, such as capabilities, tools, or policies, that ensure the secure configuration and provisioning of cloud resources, with particular focus on compliance with the applicable security standards, specifications, and regulations.

Securely managing the cloud resources provisioning and configuration involves one or more of the following activities:

- *Rapid provisioning:* Automatically deploying cloud systems based on the requested service/resources/capabilities, while ensuring the deployment mechanisms are authorized and protected from threats such as denial of service.
- *Resource changing:* Adjusting configuration/resource assignment for repairs, upgrades, and joining new nodes into the cloud based upon updated security configuration requirements form the Consumer.
- *Monitoring and Reporting:* Discovering and monitoring virtual resources, monitoring cloud operations and events, and generating performance reports to support continuous monitoring requirements and mandates.
- *Metering:* Providing a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, active user accounts) to authorized users using a mechanism that is protected from tampering.
- *SLA management:* Encompassing the SLA contract definition (basic schema with the Quality of Service parameters), SLA monitoring, and SLA enforcement according to defined security policies.

**Annex E** provides the high-level SRA Security Components mapped to the Architectural Components of a cloud Broker. The Secure Provisioning and Configuration Sub-Component is coded "C" under the "Broker" section of the table.

## 4.4.5.3 SECURE BUSINESS SUPPORT

A cloud Broker may provide business-related services by improving specific client-facing business operations and by offering value-added services to cloud Consumers. Such capabilities can be for example pricing and rating, contract management or accounting and billing.

The *Secure Business Support* architectural Sub-Component entails the set of business-related services that support Consumers' cloud consumption. The Sub-Component includes the *security components* used to run business operations in support of the Broker´s role as facilitator or agent supporting cloud Consumers.

Some of the Brokers' business support responsibilities are:

- *Customer management*: Manage customer accounts, open/close/terminate accounts, manage user profiles, manage customer relationships by providing points-of-contact and resolving customer issues and problems, etc. in accordance with Consumer's security requirements.
- *Contract management:* Manage service contracts, setup/negotiate/close/terminate contract, etc. to include the data and security requirements for continuous monitoring.
- *Inventory Management:* Set up and manage service catalogs, etc. securely.
- *Accounting and Billing:* Manage customer billing information, send billing statements, process received payments, track invoices, etc. that is authorized with the appropriate tools and processes to protect from fraudulent activities.
- *Reporting and Auditing:* Monitor users' operations; generate reports, etc. in accordance with security audit and reporting requirements of the Consumer.
- *Pricing and Rating:* Evaluate cloud services and determine prices, handle promotions and pricing rules based on a user's profile, etc. while protecting Consumer privacy.

**Annex E** provides the high-level SRA Security Components mapped to the Architectural Components of a cloud Broker. The *Secure Business Support* Sub-Component is coded "B" under the "Broker" section of the table

### 4.4.6 SECURE SERVICE INTERMEDIATION

A cloud Broker may enhance a given service by improving specific capabilities and offering value-added services to cloud Consumers. Such improvements can be, for example, managing access to cloud services, identity management, performance reporting, enhanced security, etc.

The *Secure Service Intermediation* Architectural Component (cI) addresses the Broker's responsibilities for ensuring that all capabilities added to existing cloud services offered by Providers maintain the required levels of C/I/A, and that the Consumer's requirements stated in the contract and/or SLA are met.

The Security Components that a Technical Broker offering service intermediation should implement are similar to the ones for service aggregation, but with additional emphasis and higher priority placed on the components and controls, depending on what value-added services are being offered by the intermediating Technical Broker. For example, a technical Broker offering only Identity Management (without any service aggregation or arbitrage offerings) operating as a third-party authenticator for cloud services should demonstrate strong controls in the NIST SP 800-53 (Rev. 4):

*Minimum Security Requirements for Federal Information and Information* Systems Identification and Authentication control family, while System and Communications Protection may be a lesser priority, since the Consumer's data in the cloud is not transiting the Broker's cloud system. However, the difference is only one of emphasis, since even for an intermediation service, such as performance reporting, a Broker should secure the system to ensure the reports are trusted, accurate, and provided only to authorized users.

**Annex E** provides the high-level SRA Security Components mapped to the Architectural Components of a cloud Broker. The Secure Service Intermediation Sub-Component is coded "cI" under the "Broker" section of the table.

### 4.4.7 SECURE SERVICE ARBITRAGE

The *Secure Service Arbitrage* Architectural Component is, in principle, similar to the *Secure Service Aggregation* component, with the exception that the services combined and integrated during arbitrage by the Broker are not fixed. This means that the Broker has the flexibility to dynamically choose services from multiple Providers and offer them to its cloud Consumers.

The Security Components a technical Broker offering service arbitrage should implement are similar to the ones for service aggregation, with particular emphasis on the capabilities that ensure secure service selection without service availability impairment and secure, rapid transition among the Providers under arbitrage. Also, Service Arbitrage Security Components should ensure that the levels of C/I/A required by the Consumer in the contract and/or SLA are met.

**Annex E** provides the high-level SRA Security Components mapped to the Architectural Components of a cloud Broker. The Secure Service Arbitrage Architectural Component is coded "cA" under the "Broker" section of the table.

## 4.5 CARRIER – ARCHITECTURAL COMPONENTS

As noted in **Sec. 2.4.6**, and depicted in **Fig. 29** below, the cloud Carrier is the cloud Actor that provides connectivity and transport of cloud services.

From the Consumer's standpoint, the cloud Carrier role is somewhat obscured due to the more direct relationship that a Consumer may have with a Provider and/or Broker – unless one of these parties performs the Carrier role as well. As such, the Cloud Carrier is required to provide *Secure Transport Support* for the cloud services offered by the Provider and/or Broker in order to meet contractual obligations and fulfill service requirements designated by them.
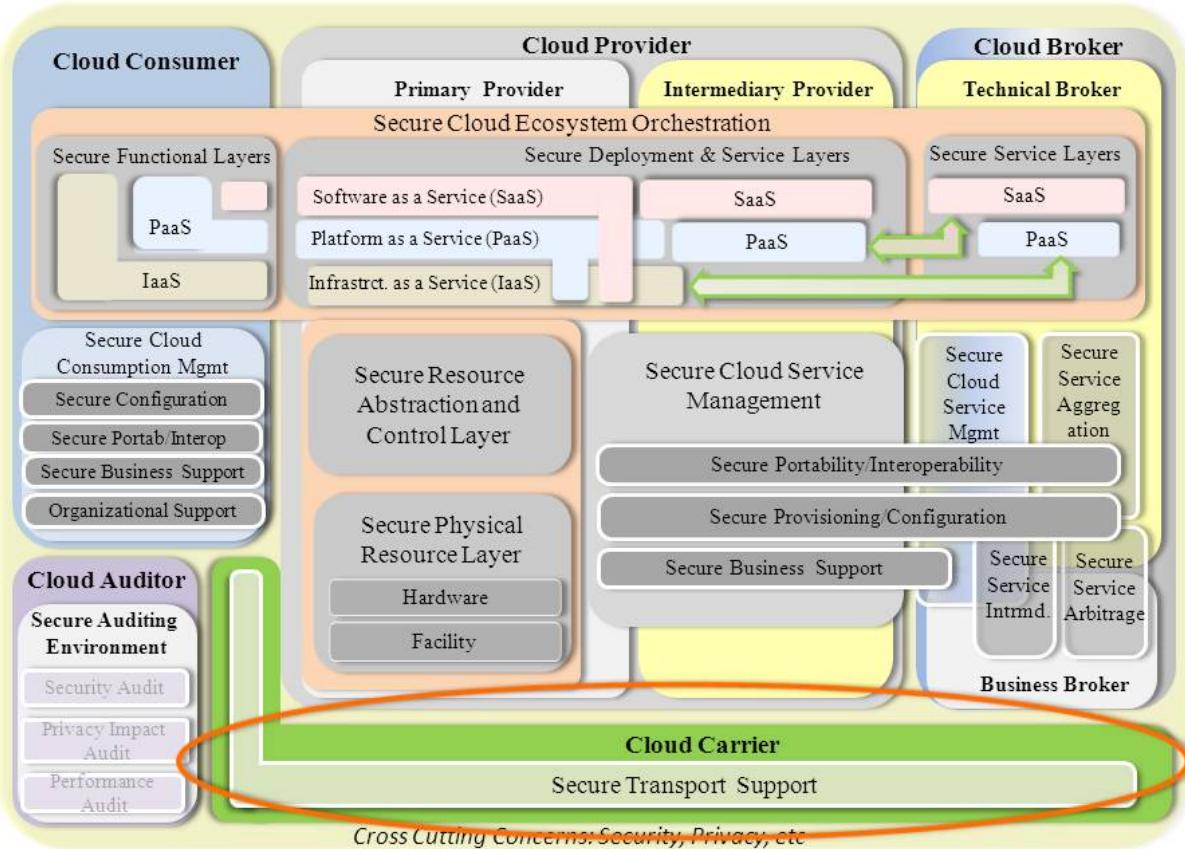
**Figure 29:** SRA – Cloud Carrier

The Cloud Carrier will also perform *Secure Service Management* functions to ensure service delivery and customer satisfaction; however, these functions are performed for internal purposes and not directly offered to the cloud Consumer.

**Annex E** provides the high-level SRA Security Components mapped to the Architectural Components of a cloud Carrier. The Secure Transport Support Architectural Component is coded "T" under the "Carrier" section of the table.

## 4.6    AUDITOR – ARCHITECTURAL COMPONENTS

As noted in **Sec. 2.4.7**, and depicted in **Fig. 30** below, the cloud Auditor is the cloud Actor who conducts independent assessments of cloud services, information systems operations, performance, privacy impact, and security of cloud implementations.
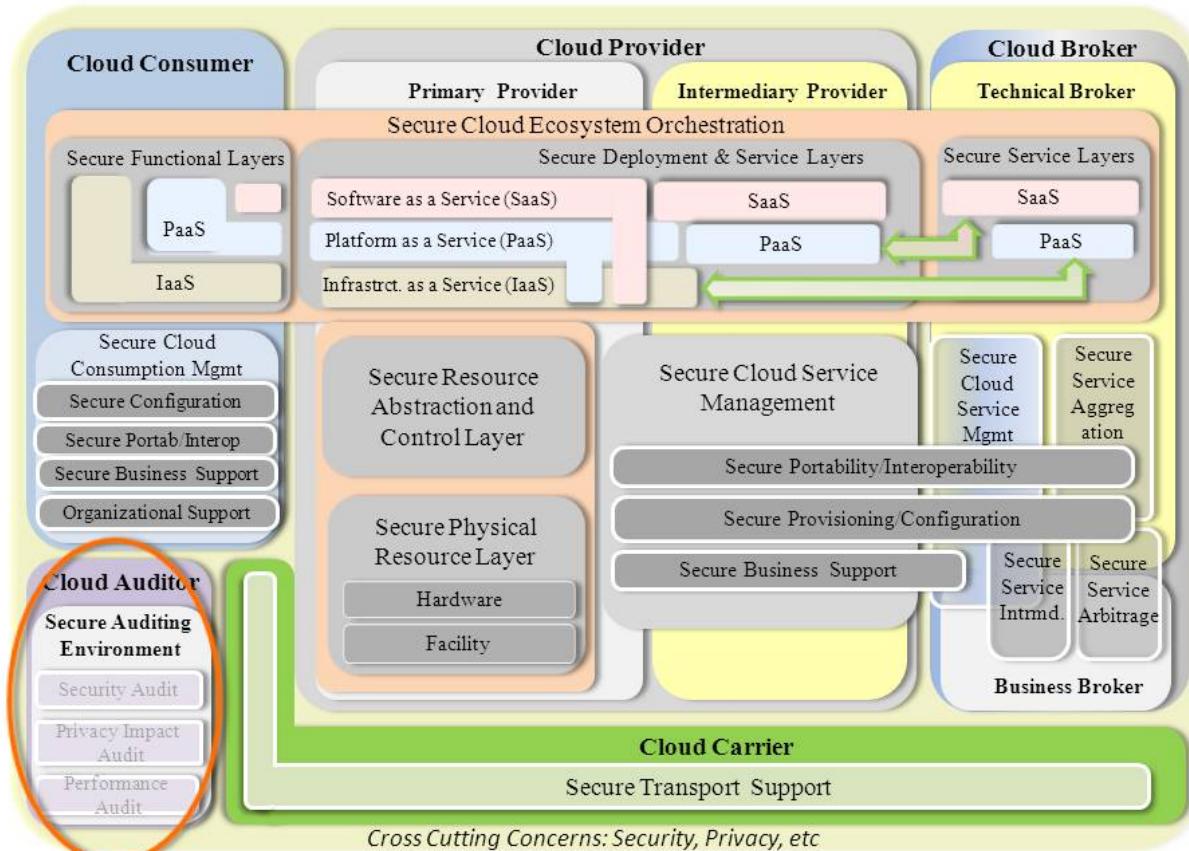
**Figure 30:** SRA – Cloud Auditor

Auditors can perform a large variety of audits for any of the other cloud Actors. The cloud Auditor requires a Secure Auditing Environment to enable the collection of objective evidence from responsible parties in a secure and trusted fashion. The Security Components and associated controls available to the cloud Auditor are typically independent of the type of cloud service model and/or cloud Actor audited.

The Secure Auditing Environment Architectural Component that supports cloud audit processes requires the following mechanisms (among others) to be in place:

- *Security Components and related security controls*: Information about the Security Components and the relevant security controls in place must be available to the Auditors.
- *Secure Archival*: In support of audit findings for legal and business processes, such as eDiscovery, archival requirements and implementations are available to the Auditors.

- *Secure Storage*: Objective evidence from responsible parties can be collected and stored in the cloud in a secure fashion for future reference, and thus encryption and obfuscation storage information can be made available to the Auditors.
- *Data Location*: During the assessment process, Auditors may be required to ensure that the relevant jurisdictional rules can be applied to the data and as such, data location information should be made available.
- *Metering*: Performance audits will require information from the metering systems in place and secure access to this information must be made available to the Auditors.
- *SLAs*: Service audits will require access to all agreements in place between the parties requiring the audit and the parties being audited, as well as any mechanisms that support the implementations of the SLAs in a secure manner.
- *Privacy*: Privacy Impact Assessments require the availability of system security and configuration information as well as any mechanisms implemented to protect data in the cloud Ecosystem.

**Annex E** provides the high-level SRA Security Components mapped to the Architectural Components of a cloud Auditor.  The Secure Auditing Environment Architectural Component is coded "E" under the "Auditor" section of the table.

# 5 SECURITY REFERENCE ARCHITECTURE: A METHODOLOGY OF ORCHESTRATING A CLOUD ECOSYSTEM

## 5.1 ORCHESTRATION METHODOLOGY OVERVIEW

The cloud Actors involved in providing or consuming cloud service offerings depend upon each other for securing the cloud Ecosystem. This dependency in orchestrating a secure cloud Ecosystem is defined by those interactions between the cloud Actors for implementing and integrating the Security Components that are relevant for each use case, and by the constructs among these Security Components. Depending on the service model being considered, cloud Actors may be either solely responsible for fulfilling the security requirements or may share the responsibility for doing so to some degree.

In any case where the responsibilities for implementing Security Components and protecting the operations and data in the Cloud are split among the Consumer, the Broker, and Provider, regulatory and/or other security requirements need to be articulated and orchestrated among the cloud Actors involved in architecting, building, and operating the cloud Ecosystem. For example, in the case of implementing Intellectual Property (IP) protections, the cloud Consumer will need to mark their IP information in transit to/from and at rest in the cloud to clearly indicate that it is not to be shared with others. In turn, the cloud Provider will assert that the IP is indeed protected and will secure and maintain it this way.
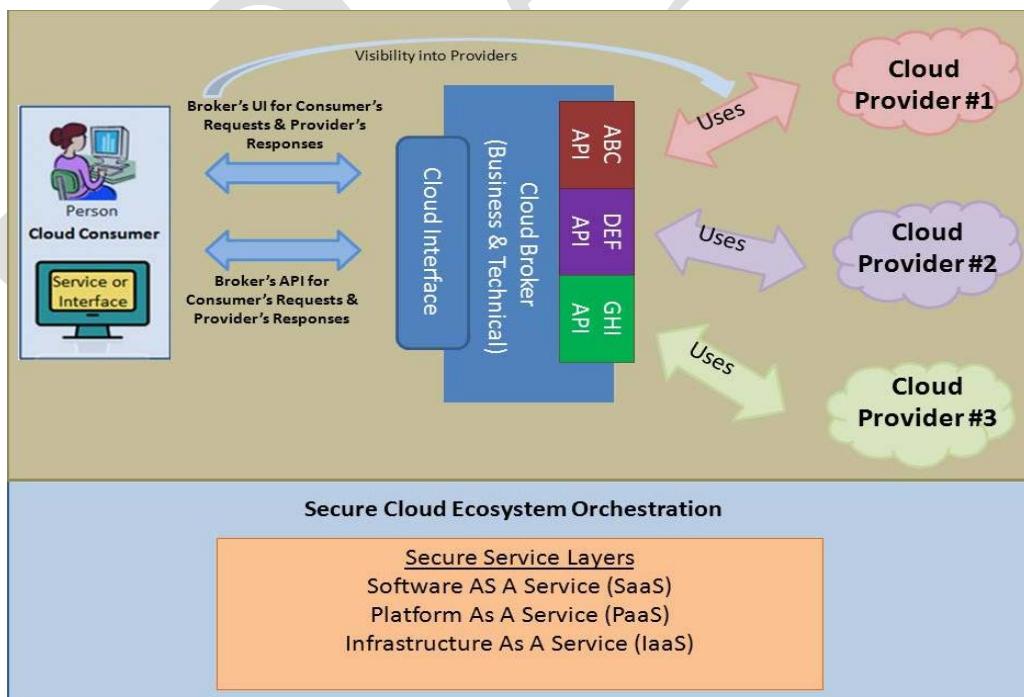


**Figure 31:** Secure Cloud Ecosystem Orchestration – Actors Interactions

**Figure 31** depicts the interactions between the Consumer, the Provider, and the Broker while orchestrating a secure Cloud Ecosystem. These interactions are defined for each of the Secure Service Layers described in NIST SP 500-292: *Cloud Computing Reference Architecture*: SaaS, PaaS, and IaaS.

## 5.2    CLOUD ECOSYSTEM ORCHESTRATION USE CASE

To better illustrate the interactions among cloud Actors and their roles and responsibilities in orchestrating a Secure Cloud Ecosystem, this document includes a use case of a USG agency service selected for migration to the cloud. The details in this use case are provided for purposes of illustration only; those in actual implementations will vary. The use case follows all the necessary steps to orchestrate a Secure Cloud Ecosystem, and identifies the security requirements and the Security Components that need to be implemented to secure the Ecosystem prior to adding important data and functionality. The approach presented in this section leverages the data aggregated for the NCC-SRA. This example follows the CRMF steps introduced in **Sec. 2.3.1**

The use case illustrates, from the cloud Consumer's perspective, the approach of applying the CRMF steps described in **Sec. 2.3.1** when tasked with migrating a service or an in-house application to the cloud Ecosystem. The scope of this exercise is to exemplify the process of securely orchestrating, in collaboration with the other cloud Actors, a cloud Ecosystem for the migration of the Consumer's Unified Messaging Service (UMS) to the cloud. This section provides more details for Step 1, 2 and 3, highlighting how to leverage the information provided in this document to complete Step 2. The rest of the steps are reviewed at a high level, with pointers to additional NIST work, when available. The CRMF steps are summarized below:

- **Step 1: Categorize** the system,
- **Step 2: Identify** the security requirements,
- **Step 3: Select** the cloud Ecosystem architecture,
- **Step 4: Assess** the other cloud Actors (i.e. Provider, Broker),
- **Step 5: Authorize** the use of the selected Provider(s) and Broker, and
- **Step 6: Monitor** the services provided.

### 5.2.1    STEP 1 – CATEGORIZE THE SYSTEM - CONSUMER'S SERVICE DESCRIPTION

The cloud Consumer aims to reduce the cost of IT services support by implementing a cloud-based UMS. This service includes e-mail, calendar, synchronization with wireless mobile devices, and collaboration services. The current e-mail system is classified as a Moderate Impact system based

on FIPS 199: *Standards for Security Categorization of Federal Information and Information Systems* [16].

### *In-House Messaging Service Capabilities*

The current e-mail system includes multiple platforms for integrated messaging, calendar, and collaboration, as well as a single sign-on (SSO) capability. The system also supports multiple clients, including e-mail (e.g., Outlook, Thunderbird, MacMail, Entourage), calendar software (e.g., Outlook 2007, Outlook 2010, iCalendar), and common browsers (e.g., Internet Explorer 7.0, 8.0 & 9.0, Chrome, Firefox 3.x, Safari) on operating systems such as Windows, Linux, and Mac OS. The current system also implements tools for spam filtering, virus and malware protection, screening of outbound messages, and auto-forwarding restrictions.

### *Cloud-Based Unified Messaging System Functional Requirements:*

The new cloud-based UMS implementation is required to seamlessly support all the capabilities of the current system. In addition, the Consumer expects to improve the management of the service and to expand collaboration capabilities through increased use of integrated messaging and collaboration tools. The new UMS should decrease system maintenance responsibilities for the Consumer, and provide end-users with new features as they become available within the cloud-based solution.

The UMS solution must include instant messaging and web conferencing. It must also provide users with the ability to share and collaborate on documents with both internal users and authenticated external users through a document repository. All aspects of the UMS must be accessible through a single unified User Interface (UI) portal.

Continuity and/or portability of services should be supported to enable prompt resumption services in the event of failures or catastrophes.

Optionally, the Consumer seeks to obtain archival and e-Discovery capabilities. In support of the data retention and e-Discovery capabilities for the cloud-based UMS, immutable, irrefutable archives for litigation holds would be created from both archived and active files using enhanced search capability, without affecting the ability of users to manage their data or files.

The classification of the in-house e-mail system as a Moderate Impact system is also targeted for the cloud-based UMS.

### 5.2.2    STEP 2 – IDENTIFY SECURITY REQUIREMENTS - A CLOUD SOLUTION ANALYSIS

After identifying all functional requirements for the system migrated to the cloud, the Consumer may leverage the SRA to: perform a risk assessment and identify the Security Components that

should be implemented to secure the UMS; prioritize them by performing a C/I/A analysis; and select the necessary security controls that best suits their needs for the UMS.

### 5.2.2.1 THE SECURITY INDEX SYSTEM

For the sake of building more flexibility into the SRA framework, this section introduces a Security Index System (SIS). We provide in **Table 5**: Security Indexes System, below, the definitions for each index based upon the adverse effects caused by the loss of C/I/A. The definitions leverage those provided by the Committee on National Security Systems in CNSSI No. 1253: *Security Categorization and Control Selection for National Security Systems* [4]. Each index of the SIS has an associated value that can be interpreted as a priority weight when applied to a Security Component.

The section shows how the cloud Consumer can assign Security Indexes to each Security Component (**Annex E)** considering the UMS service's need for C/I/A. Additionally, an Aggregated Security Index System (ASIS) can be obtained for each Security Component by summing the individual Security Indexes of the C/I/A security triad. The ASIS can be used to prioritize the implementation of the Security Components. A prioritization heat map, like the one presented in **Annex F** for the use case, can be created using the ASIS values. When necessary, heat maps of each of the C/I/A security triad's components can be created using the individual values of the Security Index in the same way demonstrated in the sample ASIS heat map. **Annex F** presents the ASIS values and can be used to prioritize the Security Components for the UMS use case. The SIS example given in this document is not provided as guidance for any UMS migration to the cloud.

To obtain an Actor-centric micro perspective or a more granular evaluation of the Security Components' implementation priority, each cloud Actor involved in the orchestration of the cloud Ecosystem can apply a logical-conjunction operation (logical "AND") between the Security Index of each C/I/A triad member and a Boolean applicability-value of 0 or 1 (0 for an empty cell or 1 for an X, B, or A cell as reflected in the **Annex D 11.1** table, for the service model adopted.

#### Table 5: Security Indexes System

| Security Index Symbol | Security Index Value | Security Index Applicability |
|---|---|---|
| SI0 | 0 | SI0 should be applied to a Security Component if the loss of a Confidentiality, Integrity, or Availability property associated with the Component is expected to have **no** adverse effects on the cloud Ecosystem's security posture. |
| SI1 | 1 | SI1 should be applied to a Security Component if the loss of a Confidentiality, Integrity, or Availability property associated with the Component is expected to have **limited**\* adverse effects on the cloud Ecosystem's security posture. |

| Security Index Symbol | Security Index Value | Security Index Applicability |
|---|---|---|
| SI2 | 2 | SI2 should be applied to a Security Component if the loss of a Confidentiality, Integrity, or Availability property associated with the Component is expected to have **serious\*\*** adverse effects on the cloud Ecosystem's security posture. |
| SI3 | 3 | SI3 should be applied to a Security Component if the loss of a Confidentiality, Integrity, or Availability property associated with the Component is expected to have **severe\*\*\*** adverse effects on the cloud Ecosystem's security posture. |
| SI4 | 4 | SI4 should be applied to a Security Component if the loss of a Confidentiality, Integrity, or Availability property associated with the Component is expected to have **critical\*\*\*\*** adverse effects on the cloud Ecosystem's security posture. |

The key words (in bold characters) that describe the Security Index Applicability in Table 5 above are defined as follows:

\* A **limited** adverse effect means that the loss of a C/I/A property might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of those functions is noticeably reduced; (ii) result in minor damage to organizational, critical infrastructure, or national security assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

\*\* A **serious** adverse effect means that the loss of a C/I/A property might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of those functions is significantly reduced; (ii) result in significant damage to organizational, critical infrastructure, or national security assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals exceeding mission expectations.

\*\*\* A **severe** adverse effect means that the loss of a C/I/A property might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational, critical infrastructure, or national security assets; (iii) result in major financial loss; or (iv) result in severe harm to individuals exceeding mission expectations.

\*\*\*\* A **critical** adverse effect means that the loss of a C/I/A property might: (i) generate vulnerabilities in system architecture/design or sabotage or subversion of a system's security functions or critical Security Components, as defined in NIST SP 800-53 (Rev. 4): *Minimum Security Requirements for Federal Information and Information Systems*; (ii) cause a catastrophic

loss of mission capability to such an extent and duration that the organization is not able to recover one or more of its system security functions; (iii) result in irrecoverable failure to organizational, critical infrastructure, or jeopardized national security assets; (iv) result in total financial loss; or (v) result in catastrophic harm to individuals exceeding mission expectations.

Coupling the prioritized set of Security Components with the data aggregated in the SRA that indicates cloud Actors' responsibilities for implementing and integrating the Components for different service models, the Consumer can make an informed decision regarding the cloud deployment model and service model that best suits the needs of their UMS.

## 5.2.2.2 SECURITY CONTROLS OVERVIEW

With the complete set of Security Components identified for the cloud Consumer, cloud Technical Broker, and cloud Providers, associated with the SIS and ASIS, the Consumer needs to ensure that, after migration to the cloud, the UMS remains compliant with FISMA and any other applicable mandates, standards, and requirements.

The cloud Consumer will perform a risk assessment and determine which security controls must be implemented for each Security Component identified as needed, for each cloud Actor involved in the Cloud Orchestration for the UMS. The Consumer will transitively apply the SIS for the C/I/A security triad and the ASIS to the selected security controls. The ASIS may provide a prioritization of the security controls. The cloud Consumer determines which security controls it is responsible for implementing in-house and which controls fall under the implementation responsibilities of the other cloud Actors.

When selecting an initial set of baseline security controls, applying tailoring guidance, and identifying any supplemental controls determined by the risk assessment, the cloud Consumer follows the guidance provided in Step 2 of the NIST CRMF, as described in **Sec. 2.3.1**. Other cloud Actors involved in supporting the cloud Ecosystem Orchestration should follow all the steps described in that section as well.

## 5.2.3 STEP 3 – SELECT THE CLOUD ECOSYSTEM ARCHITECTURE

The information aggregated in Step 2 (see **Sec. 5.2.2**) aids the cloud Consumer in selecting the cloud Ecosystem composition that best matches their internal expertise and required assurance levels. In this use case example, the Consumer selects for the implementation of the cloud-based UMS a SaaS type of Public cloud. Such a model will allow the Consumer to create, destroy, archive, and terminate individual user accounts automatically for their employees, without consuming resources for the underlying cloud infrastructure or individual application capabilities beyond selecting the application that meets its mission-critical requirements and negotiating, when necessary, the additional security controls that need to be implemented by the cloud Broker or Provider to support the necessary security posture for the UMS.

The Consumer delegates the responsibilities for installing, patching, upgrading, and backing up applications and the associated data to the cloud Provider and/or Technical Broker. However, the Consumer needs to be presented with verifiable proof that these operations are performed correctly and securely.

To achieve all of the aforementioned capabilities and comply with applicable requirements, the Consumer seeks advice from a cloud Broker on selecting an optimal mix of cloud Providers who can provide adequate secure business support and assurance levels. The cloud Consumer also seeks a full range of Technical Broker-based intermediation and service aggregation capabilities for aggregating services from multiple cloud Providers to meet its minimum requirements for service availability and capabilities (such as SSO). The Broker will provide the User Interface (UI) portal and Application Programing Interface (API) for these services in addition to the business arbitrage, secure service management, technical cloud service aggregation, and intermediation to provision, manage, and continuously monitor the cloud service across all selected cloud Providers for secure performance, recovery or other business purposes.

The cloud Broker, in its technical brokerage role, implements federated identity management and secures cloud infrastructure service orchestration within and across cloud service Providers. The Broker also integrates service-level and secure portability/interoperability metrics reporting across all cloud Providers.

In the interaction with the cloud Broker, the Consumer describes their business, technical, and secure business/organizational policy requirements. The cloud Broker, operating in a business brokerage mode, provides options that can meet the Consumer's needs and manages relationships with cloud Providers, including ensuring transparent access into cloud Provider services appropriate to the Consumer's requirements.

In sum, to increase availability and system resilience, the cloud-based UMS will be hosted by multiple cloud Providers, all known to the cloud Consumer, and to cross-border entities, third-party contractors, and subcontractors. A Technical Broker aggregates these services, and also enables additional functionality by providing a single or integrated suite of UIs and APIs for all the aggregated services. In this use case, the Technical Broker offers business brokerage arbitrage capabilities combined with technical brokerage interoperability, provisioning-intermediation, and aggregation, to provide an automated or semi-automated expert system for Secure Service Arbitrage, Secure Cloud Service Management, and Secure Service Aggregation (see **Sec. 4.4** for more details).

An overall list of all categorizations and aspects of the secure Cloud Ecosystem Orchestration use case are summarized in **Annex F**.

### 5.2.4    STEP 4 – ASSESS CLOUD SERVICES

The sets of security controls identified in Step 2 are translated into service requirements as part of the SLA negotiation process (described later in this section).

With the sets of security controls identified for each of the Security Components for each cloud Actor, and with the ASIS transitively inherited by the security controls from the Security Components, the cloud Consumer may proceed with the SA and SLA negotiation processes.

As described in **Sec. 2.3.2**, in selecting the cloud Providers and cloud Brokers, a USG cloud Consumer needs to also ensure that the selected parties have successfully completed the FedRAMP's A&A process and have been issued an ATO.

**Figure 32** presents in a side-by-side view:

- the steps followed above for applying the CRMF (left side of the diagram) and
- the FedRAMP A&A process (right side diagram).

The diagram emphasizes that a cloud Consumer remains responsible for performing a risk assessment analysis, identifying all the security requirements for their cloud-based service(s), and selecting the appropriate security controls before it consults FedRAMP's secure repository of authorized cloud suppliers to select the authorized Provider(s) and/or Broker(s) that best meet the Consumer's needs (see **Section 2.3.2** for more information).    Analyzing the cloud suppliers' Provisional ATOs, identifying remaining security controls that should be implemented to secure the service or application, and identifying the cloud Actors responsible for implementing them are very important steps in successful migration of the service or application to the cloud. The set of remaining security controls need to be addressed in agreements between the Consumer and other relevant cloud Actors.
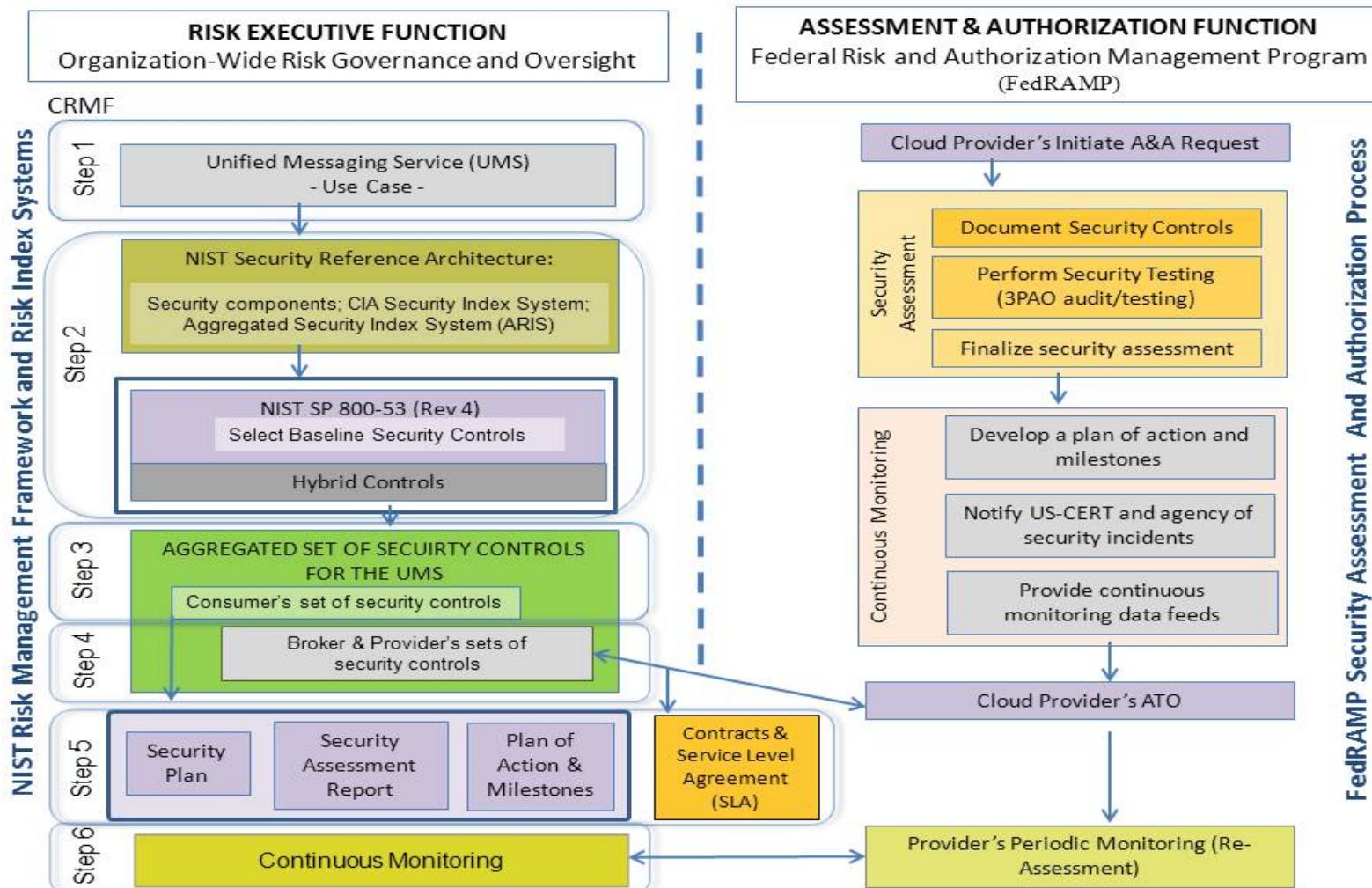
**Figure 32:** NIST Risk Management Framework and the FedRAMP A&A Process

**Figure 33** below depicts a *mind map* of the basic components of an SA, including the corresponding SLA (highlighted in blue).

The SLA is the component of the SA that details the levels and types of services that are to be provided, including but not limited to the delivery time and performance parameters. Cloud Providers use service-based agreements to detail their offers and the terms of their services to potential Consumers. In some cases, a cloud Consumer might be satisfied with the cloud Provider's offer and service terms: however, there are instances when the cloud Consumer is interested in a customer-based agreement and a customized service. The Consumer needs to pay special attention to the SLAs and involve the agency's procurement, technical, and policy experts to ensure that the terms of the SLA will allow the agency to fulfill its mission and performance requirements.

The ability of a Consumer to compare different offerings of cloud services depends on the ability to easily and accurately compare the underlying provisions of varying contracts and SLAs offered by potential cloud Providers. This comparison capability is critical to the Consumer in selecting a service that will meet all requirements at competitive cost and quality levels.
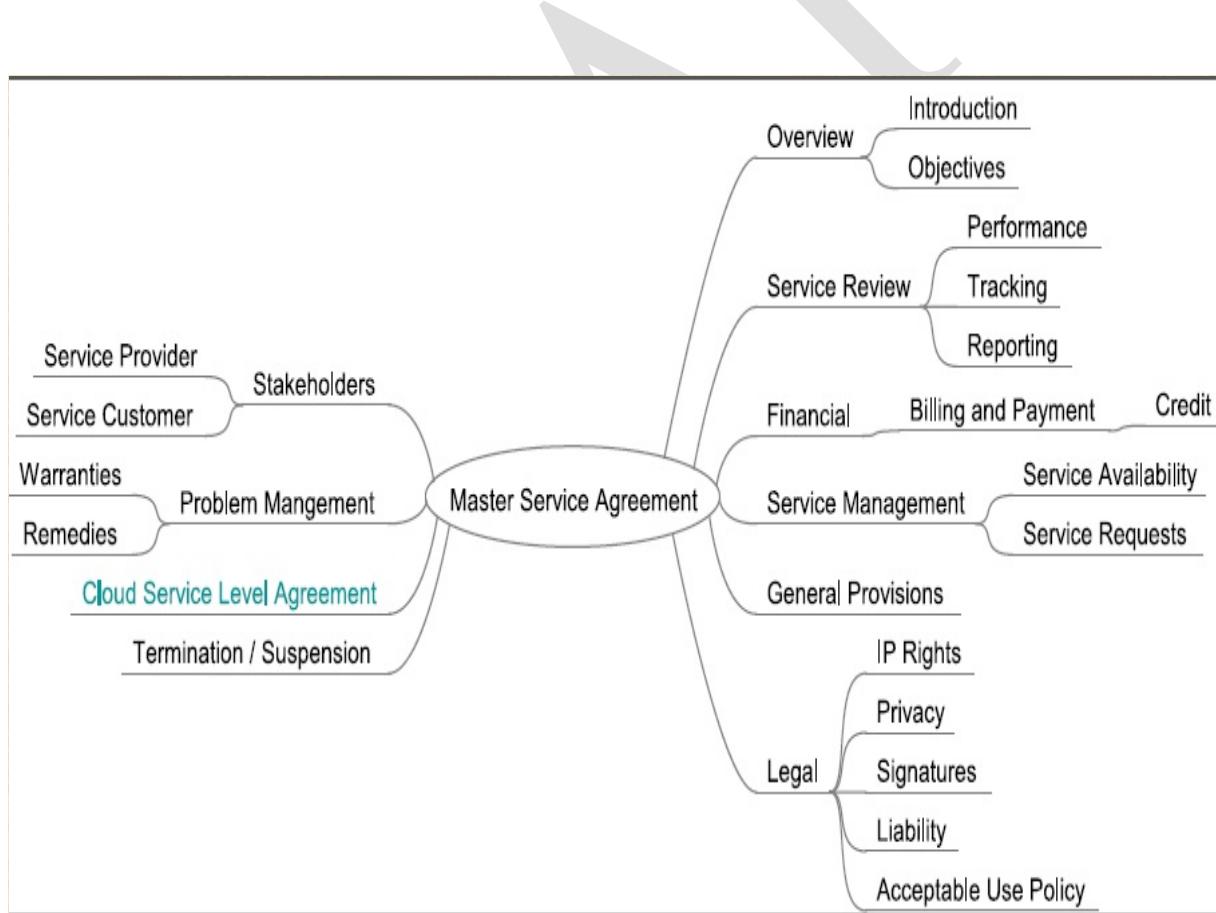


**Figure 33:** Service Agreement Mind Map

A further challenge in comparing and selecting service offerings is that cloud Providers may offer a default contract written from the Provider's perspective. Such default contracts may not adequately meet the Consumers needs and may constrain the visibility of the cloud Consumer into the delivery mechanisms of the service. The thorough risk analysis coupled with secure cloud Ecosystem orchestration introduced in this document, along with adequate guidance on negotiating SLAs, are intended to assist the Consumer in managing risk and making informed decisions in adopting cloud services.

## 5.2.5   STEP 5 – AUTHORIZE CLOUD SERVICES

Metrics are needed to assess whether the expectations defined in the customer-based SLA have been met. These metrics define the measures to be used (e.g., availability) and the range of acceptable results for a particular measurement (e.g., 99.5%). These metrics are a critical piece of the SLA since they are one of the artifacts the cloud Consumer can use to monitor the cloud service and to ensure the cloud Provider can be held accountable to the contractual terms. A set of well-defined and organized metrics for SLAs can also help cloud Consumers have a more consistent way to compare, manage and negotiate cloud services with multiple cloud Providers.[10]

Until formal guidance on SLAs and cloud service metrics are available, the set of prioritized Security Components and associated security controls to be implemented by each cloud Actor in the secure cloud Ecosystem orchestration process (as derived by the methodology described in this document) should be incorporated into SLAs and SAs, to ensure that the cloud Consumer's needs are met. Additionally, during cloud operations, cloud Providers and cloud Brokers should be periodically or continuously monitored to ensure compliance with all functional and security requirements set forth in the SLAs and SAs.

## 5.2.6   STEP 6 – MONITOR CLOUD SERVICES

NIST SP 800-37 (Rev. 1): *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* describes an effective operational continuous monitoring program as one that includes:

- Configuration management and control processes for information systems;

---

[10] NIST, in collaboration with other government agencies, is continuously striving to provide useful information on this topic. NIST's latest research and development on SLA and cloud service metrics can be found at the collaboration page of the Cloud Metrics Sub Group of the Reference Architecture Taxonomy working group: http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/RATax_CloudMetrics

- Security impact analyses on proposed or actual changes to information systems and environments of operation;
- Assessment of selected security controls (including system-specific, hybrid, and common controls) based on the defined continuous monitoring strategy;
- Security status reporting to appropriate officials; and
- Active involvement by authorizing officials in the ongoing management of information system-related security risks.

The continuous monitoring required by NIST SP 800-37 Rev. 1 for all information systems refers to the auditing and continuous monitoring requirements from the operational perspective, and not to FedRAMP's ongoing A&A, which is also referred to as continuous monitoring in FedRAMP's *Concept of Operations* (CONOPS)[11] document. However, FedRAMP does work in coordination with the Department of Homeland Security (DHS) to establish a framework for continuous monitoring, FISMA reporting, incident response, and remediation.

The objective of Step 6 – Continuous Monitoring - is to determine the effectiveness of the security controls deployed to secure the cloud-based service or application, and to evaluate the need to change or supplement the control set. For this purpose, cloud Consumers need to develop a continuous monitoring strategy and ensure that the strategy is implemented by the Provider and cloud Technical Broker when applicable. The strategy should define how the security and privacy controls will be monitored over time (e.g., frequency of monitoring activities, rigor and extent of monitoring activities, and the data feeds provided to the organization from the cloud service provider). The continuous monitoring data feeds need to be used by the cloud Consumer for ongoing authorization decisions as part of its enterprise-wide risk management program.

Monitoring the cloud services of the Provider(s) and Broker(s) (when applicable) ensures that all SA and SLA terms are met and that the cloud-based information system maintains the necessary security posture.

---

[11] http://www.gsa.gov/portal/category/102371

# 6 GLOSSARY AND ACRONYMS

A&A:                 Assessment and Authorization

ASIS:                Aggregated Security Index System

Assessment:          In this context, the process by which a third party assessment organization generates a security assessment package for review.

Authorization:       In this context, the process by which the FedRAMP Joint Authorization Board (JAB) reviews the security assessment package based on a prioritized approach and decides on a grant of provisional authorization. See http://www.gsa.gov/portal/category/102371 for more information.

BOSS:                Business Operation Support Service

Business Broker:     A Business Broker only provides business and relationship services, and does not have any contact with the cloud Consumer's data, operations, or artifacts (e.g., images, volumes, firewalls) in the cloud.

C&A:                 Certification and Accreditation – terminology replaced by "Assessment and Authorization" (A&A).

C/I/A:               Confidentiality, Integrity, Availability

CA:                  Certificate Authority

Chain of custody:    The seizure, custody, control, transfer, analysis, and disposition of physical or electronic evidence.

Cloud Auditor:       A cloud Auditor is a party that can conduct an independent assessment of cloud services, with the intent to express an opinion thereon.  A cloud Auditor can evaluate the services provided by a cloud Provider in terms of security controls, privacy impact, performance, etc.  Audits can be used to verify conformance to standards (set forth in mandates, the service contract, industry best practices, or other sources) through review of objective evidence.

Cloud Broker:    Broker as an entity that manages the use, performance and delivery of cloud services, and negotiates relationships between cloud Providers and cloud Consumers. *See also* Business Broker *and* Technical Broker.

Cloud Carrier:    A cloud Carrier acts as an intermediary that provides connectivity and transport of cloud services between cloud Consumers and cloud Providers through network, telecommunications, and other access devices.

Cloud Consumer:    An organization that uses, or consumes, cloud services. Cloud Consumers are ultimately responsible for ensuring the security and compliance of the cloud services they use.

Cloud Provider:    An entity that provides cloud computing services. Providers may offer its services directly to Consumers or do so through a third party, such as an Intermediary Provider or Broker. *See also* Broker, Intermediary Provider, *and* Primary Provider.

Community Cloud:    In a *Community* cloud, the cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

CPE:    Customer Premises Equipment

CRMF:    The NIST Cloud Risk Management Framework, based on the original RMF and customized for application to cloud-based services.

CSA:    The Cloud Security Alliance

DoS *or* DDoS:    Denial of Service or Distributed Denial of Service attack. This type of attack can jeopardize the cloud service by saturating the limited network bandwidth and interrupting the configuration/routing information. It can also cause the computing platform to slow down responses to legitimate requests because it is overloaded with non-legitimate traffic.

FedRAMP:    The Federal Risk and Authorization Management Program – see http://www.gsa.gov/portal/category/102371 for more information.

FIPS:                    Federal Information Processing Standard – see
                         http://www.nist.gov/itl/fips.cfm for more information.

FISMA:                   Federal Information Security Management Act – see
                         http://www.nist.gov/itl/csd/sma/fisma.cfm  for more information.

GSA:                     General Service Administration – see http://www.gsa.gov for more
                         information.

Hypervisor:              One of many hardware virtualization techniques allowing multiple
                         operating systems to run concurrently on a host computer. *See also* Virtual
                         Machine Manager (VMM).

IaaS:                    Infrastructure as a Service.  In an IaaS deployment, the capability provided
                         to the consumer is to provision processing, storage, networks, and other
                         fundamental computing resources where the consumer is able to deploy
                         and run arbitrary software, which can include operating systems and
                         applications. The consumer does not manage or control the underlying
                         cloud infrastructure but has control over operating systems, storage, and
                         deployed applications; and possibly limited control of select networking
                         components (e.g., host firewalls).

Intermediary Provider:   An Intermediary Provider has the capability to interact with other cloud
                         Providers without offering visibility or transparency into the Primary
                         Provider(s).  An Intermediary Provider uses services offered by Primary
                         Provider as invisible components of its own service, which it presents to
                         the customer as an integrated offering.

ITOS:                    Information Technology Operation and Support

Multi-tenancy:           The concept of Cloud Consumers sharing both virtualized infrastructure
                         and application servers.  In multi-tenant Cloud architectures, database and
                         application servers are typically shared to reduce the cost to Consumers,
                         but with sharing resources and co-location of data come risks to data that
                         must be mitigated.

NCC-SRA:                 NIST Cloud Computing Security Reference Architecture

| | |
|---|---|
| PaaS: | Platform as a Service. In a PaaS deployment, the capability provided to the Consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming, libraries, services, and tools supported by the Provider. The 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 configuration settings for the application-hosting environment. |
| Primary Provider: | A Primary Provider offers services hosted on infrastructure that it owns. It may make these services available to Consumers through a third party (such as a Broker or Intermediary Provider), but the defining characteristic of a Primary Provider is that it does not source its service offerings from other Providers. |
| Private Cloud: | In a *Private* cloud, the cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises. |
| Public Cloud: | In a *Public* cloud, the cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider. |
| RA: | The NIST Cloud Computing Reference Architecture, described in the document of the same name (NIST SP 500-292). The NCC-SRA builds upon the RA. |
| RMF: | The NIST Risk Management Framework |
| S&RM: | Security and Risk Management |
| SA: | Service Agreement |
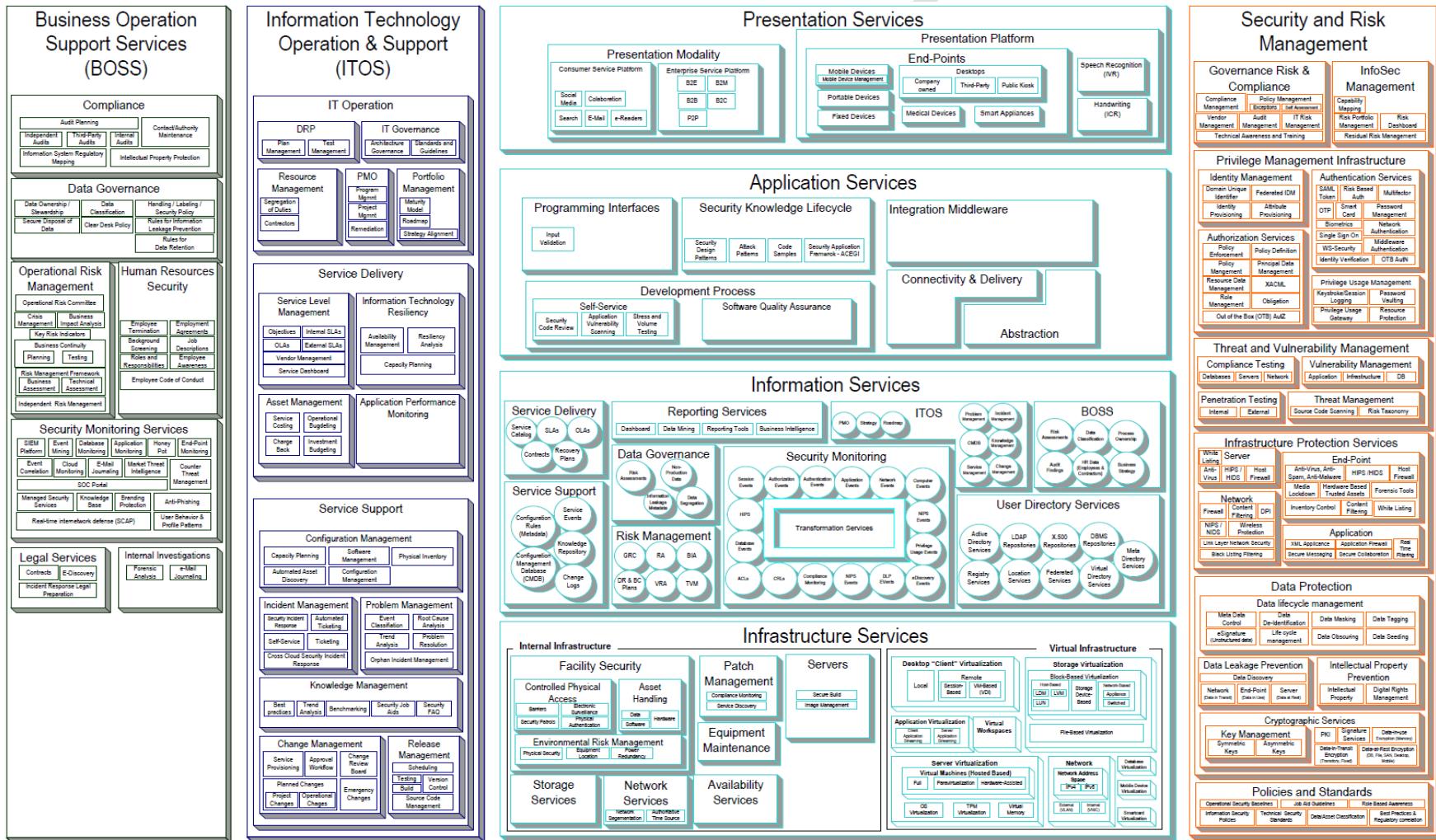
SaaS:            Software as a Service.  In a SaaS deployment, the capability provided to
                 the Consumer is to use the provider's applications running on a cloud
                 infrastructure.  The applications are accessible from various client devices
                 through either a thin client interface, such as a web browser (e.g., web-
                 based email), or a program interface.  The 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.

SIS:             Security Index System

SLA:             Service Level Agreement

TCI-RA:          The Cloud Security Alliance's (CSA) Trusted Cloud Initiative Reference
                 Architecture.

Technical Broker: A Technical Broker interacts with the Consumer's operational processes,
                 cloud artifacts, and/or consumer data by aggregating services from
                 multiple cloud Providers and adding a layer of technical functionality by
                 addressing single-point-of-entry and interoperability issues.

VMM:             Virtual Machine Manager.  One of many hardware virtualization
                 techniques allowing multiple operating systems to run concurrently on a
                 host computer.  *See also* Hypervisor.

## 7 REFERENCES
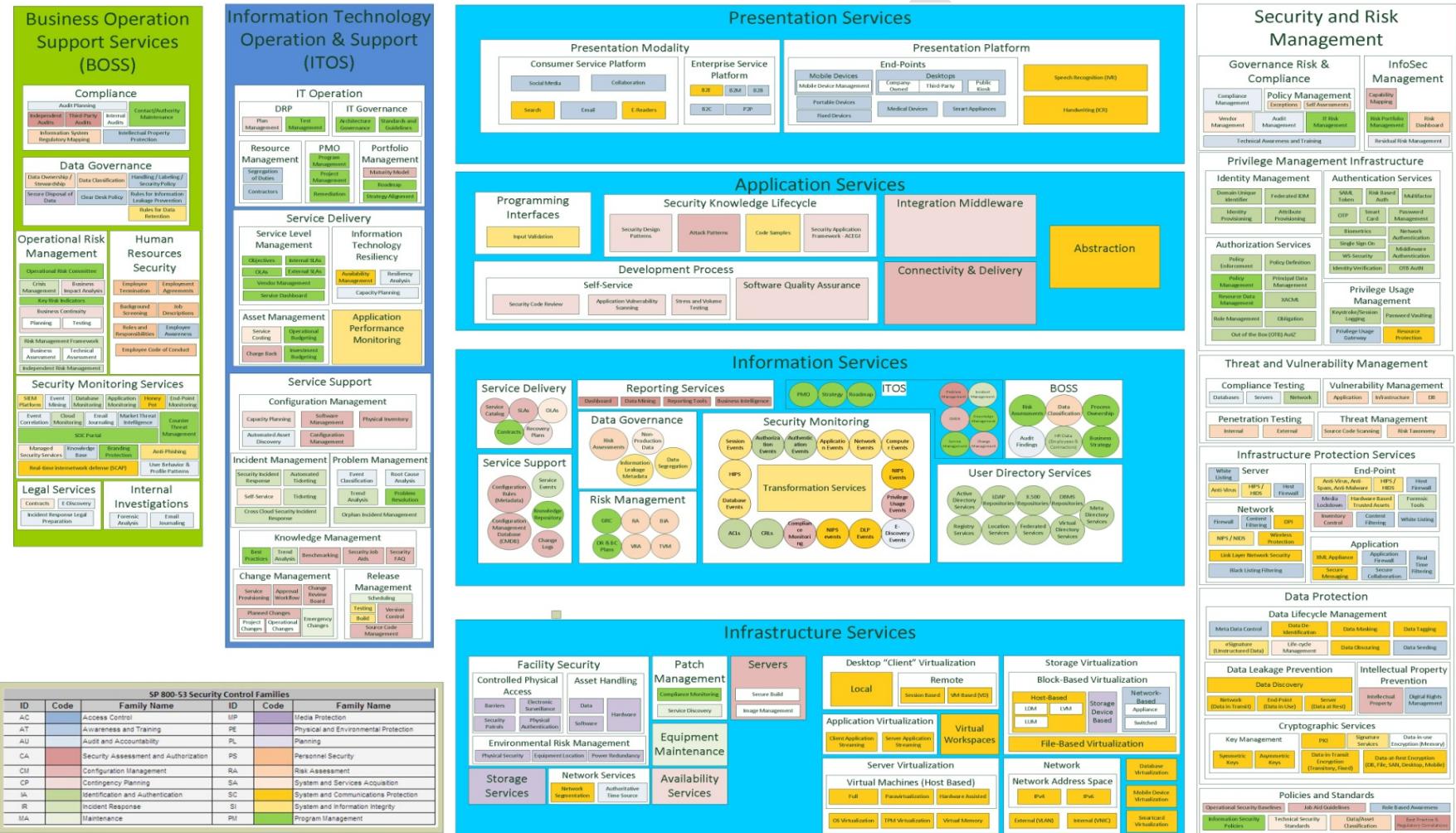
[1] L. Badger, D. Berstein, R. Bohn, F. de Valux, M. Hogan, J. Mao, J. Messina, K. Mills, A. Sokol, J. Tong, F. Whiteside, and D. Leaf, US government cloud computing technology roadmap volume 1: High-priority requirements to further USG agency cloud computing adoption (NIST SP 500-293, Vol. 1), National Institute of Standards and Technology, U.S. Department of Commerce (2011).
http://www.nist.gov/itl/cloud/upload/SP_500_293_volumeI-2.pdf

[2] L. Badger, R. Bohn, S. Chu, M. Hogan, F. Liu, V. Kaufmann, J. Mao, J. Messina, K. Mills, A. Sokol, J. Tong, F. Whiteside, and D. Leaf, US government cloud computing technology roadmap volume II: Useful information for cloud adopters (NIST SP 500-293, Vol. 2), National Institute of Standards and Technology, U.S. Department of Commerce (2011).
http://www.nist.gov/itl/cloud/upload/SP_500_293_volumeII.pdf.

[3] L. Badger, T. Grance, R. Patt-Corner, and J. Voas, Cloud computing synopsis and recommendations (NIST SP 800-146), National Institute of Standards and Technology, U.S. Department of Commerce (2012). http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf

[4] Committee on National Security Systems, Security categorization and control selection for national security systems (CNSSI No. 1253, Ver. 2) (2012).
http://www.cnss.gov/Assets/pdf/Final_CNSSI_1253.pdf

[5] K. Dempsey, N.S. Chawla, A. Johnson, R. Johnston, A.C. Jones, A. Orebaugh, M. Scholl, and K. Stine, Information security continuous monitoring (ISCM) for federal information systems and organizations (NIST SP 800-137), National Institute of Standards and Technology, U.S. Department of Commerce (2011)
http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf

[6] Federal Information Security Management Act of 2002, Tit. III, E-Government Act of 2002, Pub. L. No. 107-296 (Tit. X), 116 Stat. 2259; Pub. L. No. 107-347 (Tit. III), 116 Stat. 2946. 44 U.S.C. Ch. 35, Subchapters II and III, *codified at* 40 U.S.C. §11331, 15 U.S.C. 278g-3 & 4 (2002). http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

[7] M. Hogan, F. Liu, L. Sokol, and J. Tong, NIST Cloud Computing Standards Roadmap (NIST SP 500-291), National Institute of Standards and Technology, U.S. Department of Commerce (2011). http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909024

[8] W. Jansen and T. Grance, Guidelines on security and privacy in public cloud computing (NIST SP 800-144). National Institute of Standards and Technology, U.S. Department of Commerce (2011). http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf.

[9] Joint Task Force Transformation Initiative, Guide for applying the risk management framework to federal information systems: A security life cycle approach (NIST SP 800-37,

Rev. 1), National Institute of Standards and Technology, U.S.  Department of Commerce (2010). http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

[10] Joint Task Force Transformation Initiative, Recommended security controls for federal information systems and organizations (NIST SP 800-53, Rev. 3),  National Institute of Standards and Technology, U.S.  Department of Commerce (2010). http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

[11] V. Kundra, 25 point implementation plan to reform federal information technology management, The White House, U.S. Chief Information Officer, (2010). https://cio.gov/wp-content/uploads/downloads/2012/09/25-Point-Implementation-Plan-to-Reform-Federal-IT.pdf

[12] V. Kundra, Federal cloud computing strategy, The White House, U.S. Chief Information Officer, (2012). http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf.

[13] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, NIST Cloud Computing Reference Architecture (NIST SP 500-292), National Institute of Standards and Technology, U.S. Department of Commerce (2011). http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505

[14] P. Mell and T. Grance, The NIST definition of cloud computing (NIST SP 800-145), National Institute of Standards and Technology, U.S. Department of Commerce (2011) http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[15] C. Metz, DDoS attack rains down on Amazon cloud: Code haven tumbles from sky. *The Register* (2009, October 5). http://www.theregister.co.uk/2009/10/05/amazon_bitbucket_outage/

[16] Information Technology Laboratory (ITL), Standards for Security Categorization of Federal Information Processing Systems (FIPS PUB 199), National Institute of Standards and Technology, U.S. Department of Commerce (2004). http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

[17] Information Technology Laboratory (ITL), Minimum Security Requirements for Federal Information and Information Systems (FIPS PUB 200), National Institute of Standards and Technology, U.S. Department of Commerce (2006). http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

[18] U.S. Office of Management and Budget, Securing agency information systems (Circular A-130, Section 8b (3)) (2000). http://csrc.nist.gov/drivers/documents/a130trans4.pdf

[19] Z. Xiao and Y. Ziao, Security and Privacy in Cloud Computing, *IEEE Communication Surveys & Tutorials*, (in press, 2012). http://zxiao.students.cs.ua.edu/pub/Xiao_CloudSecurity.pdf

## Business Operation Support Services (BOSS)

### Compliance
Audit Planning
- Independent Audits
- Third-Party Audits
- Internal Audits
- Contact/Authority Maintenance
- Information System Regulatory Mapping
- Intellectual Property Protection

### Data Governance
- Data Ownership / Stewardship
- Data Classification
- Handling / Labeling / Security Policy
- Secure Disposal of Data
- Clear Desk Policy
- Rules for Information Leakage Prevention
- Rules for Data Retention

### Operational Risk Management
- Operational Risk Committee
- Crisis Management
- Business Impact Analysis
- Key Risk Indicators
- Business Continuity
  - Planning
  - Testing
- Risk Management Framework
  - Business Assessment
  - Technical Assessment
- Independent Risk Assessment

### Human Resources Security
- Employee Termination
- Employment Agreements
- Background Screening
- Job Descriptions
- Roles and Responsibilities
- Employee Awareness
- Employee Code of Conduct

### Security Monitoring Services
- SIEM Platform
- Event Mining
- Database Monitoring
- Application Monitoring
- Honey Pot
- End-Point Monitoring
- Event Correlation
- Cloud Monitoring
- E-Mail Journaling
- Market Threat Intelligence
- Counter Threat Management
- SOC Portal
- Managed Security Services
- Knowledge Base
- Branding Protection
- Anti-Phishing
- Real-time internetwork defense (SCAP)
- User Behavior & Profile Patterns

### Legal Services
- Contracts
- E-Discovery
- Incident Response Legal Preparation

### Internal Investigations
- Forensic Analysis
- e-Mail Journaling

## Information Technology Operation & Support (ITOS)

### IT Operation
- DRP
  - Plan Management
  - Test Management
- IT Governance
  - Architecture Governance
  - Standards and Guidelines
- Resource Management
  - Segregation of Duties
  - Contractors
- PMO
  - Program Mgmt
  - Project Mgmt
  - Remediation
- Portfolio Management
  - Maturity Model
  - Roadmap
  - Strategy Alignment

### Service Delivery
- Service Level Management
  - Objectives
  - Internal SLAs
  - OLAs
  - External SLAs
  - Vendor Management
  - Service Dashboard
- Information Technology Resiliency
  - Availability Management
  - Resiliency Analysis
  - Capacity Planning
- Asset Management
  - Service Costing
  - Operational Budgeting
  - Change Back
  - Investment Budgeting
- Application Performance Monitoring

### Service Support
- Configuration Management
  - Capacity Planning
  - Software Management
  - Physical Inventory
  - Automated Asset Discovery
  - Configuration Management
- Incident Management
  - Security Incident Response
  - Automated Ticketing
  - Self-Service
  - Ticketing
  - Cross Cloud Security Incident Response
- Problem Management
  - Event Classification
  - Root Cause Analysis
  - Trend Analysis
  - Problem Resolution
  - Orphan Incident Management
- Knowledge Management
  - Best practices
  - Trend Analysis
  - Benchmarking
  - Security Job Aids
  - Security FAQ
- Change Management
  - Service Provisioning
  - Approval Workflow
  - Change Review Board
  - Planned Changes
  - Project Changes
  - Operational Changes
  - Emergency Changes
- Release Management
  - Scheduling
  - Testing
  - Build
  - Version Control
  - Source Code Management

## Presentation Services

### Presentation Modality
- Consumer Service Platform
  - Social Media
  - Collaboration
  - Search
  - E-Mail
  - e-Readers
- Enterprise Service Platform
  - B2E
  - B2M
  - B2B
  - B2C
  - P2P

### Presentation Platform
- End-Points
  - Mobile Devices
    - Mobile Device Management
  - Portable Devices
  - Fixed Devices
  - Desktops
    - Company owned
    - Third-Party
    - Public Kiosk
  - Medical Devices
  - Smart Appliances
- Speech Recognition (IVR)
- Handwriting (ICR)

## Application Services

### Programming Interfaces
- Input Validation

### Security Knowledge Lifecycle
- Security Design Patterns
- Attack Patterns
- Code Samples
- Security Application Framework - ACEGI

### Integration Middleware

### Development Process
- Self-Service
  - Security Code Review
  - Application Vulnerability Scanning
  - Stress and Volume Testing
- Software Quality Assurance

### Connectivity & Delivery
- Abstraction

## Information Services

### Service Delivery
- Service Catalog
- SLAs
- OLAs
- Contracts
- Recovery Plans

### Reporting Services
- Dashboard
- Data Mining
- Reporting Tools
- Business Intelligence

### ITOS
- PMO
- Strategy
- Roadmap
- Problem Management
- Incident Management
- CMDB
- Knowledge Management
- Service Management
- Change Management

### BOSS
- Risk Assessments
- Data Classification
- Process Ownership
- Audit Findings
- HR Data (Employee & Contractors)
- Business Strategy

### Data Governance
- Risk Assessments
- Non-Production Data
- Information Leakage Metadata
- Data Segregation

### Security Monitoring
- Session Events
- Authorization Events
- Authentication Events
- Application Events
- Network Events
- Computer Events
- HIPS
- NIPS Events
- Database Events
- Transformation Services
- Privilege Usage Events
- ACLs
- CRLs
- Compliance Monitoring
- NIPS Events
- DLP Events
- eDiscovery Events

### Risk Management
- GRC
- RA
- BIA
- DR & BC Plans
- VRA
- TVM

### Service Support
- Configuration Rules (Metadata)
- Configuration Management Database (CMDB)
- Service Events
- Knowledge Repository
- Change Logs

### User Directory Services
- Active Directory Services
- LDAP Repositories
- X.500 Repositories
- DBMS Repositories
- Meta Directory Services
- Registry Services
- Location Services
- Federated Services
- Virtual Directory Services

## Infrastructure Services

### Internal Infrastructure

#### Facility Security
- Controlled Physical Access
  - Barriers
  - Electronic Surveillance
  - Security Patrols
  - Physical Authentication
- Asset Handling
  - Data
  - Software
  - Hardware
- Environmental Risk Management
  - Physical Security
  - Equipment Location
  - Power Redundancy

#### Patch Management
- Compliance Monitoring
- Service Discovery

#### Servers
- Secure Build
- Image Management

#### Equipment Maintenance

#### Storage Services

#### Network Services
- Network Segmentation
- Authoritative Time Source

#### Availability Services

### Virtual Infrastructure

#### Desktop "Client" Virtualization
- Local
- Remote Session-Based
- Virt-Based (VDI)

#### Storage Virtualization
- Block-Based Virtualization
  - Host-Based: LDM, LVM, LUN
  - Storage Device-Based
  - Network-Based Appliance
  - Switched
- File-Based Virtualization

#### Application Virtualization
- Client Application Streaming
- Server Application Streaming
- Virtual Workspaces

#### Server Virtualization
- Virtual Machines (Hosted Based)
  - Full
  - Paravirtualization
  - Hardware-Assisted
- OS Virtualization
- TPM Virtualization
- Virtual Memory

#### Network
- Network Address Space: IPv4, IPv6
- External (VLAN)
- Internal (VNIC)
- Mobile Device Virtualization
- Database Virtualization
- Smartcard Virtualization

## Security and Risk Management

### Governance Risk & Compliance
- Compliance Management
- Policy Management
- Exceptions
- Self Assessment
- Vendor Management
- Audit Management
- IT Risk Management
- Technical Awareness and Training

### InfoSec Management
- Capability Mapping
- Risk Portfolio Management
- Risk Dashboard
- Residual Risk Management

### Privilege Management Infrastructure
- Identity Management
  - Domain Unique Identifier
  - Federated IDM
  - Identity Provisioning
  - Attribute Provisioning
- Authentication Services
  - SAML Token
  - Risk Based Auth
  - Multifactor
  - OTP
  - Smart Card
  - Password Management
  - Biometrics
  - Network Authentication
  - Single Sign On
  - Middleware Authentication
  - WS-Security
  - Identity Verification
  - OTB AuTN
- Authorization Services
  - Policy Enforcement
  - Policy Definition
  - Policy Management
  - Principal Data Management
  - Resource Data Management
  - XACML
  - Role Management
  - Obligation
  - Out of the Box (OTB) AuTZ
- Privilege Usage Management
  - Keystroke/Session Logging
  - Password Vaulting
  - Privilege Usage Gateway
  - Resource Protection

### Threat and Vulnerability Management
- Compliance Testing
  - Databases
  - Servers
  - Network
- Vulnerability Management
  - Application
  - Infrastructure
  - DB
- Penetration Testing
  - Internal
  - External
- Threat Management
  - Source Code Scanning
  - Risk Taxonomy

### Infrastructure Protection Services
- End-Point
  - White Listing
  - Anti-Virus
  - HIPS / HIDS
  - Host Firewall
  - Server
    - Anti-Virus, Anti-Spam, Anti-Malware
    - HIPS / HIDS
    - Host Firewall
  - Media Lockdown
  - Hardware Based Trusted Assets
  - Forensic Tools
  - Inventory Control
  - Content Filtering
  - White Listing
- Network
  - Firewall
  - Content Filtering
  - DPI
  - NIPS / NIDS
  - Wireless Protection
  - Link Layer Network Security
  - Black Listing Filtering
- Application
  - XML Appliance
  - Application Firewall
  - Real Time Filtering
  - Secure Messaging
  - Secure Collaboration

### Data Protection
- Data lifecycle management
  - Meta Data Control
  - Data De-Identification
  - Data Masking
  - Data Tagging
  - eSignature (Unstructured data)
  - Life cycle management
  - Data Obscuring
  - Data Seeding
- Data Leakage Prevention
  - Data Discovery
  - Network (Data in Transit)
  - End-Point (Data in Use)
  - Server (Data at Rest)
- Intellectual Property Prevention
  - Intellectual Property
  - Digital Rights Management
- Cryptographic Services
  - Key Management
    - Symmetric Keys
    - Asymmetric Keys
  - PKI
  - Signature Services
  - Data-in-Use Encryption (Memory)
  - Data-in-Transit Encryption (SSL, File, SAN, Desktop, Mobile)
  - Data-at-Rest Encryption (Transitory, Fixed)

### Policies and Standards
- Operational Security Baselines
- Job Aid Guidelines
- Role Based Awareness
- Information Security Policies
- Technical Security Standards
- Data/Asset Classification
- Best Practices & Regulatory correlation

Page 107

# Business Operation Support Services (BOSS)

## Compliance
Audit Planning | Contact/Authority Maintenance
Independent Audits | Third-Party Audits | Internal Audits
Information System Regulatory Mapping | Intellectual Property Protection

## Data Governance
Data Ownership / Stewardship | Data Classification | Handling / Labeling / Security Policy
Secure Disposal of Data | Clear Desk Policy | Rules for Information Leakage Prevention
Rules for Data Retention

## Operational Risk Management
Operational Risk Committee
Crisis Management | Business Impact Analysis
Key Risk Indicators
Business Continuity
Planning | Testing
Risk Management Framework
Business Assessment | Technical Assessment
Independent Risk Management

## Human Resources Security
Employee Termination | Employment Agreements
Background Screening | Job Descriptions
Roles and Responsibilities | Employee Awareness
Employee Code of Conduct

## Security Monitoring Services
SIEM Platform | Event Mining | Database Monitoring | Application Monitoring | Honey Pot | End-Point Monitoring
Event Correlation | Cloud Monitoring | Email Journaling | Market Threat Intelligence | Counter Threat Management
Managed Security Services | Knowledge Base | Branding Protection | Anti-Phishing
Real-time Internetwork defense (SCAP) | User Behavior & Profile Patterns

## Legal Services
Contracts | E-Discovery
Incident Response Legal Preparation

## Internal Investigations
Forensic Analysis | Email Journaling

# Information Technology Operation & Support (ITOS)

## IT Operation
### DRP
Plan Management | Test Management
### IT Governance
Architecture Governance | Standards and Guidelines

### Resource Management
Segregation of Duties
Contractors
### PMO
Program Management
Project Management
Remediation
### Portfolio Management
Maturity Model
Roadmap
Strategy Alignment

## Service Delivery
### Service Level Management
Objectives | Internal SLAs
OLAs | External SLAs
Vendor Management
Service Dashboard
### Information Technology Resiliency
Availability Management | Resiliency Analysis
Capacity Planning

### Asset Management
Service Costing
Charge Back
Operational Budgeting
Investment Budgeting
### Application Performance Monitoring

## Service Support
### Configuration Management
Capacity Planning | Software Management | Physical Inventory
Automated Asset Discovery | Configuration Management

### Incident Management
Security Incident Response | Automated Ticketing
Self-Service | Ticketing
Cross Cloud Security Incident Response
### Problem Management
Event Classification | Root Cause Analysis
Trend Analysis | Problems Resolution
Orphan Incident Management

## Knowledge Management
Best Practices | Trend Analysis | Benchmarking | Security Job Aids | Security FAQ

### Change Management
Service Provisioning | Approval Workflow | Change Review Board
Planned Changes
Project Changes | Operational Changes | Emergency Changes
### Release Management
Scheduling
Testing | Version Control
Build
Source Code Management

# Presentation Services
## Presentation Modality
### Consumer Service Platform
Social Media | Collaboration
Search | Email | E-Readers
### Enterprise Service Platform
B2E | B2M | B2B
B2C | P2P

## Presentation Platform
### End-Points
#### Mobile Devices
Mobile Device Management
Portable Devices
Fixed Devices
#### Desktops
Company-Owned | Third-Party | Public Kiosk
Medical Devices | Smart Appliances
Speech Recognition (IVR)
Handwriting (ICR)

# Application Services
## Programming Interfaces
Input Validation
## Security Knowledge Lifecycle
Security Design Patterns | Attack Patterns | Code Samples | Security Application Framework - ACEGI
## Integration Middleware
Abstraction
## Development Process
### Self-Service
Security Code Review | Application Vulnerability Scanning | Stress and Volume Testing
### Software Quality Assurance
### Connectivity & Delivery

# Information Services
## Service Delivery
Service Catalog | SLAs | OLAs
Contracts | Recovery Plans
## Service Support
Configuration Rules (Metadata)
Configuration Management Database (CMDB) | Change Logs
## Reporting Services
Dashboard | Data Mining | Reporting Tools | Business Intelligence
## Data Governance
Risk Assessments | Non-Production Data
Information Leakage Metadata | Data Segregation
## Risk Management
GRC | RA | BIA
DR & BC Plans | VRA | TVM
## Security Monitoring
Session Events | Authorization Events | Authentication Events | Application Events | Network Events | Computer Events
HIPS | NIPS Events
### Transformation Services
Database Events | Privilege Usage Events
ACLs | CIRLs | Compliance Monitoring | NIPS Events | DLP Events | E-Discovery Events
## User Directory Services
Active Directory Services | LDAP Repositories | X.500 Repositories | DBMS Repositories | Meta Directory Services
Registry Services | Location Services | Federated Services | Virtual Directory Services

ITOS
PMO | Strategy | Roadmap
BOSS
Risk Assessments | Data Classification | Process Ownership
Audit Findings | HR Data (Employees & Contractors) | Business Strategy

# Infrastructure Services
## Facility Security
### Controlled Physical Access
Barriers | Electronic Surveillance
Security Patrols | Physical Authentication
### Asset Handling
Data | Hardware
Software
### Environmental Risk Management
Physical Security | Equipment Location | Power Redundancy
## Patch Management
Compliance Monitoring
Service Discovery
## Servers
Secure Build
Image Management
## Equipment Maintenance
## Storage Services
## Network Services
Network Segmentation | Authoritative Time Source
## Availability Services

## Desktop "Client" Virtualization
### Remote
Local | Session Based | VM Based (VDI)
### Application Virtualization
Client Application Streaming | Server Application Streaming | Virtual Workspaces

## Storage Virtualization
### Block-Based Virtualization
#### Host-Based
LDM | LVM | Storage Device Based | Network-Based Appliance
LUM | Switched
### File-Based Virtualization

## Server Virtualization
### Virtual Machines (Host Based)
Full | Paravirtualization | Hardware Assisted
OS Virtualization | TPM Virtualization | Virtual Memory
## Network
### Network Address Space
IPv4 | IPv6
External (VLAN) | Internal (VNIC)
Database Virtualization
Mobile Device Virtualization
Smartcard Virtualization

# Security and Risk Management
## Governance Risk & Compliance
### Compliance Management
### Policy Management
Exceptions | Self Assessments
Vendor Management | Audit Management | IT Risk Management
Technical Awareness and Training

## InfoSec Management
Capability Mapping
Risk Portfolio Management | Risk Dashboard
Residual Risk Management

## Privilege Management Infrastructure
### Identity Management
Domain Unique Identifier | Federated IDM
Identity Provisioning | Attribute Provisioning
### Authentication Services
SAML Token | Risk Based Auth | Multifactor
OTP | Smart Card | Password Management
Biometrics
Single Sign On | WS-Security | Middleware Authentication
### Authorization Services
Policy Enforcement | Policy Definition
Policy Management | Principal Data Management
Resource Data Management | XACML
Role Management | Obligation
Identity Verification | OTB AuthN
### Privilege Usage Management
Keystroke/Session Logging | Password Vaulting
Privilege Usage Gateway | Resource Protection
Out of the Box (OTB) AuthZ

## Threat and Vulnerability Management
### Compliance Testing
Databases | Servers | Network
### Vulnerability Management
Application | Infrastructure | DB
### Penetration Testing
Internal | External
### Threat Management
Source Code Scanning | Risk Taxonomy

## Infrastructure Protection Services
### Server
White Listing
Anti Virus | HIPS / HIDS | Host Firewall
### Network
Firewall | Content Filtering | DPI
NIPS / NIDS | Wireless Protection
Link Layer Network Security
Black Listing Filtering
### End-Point
Anti-Virus, Anti-Spam, Anti-Malware | HIPS / HIDS | Host Firewall
Media Lockdown | Hardware Based Trusted Assets | Forensic Tools
Inventory Control | Content Filtering | White Listing
### Application
Application Firewall | Real Time Filtering
XML Appliance | Secure Messaging | Secure Collaboration

## Data Protection
### Data Lifecycle Management
Meta Data Control | Data De-Identification | Data Masking | Data Tagging
eSignature (Unstructured Data) | Life-cycle Management | Data Obscuring | Data Seeding
### Data Leakage Prevention
#### Data Discovery
Network (Data In Transit) | Intellectual Property | Digital Rights Management
### Intellectual Property Prevention
Network (Data in Transit) | End-Point (Data in Use) | Server (Data at Rest)
### Cryptographic Services
#### Key Management
Symmetric Keys | Asymmetric Keys | Data-in-Transit Encryption (Transitory, Fixed) | Data-at-Rest Encryption (DB, File, SAN, Desktop, Mobile)
PKI | Signature Services | Data-in-use Encryption (Memory)

## Policies and Standards
Operational Security Baselines | Job-Aid Guidelines | Role Based Awareness
Information Security Policies | Technical Security Standards | Data/Asset Classification | Best Practice & Regulatory Correlations

| SP 800-53 Security Control Families | | | | | |
|---|---|---|---|---|---|
| ID | Code | Family Name | ID | Code | Family Name |
| AC | | Access Control | MP | | Media Protection |
| AT | | Awareness and Training | PE | | Physical and Environmental Protection |
| AU | | Audit and Accountability | PL | | Planning |
| CA | | Security Assessment and Authorization | PS | | Personnel Security |
| CM | | Configuration Management | RA | | Risk Assessment |
| CP | | Contingency Planning | SA | | System and Services Acquisition |
| IA | | Identification and Authentication | SC | | System and Communications Protection |
| IR | | Incident Response | SI | | System and Information Integrity |
| MA | | Maintenance | PM | | Program Management |

# 10 ANNEX C: GENERIC HEAT MAP

# 11 ANNEX D: AGGREGATED DATA

## 11.1 ACTORS-BASED DATA AGGREGATION

LEGEND:

In the table below

"X" - indicates that the Security Component should be implemented by the Actor to secure the Consumer's applications and data in the Cloud.

"A" - indicates that the Security Component should be implemented internally, independent of the Consumer's data, for administrative or best-practice reasons.

"B" – is specific to Business Brokers only, and indicates that the Security Component should be implemented to secure the cloud computing business-oriented service.  The marking also emphasizes that the Business Broker only provides business and relationship services, and does not have any contact with the cloud Consumer's data migrated to the cloud.

" " – no marking or blank cell - indicates that the Security Component cannot be implemented by the particular cloud Actor or is not necessary in securing the cloud Ecosystem.

Security components descriptions available on CSA's interactive site:
https://research.cloudsecurityalliance.org/tci/ or
https://research.cloudsecurityalliance.org/tci/index.php/explore/

| Domain | High-level Security Component | Mid-level Security Component | Low-level Security Component | 800-53 Fami | Consumer | | | Provider | | | Broker | | | Carrier | Auditor |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | IaaS | PaaS | SaaS | IaaS | PaaS | SaaS | IaaS | PaaS | SaaS | ALL | ALL |
| BOSS | Compliance | Intellectual Property Protection | | AC | X | A | A | X | X | X | A | A | A | X | A |
| BOSS | Data Governance | Handling/ Labeling/ Security Policy | | AC | X | X | X | X | X | X | A | A | A | X | A |
| BOSS | Data Governance | Clear Desk Policy | | AC | A | A | A | A | A | A | A | A | A | X | A |
| BOSS | Data Governance | Rules for Information Leakage Prevention | | AC | X | A | A | X | X | X | B | B | B | X | |
| BOSS | Human Resource Security | Employee Awareness | | AT | A | A | A | A | A | A | A | A | A | X | A |
| BOSS | Security Monitoring Services | Market Threat Intelligence | | AT | A | A | A | X | X | X | B | B | B | X | A |
| BOSS | Security Monitoring Services | Knowledge Base | | AT | A | A | A | A | A | A | B | B | B | A | |

| Tower | Category | Service | | Code | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| BOSS | Compliance | Audit Planning | | AU | A | A | A | A | A | A | B | B | B | A | A |
| BOSS | Compliance | Internal Audits | | AU | A | A | A | A | A | A | B | B | B | A | A |
| BOSS | Security Monitoring Services | Event Mining | | AU | X | X | A | A | X | X | B | B | B | A | |
| BOSS | Security Monitoring Services | Event Correlation | | AU | X | X | A | A | X | X | B | B | B | A | |
| BOSS | Security Monitoring Services | Email Journaling | | AU | X | X | A | A | X | X | B | B | B | A | |
| BOSS | Security Monitoring Services | User Behaviors and Profile Patterns | | AU | X | X | A | A | X | X | B | B | B | X | A |
| BOSS | Legal Services | E-Discovery | | AU | X | X | X | X | X | X | A | A | A | A | A |
| BOSS | Legal Services | Incident Response Legal Preparation | | AU | X | X | X | X | X | X | A | A | A | A | |
| BOSS | Internal Investigations | Forensic Analysis | | AU | X | X | X | X | X | X | A | A | A | X | A |
| BOSS | Internal Investigations | e-Mail Journaling | | AU | A | A | A | A | A | A | A | A | A | A | A |
| BOSS | Compliance | Independent Audits | | CA | A | A | A | A | A | A | B | B | B | A | A |
| BOSS | Compliance | Third Party Audits | | CA | A | A | A | A | A | A | B | B | B | X | A |
| BOSS | Operational Risk Management | Business Impact Analysis | | CP | A | A | A | X | X | X | A | A | A | A | A |
| BOSS | Operational Risk Management | Business Continuity | | CP | X | A | A | X | X | X | B | B | B | X | |
| BOSS | Operational Risk Management | Crisis Management | | IR | A | A | A | X | X | X | B | B | B | A | A |
| BOSS | Operational Risk Management | Risk Management Framework | | IR | A | A | A | A | A | A | A | A | A | A | A |
| BOSS | Operational Risk Management | Independent Risk Management | | IR | A | A | A | X | X | X | B | B | B | A | A |
| BOSS | Security Monitoring Services | Database Monitoring | | IR | X | A | | A | X | X | B | B | B | A | |
| BOSS | Security Monitoring Services | Application Monitoring | | IR | X | X | X | A | X | X | B | B | B | A | |
| BOSS | Security Monitoring Services | End-Point Monitoring | | IR | X | X | X | A | A | A | B | B | B | A | |
| BOSS | Security Monitoring Services | Cloud Monitoring | | IR | X | X | X | X | X | X | B | B | B | A | |

| | Category | Subcategory | | Code | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| BOSS | Data Governance | Secure Disposal of Data | | MP | X | A | A | X | X | X | A | A | A | X | A |
| BOSS | Human Resource Security | Employee Termination | | PS | X | X | X | X | X | X | B | B | B | A | A |
| BOSS | Human Resource Security | Employment Agreements | | PS | X | X | X | X | X | X | B | B | B | A | A |
| BOSS | Human Resource Security | Background Screening | | PS | X | X | X | X | X | X | B | B | B | A | A |
| BOSS | Human Resource Security | Job Descriptions | | PS | X | X | X | X | X | X | B | B | B | | A |
| BOSS | Human Resource Security | Roles and Responsibilities | | PS | X | X | X | X | X | X | B | B | B | A | A |
| BOSS | Human Resource Security | Employee Code of Conduct | | PS | X | X | X | X | X | X | B | B | B | X | A |
| BOSS | Compliance | Information Systems Regulatory Mapping | | RA | A | A | A | X | X | X | B | B | B | A | A |
| BOSS | Data Governance | Data Ownership - Personnel Responsibilities/ Stewardship | | RA | X | X | X | A | X | X | A | A | A | A | A |
| BOSS | Data Governance | Data Classification | | RA | X | X | X | X | X | X | A | A | A | A | A |
| BOSS | Security Monitoring Services | Managed (Outsourced) Security Services | | SA | X | X | X | A | X | X | B | B | B | A | |
| BOSS | Legal Services | Contracts | | SA | X | X | X | X | X | X | A | A | A | X | A |
| BOSS | Security Monitoring Services | Honey Pot | | SC | A | A | | | A | A | | | | A | |
| BOSS | Security Monitoring Services | Real Time Internetwork Defense (SCAP) | | SC | A | A | A | X | X | X | B | B | B | A | |
| BOSS | Data Governance | Rules for Data Retention | | SI | A | A | A | X | X | X | B | B | B | A | A |
| BOSS | Security Monitoring Services | SIEM Platform | | SI | X | X | A | A | X | X | B | B | B | A | A |
| BOSS | Security Monitoring Services | Anti Phishing | | SI | A | A | A | A | A | A | B | B | B | X | |
| BOSS | Compliance | Contract/ Authority Maintenance | | PM | X | X | A | A | A | X | B | B | B | A | A |
| BOSS | Operational Risk Management | Operational Risk Committee | | PM | X | A | A | X | X | X | A | A | A | A | A |
| BOSS | Operational Risk Management | Key Risk Indicators | | PM | X | X | A | A | A | X | A | A | A | A | |

| | | | | | | | | | | | | | | |
|------|------|------|------|------|---|---|---|---|---|---|---|---|---|---|
| BOSS | Security Monitoring Services | Counter Threat Management | | P M | A | A | A | X | X | X | B | B | B | A | |
| BOSS | Security Monitoring Services | SOC Portal | | P M | A | A | A | A | A | A | B | B | B | A | |
| BOSS | Security Monitoring Services | Branding Protection | | P M | A | A | A | A | A | A | B | B | B | A | A |
| ITOS | IT Operations | Resource Management | Segregation of duties | A C | X | X | X | X | X | X | B | B | B | A | A |
| ITOS | IT Operations | Resource Management | Contractors | A C | A | A | A | A | A | A | A | A | A | A | A |
| ITOS | Service Delivery | Information Technology Resiliency | Resiliency Analysis | A U | X | A | A | X | X | X | B | B | B | A | |
| ITOS | Service Delivery | Information Technology Resiliency | Capacity Planning | A U | X | A | A | X | X | X | B | B | B | A | |
| ITOS | Service Support | Configuration Management | Automated Asset Discovery | A U | A | A | A | A | A | A | B | B | B | A | |
| ITOS | Service Support | Problem Management | Event Classification | A U | X | X | X | A | X | X | B | B | B | A | A |
| ITOS | Service Support | Problem Management | Root Cause Analysis | A U | A | A | A | X | X | X | B | B | B | A | |
| ITOS | IT Operations | Portfolio Management | Maturity Model | C M | A | A | A | A | A | A | A | A | A | A | |
| ITOS | Service Delivery | Asset Management | Change Back | C M | A | A | A | A | A | A | A | A | A | A | |
| ITOS | Service Support | Configuration Management | Software Management | C M | X | X | A | X | X | X | B | B | B | A | |
| ITOS | Service Support | Configuration Management | Configuration Management | C M | X | X | A | X | X | X | B | B | B | A | |
| ITOS | Service Support | Configuration Management | Physical Inventory | C M | A | A | A | A | A | A | B | B | B | A | |
| ITOS | Service Support | Knowledge Management | Benchmarking | C M | A | A | A | A | A | A | A | A | A | X | A |
| ITOS | Service Support | Knowledge Management | Security Job Aids | C M | A | A | A | A | A | A | A | A | A | X | A |
| ITOS | Service Support | Knowledge Management | Security FAQ | C M | A | A | A | A | A | A | A | A | A | A | A |
| ITOS | Service Support | Change Management | Service Provisioning | C M | A | A | A | X | X | X | A | A | A | X | A |
| ITOS | Service Support | Change Management | Approval Workflow | C M | A | A | A | X | X | X | A | A | A | A | |
| ITOS | Service Support | Change Management | Change Review Board | C M | A | A | A | X | X | X | A | A | A | A | |
| ITOS | Service Support | Change Management | Planned Changes | C M | A | A | A | X | X | X | A | A | A | A | |

| ITOS | Category | Function | Subfunction | Code | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ITOS | Service Support | Release Management | Version Control | CM | X | X | X | X | X | X | A | A | A | A | |
| ITOS | Service Support | Release Management | Source Code Management | CM | X | X | X | X | X | X | A | A | A | A | |
| ITOS | IT Operations | DRP | Plan Management | CP | X | A | A | X | X | X | B | B | B | A | |
| ITOS | Service Support | Configuration Management | Capacity Planning | CP | X | A | A | X | X | X | B | B | B | A | |
| ITOS | Service Support | Incident Management | Security Incident Response | IR | X | X | X | X | X | X | B | B | B | A | |
| ITOS | Service Support | Incident Management | Automated Ticketing | IR | A | A | A | X | X | X | B | B | B | A | A |
| ITOS | Service Support | Incident Management | Ticketing | IR | X | X | X | X | X | X | B | B | B | A | A |
| ITOS | Service Support | Incident Management | Cross Cloud Security Incident Response | IR | X | X | X | X | X | X | B | B | B | A | |
| ITOS | Service Support | Problem Management | Trend Analysis | IR | A | A | A | X | X | X | B | B | B | A | |
| ITOS | Service Support | Problem Management | Orphan Incident Management | IR | A | A | A | X | X | X | B | B | B | A | |
| ITOS | Service Support | Knowledge Management | Trend Analysis | IR | A | A | A | X | X | X | A | A | A | A | A |
| ITOS | Service Support | Change Management | Emergency Changes | MA | A | A | A | X | X | X | A | A | A | A | |
| ITOS | Service Support | Release Management | Scheduling | MA | A | A | A | X | X | X | A | A | A | X | |
| ITOS | Service Delivery | Asset Management | Service Costing (Internal) | SA | A | A | A | A | A | A | B | B | B | x | |
| ITOS | Service Support | Incident Management | Self-Service | SA | A | A | A | X | X | X | B | B | B | x | |
| ITOS | Service Delivery | Information Technology Resiliency | Availability Management | SC | X | A | A | X | X | X | B | B | B | A | |
| ITOS | Service Delivery | Application Performance Monitoring | | SI | X | X | A | A | X | X | A | A | A | x | |
| ITOS | Service Support | Release Management | Testing | SI | A | A | A | X | X | X | A | A | A | X | |
| ITOS | Service Support | Release Management | Build | SI | A | A | | X | X | X | A | A | A | X | |
| ITOS | IT Operations | DRP | Test Management | PM | X | A | A | X | X | X | B | B | B | X | A |
| ITOS | IT Operations | IT Governance | Architecture Governance | PM | A | A | A | A | A | A | A | A | A | X | - |
| ITOS | IT Operations | IT Governance | Standards and Guidelines | PM | X | X | X | A | X | X | A | A | A | A | |
| ITOS | IT Operations | PMO | Program Mngmt | PM | A | A | A | A | A | A | A | A | A | A | A |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ITOS | IT Operations | PMO | Project Mgnmt | P M | A | A | A | A | A | A | A | A | A | A | A |
| ITOS | IT Operations | PMO | Remediation | P M | A | A | A | A | A | A | A | A | A | A | A |
| ITOS | IT Operations | Portfolio Management | Roadmap | P M | A | A | A | A | A | A | A | A | A | A | |
| ITOS | IT Operations | Portfolio Management | Strategy Alignment | P M | A | A | A | A | A | A | A | A | A | A | |
| ITOS | Service Delivery | Service Level Management | Objectives | P M | X | X | X | X | X | X | B | B | B | A | |
| ITOS | Service Delivery | Service Level Management | OLAs | P M | X | X | X | A | X | X | B | B | B | A | A |
| ITOS | Service Delivery | Service Level Management | Internal SLAs | P M | X | X | X | A | A | A | A | A | A | A | A |
| ITOS | Service Delivery | Service Level Management | External SLAs | P M | X | X | X | X | X | X | B | B | B | A | A |
| ITOS | Service Delivery | Service Level Management | Vendor Management | P M | A | A | A | A | A | A | A | A | A | A | A |
| ITOS | Service Delivery | Service Level Management | Service Dashboard | P M | X | A | A | X | X | X | B | B | B | A | A |
| ITOS | Service Delivery | Asset Management | Operational Budgeting | P M | A | A | A | A | A | A | A | A | A | A | |
| ITOS | Service Delivery | Asset Management | Investment Budgeting | P M | A | A | A | A | A | A | A | A | A | A | |
| ITOS | Service Support | Problem Management | Problem Resolutions | P M | A | A | A | X | X | X | B | B | B | A | |
| ITOS | Service Support | Knowledge Management | Best Practices | P M | X | X | A | X | X | X | A | A | A | A | |
| Presentation Services | Presentation Modality | Consumer Service Platform | Social Media | A C | X | X | | | | X | B | B | B | | |
| Presentation Services | Presentation Modality | Consumer Service Platform | Collaboration | A C | X | X | | | | X | B | B | B | | |
| Presentation Services | Presentation Modality | Consumer Service Platform | E-Mail | A C | X | X | | | | X | B | B | B | | |
| Presentation Services | Presentation Modality | Enterprise Service Platform | B2M | A C | X | X | X | A | A | X | B | B | B | | |
| Presentation Services | Presentation Modality | Enterprise Service Platform | B2B | A C | X | X | X | A | A | X | B | B | B | | |
| Presentation Services | Presentation Modality | Enterprise Service Platform | B2C | A C | X | X | X | A | A | X | B | B | B | | |
| Presentation Services | Presentation Modality | Enterprise Service Platform | P2P | A C | X | X | X | A | A | X | B | B | B | | |

| Col1 | Col2 | Col3 | Col4 | Code | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Presentation Services | Presentation Platform | End-Points | Mobile Devices | AC | X | X | X | A | A | A | B | B | B | | | |
| Presentation Services | Presentation Platform | End-Points | Fixed Devices | AC | X | X | X | A | A | A | B | B | B | | | |
| Presentation Services | Presentation Platform | End-Points | Desktops | AC | X | X | X | A | A | A | B | B | B | | | |
| Presentation Services | Presentation Platform | End-Points | Portable Devices | AC | X | X | X | A | A | A | B | B | B | | | |
| Presentation Services | Presentation Platform | End-Points | Medical Devices | AC | X | X | X | A | A | A | B | B | B | | | |
| Presentation Services | Presentation Platform | End-Points | Smart Appliances | AC | X | X | X | A | A | A | B | B | B | | | |
| Presentation Services | Presentation Modality | Consumer Service Platform | Search | SC | X | X | | | | X | B | B | B | | | |
| Presentation Services | Presentation Modality | Consumer Service Platform | e-Readers | SC | X | X | | | | X | B | B | B | | | |
| Presentation Services | Presentation Modality | Enterprise Service Platform | B2E | SC | X | X | X | A | A | X | B | B | B | | | |
| Presentation Services | Presentation Platform | Speech Recognition (IVR) | | SC | X | X | X | | | | B | B | B | | | |
| Presentation Services | Presentation Platform | Handwriting (ICR) | | SC | X | X | X | | | | B | B | B | | | |
| Application Services | Security Knowledge Lifecycle | Attack Patterns | | CM | X | A | A | X | X | X | B | B | B | A | | A |
| Application Services | Security Knowledge Lifecycle | Security Design Patterns | | SA | X | A | A | X | X | X | B | B | B | A | | |
| Application Services | Security Knowledge Lifecycle | Security Application Framework - ACEGI | | SA | X | A | A | A | X | X | B | B | B | A | | A |
| Application Services | Development Processes | Self Service | Security Code Review | SA | X | X | X | X | X | X | B | B | B | A | | A |
| Application Services | Development Processes | Self Service | Application Vulnerability Scanning | SA | X | X | A | X | X | X | B | B | B | A | | A |
| Application Services | Development Processes | Self Service | Stress Volume Testing | SA | A | A | A | X | X | X | B | B | B | A | | A |

| Service | Area | Item | Code | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Application Services | Development Processes | Software Quality Assurance | SA | X | X | X | X | X | X | B | B | B | A | | A |
| Application Services | Integration Middleware | | SA | X | X | A | A | X | X | B | B | B | A | | |
| Application Services | Connectivity & Delivery | | CM | X | A | A | X | X | X | B | B | B | A | | |
| Application Services | Programming Interfaces | Input Validation | SI | A | A | A | X | X | X | B | B | B | A | | |
| Application Services | Security Knowledge Lifecycle | Code Samples | SI | A | A | | X | X | X | B | B | B | A | | A |
| Application Services | Abstraction | | SC | X | X | A | A | X | X | A | A | A | A | | |
| Information Services | BOSS | Audit Findings | AU | A | A | A | A | A | A | A | A | A | A | | |
| Information Services | Security Monitoring | eDiscovery Events | AU | X | X | X | X | X | X | B | B | B | X | | |
| Information Services | Reporting Services | Dashboard | CA | A | A | A | X | X | X | A | A | A | A | | |
| Information Services | Reporting Services | Data Mining | CA | A | A | A | A | A | A | A | A | A | A | | |
| Information Services | Reporting Services | Reporting Tools | CA | A | A | A | A | A | A | B | B | B | A | | |
| Information Services | Reporting Services | Business Intelligence | CA | A | A | A | | | | A | A | A | A | | |
| Information Services | ITOS | Problem Management | CA | A | A | A | X | X | X | B | B | B | A | | |
| Information Services | Service Delivery | Service Catalog | CM | A | A | A | A | A | A | A | A | A | x | | |
| Information Services | Service Delivery | SLA´s | CM | A | A | A | X | X | X | B | B | B | A | | |
| Information Services | ITOS | CMDB | CM | A | A | A | X | X | X | B | B | B | A | | |
| Information Services | ITOS | Change Management | CM | A | A | A | X | X | X | B | B | B | A | | |

| Information Services | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Information Services | Service Support | Configuration Rules (Metadata) | | C M | A | A | A | A | A | A | B | B | B | A |
| Information Services | Service Support | Configuration Management Database (CMDB) | | C M | A | A | A | A | A | A | B | B | B | X |
| Information Services | Service Support | Change Logs | | C M | A | A | A | A | A | A | B | B | B | X |
| Information Services | Security Monitoring | Compliance Monitoring | | C M | A | A | A | X | X | X | B | B | B | A |
| Information Services | Security Monitoring | Privilege Usage Events | | C M | X | X | X | X | X | X | B | B | B | A |
| Information Services | Service Delivery | Recovery Plans | | C P | A | A | A | X | X | X | A | A | A | A |
| Information Services | BOSS | GR Data (Employee & contractors) | | I A | A | A | A | A | A | A | A | A | A | X |
| Information Services | Security Monitoring | Authorization Events | | I A | X | X | X | A | X | X | B | B | B | X |
| Information Services | Security Monitoring | Authentication Events | | I A | X | X | X | X | X | X | B | B | B | A |
| Information Services | Security Monitoring | ACL´s | | I A | A | A | A | X | X | X | B | B | B | A |
| Information Services | Security Monitoring | CRL´s | | I A | A | A | A | X | X | X | B | B | B | A |
| Information Services | User Directory Services | Active Directory Services | | I A | A | A | A | X | X | X | B | B | B | A |
| Information Services | User Directory Services | LDAP Repositories | | I A | A | A | A | X | X | X | B | B | B | A |
| Information Services | User Directory Services | X.500 Repositories | | I A | A | A | A | X | X | X | B | B | B | A |
| Information Services | User Directory Services | DBMS Repositories | | I A | X | A | A | A | X | X | B | B | B | A |
| Information Services | User Directory Services | Registry Services | | I A | A | A | A | X | X | X | B | B | B | A |
| Information Services | User Directory Services | Location Services | | I A | A | A | A | | | | B | B | B | x |

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Information Services | User Directory Services | Federated Services | | I A | X | X | A | A | A | X | B | B | B | X | | |
| Information Services | User Directory Services | Virtual Directory Services | | I A | X | A | A | A | X | X | B | B | B | X | | |
| Information Services | User Directory Services | Meta Directory Services | | I A | X | A | A | A | X | X | B | B | B | A | | |
| Information Services | ITOS | Incident Management | | I R | X | X | X | X | X | X | B | B | B | A | | |
| Information Services | Service Support | Service Events | | I R | X | X | A | X | X | X | B | B | B | A | | |
| Information Services | BOSS | Data Classification | | R A | X | X | X | X | X | X | A | A | A | A | | |
| Information Services | Data Governance | Risk Assessments | | R A | X | X | X | A | A | A | B | B | B | X | | |
| Information Services | Risk Management | Risk Assessments | | R A | X | X | X | A | A | A | B | B | B | A | | |
| Information Services | Risk Management | Business Impact Assessment. | | R A | X | X | X | X | X | X | B | B | B | X | | |
| Information Services | Risk Management | VRA | | R A | X | X | X | A | A | X | B | B | B | x | A | |
| Information Services | Risk Management | TVM | | R A | X | X | X | A | A | X | B | B | B | x | | |
| Information Services | Service Delivery | OLA´s | | S A | A | A | A | A | A | A | A | A | A | A | | |
| Information Services | Data Governance | Non-Production Data | | S A | X | X | X | A | X | X | B | B | B | A | | |
| Information Services | Security Monitoring | NIPS Events | | S C | X | A | A | X | X | X | B | B | B | A | | |
| Information Services | Security Monitoring | DLP Events | | S C | X | A | A | X | X | X | B | B | B | A | | |
| Information Services | Data Governance | Information Leakage Metadata | | S I | X | X | A | A | A | X | B | B | B | A | | |
| Information Services | Data Governance | Data Segregation | | S I | X | A | | X | X | X | B | B | B | X | | |

| Information Services | Category | Service | | Type | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Information Services | Security Monitoring | Transformation Services | | S I | X | X | A | X | X | X | B | B | B | A | |
| Information Services | Security Monitoring | Session Events | | S I | X | X | A | X | X | X | B | B | B | A | |
| Information Services | Security Monitoring | Application Events | | S I | X | X | A | A | A | X | B | B | B | A | |
| Information Services | Security Monitoring | Network Events | | S I | X | X | A | A | X | X | B | B | B | X | |
| Information Services | Security Monitoring | Computer Events | | S I | X | X | A | A | X | X | B | B | B | x | |
| Information Services | Security Monitoring | Host Intrusion Protection Systems (HIPS) | | S I | X | X | A | A | A | X | B | B | B | A | |
| Information Services | Security Monitoring | Database Events | | S I | X | X | A | A | A | X | B | B | B | X | |
| Information Services | Service Delivery | Contracts | | P M | A | A | A | A | A | A | A | A | A | A | |
| Information Services | ITOS | PMO | | P M | A | A | A | | | | A | A | A | A | |
| Information Services | ITOS | Strategy | | P M | A | A | A | A | A | A | A | A | A | A | |
| Information Services | ITOS | Roadmap | | P M | A | A | A | A | A | A | A | A | A | A | |
| Information Services | ITOS | Knowledge Management | | P M | A | A | A | A | A | A | B | B | B | A | |
| Information Services | ITOS | Service Management | | P M | X | X | A | A | X | X | B | B | B | A | |
| Information Services | BOSS | Risk Assessments | | P M | X | X | X | A | A | A | A | A | A | A | |
| Information Services | BOSS | Process Ownership | | P M | X | X | X | A | A | A | A | A | A | A | |
| Information Services | BOSS | Business Strategy | | P M | A | A | A | A | A | A | A | A | A | A | |
| Information Services | Service Support | Knowledge Repository | | P M | A | A | A | A | A | A | B | B | B | A | |

| Service | Category | Subcategory | Detail | Code | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Information Services | Risk Management | GRC | | PM | X | X | X | A | X | X | A | A | A | A | A |
| Information Services | Risk Management | DR & BC Plans | | PM | X | X | X | X | X | X | B | B | B | A | |
| Infrastructure Services | Virtual Infrastructure: Storage Virtualization | Block-Based Virtualization | Network-Based | AC | X | A | A | X | X | X | B | B | B | A | |
| Infrastructure Services | Internal Infrastructure: Network Services | Authoritative Time Source | | AU | | | | X | X | X | B | B | B | A | |
| Infrastructure Services | Internal Infrastructure: Patch Management | Service Discovery | | MA | | | | A | A | A | B | B | B | A | |
| Infrastructure Services | Internal Infrastructure: Equipment Maintenance | | | MA | | | | A | A | A | B | B | B | A | |
| Infrastructure Services | Internal Infrastructure: Storage Services | | | MP | | | | A | A | A | B | B | B | A | A |
| Infrastructure Services | Virtual Infrastructure: Storage Virtualization | Block-Based Virtualization | Storage Device-Based | MP | X | A | A | X | X | X | B | B | B | A | |
| Infrastructure Services | Internal Infrastructure: Facility Security | Controlled Physical Access | Barriers | PE | | | | A | A | A | B | B | B | A | |
| Infrastructure Services | Internal Infrastructure: Facility Security | Controlled Physical Access | Security Patrols | PE | | | | A | A | A | B | B | B | A | |
| Infrastructure Services | Internal Infrastructure: Facility Security | Controlled Physical Access | Electronic Surveillance | PE | | | | A | A | A | B | B | B | A | A |
| Infrastructure Services | Internal Infrastructure: Facility Security | Controlled Physical Access | Physical Authentication | PE | | | | A | A | A | B | B | B | A | A |
| Infrastructure Services | Internal Infrastructure: Facility Security | Asset Handling | Data | PE | | | | A | A | A | B | B | B | A | A |
| Infrastructure Services | Internal Infrastructure: Facility Security | Asset Handling | Storage | PE | | | | A | A | A | B | B | B | X | |
| Infrastructure Services | Internal Infrastructure: Facility Security | Asset Handling | Hardware | PE | | | | A | A | A | B | B | B | X | A |
| Infrastructure Services | Internal Infrastructure: Facility Security | Environmental Risk Management | Physical Security | PE | | | | A | A | A | B | B | B | X | |

| Service | Subcategory | Detail | Detail 2 | Type | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Infrastructure Services | Internal Infrastructure: Facility Security | Environmental Risk Management | Equipment Location | PE | | | | A | A | A | B | B | B | X | A |
| Infrastructure Services | Internal Infrastructure: Facility Security | Environmental Risk Management | Power Redundancy | PE | | | | A | A | A | B | B | B | A | A |
| Infrastructure Services | Internal Infrastructure: Servers | | | CM | | | | A | A | A | B | B | B | X | |
| Infrastructure Services | Internal Infrastructure: Availability Services | | | CP | | | | A | A | A | B | B | B | A | |
| Infrastructure Services | Internal Infrastructure: Network Services | Network Segmentation | | SC | A | A | A | X | X | X | B | B | B | A | |
| Infrastructure Services | Virtual Infrastructure: Desktop "Client" Virtualization | Local | | SC | X | A | A | A | X | X | B | B | B | A | |
| Infrastructure Services | Virtual Infrastructure: Desktop "Client" Virtualization | Remote | Session-Based | SC | X | A | A | X | X | X | B | B | B | A | |
| Infrastructure Services | Virtual Infrastructure: Desktop "Client" Virtualization | Remote | VM-Based (VDI) | SC | X | A | A | X | X | X | B | B | B | A | |
| Infrastructure Services | Virtual Infrastructure: Storage Virtualization | Block-Based Virtualization | Host-Based | SC | X | A | A | X | X | X | B | B | B | A | |
| Infrastructure Services | Virtual Infrastructure: Storage Virtualization | File-Based virtualization | | SC | X | A | A | X | X | X | B | B | B | A | |
| Infrastructure Services | Virtual Infrastructure: Application Virtualization | Client Application Streaming | | SC | X | A | A | X | X | X | B | B | B | A | |
| Infrastructure Services | Virtual Infrastructure: Application Virtualization | Server Application Streaming | | SC | X | X | | X | X | X | B | B | B | A | |
| Infrastructure Services | Virtual Infrastructure: Virtual Workspaces | | | SC | X | A | A | X | X | X | B | B | B | A | |
| Infrastructure Services | Virtual Infrastructure: Server Virtualization | Virtual Machines (host based) | Full | SC | X | A | A | X | X | X | B | B | B | A | |
| | | | Paravirtualization | SC | X | A | A | X | X | X | B | B | B | A | |
| | | | Hardware-Assisted | SC | X | A | A | X | X | X | B | B | B | A | |
| | | OS Virtualization | | S | X | A | A | X | X | X | B | B | B | A | |

| Category | Sub 1 | Sub 2 | Sub 3 | Code | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | C | | | | | | | | | | | |
| | | TPM Virtualization | | SC | X | X | A | X | X | X | B | B | B | A | |
| | | Virtual Memory | | SC | X | A | A | X | X | X | B | B | B | A | |
| Infrastructure Services | Virtual Infrastructure: Network | Network Address Space | IPv4 | SC | X | X | X | X | X | X | B | B | B | | |
| | | | IPv6 | SC | X | X | X | X | X | X | B | B | B | X | |
| | | VLAN | | SC | X | A | A | X | X | X | B | B | B | X | |
| | | VNIC | | SC | X | A | A | X | X | X | B | B | B | X | |
| Infrastructure Services | Virtual Infrastructure: Database Virtualization | | | SC | X | X | A | X | X | X | B | B | B | | |
| Infrastructure Services | Virtual Infrastructure: Mobile Device Virtualization | | | SC | X | A | A | X | X | X | B | B | B | | |
| Infrastructure Services | Virtual Infrastructure: Smartcard Virtualization | | | SC | X | A | A | X | X | X | B | B | B | | |
| Infrastructure Services | Internal Infrastructure: Patch Management | Compliance Monitoring | | PM | | | | A | A | A | B | B | B | | |
| S & RM | Privilege Management Infrastructure | Privilege Usage Management | Privilege Usage Gateway | AC | A | A | A | X | X | X | B | B | B | X | |
| S & RM | Infrastructure Protection Services | Server | White Listing | AC | X | A | A | A | X | X | B | B | B | X | A |
| S & RM | Infrastructure Protection Services | Server | Host Firewall | AC | X | A | A | X | X | X | B | B | B | A | |
| S & RM | Infrastructure Protection Services | End-Point | Host Firewall | AC | X | X | A | A | X | X | B | B | B | A | A |
| S & RM | Infrastructure Protection Services | End-Point | Content Filtering | AC | X | X | A | A | A | X | B | B | B | A | A |
| S & RM | Infrastructure Protection Services | End-Point | White Listing | AC | X | A | A | A | X | X | B | B | B | X | A |
| S & RM | Infrastructure Protection Services | Network | Content Filtering | AC | X | X | A | A | X | X | B | B | B | A | A |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S & RM | Infrastructure Protection Services | Network | Firewall | AC | X | X | A | X | X | X | B | B | B | X | A |
| S & RM | Infrastructure Protection Services | Network | Black Listing Filtering | AC | X | A | A | X | X | X | B | B | B | A | A |
| S & RM | Infrastructure Protection Services | Application | Application Firewall | AC | X | X | A | X | X | X | B | B | B | A | A |
| S & RM | Infrastructure Protection Services | Application | Secure Collaboration | AC | X | X | A | A | X | X | B | B | B | A | A |
| S & RM | Infrastructure Protection Services | Application | Real Time Filtering | AC | X | X | A | A | X | | B | B | B | A | A |
| S & RM | Data Protection | Data Lifecycle Management | Meta data Control | AC | X | X | A | A | X | X | B | B | B | A | A |
| S & RM | Data Protection | Data Lifecycle Management | Data Seeding | AC | X | X | X | A | A | X | B | B | B | A | A |
| S & RM | Data Protection | Intellectual Property Prevention | Digital Rights Management | AC | A | A | A | X | X | X | B | B | B | A | A |
| S & RM | Policies and Standards | Role Based Awareness | | AC | X | X | X | A | A | A | A | A | A | A | A |
| S & RM | Governance Risk & Compliance | Technical Awareness and Training | | AT | X | X | X | X | X | X | B | B | B | A | |
| S & RM | Governance Risk & Compliance | Compliance Management | | AU | X | X | X | X | X | X | B | B | B | A | |
| S & RM | Governance Risk & Compliance | Audit Management | | AU | X | X | X | X | X | X | B | B | B | A | |
| S & RM | Threat and Vulnerability Management | Compliance Testing | Databases | AU | X | X | A | X | X | X | B | B | B | A | |
| | | | Servers | AU | X | A | A | X | X | X | B | B | B | A | A |
| S & RM | Policies and Standards | Best Practices & Regulatory correlation | | CA | A | A | A | X | X | X | A | A | A | A | A |
| S & RM | InfoSec Management | Capability Mapping | | CM | X | X | X | X | X | X | B | B | B | A | A |
| S & RM | Infrastructure Protection Services | End-Point | Inventory Control | CM | X | A | A | A | X | X | B | B | B | A | A |
| S & RM | Data Protection | Intellectual Property Prevention | Intellectual Property | CM | X | X | X | A | X | X | B | B | B | A | A |
| S & RM | Policies and Standards | Operational Security Baselines | | CM | A | A | A | A | A | A | A | A | A | A | A |
| | Policies and Standards | Job Aid Guidelines | | CM | A | A | A | A | A | A | A | A | A | A | A |

| S & RM | | | | I/A | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S & RM | Privilege Management Infrastructure | Identity Management | Domain Unique Identifier | I A | A | A | A | A | A | A | B | B | B | A | |
| S & RM | Privilege Management Infrastructure | Identity Management | Federated IDM | I A | X | X | A | A | A | X | B | B | B | A | |
| S & RM | Privilege Management Infrastructure | Identity Management | Identity Provisioning | I A | X | X | X | A | A | X | B | B | B | A | |
| S & RM | Privilege Management Infrastructure | Identity Management | Attribute Provisioning | I A | X | X | X | A | A | X | B | B | B | A | |
| S & RM | Privilege Management Infrastructure | Authorization Services | Policy Enforcement | I A | X | X | X | A | A | X | B | B | B | X | |
| S & RM | Privilege Management Infrastructure | Authorization Services | Policy definition | I A | X | X | X | A | A | X | B | B | B | A | |
| S & RM | Privilege Management Infrastructure | Authorization Services | Principal Data Management | I A | X | X | X | A | A | X | B | B | B | A | |
| S & RM | Privilege Management Infrastructure | Authorization Services | XACML | I A | A | A | A | X | X | X | B | B | B | A | |
| S & RM | Privilege Management Infrastructure | Authorization Services | Role Management | I A | X | X | X | X | X | X | B | B | B | A | |
| S & RM | Privilege Management Infrastructure | Authorization Services | Obligation | I A | A | A | A | X | X | X | B | B | B | A | |
| S & RM | Privilege Management Infrastructure | Authorization Services | Out of the Box (OTB) autZ | I A | X | A | A | X | X | X | B | B | B | A | |
| S & RM | Privilege Management Infrastructure | Authentication Services | SAML Token | I A | A | A | A | X | X | X | B | B | B | X | |
| S & RM | Privilege Management Infrastructure | Authentication Services | Risk Based Authentication | I A | X | X | X | X | X | X | B | B | B | X | |
| S & RM | Privilege Management Infrastructure | Authentication Services | Multifactor | I A | X | X | A | X | X | X | B | B | B | X | |
| S & RM | Privilege Management Infrastructure | Authentication Services | OTP | I A | A | A | A | X | X | X | B | B | B | A | |
| S & RM | Privilege Management Infrastructure | Authentication Services | Smart Card | I A | X | X | A | A | A | X | B | B | B | A | |
| S & RM | Privilege Management Infrastructure | Authentication Services | Password Management | I A | X | X | X | X | X | X | B | B | B | X | |

| S & RM | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S & RM | Privilege Management Infrastructure | Authentication Services | Biometrics | I A | X | X | X | A | A | X | B | B | B | A | |
| S & RM | Privilege Management Infrastructure | Authentication Services | Network Authentication | I A | X | A | A | X | X | X | B | B | B | A | |
| S & RM | Privilege Management Infrastructure | Authentication Services | Single Sign On | I A | A | A | A | X | X | X | B | B | B | A | |
| S & RM | Privilege Management Infrastructure | Authentication Services | WS-Security | I A | X | X | A | X | X | X | B | B | B | A | |
| S & RM | Privilege Management Infrastructure | Authentication Services | Middleware Authentication | I A | X | X | A | X | X | X | B | B | B | A | |
| S & RM | Privilege Management Infrastructure | Authentication Services | Identity Verification | I A | X | X | X | X | X | X | B | B | B | A | |
| S & RM | Privilege Management Infrastructure | Authentication Services | Out-of-The-Box (OTB) Authentication | I A | X | X | A | X | X | X | B | B | B | A | |
| S & RM | Privilege Management Infrastructure | Privilege Usage Management | Keystroke/Session Logging | I A | X | X | X | X | X | X | B | B | B | A | |
| S & RM | Privilege Management Infrastructure | Privilege Usage Management | Password Vaulting | I A | X | X | A | X | X | X | B | B | B | A | |
| S & RM | Threat and Vulnerability Management | Compliance Testing | Network Authentication | I A | X | X | A | X | X | X | B | B | B | A | A |
| S & RM | Infrastructure Protection Services | End-Point | Forensic Tools | I R | X | X | X | A | A | X | B | B | B | A | A |
| S & RM | Infrastructure Protection Services | End-Point | Media Lockdown | M P | A | A | A | X | X | X | B | B | B | A | A |
| S & RM | InfoSec Management | Residual Risk Management | | P L | X | X | A | A | X | X | B | B | B | A | |
| S & RM | Governance Risk & Compliance | Policy Management | Exceptions | R A | X | X | X | X | X | X | B | B | B | X | A |
| S & RM | Governance Risk & Compliance | Policy Management | Self-Assessment | R A | X | X | X | A | A | A | B | B | B | A | A |
| S & RM | InfoSec Management | Risk Dashboard | | R A | X | X | X | X | X | X | B | B | B | A | |
| S & RM | Threat and Vulnerability Management | Vulnerability Management | application | R A | X | X | A | X | X | X | B | B | B | A | A |
| | | | Infrastructure | R A | X | A | A | X | X | X | B | B | B | A | A |
| | | | DB | R A | X | X | A | X | X | X | B | B | B | X | A |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Penetration Testing | Internal | R A | X | X | A | A | X | X | B | B | B | X | A |
| | | | External | R A | X | X | A | X | X | X | B | B | B | X | A |
| | | Threat Management | Source Code Scanning | R A | X | X | X | X | X | X | B | B | B | X | A |
| | | | Risk Taxonomy | R A | X | X | X | A | X | X | B | B | B | X | |
| S & RM | Policies and Standards | Data/ Asset Classification | | R A | X | X | X | X | X | X | A | A | A | X | A |
| S & RM | Governance Risk & Compliance | Vendor Management | | S A | X | X | X | X | X | X | B | B | B | X | A |
| S & RM | Data Protection | Data Lifecycle Management | Life cycle management | S A | X | X | X | X | X | X | B | B | B | X | A |
| S & RM | Policies and Standards | Technical Security Standards | | S A | X | X | X | X | X | X | A | A | A | X | A |
| S & RM | Privilege Management Infrastructure | Privilege Usage Management | Resource Protection | S C | A | A | A | X | X | X | B | B | B | A | |
| S & RM | Infrastructure Protection Services | Network | Deep Packet Inspection (DPI) | S C | X | A | A | X | X | X | B | B | B | A | A |
| S & RM | Infrastructure Protection Services | Network | Wireless Protection | S C | A | A | A | X | X | X | B | B | B | A | A |
| S & RM | Infrastructure Protection Services | Network | Link Layer Network secuiry | S C | A | A | A | X | X | X | B | B | B | A | A |
| S & RM | Infrastructure Protection Services | Application | XML Appliance | S C | X | X | A | A | X | X | B | B | B | A | A |
| S & RM | Infrastructure Protection Services | Application | Secure Messaging | S C | X | X | A | A | A | X | B | B | B | A | A |
| S & RM | Data Protection | Data Lifecycle Management | Data De-Identification | S C | X | X | X | A | X | X | B | B | B | A | A |
| S & RM | Data Protection | Data Lifecycle Management | Data Masking | S C | X | X | X | A | X | X | B | B | B | A | A |
| S & RM | Data Protection | Data Lifecycle Management | Data Tagging | S C | X | X | A | A | X | X | B | B | B | A | A |
| S & RM | Data Protection | Data Lifecycle Management | Data Obscuring | S C | X | X | X | A | X | X | B | B | B | A | A |
| S & RM | Data Protection | Data Leakage Prevention | Data Discovery | S C | X | X | X | A | X | X | B | B | B | A | A |
| S & RM | Data Protection | Data Leakage Prevention | Network (Data in Transit) | S C | X | X | A | X | X | X | B | B | B | A | A |
| S & RM | Data Protection | Data Leakage Prevention | End-Point (data in Use) | S C | X | X | X | X | X | X | B | B | B | A | A |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S & RM | Data Protection | Data Leakage Prevention | Server (data at Rest) | S C | X | X | A | X | X | X | B | B | B | A | A |
| S & RM | Cryptographic Services | Key Management | Symmetric Keys | S C | X | X | X | X | X | X | B | B | B | A | A |
| S & RM | Cryptographic Services | Key Management | Asymmetric Keys | S C | X | X | X | X | X | X | B | B | B | A | A |
| S & RM | Cryptographic Services | PKI | | S C | X | X | X | X | X | X | B | B | B | A | A |
| S & RM | Cryptographic Services | Data in use (memory) Encryption | | S C | X | X | A | X | X | X | B | B | B | A | A |
| S & RM | Cryptographic Services | Data in Transit Encryption (Transitory, Fixed) | | S C | X | X | X | X | X | X | B | B | B | A | A |
| S & RM | Cryptographic Services | Data as Rest Encryption (DB, File, SAN, Desktop, Mobile) | | S C | X | X | X | X | X | X | B | B | B | X | A |
| S & RM | Infrastructure Protection Services | Server | Anti-virus | S I | X | X | A | X | X | X | B | B | B | X | |
| S & RM | Infrastructure Protection Services | Server | HIPS/HIDS (Intrusion Protection /Detection) | S I | X | A | A | X | X | X | B | B | B | X | |
| S & RM | Infrastructure Protection Services | End-Point | Anti-Virus, Anti-Spam, Anti-Malware | S I | X | X | A | A | A | X | B | B | B | X | |
| S & RM | Infrastructure Protection Services | End-Point | HIPS/HIDS (Intrusion Protection /Detection) | S I | X | X | A | A | X | X | B | B | B | X | A |
| S & RM | Infrastructure Protection Services | End-Point | Hardware Based trusted Assets | S I | A | A | A | X | X | X | B | B | B | X | A |
| S & RM | Infrastructure Protection Services | Network | NIPS/NIDS | S I | X | A | A | X | X | X | B | B | B | X | A |
| S & RM | Data Protection | Data Lifecycle Management | eSignature | S I | X | X | X | A | X | X | B | B | B | A | A |
| S & RM | Cryptographic Services | Signature Services | | S I | X | X | X | X | X | X | B | B | B | A | A |
| S & RM | Governance Risk & Compliance | IT Risk Management | | P M | X | X | X | X | X | X | B | B | B | A | A |
| S & RM | InfoSec Management | Risk Portfolio Management | | P M | A | A | A | A | A | A | B | B | B | A | |
| S & RM | Privilege Management Infrastructure | Authorization Services | Policy Management | P M | X | X | X | A | A | X | B | B | B | X | |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S & RM | Privilege Management Infrastructure | Authorization Services | Resource Data management | P M | X | X | X | A | A | X | B | B | B | A | |
| S & RM | Policies and Standards | Information Security Polices | | P M | A | A | A | A | A | A | A | A | A | X | A |

DRAFT

## 11.2 SERVICE-BASED ECOSYSTEM-LEVEL DATA AGGREGATION

Security component definitions can be found on the https://research.cloudsecurityalliance.org/tci

| Domain | High-level Security Component | Mid-level Security Component | Low-level Security Component | 800-53 Family | IaaS | | | | PaaS | | | | SaaS | | | | ALL | ALL |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Consumer | Provider | Broker | U | Consumer | Provider | Broker | U | Consumer | Provider | Broker | U | Carrier | Auditor |
| BOSS | Compliance | Intellectual Property Protection | | AC | X | X | A | X | A | X | A | X | A | X | A | X | A | A |
| BOSS | Data Governance | Handling/ Labeling/ Security Policy | | AC | X | X | A | X | X | X | A | X | X | X | A | X | A | A |
| BOSS | Data Governance | Clear Desk Policy | | AC | A | A | A | A | A | A | A | A | A | A | A | A | A | A |
| BOSS | Data Governance | Rules for Information Leakage Prevention | | AC | X | X | B | X | A | X | B | X | A | X | B | X | X | |
| BOSS | Human Resource Security | Employee Awareness | | AT | A | A | A | A | A | A | A | A | A | A | A | A | A | A |
| BOSS | Security Monitoring Services | Market Threat Intelligence | | AT | A | X | B | X | A | X | B | X | A | X | B | X | A | A |
| BOSS | Security Monitoring Services | Knowledge Base | | AT | A | A | B | Ab | A | A | B | Ab | A | A | B | Ab | A | |
| BOSS | Compliance | Audit Planning | | AU | A | A | B | Ab | A | A | B | Ab | A | A | B | Ab | X | A |
| BOSS | Compliance | Internal Audits | | AU | A | A | B | Ab | A | A | B | Ab | A | A | B | Ab | X | A |
| BOSS | Security Monitoring Services | Event Mining | | AU | X | A | B | X | X | X | B | X | A | X | B | X | A | |
| BOSS | Security Monitoring Services | Event Correlation | | AU | X | A | B | X | X | X | B | X | A | X | B | X | X | |
| BOSS | Security Monitoring Services | Email Journaling | | AU | X | A | B | X | X | X | B | X | A | X | B | X | A | |

| BOSS | Service | Sub-Service | | Code | | | | | | | | | | | | | | |
|------|---------|-------------|--|------|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
| BOSS | Security Monitoring Services | User Behaviors and Profile Patterns | | AU | X | A | B | X | X | X | B | X | A | X | B | X | A | A |
| BOSS | Legal Services | E-Discovery | | AU | X | X | A | X | X | X | A | X | X | X | A | X | A | A |
| BOSS | Legal Services | Incident Response Legal Preparation | | AU | X | X | A | X | X | X | A | X | X | X | A | X | A | |
| BOSS | Internal Investigations | Forensic Analysis | | AU | X | X | A | X | X | X | A | X | X | X | A | X | A | A |
| BOSS | Internal Investigations | e-Mail Journaling | | AU | A | A | A | A | A | A | A | A | A | A | A | A | A | A |
| BOSS | Compliance | Independent Audits | | CA | A | A | B | Ab | A | A | B | Ab | A | A | B | Ab | X | A |
| BOSS | Compliance | Third Party Audits | | CA | A | A | B | Ab | A | A | B | Ab | A | A | B | Ab | X | A |
| BOSS | Operational Risk Management | Business Impact Analysis | | CP | A | X | A | X | A | X | A | X | A | X | A | X | A | A |
| BOSS | Operational Risk Management | Business Continuity | | CP | X | X | B | X | A | X | B | X | A | X | B | X | X | |
| BOSS | Operational Risk Management | Crisis Management | | IR | A | X | B | X | A | X | B | X | A | X | B | X | X | A |
| BOSS | Operational Risk Management | Risk Management Framework | | IR | A | A | A | A | A | A | A | A | A | A | A | A | A | A |
| BOSS | Operational Risk Management | Independent Risk Management | | IR | A | X | B | X | A | X | B | X | A | X | B | X | X | A |
| BOSS | Security Monitoring Services | Database Monitoring | | IR | X | A | B | X | A | X | B | X | | X | B | X | A | |
| BOSS | Security Monitoring Services | Application Monitoring | | IR | X | A | B | X | X | X | B | X | X | X | B | X | A | |
| BOSS | Security Monitoring Services | End-Point Monitoring | | IR | X | A | B | X | X | A | B | X | X | A | B | X | A | |
| BOSS | Security Monitoring | Cloud Monitoring | | IR | X | X | B | X | X | X | B | X | X | X | B | X | A | |

| BOSS | Category | Subcategory | | Code | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Services | | | | | | | | | | | | | | | | | |
| BOSS | Data Governance | Secure Disposal of Data | | MP | X | X | A | X | A | X | A | X | A | X | A | X | A | A |
| BOSS | Human Resource Security | Employee Termination | | PS | X | X | B | X | X | X | B | X | X | X | B | X | A | A |
| BOSS | Human Resource Security | Employment Agreements | | PS | X | X | B | X | X | X | B | X | X | X | B | X | A | A |
| BOSS | Human Resource Security | Background Screening | | PS | X | X | B | X | X | X | B | X | X | X | B | X | A | A |
| BOSS | Human Resource Security | Job Descriptions | | PS | X | X | B | X | X | X | B | X | X | X | B | X | A | A |
| BOSS | Human Resource Security | Roles and Responsibilities | | PS | X | X | B | X | X | X | B | X | X | X | B | X | A | A |
| BOSS | Human Resource Security | Employee Code of Conduct | | PS | X | X | B | X | X | X | B | X | X | X | B | X | A | A |
| BOSS | Compliance | Information Systems Regulatory Mapping | | RA | A | X | B | X | A | X | B | X | A | X | B | X | X | A |
| BOSS | Data Governance | Data Ownership - Personnel Responsibilities/ Stewardship | | RA | X | A | A | X | X | X | A | X | X | X | A | X | A | A |
| BOSS | Data Governance | Data Classification | | RA | X | X | A | X | X | X | A | X | X | X | A | X | A | A |
| BOSS | Security Monitoring Services | Managed (Outsourced) Security Services | | SA | X | A | B | X | X | X | B | X | X | X | B | X | A | |
| BOSS | Legal Services | Contracts | | SA | X | X | A | X | X | X | A | X | X | X | A | X | A | A |
| BOSS | Security Monitoring Services | Honey Pot | | SC | A | | | Ab | A | A | | Ab | | A | | Ab | | |
| BOSS | Security Monitoring Services | Real Time Internetwork Defense (SCAP) | | SC | A | X | B | X | A | X | B | X | A | X | B | X | X | |

| Domain | Category | Subcategory | Detail | Code | G1a | G1b | G1c | G1d | G2a | G2b | G2c | G2d | G3a | G3b | G3c | G3d | C1 | C2 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| BOSS | Data Governance | Rules for Data Retention | | SI | A | X | B | X | A | X | B | X | A | X | B | X | A | A |
| BOSS | Security Monitoring Services | SIEM Platform | | SI | X | A | B | X | X | X | B | X | A | X | B | X | X | A |
| BOSS | Security Monitoring Services | Anti Phishing | | SI | A | A | B | Ab | A | A | B | Ab | A | A | B | Ab | A | |
| BOSS | Compliance | Contract/ Authority Maintenance | | PM | X | A | B | X | X | A | B | X | A | X | B | X | X | A |
| BOSS | Operational Risk Management | Operational Risk Committee | | PM | X | X | A | X | A | X | A | X | A | X | A | X | A | A |
| BOSS | Operational Risk Management | Key Risk Indicators | | PM | X | A | A | X | X | A | A | X | A | X | A | X | A | |
| BOSS | Security Monitoring Services | Counter Threat Management | | PM | A | X | B | X | A | X | B | X | A | X | B | X | A | |
| BOSS | Security Monitoring Services | SOC Portal | | PM | A | A | B | Ab | A | A | B | Ab | A | A | B | Ab | X | |
| BOSS | Security Monitoring Services | Branding Protection | | PM | A | A | B | Ab | A | A | B | Ab | A | A | B | Ab | A | A |
| ITOS | IT Operations | Resource Management | Segregation of duties | AC | X | X | B | X | X | X | B | X | X | X | B | X | A | A |
| ITOS | IT Operations | Resource Management | Contractors | AC | A | A | A | A | A | A | A | A | A | A | A | A | A | A |
| ITOS | Service Delivery | Information Technology Resiliency | Resiliency Analysis | AU | X | X | B | X | A | X | B | X | A | X | B | X | X | |
| ITOS | Service Delivery | Information Technology Resiliency | Capacity Planning | AU | X | X | B | X | A | X | B | X | A | X | B | X | X | |
| ITOS | Service Support | Configuration Management | Automated Asset Discovery | AU | A | A | B | Ab | A | A | B | Ab | A | A | B | Ab | A | |
| ITOS | Service Support | Problem Managem | Event Classificati | AU | X | A | B | X | X | X | B | X | X | X | B | X | X | A |

| ITOS | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | ent | on | | | | | | | | | | | | | | | |
| ITOS | Service Support | Problem Management | Root Cause Analysis | AU | A | X | B | X | A | X | B | X | A | X | B | X | X | |
| ITOS | IT Operations | Portfolio Management | Maturity Model | CM | A | A | A | A | A | A | A | A | A | A | A | A | A | |
| ITOS | Service Delivery | Asset Management | Change Back | CM | A | A | A | A | A | A | A | A | A | A | A | A | A | |
| ITOS | Service Support | Configuration Management | Software Management | CM | X | X | B | X | X | X | B | X | A | X | B | X | A | |
| ITOS | Service Support | Configuration Management | Configuration Management | CM | X | X | B | X | X | X | B | X | A | X | B | X | A | |
| ITOS | Service Support | Configuration Management | Physical Inventory | CM | A | A | B | Ab | A | A | B | Ab | A | A | B | Ab | A | |
| ITOS | Service Support | Knowledge Management | Benchmarking | CM | A | A | A | A | A | A | A | A | A | A | A | A | A | A |
| ITOS | Service Support | Knowledge Management | Security Job Aids | CM | A | A | A | A | A | A | A | A | A | A | A | A | A | A |
| ITOS | Service Support | Knowledge Management | Security FAQ | CM | A | A | A | A | A | A | A | A | A | A | A | A | A | A |
| ITOS | Service Support | Change Management | Service Provisioning | CM | A | X | A | X | A | X | A | X | A | X | A | X | A | A |
| ITOS | Service Support | Change Management | Approval Workflow | CM | A | X | A | X | A | X | A | X | A | X | A | X | A | |
| ITOS | Service Support | Change Management | Change Review Board | CM | A | X | A | X | A | X | A | X | A | X | A | X | A | |
| ITOS | Service Support | Change Management | Planned Changes | CM | A | X | A | X | A | X | A | X | A | X | A | X | A | |
| ITOS | Service Support | Release Management | Version Control | CM | X | X | A | X | X | X | A | X | X | X | A | X | A | |
| ITOS | Service Support | Release Management | Source Code Manageme | CM | X | X | A | X | X | X | A | X | X | X | A | X | A | |

| ITOS | Category | Subcategory | Item | Code | | | | | | | | | | | | | | |
|------|----------|-------------|------|------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | nt | | | | | | | | | | | | | | | |
| ITOS | IT Operations | DRP | Plan Management | CP | X | X | B | X | A | X | B | X | A | X | B | X | A | |
| ITOS | Service Support | Configuration Management | Capacity Planning | CP | X | X | B | X | A | X | B | X | A | X | B | X | A | |
| ITOS | Service Support | Incident Management | Security Incident Response | IR | X | X | B | X | X | X | B | X | X | X | B | X | X | |
| ITOS | Service Support | Incident Management | Automated Ticketing | IR | A | X | B | X | A | X | B | X | A | X | B | X | X | A |
| ITOS | Service Support | Incident Management | Ticketing | IR | X | X | B | X | X | X | B | X | X | X | B | X | X | A |
| ITOS | Service Support | Incident Management | Cross Cloud Security Incident Response | IR | X | X | B | X | X | X | B | X | X | X | B | X | X | |
| ITOS | Service Support | Problem Management | Trend Analysis | IR | A | X | B | X | A | X | B | X | A | X | B | X | X | |
| ITOS | Service Support | Problem Management | Orphan Incident Management | IR | A | X | B | X | A | X | B | X | A | X | B | X | A | |
| ITOS | Service Support | Knowledge Management | Trend Analysis | IR | A | X | A | X | A | X | A | X | A | X | A | X | A | A |
| ITOS | Service Support | Change Management | Emergency Changes | MA | A | X | A | X | A | X | A | X | A | X | A | X | A | |
| ITOS | Service Support | Release Management | Scheduling | MA | A | X | A | X | A | X | A | X | A | X | A | X | A | |
| ITOS | Service Delivery | Asset Management | Service Costing (Internal) | SA | A | A | B | Ab | A | A | B | Ab | A | A | B | Ab | X | |
| ITOS | Service Support | Incident Management | Self-Service | SA | A | X | B | X | A | X | B | X | A | X | B | X | A | |
| ITOS | Service Delivery | Information Technology Resiliency | Availability Management | SC | X | X | B | X | A | X | B | X | A | X | B | X | X | |
| ITOS | Service Delivery | Application Performan | | SI | X | A | A | X | X | X | A | X | A | X | A | X | A | |

| ITOS | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | ce Monitoring | | | | | | | | | | | | | | | |
| ITOS | Service Support | Release Management | Testing | SI | A | X | A | X | A | X | A | X | A | X | A | X | A | |
| ITOS | Service Support | Release Management | Build | SI | A | X | A | X | A | X | A | X | | X | A | X | A | |
| ITOS | IT Operations | DRP | Test Management | PM | X | X | B | X | A | X | B | X | A | X | B | X | A | A |
| ITOS | IT Operations | IT Governance | Architecture Governance | PM | A | A | A | A | A | A | A | A | A | A | A | A | A | - |
| ITOS | IT Operations | IT Governance | Standards and Guidelines | PM | X | A | A | X | X | X | A | X | X | X | A | X | A | |
| ITOS | IT Operations | PMO | Program Mngmt | PM | A | A | A | A | A | A | A | A | A | A | A | A | A | A |
| ITOS | IT Operations | PMO | Project Mgnmt | PM | A | A | A | A | A | A | A | A | A | A | A | A | A | A |
| ITOS | IT Operations | PMO | Remediation | PM | A | A | A | A | A | A | A | A | A | A | A | A | A | A |
| ITOS | IT Operations | Portfolio Management | Roadmap | PM | A | A | A | A | A | A | X | A | A | A | A | A | A | |
| ITOS | IT Operations | Portfolio Management | Strategy Alignment | PM | A | A | A | A | A | A | A | A | A | A | A | A | A | |
| ITOS | Service Delivery | Service Level Management | Objectives | PM | X | X | B | X | X | X | B | X | X | X | B | X | X | |
| ITOS | Service Delivery | Service Level Management | OLAs | PM | X | A | B | X | X | X | B | X | X | X | B | X | X | A |
| ITOS | Service Delivery | Service Level Management | Internal SLAs | PM | X | A | A | X | X | A | A | X | X | A | A | X | A | A |
| ITOS | Service Delivery | Service Level Management | External SLAs | PM | X | X | B | X | X | X | B | X | X | X | B | X | X | A |
| ITOS | Service Delivery | Service Level Management | Vendor Management | PM | A | A | A | A | A | A | A | A | A | A | A | A | A | A |
| ITOS | Service Delivery | Service Level Managem | Service Dashboard | PM | X | X | B | X | A | X | B | X | A | X | B | X | A | A |

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | ent | | | | | | | | | | | | | | | | | |
| ITOS | Service Delivery | Asset Management | Operational Budgeting | P M | A | A | A | A | | A | A | A | A | | A | A | A | A | A |
| ITOS | Service Delivery | Asset Management | Investment Budgeting | P M | A | A | A | A | | A | A | A | A | | A | A | A | A | A |
| ITOS | Service Support | Problem Management | Problem Resolutions | P M | A | X | B | X | | A | X | B | X | | A | X | B | X | X |
| ITOS | Service Support | Knowledge Management | Best Practices | P M | X | X | A | X | | X | X | A | X | | A | X | A | X | A |
| Presentation Services | Presentation Modality | Consumer Service Platform | Social Media | AC | X | | B | X | | X | | B | X | | | X | B | X | |
| Presentation Services | Presentation Modality | Consumer Service Platform | Collaboration | AC | X | | B | X | | X | | B | X | | | X | B | X | |
| Presentation Services | Presentation Modality | Consumer Service Platform | E-Mail | AC | X | | B | X | | X | | B | X | | | X | B | X | |
| Presentation Services | Presentation Modality | Enterprise Service Platform | B2M | AC | X | A | B | X | | X | A | B | X | | X | X | B | X | |
| Presentation Services | Presentation Modality | Enterprise Service Platform | B2B | AC | X | A | B | X | | X | A | B | X | | X | X | B | X | |
| Presentation Services | Presentation Modality | Enterprise Service Platform | B2C | AC | X | A | B | X | | X | A | B | X | | X | X | B | X | |
| Presentation Services | Presentation Modality | Enterprise Service Platform | P2P | AC | X | A | B | X | | X | A | B | X | | X | X | B | X | |
| Presentation | Presentation Platform | End-Points | Mobile Devices | AC | X | A | B | X | | X | A | B | X | | X | A | B | X | |

| | | | | | X | A | B | X | | X | A | B | X | | X | A | B | X | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Services | | | | | | | | | | | | | | | | | | | | | | | |
| Presentation Services | Presentation Platform | End-Points | Fixed Devices | AC | X | A | B | X | | X | A | B | X | | X | A | B | X | | | | | |
| Presentation Services | Presentation Platform | End-Points | Desktops | AC | X | A | B | X | | X | A | B | X | | X | A | B | X | | | | | |
| Presentation Services | Presentation Platform | End-Points | Portable Devices | AC | X | A | B | X | | X | A | B | X | | X | A | B | X | | | | | |
| Presentation Services | Presentation Platform | End-Points | Medical Devices | AC | X | A | B | X | | X | A | B | X | | X | A | B | X | | | | | |
| Presentation Services | Presentation Platform | End-Points | Smart Appliances | AC | X | A | B | X | | X | A | B | X | | X | A | B | X | | | | | |
| Presentation Services | Presentation Modality | Consumer Service Platform | Search | SC | X | | B | X | | X | | B | X | | | X | B | X | | | | | |
| Presentation Services | Presentation Modality | Consumer Service Platform | e-Readers | SC | X | | B | X | | X | | B | X | | | X | B | X | | | | | |
| Presentation Services | Presentation Modality | Enterprise Service Platform | B2E | SC | X | A | B | X | | X | A | B | X | | X | X | B | X | | | | | |
| Presentation Services | Presentation Platform | Speech Recognition (IVR) | | SC | X | | B | X | | X | | B | X | | X | | B | X | | | | | |
| Presentation Services | Presentation Platform | Handwriting (ICR) | | SC | X | | B | X | | X | | B | X | | X | | B | X | | | | | |

| Domain | Category | Subcategory | Detail | Code | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Application Services | Security Knowledge Lifecycle | Attack Patterns | | CM | X | X | B | X | A | X | B | X | A | X | B | X | A | A |
| Application Services | Security Knowledge Lifecycle | Security Design Patterns | | SA | X | X | B | X | A | X | B | X | A | X | B | X | A | |
| Application Services | Security Knowledge Lifecycle | Security Application Framework - ACEGI | | SA | X | A | B | X | A | X | B | X | A | X | B | X | A | A |
| Application Services | Development Processes | Self Service | Security Code Review | SA | X | X | B | X | X | X | B | X | X | X | B | X | A | A |
| Application Services | Development Processes | Self Service | Application Vulnerability Scanning | SA | X | X | B | X | X | X | B | X | A | X | B | X | A | A |
| Application Services | Development Processes | Self Service | Stress Volume Testing | SA | A | X | B | X | A | X | B | X | A | X | B | X | X | A |
| Application Services | Development Processes | Software Quality Assurance | | SA | X | X | B | X | X | X | B | X | X | X | B | X | A | A |
| Application Services | Integration Middleware | | | SA | X | A | B | X | X | X | B | X | A | X | B | X | A | |
| Application Services | Connectivity & Delivery | | | CM | X | X | B | X | A | X | B | X | A | X | B | X | A | |
| Application Services | Programming Interfaces | Input Validation | | SI | A | X | B | X | A | X | B | X | A | X | B | X | A | |
| Application | Security Knowledge Lifecycle | Code Samples | | SI | A | X | B | X | A | X | B | X | | X | B | X | A | A |

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Services | | | | | | | | | | | | | | | | | | |
| Application Services | Abstraction | | | SC | X | A | A | X | X | X | A | X | A | X | A | X | A | |
| Information Services | BOSS | Audit Findings | | AU | A | A | A | A | A | A | A | A | A | A | A | A | A | |
| Information Services | Security Monitoring | eDiscovery Events | | AU | X | X | B | X | X | X | B | X | X | X | B | X | A | |
| Information Services | Reporting Services | Dashboard | | CA | A | X | A | X | A | X | A | X | A | X | A | X | A | |
| Information Services | Reporting Services | Data Mining | | CA | A | A | A | A | A | A | A | A | A | A | A | A | A | |
| Information Services | Reporting Services | Reporting Tools | | CA | A | A | B | Ab | A | A | B | Ab | A | A | B | Ab | X | |
| Information Services | Reporting Services | Business Intelligence | | CA | A | | A | A | A | | A | A | A | | A | A | A | |
| Information Services | ITOS | Problem Management | | CA | A | X | B | X | A | X | B | X | A | X | B | X | X | |
| Information Services | Service Delivery | Service Catalog | | CM | A | A | A | A | A | A | A | A | A | A | A | A | A | |
| Information Services | Service Delivery | SLA´s | | CM | A | X | B | X | A | X | B | X | A | X | B | X | X | |

| Information Services | Function | Asset | | Type | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Information Services | ITOS | CMDB | | CM | A | X | B | X | A | X | B | X | A | X | B | X | A |
| Information Services | ITOS | Change Management | | CM | A | X | B | X | A | X | B | X | A | X | B | X | X |
| Information Services | Service Support | Configuration Rules (Metadata) | | CM | A | A | B | Ab | A | A | B | Ab | A | A | B | Ab | A |
| Information Services | Service Support | Configuration Management Database (CMDB) | | CM | A | A | B | Ab | A | A | B | Ab | A | A | B | Ab | A |
| Information Services | Service Support | Change Logs | | CM | A | A | B | Ab | A | A | B | Ab | A | A | B | Ab | X |
| Information Services | Security Monitoring | Compliance Monitoring | | CM | A | X | B | X | A | X | B | X | A | X | B | X | A |
| Information Services | Security Monitoring | Privilege Usage Events | | CM | X | X | B | X | X | X | B | X | X | X | B | X | A |
| Information Services | Service Delivery | Recovery Plans | | CP | A | X | A | X | A | X | A | X | A | X | A | X | A |
| Information Services | BOSS | GR Data (Employee & contractors) | | IA | A | A | A | A | A | A | A | A | A | A | A | A | A |
| Information Services | Security Monitoring | Authorization Events | | IA | X | A | B | X | X | X | B | X | X | X | B | X | A |
| Informatio | Security Monitoring | Authentication | | IA | X | X | B | X | X | X | B | X | X | X | B | X | A |

| Infor mation Servi ces | | Events | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Infor mation Servi ces | Security Monitoring | ACL´s | | IA | A | X | B | X | A | X | B | X | A | X | B | X | X | |
| Infor mation Servi ces | Security Monitoring | CRL´s | | IA | A | X | B | X | A | X | B | X | A | X | B | X | X | |
| Infor mation Servi ces | User Directory Services | Active Directory Services | | IA | A | X | B | X | A | X | B | X | A | X | B | X | A | |
| Infor mation Servi ces | User Directory Services | LDAP Repositori es | | IA | A | X | B | X | A | X | B | X | A | X | B | X | A | |
| Infor mation Servi ces | User Directory Services | X.500 Repositori es | | IA | A | X | B | X | A | X | B | X | A | X | B | X | A | |
| Infor mation Servi ces | User Directory Services | DBMS Repositori es | | IA | X | A | B | X | A | X | B | X | A | X | B | X | A | |
| Infor mation Servi ces | User Directory Services | Registry Services | | IA | A | X | B | X | A | X | B | X | A | X | B | X | A | |
| Infor mation Servi ces | User Directory Services | Location Services | | IA | A | | B | A b | A | | B | A b | A | | B | A b | A | |
| Infor mation Servi ces | User Directory Services | Federated Services | | IA | X | A | B | X | X | A | B | X | A | X | B | X | A | |
| Infor mation Servi ces | User Directory Services | Virtual Directory Services | | IA | X | A | B | X | A | X | B | X | A | X | B | X | A | |

| Information Services | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Information Services | User Directory Services | Meta Directory Services | | IA | X | A | B | X | A | X | B | X | A | X | B | X | A | |
| Information Services | ITOS | Incident Management | | IR | X | X | B | X | X | X | B | X | X | X | B | X | X | |
| Information Services | Service Support | Service Events | | IR | X | X | B | X | X | X | B | X | A | X | B | X | X | |
| Information Services | BOSS | Data Classification | | RA | X | X | A | X | X | X | A | X | X | X | A | X | A | |
| Information Services | Data Governance | Risk Assessments | | RA | X | A | B | X | X | A | B | X | X | A | B | X | X | |
| Information Services | Risk Management | Risk Assessments | | RA | X | A | B | X | X | A | B | X | X | A | B | X | X | |
| Information Services | Risk Management | Business Impact Assessment. | | RA | X | X | B | X | X | X | B | X | X | X | B | X | A | |
| Information Services | Risk Management | VRA | | RA | X | A | B | X | X | A | B | X | X | X | B | X | A | A |
| Information Services | Risk Management | TVM | | RA | X | A | B | X | X | A | B | X | X | X | B | X | X | |
| Information Services | Service Delivery | OLA´s | | SA | A | A | A | A | A | A | A | A | A | A | A | A | A | |
| Information Services | Data Governance | Non-Production Data | | SA | X | A | B | X | X | X | B | X | X | X | B | X | A | |

| Services ces | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Information Services | Security Monitoring | NIPS Events | | SC | X | X | B | X | A | X | B | X | A | X | B | X | X |
| Information Services | Security Monitoring | DLP Events | | SC | X | X | B | X | A | X | B | X | A | X | B | X | A |
| Information Services | Data Governance | Information Leakage Metadata | | SI | X | A | B | X | X | A | B | X | A | X | B | X | A |
| Information Services | Data Governance | Data Segregation | | SI | X | X | B | X | A | X | B | X | | X | B | X | A |
| Information Services | Security Monitoring | Transformation Services | | SI | X | X | B | X | X | X | B | X | A | X | B | X | A |
| Information Services | Security Monitoring | Session Events | | SI | X | X | B | X | X | X | B | X | A | X | B | X | A |
| Information Services | Security Monitoring | Application Events | | SI | X | A | B | X | X | A | B | X | A | X | B | X | A |
| Information Services | Security Monitoring | Network Events | | SI | X | A | B | X | X | X | B | X | A | X | B | X | X |
| Information Services | Security Monitoring | Computer Events | | SI | X | A | B | X | X | X | B | X | A | X | B | X | A |
| Information Services | Security Monitoring | Host Intrusion Protection Systems (HIPS) | | SI | X | A | B | X | X | A | B | X | A | X | B | X | A |

| Information Services | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Information Services | Security Monitoring | Database Events | | SI | X | A | B | X | | X | A | B | X | | A | X | B | X | | A | |
| Information Services | Service Delivery | Contracts | | PM | A | A | A | A | | A | A | A | A | | A | A | A | A | | A | |
| Information Services | ITOS | PMO | | PM | A | | A | A | | A | | A | A | | A | | A | A | | A | |
| Information Services | ITOS | Strategy | | PM | A | A | A | A | | A | A | A | A | | A | A | A | A | | A | |
| Information Services | ITOS | Roadmap | | PM | A | A | A | A | | A | A | A | A | | A | A | A | A | | A | |
| Information Services | ITOS | Knowledge Management | | PM | A | A | B | Ab | | A | A | B | Ab | | A | A | B | Ab | | A | |
| Information Services | ITOS | Service Management | | PM | X | A | B | X | | X | X | B | X | | A | X | B | X | | A | |
| Information Services | BOSS | Risk Assessments | | PM | X | A | A | X | | X | A | A | X | | X | A | A | X | | X | |
| Information Services | BOSS | Process Ownership | | PM | X | A | A | X | | X | A | A | X | | X | A | A | X | | A | |
| Information Services | BOSS | Business Strategy | | PM | A | A | A | A | | A | A | A | A | | A | A | A | A | | A | |
| Information Services | Service Support | Knowledge Repository | | PM | A | A | B | Ab | | A | A | B | Ab | | A | A | B | Ab | | A | |

| Service | Function | Detail | Sub-detail | Code | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Services | | | | | | | | | | | | | | | | | | |
| Information Services | Risk Management | GRC | | PM | X | A | A | X | X | X | A | X | X | X | A | X | A | A |
| Information Services | Risk Management | DR & BC Plans | | PM | X | X | B | X | X | X | B | X | X | X | B | X | X | |
| Infrastructure Services | **Virtual Infrastructure:** Storage Virtualization | Block-Based Virtualization | Network-Based | AC | X | X | B | X | A | X | B | X | A | X | B | X | A | |
| Infrastructure Services | **Internal Infrastructure:** Network Services | Authoritative Time Source | | AU | | X | B | X | | X | B | X | | X | B | X | X | |
| Infrastructure Services | **Internal Infrastructure:** Patch Management | Service Discovery | | MA | | A | B | Ab | | A | B | Ab | | A | B | Ab | X | |
| Infrastructure Services | **Internal Infrastructure:** Equipment Maintenance | | | MA | | A | B | Ab | | A | B | Ab | | A | B | Ab | X | |
| Infrastructure Services | **Internal Infrastructure:** Storage Services | | | MP | | A | B | Ab | | A | B | Ab | | A | B | Ab | A | A |
| Infrastructure Services | **Virtual Infrastructure:** Storage Virtualization | Block-Based Virtualization | Storage Device-Based | MP | X | X | B | X | A | X | B | X | A | X | B | X | A | |
| Infrastructure Services | **Internal Infrastructure:** Facility Security | Controlled Physical Access | Barrieers | PE | | A | B | Ab | | A | B | Ab | | A | B | Ab | A | |
| Infrastructure Services | **Internal Infrastruc...** | Controlled Physical | Security Patrols | PE | | A | B | A | | A | B | A | | A | B | A | A | |

| Service | Category | Subcategory | Item | Type | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ...re Services | ...ture: Facility Security | Access | | | | | b | | | b | | | b | | |
| Infrastructure Services | Internal Infrastructure: Facility Security | Controlled Physical Access | Electronic Surveillance | PE | A | B | Ab | A | B | Ab | A | B | Ab | A | A |
| Infrastructure Services | Internal Infrastructure: Facility Security | Controlled Physical Access | Physical Authentication | PE | A | B | Ab | A | B | Ab | A | B | Ab | A | A |
| Infrastructure Services | Internal Infrastructure: Facility Security | Asset Handling | Data | PE | A | B | Ab | A | B | Ab | A | B | Ab | A | A |
| Infrastructure Services | Internal Infrastructure: Facility Security | Asset Handling | Storage | PE | A | B | Ab | A | B | Ab | A | B | Ab | A | |
| Infrastructure Services | Internal Infrastructure: Facility Security | Asset Handling | Hardware | PE | A | B | Ab | A | B | Ab | A | B | Ab | A | A |
| Infrastructure Services | Internal Infrastructure: Facility Security | Environmental Risk Management | Physical Security | PE | A | B | Ab | A | B | Ab | A | B | Ab | A | |
| Infrastructure Services | Internal Infrastructure: Facility Security | Environmental Risk Management | Equipment Location | PE | A | B | Ab | A | B | Ab | A | B | Ab | A | A |
| Infrastructure Services | Internal Infrastructure: Facility Security | Environmental Risk Management | Power Redundancy | PE | A | B | Ab | A | B | Ab | A | B | Ab | A | A |
| Infrastructure Services | Internal Infrastructure: Servers | | | CM | A | B | Ab | A | B | Ab | A | B | Ab | A | |
| Infrastructure Services | Internal Infrastructure: Availability Services | | | CP | A | B | Ab | A | B | Ab | A | B | Ab | X | |

| Category | Service | Type | Sub-type | SC | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Infrastructure Services | **Internal Infrastructure:** Network Services | Network Segmentation | | SC | A | X | B | X | A | X | B | X | A | X | B | X | X |
| Infrastructure Services | **Virtual Infrastructure**: Desktop "Client" Virtualization | Local | | SC | X | A | B | X | A | X | B | X | A | X | B | X | A |
| Infrastructure Services | **Virtual Infrastructure**: Desktop "Client" Virtualization | Remote | Session-Based | SC | X | X | B | X | A | X | B | X | A | X | B | X | A |
| Infrastructure Services | **Virtual Infrastructure**: Desktop "Client" Virtualization | Remote | VM-Based (VDI) | SC | X | X | B | X | A | X | B | X | A | X | B | X | A |
| Infrastructure Services | **Virtual Infrastructure**: Storage Virtualization | Block-Based Virtualization | Host-Based | SC | X | X | B | X | A | X | B | X | A | X | B | X | A |
| Infrastructure Services | **Virtual Infrastructure**: Storage Virtualization | File-Based virtualization | | SC | X | X | B | X | A | X | B | X | A | X | B | X | A |
| Infrastructure Services | **Virtual Infrastructure**: Application Virtualization | Client Application Streaming | | SC | X | X | B | X | A | X | B | X | A | X | B | X | A |
| Infrastructure Services | **Virtual Infrastructure**: Application Virtualization | Server Application Streaming | | SC | X | X | B | X | X | X | B | X | | X | B | X | A |
| Infrastructure Services | **Virtual Infrastructure**: Virtual Workspaces | | | SC | X | X | B | X | A | X | B | X | A | X | B | X | A |
| Infrastructu | **Virtual Infrastruc** | Virtual Machines | Full | SC | X | X | B | X | A | X | B | X | A | X | B | X | A |

| Service | Category | Sub 1 | Sub 2 | Code | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| re Services | ture: Server Virtualization | (host based) | Paravirtualization | SC | X | X | B | x | A | X | B | x | A | X | B | x | A | |
| | | | Hardware-Assisted | SC | X | X | B | x | A | X | B | x | A | X | B | x | A | |
| | | OS Virtualization | | SC | X | X | B | x | A | X | B | x | A | X | B | x | A | |
| | | TPM Virtualization | | SC | X | X | B | x | X | X | B | x | A | X | B | x | A | |
| | | Virtual Memory | | SC | X | X | B | x | A | X | B | x | A | X | B | x | A | |
| Infrastructure Services | Virtual Infrastructure: Network | Network Address Space | IPv4 | SC | X | X | B | x | X | X | B | x | X | X | B | x | X | |
| | | | IPv6 | SC | X | X | B | x | X | X | B | x | X | X | B | x | X | |
| | | VLAN | | SC | X | X | B | x | A | X | B | x | A | X | B | x | X | |
| | | VNIC | | SC | X | X | B | x | A | X | B | x | A | X | B | x | | |
| Infrastructure Services | Virtual Infrastructure: Database Virtualization | | | SC | X | X | B | x | X | X | B | x | A | X | B | x | | |
| Infrastructure Services | Virtual Infrastructure: Mobile Device Virtualization | | | SC | X | X | B | x | A | X | B | x | A | X | B | x | | |
| Infrastructure Services | Virtual Infrastructure: Smartcard Virtualization | | | SC | X | X | B | x | A | X | B | | A | X | B | | | |
| Infrastructure Services | Internal Infrastructure: Patch Management | Compliance Monitoring | | PM | | A | B | Ab | | A | B | Ab | | A | B | Ab | X | |
| S & RM | Privilege Management Infrastructure | Privilege Usage Management | Privilege Usage Gateway | AC | A | X | B | x | A | X | B | | A | X | B | | X | |
| S & RM | Infrastructure Protection | Server | White Listing | AC | X | A | B | x | A | X | B | | A | X | B | | A | A |

Page 149

| S & RM | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Services | | | | | | | | | | | | | | | | | |
| S & RM | Infrastructure Protection Services | Server | Host Firewall | AC | X | X | B | X | A | X | B | | A | X | B | | A | |
| S & RM | Infrastructure Protection Services | End-Point | Host Firewall | AC | X | A | B | X | X | X | B | | A | X | B | | X | A |
| S & RM | Infrastructure Protection Services | End-Point | Content Filtering | AC | X | A | B | X | X | A | B | | A | X | B | | X | A |
| S & RM | Infrastructure Protection Services | End-Point | White Listing | AC | X | A | B | X | A | X | B | | A | X | B | | X | A |
| S & RM | Infrastructure Protection Services | Network | Content Filtering | AC | X | A | B | X | X | X | B | | A | X | B | | X | A |
| S & RM | Infrastructure Protection Services | Network | Firewall | AC | X | X | B | X | X | X | B | | A | X | B | | X | A |
| S & RM | Infrastructure Protection Services | Network | Black Listing Filtering | AC | X | X | B | X | A | X | B | | A | X | B | | X | A |
| S & RM | Infrastructure Protection Services | Application | Application Firewall | AC | X | X | B | X | X | X | B | | A | X | B | | A | A |
| S & RM | Infrastructure Protection Services | Application | Secure Collaboration | AC | X | A | B | X | X | X | B | | A | X | B | | A | A |
| S & RM | Infrastructure Protection Services | Application | Real Time Filtering | AC | X | A | B | X | X | A | B | | A | X | B | | A | A |
| S & RM | Data Protection | Data Lifecycle Management | Meta data Control | AC | X | A | B | X | X | X | B | | A | X | B | | A | A |
| S & RM | Data Protection | Data Lifecycle Management | Data Seeding | AC | X | A | B | X | X | A | B | | X | X | B | | A | A |
| S & RM | Data Protection | Intellectual Property Prevention | Digital Rights Manageme | AC | A | X | B | X | A | X | B | | A | X | B | | A | A |

| S & RM | Domain | Function | Sub | Family | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | nt | | | | | | | | | | | | | | | |
| S & RM | Policies and Standards | Role Based Awareness | | AC | X | A | A | X | X | A | A | | X | A | A | | A | A |
| S & RM | Governance Risk & Compliance | Technical Awareness and Training | | AT | X | X | B | X | X | X | B | | X | X | B | | A | |
| S & RM | Governance Risk & Compliance | Compliance Management | | AU | X | X | B | X | X | X | B | | X | X | B | | X | |
| S & RM | Governance Risk & Compliance | Audit Management | | AU | X | X | B | X | X | X | B | | X | X | B | | X | |
| S & RM | Threat and Vulnerability Management | Compliance Testing | Databases | AU | X | X | B | X | X | X | B | | A | X | B | | A | |
| | | | Servers | AU | X | X | B | X | A | X | B | | A | X | B | | A | A |
| S & RM | Policies and Standards | Best Practices & Regulatory correlation | | CA | A | X | A | X | A | X | A | | A | X | A | | X | A |
| S & RM | InfoSec Management | Capability Mapping | | CM | X | X | B | X | X | X | B | | X | X | B | | X | A |
| S & RM | Infrastructure Protection Services | End-Point | Inventory Control | CM | X | A | B | X | A | X | B | | A | X | B | | A | A |
| S & RM | Data Protection | Intellectual Property Prevention | Intellectual Property | CM | X | A | B | X | X | X | B | | A | X | B | | A | A |
| S & RM | Policies and Standards | Operational Security Baselines | | CM | A | A | A | A | A | A | A | A | A | A | A | A | A | A |
| | Policies and Standards | Job Aid Guidelines | | CM | A | A | A | A | A | A | A | A | A | A | A | A | A | A |
| S & RM | Privilege Management Infrastructure | Identity Management | Domain Unique Identifier | IA | A | A | B | Ab | A | A | B | Ab | A | A | B | Ab | A | |
| S & RM | Privilege Management Infrastruct | Identity Management | Federated IDM | IA | X | A | B | X | X | A | B | | A | X | B | | A | |

| Domain | Category | Sub-category | Item | IA | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ure | | | | | | | | | | | | | | | |
| S & RM | Privilege Management Infrastructure | Identity Management | Identity Provisioning | IA | X | A | B | X | X | A | B | | X | X | B | A |
| S & RM | Privilege Management Infrastructure | Identity Management | Attribute Provisioning | IA | X | A | B | X | X | A | B | | X | X | B | A |
| S & RM | Privilege Management Infrastructure | Authorization Services | Policy Enforcement | IA | X | A | B | X | X | A | B | | X | X | B | A |
| S & RM | Privilege Management Infrastructure | Authorization Services | Policy definition | IA | X | A | B | X | X | A | B | | X | X | B | A |
| S & RM | Privilege Management Infrastructure | Authorization Services | Principal Data Mngmnt | IA | X | A | B | X | X | A | B | | X | X | B | A |
| S & RM | Privilege Management Infrastructure | Authorization Services | XACML | IA | A | X | B | X | A | X | B | | A | X | B | A |
| S & RM | Privilege Management Infrastructure | Authorization Services | Role Management | IA | X | X | B | X | X | X | B | | X | X | B | A |
| S & RM | Privilege Management Infrastructure | Authorization Services | Oligation | IA | A | X | B | X | A | X | B | | A | X | B | A |
| S & RM | Privilege Management Infrastructure | Authorization Services | Out of the Box (OTB) autZ | IA | X | X | B | X | A | X | B | | A | X | B | A |
| S & RM | Privilege Management Infrastructure | Authentication Services | SAML Token | IA | A | X | B | X | A | X | B | | A | X | B | A |
| S & | Privilege | Authentica | Risk Based | IA | X | X | B | | X | X | B | | X | X | B | A |

| Domain | Infrastructure | Service | Item | IA | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| RM | Management Infrastructure | tion Services | Auth | | | | | X | | | | | | | | | | |
| S & RM | Privilege Management Infrastructure | Authentication Services | Multifactor | IA | X | X | B | X | X | X | B | | A | X | B | | A | |
| S & RM | Privilege Management Infrastructure | Authentication Services | OTP | IA | A | X | B | X | A | X | B | | A | X | B | | A | |
| S & RM | Privilege Management Infrastructure | Authentication Services | Smart Card | IA | X | A | B | X | X | A | B | | A | X | B | | A | |
| S & RM | Privilege Management Infrastructure | Authentication Services | Password Management | IA | X | X | B | X | X | X | B | | X | X | B | | A | |
| S & RM | Privilege Management Infrastructure | Authentication Services | Biometrics | IA | X | A | B | X | X | A | B | | X | X | B | | A | |
| S & RM | Privilege Management Infrastructure | Authentication Services | Network Authentication | IA | X | X | B | X | A | X | B | | A | X | B | | X | |
| S & RM | Privilege Management Infrastructure | Authentication Services | Single Sign On | IA | A | X | B | X | A | X | B | | A | X | B | | A | |
| S & RM | Privilege Management Infrastructure | Authentication Services | WS-Security | IA | X | X | B | X | X | X | B | | A | X | B | | A | |
| S & RM | Privilege Management Infrastructure | Authentication Services | Middleware Auth | IA | X | X | B | X | X | X | B | | A | X | B | | A | |
| S & RM | Privilege Management Infrastruct | Authentication Services | Identity Verification | IA | X | X | B | X | X | X | B | | X | X | B | | A | |

| Domain | Category | SubCategory | Item | Code | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ...ure | | | | | | | | | | | | | | | | |
| S & RM | Privilege Management Infrastructure | Authentication Services | Out-of-The-Box (OTB) Auth | IA | X | X | B | X | X | X | B | | A | X | B | | A | |
| S & RM | Privilege Management Infrastructure | Privilege Usage Management | Keystroke/ Session Logging | IA | X | X | B | X | X | X | B | | X | X | B | | A | |
| S & RM | Privilege Management Infrastructure | Privilege Usage Management | Password Vaulting | IA | X | X | B | X | X | X | B | | A | X | B | | X | |
| S & RM | Threat and Vulnerability Management | Compliance Testing | Network Autehntication | IA | X | X | B | X | X | X | B | | A | X | B | | X | A |
| S & RM | Infrastructure Protection Services | End-Point | Forensic Tools | IR | X | A | B | X | X | A | B | | X | X | B | | A | A |
| S & RM | Infrastructure Protection Services | End-Point | Media Lockdown | MP | A | X | B | X | A | X | B | | A | X | B | | X | A |
| S & RM | InfoSec Management | Residual Risk Management | | PL | X | A | B | X | X | X | B | | A | X | B | | A | |
| S & RM | Governance Risk & Compliance | Policy Management | Exceptions | RA | X | X | B | X | X | X | B | | X | X | B | | X | A |
| S & RM | Governance Risk & Compliance | Policy Management | Self Assessment | RA | X | A | B | X | X | A | B | | X | A | B | | X | A |
| S & RM | InfoSec Management | Risk Dashboard | | RA | X | X | B | X | X | X | B | | X | X | B | | A | |
| S & RM | Threat and Vulnerability Management | Vulnerability Management | application | RA | X | X | B | X | X | X | B | | A | X | B | | A | A |
| | | | Infrastructure | RA | X | X | B | X | A | X | B | | A | X | B | | A | A |
| | | | DB | RA | X | X | B | | X | X | B | | A | X | B | | A | A |

Page 154

| Domain | Category | Subcategory | Item | Code | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | X | | | | | | | | | | |
| | | Penetration Testing | Inernal | RA | X | A | B | X | X | X | B | | A | X | B | | A | A |
| | | | External | RA | X | X | B | X | X | X | B | | A | X | B | | A | A |
| | | Threat Management | Source Code Scanning | RA | X | X | B | X | X | X | B | | X | X | B | | A | A |
| | | | Risk Taxonomy | RA | X | A | B | X | X | X | B | | X | X | B | | A | |
| S & RM | Policies and Standards | Data/ Asset Classification | | RA | X | X | A | X | X | X | A | | X | X | A | | A | A |
| S & RM | Governance Risk & Compliance | Vendor Management | | SA | X | X | B | X | X | X | B | | X | X | B | | A | A |
| S & RM | Data Protection | Data Lifecycle Management | Life cycle management | SA | X | X | B | X | X | X | B | | X | X | B | | A | A |
| S & RM | Policies and Standards | Technical Security Standards | | SA | X | X | A | X | X | X | A | | X | X | A | | X | A |
| S & RM | Privilege Management Infrastructure | Privilege Usage Management | Resource Protection | SC | A | X | B | X | A | X | B | | A | X | B | | X | |
| S & RM | Infrastructure Protection Services | Network | Deep Packet Inspection (DPI) | SC | X | X | B | X | A | X | B | | A | X | B | | X | A |
| S & RM | Infrastructure Protection Services | Network | Wireless Protection | SC | A | X | B | X | A | X | B | | A | X | B | | X | A |
| S & RM | Infrastructure Protection Services | Network | Link Layer Network secuiry | SC | A | X | B | X | A | X | B | | A | X | B | | X | A |
| S & RM | Infrastructure Protection Services | Application | XML Appliance | SC | X | A | B | X | X | X | B | | A | X | B | | A | A |
| S & RM | Infrastructure Protection Services | Application | Secure Messaging | SC | X | A | B | X | X | A | B | | A | X | B | | A | A |
| S & RM | Data Protection | Data Lifecycle | Data De-Identificatio | SC | X | A | B | X | X | X | B | | X | X | B | | A | A |

| Domain | Category | Subcategory | Item | Class | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Management | n | | | | | | | | | | | | | |
| S & RM | Data Protection | Data Lifecycle Management | Data Masking | SC | X | A | B | X | X | X | B | X | X | B | A | A |
| S & RM | Data Protection | Data Lifecycle Management | Data Tagging | SC | X | A | B | X | X | X | B | A | X | B | A | A |
| S & RM | Data Protection | Data Lifecycle Management | Data Obscuring | SC | X | A | B | X | X | X | B | X | X | B | A | A |
| S & RM | Data Protection | Data Leakage Prevention | Data Discovery | SC | X | A | B | X | X | X | B | X | X | B | A | A |
| S & RM | Data Protection | Data Leakage Prevention | Network (Data in Transit) | SC | X | X | B | X | X | X | B | A | X | B | A | A |
| S & RM | Data Protection | Data Leakage Prevention | End-Point (data in Use) | SC | X | X | B | X | X | X | B | X | X | B | A | A |
| S & RM | Data Protection | Data Leakage Prevention | Server (data at Rest) | SC | X | X | B | X | X | X | B | A | X | B | A | A |
| S & RM | Cryptographic Services | Key Management | Symmetric Keys | SC | X | X | B | X | X | X | B | X | X | B | X | A |
| S & RM | Cryptographic Services | Key Management | Asymmetric Keys | SC | X | X | B | X | X | X | B | X | X | B | X | A |
| S & RM | Cryptographic Services | PKI | | SC | X | X | B | X | X | X | B | X | X | B | X | A |
| S & RM | Cryptographic Services | Data in use (memory) Encryption | | SC | X | X | B | X | X | X | B | A | X | B | X | A |
| S & RM | Cryptographic Services | Data in Transit Encryption (Transitory, Fixed) | | SC | X | X | B | X | X | X | B | X | X | B | X | A |
| S & RM | Cryptographic Services | Data as Rest Encryption (DB, File, SAN, Desktop, Mobile) | | SC | X | X | B | X | X | X | B | X | X | B | A | A |
| S & RM | Infrastructure | Server | Anti-virus | SI | X | X | B | X | X | X | B | A | X | B | A | |

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Protection Services | | | | | | | | | | | | | | | | | | |
| S & RM | Infrastructure Protection Services | Server | HIPS/HIDS (Intrusion Protection /Detection) | SI | X | X | B | X | A | X | B | | A | X | B | | A | |
| S & RM | Infrastructure Protection Services | End-Point | Anti-Virus, Anti-Spam, Anti-Malware | SI | X | A | B | X | X | A | B | | A | X | B | | A | |
| S & RM | Infrastructure Protection Services | End-Point | HIPS/HIDS (Intrusion Protection /Detection) | SI | X | A | B | X | X | X | B | | A | X | B | | A | A |
| S & RM | Infrastructure Protection Services | End-Point | Hardware Based trusted Assets | SI | A | X | B | X | A | X | B | | A | X | B | | X | A |
| S & RM | Infrastructure Protection Services | Network | NIPS/NIDS | SI | X | X | B | X | A | X | B | | A | X | B | | X | A |
| S & RM | Data Protection | Data Lifecycle Management | eSignature | SI | X | A | B | X | X | X | B | | X | X | B | | A | A |
| S & RM | Cryptographic Services | Signature Services | | SI | X | X | B | X | X | X | B | | X | X | B | | X | A |
| S & RM | Governance Risk & Compliance | IT Risk Management | | PM | X | X | B | X | X | X | B | | X | X | B | | X | A |
| S & RM | InfoSec Management | Risk Portfolio Management | | PM | A | A | B | Ab | A | A | B | Ab | A | A | B | Ab | A | |
| S & RM | Privilege Management Infrastructure | Authorization Services | Policy Management | PM | X | A | B | X | X | A | B | | X | X | B | | A | |
| S & RM | Privilege Management Infrastructure | Authorization Services | Resource Data management | PM | X | A | B | X | X | A | B | | X | X | B | | A | |
| S & RM | Policies and Standards | Information Security Polices | | PM | A | A | A | A | A | A | A | A | A | A | A | A | A | A |

## 12 ANNEX E: MAPPING OF THE ARCHITECTURAL COMPONENTS

| CONSUMER | PROVIDER | BROKER | CARRIER | AUDITOR |
|---|---|---|---|---|
| • Secure Cloud Consumption / Service Management [=B+C+I+O] | • Secure Cloud Provisioning / Service Management [=B+C+I] | • Secure Cloud Service Management [=B+C+I] | • Secure Transport Support [T] | • Secure Auditing Environment [E] |
| o   Secure Business / Payments Support [B] | o   Secure Business Support [B] | o   Secure Business Support [B] | | |
| o   Secure Consumption / Configuration [C] | o   Secure Provisioning / Configuration [C] | o   Secure Provisioning / Configuration [C] | | |
| o   Secure Portability/ Interoperability [I] | o   Secure Portability / Interoperability [I] | o   Secure Portability / Interoperability [I] | | |
| o   Secure Organizational Support [O] | • Secure Cloud Ecosystem Orchestration [=L] | • Secure Cloud Ecosystem Orchestration [=L] | | |
| • Secure Cloud Ecosystem Orchestration [=L] | o   Secure Service Layers [L] | o   Secure Service Layers [L] | | |
| o   Secure Functional Layers [L] | o   Secure Resource Abstraction & Control Layer [R] | • Secure Cloud Aggregation [=C2+I2] | | |
| | o   Secure Physical Resource Layers [P] | o   Secure Provisioning / Configuration [aC] | | |
| | | o   Secure Portability/Interoperability [aI] | | |
| | | • Secure Cloud Arbitrage [cA] | | |
| | | • Secure Cloud Intermediation [cI] | | |

**Table 6:** Cloud Actors' Architectural Components

Page 158

| | | | CONSUMER | | | | | PROVIDER | | | | | | BROKER | | | | | | | | CARRIER | AUDITOR |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | B | C | I | O | L | B | C | I | L | R | P | B | C | I | L | aC | aI | cA | cI | | |
| BOSS | Compliance | Intellectual Property Protection | B | | | | | B | | | L | | | B | | | | | | | | | | E |
| BOSS | Data Governance | Handling/ Labeling/ Security Policy | | C | I | | L | B | | | L | | | B | | | | | | | cI | | E |
| BOSS | Data Governance | Clear Desk Policy | B | | | | | | | | | | | B | | | | | | | | | | E |
| BOSS | Data Governance | Rules for Information Leakage Prevention | B | | | | | B | C | | L | | | | | I | L | aC | aI | cA | cI | T | |
| ITOS | IT Operations | Resource Management | B | | | | | B | C | I | L | | | B | C | | L | aC | | cA | cI | | E |
| Presentation Services | Presentation Modality | Consumer Service Platform | | | | O | | | | I | L | | | | | | | | | | | | |
| Presentation Services | Presentation Modality | Enterprise Service Platform | | | | | L | | | I | L | | | | | | | | | | | | |
| Presentation Services | | | | | | | | | | | | | | | | | | | | | | | |
| Presentation Services | | | | | | | | | | | | | | | | | | | | | | | |
| Presentation Services | | | | | | | | | | | | | | | | | | | | | | | |
| Presentation Services | Presentation Platform | End-Points | | C | | | L | | | I | | | | | | | | | | | | | |
| Presentation Services | | | | | | | | | | | | | | | | | | | | | | | |

| | | | CONSUMER | | | | | PROVIDER | | | | | | BROKER | | | | | | | | CARRIER | AUDITOR |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | B | C | I | O | L | B | C | I | L | R | P | B | C | I | L | aC | aI | cA | cI | | |
| Presentation Services | | | | | | | | | | | | | | | | | | | | | | | |
| Presentation Services | | | | | | | | | | | | | | | | | | | | | | | |
| Presentation Services | | | | | | | | | | | | | | | | | | | | | | | |
| Presentation Services | | | | | | | | | | | | | | | | | | | | | | | |
| Infrastructure Services | Virtual Infrastructure: Storage Virtualization | Block-Based Virtualization | | C | | | L | | | | L | R | P | | | | | | | | | | E |
| S & RM | Privilege Management Infrastructure | Privilege Usage Management | | | | | L | | C | | L | | | | | I | L | aC | aI | cA | cI | T | |
| S & RM | Infrastructure Protection Services | Server | | C | | | L | | C | | L | | P | | | | | | | cA | cI | | E |
| S & RM | Infrastructure Protection Services | End-Point | | C | | | | | C | | L | | P | | | | | | | | | T | E |
| S & RM | Infrastructure Protection Services | Network | | C | | | L | | C | | L | | P | | | | | | | | | T | E |
| S & RM | Infrastructure Protection Services | Application | | C | | | L | | C | | L | | P | | | | | | | cA | cI | | E |
| S & RM | | | | | | | | | | | | | | | | | | | | cA | cI | | E |
| S & RM | Data Protection | Data Lifecycle Management | | | I | | L | | C | I | L | | P | | C | I | L | aC | aI | cA | cI | | E |
| S & RM | | | | | | | | | | | | | | | | | | | | | | | |

| | | | CONSUMER | | | | | PROVIDER | | | | | | BROKER | | | | | | | | CARRIER | AUDITOR |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | B | C | I | O | L | B | C | I | L | R | P | B | C | I | L | aC | al | cA | cl | | |
| S & RM | Data Protection | Intellectual Property Prevention | B | | | | L | | C | I | L | | P | B | | | | | | | | | E |
| S & RM | Policies and Standards | Role Based Awareness | | C | | | | | C | | | | P | | C | | | aC | | | cl | | |
| BOSS | Human Resource Security | Employee Awareness | B | | I | | | B | | | | | P | B | | | | | | | | | E |
| BOSS | Security Monitoring Services | Market Threat Intelligence | | | | | L | B | | | L | | | | | | L | | | cA | cl | | |
| BOSS | Security Monitoring Services | Knowledge Base | | | I | | L | B | | | | | | | | | L | | | cA | cl | | E |
| S & RM | Governance Risk & Compliance | Technical Awareness and Training | B | | | | | | C | | L | | P | | | | L | | | cA | cl | | E |
| BOSS / BOSS | Compliance | Audit Planning & Internal Audits | B | | | | | B | C | I | | | P | | | | L | | | cA | cl | T | |
| BOSS | Security Monitoring Services | Event Mining | | C | I | | | | C | I | L | | | | | I | L | | al | cA | cl | | |
| BOSS | Security Monitoring Services | Event Correlation | | C | I | | | | C | I | L | | | | | I | L | | al | cA | cl | T | E |
| BOSS | Security Monitoring Services | Email Journaling | | | | | L | | C | | L | | | | | | | | | | | | E |

| | | | CONSUMER | | | | | PROVIDER | | | | | | BROKER | | | | | | | | CARRIER | AUDITOR |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | B | C | I | O | L | B | C | I | L | R | P | B | C | I | L | aC | al | cA | cl | | |
| BOSS | Security Monitoring Services | User Behaviors and Profile Patterns | | C | I | | | | C | | L | | | | | | L | | | cA | cl | | |
| BOSS | Legal Services | E-Discovery | | C | I | | | B | C | I | L | | P | B | | | | | | | | | E |
| BOSS | Legal Services | Incident Response Legal Preparation | | C | I | | | B | C | I | L | | | B | | | | | | | | | E |
| BOSS | Internal Investigations | Forensic Analysis | | C | | | L | B | C | I | L | | | | | I | L | | al | cA | cl | | |
| BOSS | Internal Investigations | e-Mail Journaling | | | | | L | B | | | | R | | | | | | | | | | | |
| ITOS | Service Delivery | Information Technology Resiliency | B | C | I | | | | C | I | L | | P | | | I | L | | al | cA | cl | T | |
| ITOS | | | | | | | | | | | L | | | | | | L | | | cA | cl | | E |
| ITOS | Service Support | Configuration Management | B | C | I | | | | C | I | | | P | | | | L | | | cA | cl | | |
| ITOS | Service Support | Problem Management | B | C | I | | | | C | I | L | | P | | | I | L | | al | cA | cl | T | |
| ITOS | | | | | | | | | | | | | | | | | | | | | | | |
| Information Services | BOSS | Audit Findings | | | | O | | B | | | | | | | | | L | | | cA | cl | | |
| Information Services | Security Monitoring | eDiscovery Events | B | | I | | L | B | C | I | L | | P | B | | | | | | | | | |
| Infrastructure Services | Internal Infrastructure: Network Services | Authoritative Time Source | | | | | L | | C | I | L | R | P | | | I | L | | al | cA | cl | T | |
| S & RM | Governance Risk & Compliance | Compliance Management | | | | O | | B | C | I | L | | P | | | | L | | | cA | cl | T | |

Page 162

| | | | CONSUMER | | | | | PROVIDER | | | | | | BROKER | | | | | | | | CARRIER | AUDITOR |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | B | C | I | O | L | B | C | I | L | R | P | B | C | I | L | aC | al | cA | cl | | |
| S & RM | Governance Risk & Compliance | Audit Management | | | | O | | B | | | L | | | | | | L | | | cA | cl | T | E |
| S & RM | Threat and Vulnerability Management | Compliance Testing | | | | O | | | C | I | L | | P | | | | L | | | cA | cl | | E |
| BOSS | Compliance | Independent Audits | B | | | | L | B | | I | | | P | | | | L | | | cA | cl | T | |
| BOSS | Compliance | Third Party Audits | B | | | | L | B | | I | | | P | | | | L | | | cA | cl | T | |
| Information Services | Reporting Services | Dashboard | | | I | O | L | B | C | | L | | P | | | | L | | | cA | cl | | |
| Information Services | Reporting Services | Data Mining | | | | O | | B | C | | L | | P | | | | L | | | cA | cl | | |
| Information Services | Reporting Services | Reporting Tools | | | | O | | B | | | | | | | | | L | | | cA | cl | T | |
| Information Services | Reporting Services | Business Intelligence | B | | | O | | B | | | | | | B | | | | | | | | | E |
| Information Services | ITOS | Problem Management | B | | | O | | | C | I | L | | | | | I | L | | al | cA | cl | T | |
| S & RM | Policies and Standards | Best Practices & Regulatory correlation | | | | O | | B | C | | L | | P | | | | L | | | cA | cl | T | |
| ITOS | IT Operations | Portfolio Management | | C | | | | B | | | | | | | | | | | | | | | |
| ITOS | Service Delivery | Asset Management | B | C | | | L | B | C | I | | | P | | | | L | | | cA | cl | | |
| ITOS ITOS ITOS | Service Support | Configuration Management | B | C | I | | | | C | I | L | | P | | C | | L | aC | | cA | cl | | E |
| ITOS | Service Support | Knowledge | B | C | | | L | | C | | | | P | | | | L | | | cA | cl | | E |

| Category | Subcategory | Item | CONSUMER | | | | | PROVIDER | | | | | | BROKER | | | | | | | | CARRIER | AUDITOR |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | B | C | I | O | L | B | C | I | L | R | P | B | C | I | L | aC | aI | cA | cI | | |
| ITOS | | Management | | | | | | | | | | | | | | | | | | | | | |
| ITOS | Service Support | Change Management | | C | | | | | C | I | L | | P | | C | | | aC | | | | | |
| ITOS | Service Support | Release Management | | C | | | | | C | I | L | | P | | C | | | aC | | | | | |
| ITOS | Support | Management | | | | | | | | | | | | | | | | | | | | | |
| Application Services | Security Knowledge Lifecycle | Attack Patterns | | | | | L | | C | | L | | | | | | | | | | | | | E |
| Application Services | Connectivity & Delivery | | | | | | L | | | I | L | | | | | | | | | | | | |
| Information Services | Service Delivery | Service Catalog | B | | | | L | B | | I | | | P | | | | | | | | | | | |
| Information Services | Service Delivery | SLA´s | B | | | | | B | C | I | L | | P | | | | | | | | | | T | |
| Information Services | ITOS | CMDB | | C | I | O | L | | C | I | L | | | | | | | | | | | | |
| Information Services | ITOS | Change Management | | | | O | | | C | I | L | | | | | | | | | | | | T | |
| Information Services | Service Support | Configuration Rules (Metadata) | | C | | O | | | C | I | | | P | | | | | | | | | | |
| Information Services | Service Support | Configuration Management Database (CMDB) | | | I | | L | | C | | | | P | | | | | | | | | | |
| Information Services | Service Support | Change Logs | | C | | O | | | C | I | | | P | | | | | | | | | | T | |

| | | | CONSUMER | | | | | PROVIDER | | | | | | BROKER | | | | | | | | CARRIER | AUDITOR |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | B | C | I | O | L | B | C | I | L | R | P | B | C | I | L | aC | al | cA | cl | | |
| Information Services | Security Monitoring | Compliance Monitoring | | C | | O | | | C | I | L | | P | | | | L | | | cA | cl | | |
| Information Services | Security Monitoring | Privilege Usage Events | | C | | O | | | C | | L | | P | | | | L | | | cA | cl | | |
| Infrastructure Services | **Internal Infrastructure:** Servers | | | | | | L | | | | | | P | | | | | | | | | | |
| S & RM | InfoSec Management | Capability Mapping | B | | | O | | B | | I | L | | P | B | C | | | | | | | T | E |
| S & RM | Infrastructure Protection Services | End-Point | | C | | O | | B | | | L | | P | B | C | | | | | | | T | E |
| S & RM | Data Protection | Intellectual Property Prevention (Protection?) | B | | | O | | B | C | | L | | P | | | | | | | | | | E |
| S & RM | Policies and Standards | Operational Security Baselines & Job Aid Guidance | | | | | | | | | | | P | | | | | | | | | | E |
| BOSS BOSS | Operational Risk Management | Business Impact Analysis & Business Continuity | B | | | | | | | I | L | | | | | | | | | | | T | E |
| ITOS | IT Operations | DRP | B | C | | | | | C | I | L | | P | B | | | | | | | | | |
| ITOS | Service Support | Configuration Management | B | C | | | | | C | I | L | | | | | | | | | | | | |
| Information Services | Service Delivery | Recovery Plans | | | | O | L | B | C | I | L | | P | | | | | | | | | | |

| | | | CONSUMER | | | | | PROVIDER | | | | | | BROKER | | | | | | | | CARRIER | AUDITOR |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | B | C | I | O | L | B | C | I | L | R | P | B | C | I | L | aC | aI | cA | cI | | |
| Infrastructure Services | Internal Infrastructure: Availability Services | | | C | I | | | | | | | | P | | | | | | | | | T | |
| Information Services | BOSS | Human Resources Data (Employee & contractors) | B | | | O | L | | C | I | L | | P | | | | | | | | | T | |
| Information Services | Security Monitoring | Authorization, Authentication, ACL & CRL Events | B | | | O | L | | C | I | L | | P | | | | | | | | | | |
| Information Services | User Directory Services | Directory Services (Active, LDAP, Virtual, Meta) Repositories (X.500, DBMS), Registry and Location Services | | | | O | L | | C | I | L | | | | | | | aC | | | | | |
| Information Services | | | | | | | | | | | | | | | | | | | | | | | |
| Information Services | | | | | | | | | | | | | | | | | | | | | | | |
| Information Services | | | | | | | | | | | | | | | | | | | | | | | |
| Information Services | | | | | | | | | | | | | | | | | | | | | | | |
| Information Services | | | | | | | | | | | | | | | | | | | | | | | |
| Information Services | | | | | | | | | | | | | | | | | | | | | | | |

| Information Services | | | | CONSUMER | | | | | PROVIDER | | | | | | BROKER | | | | | | | | CARRIER | AUDITOR |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | B | C | I | O | L | B | C | I | L | R | P | B | C | I | L | aC | aI | cA | cI | | |
| S & RM | Privilege Management Infrastructure | Identity Management | | | C | | | L | | C | I | L | | P | B | | | | aC | | | | | |
| S & RM | Privilege Management Infrastructure | Authorization Services | | | C | | | L | | C | I | L | | P | B | | | | | | | | | |
| S & RM | Privilege Management Infrastructure | Privilege Usage Management | | | | | | L | | C | I | L | | P | | | | L | | | | | | |

| | | | CONSUMER | | | | | PROVIDER | | | | | | BROKER | | | | | | | | CARRIER | AUDITOR |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | B | C | I | O | L | B | C | I | L | R | P | B | C | I | L | aC | al | cA | cl | | |
| S & RM | Threat and Vulnerability Management | Compliance Testing | | | | | L | | C | | L | | P | | | | | | | | | | | E |
| BOSS | Operational Risk Management | Crisis Management | B | | | | | B | C | I | L | | | | | | | | | | | | T | E |
| BOSS | Operational Risk Management | Risk Management Framework | B | | | | | | C | I | | | | | | | | | | | | | | E |
| BOSS | Operational Risk Management | Independent Risk Management | B | | | | | B | C | I | L | | | | | | | | | | | | T | E |
| BOSS | Security Monitoring Services | Database Monitoring | | | I | | L | | C | I | L | | P | | | | | | | | | | | |
| BOSS | Security Monitoring Services | Application Monitoring | | | I | | L | | C | I | L | | P | | | | | | | | | | | |
| BOSS | Security Monitoring Services | End-Point Monitoring | | | I | | L | | C | I | | | P | | | | | | | | | | | |
| BOSS | Security Monitoring Services | Cloud Monitoring | | | I | | L | B | C | | L | | P | B | | | L | | | | | | | |
| ITOS / ITOS / ITOS / ITOS | Service Support | Incident Management | B | | | | L | B | C | | L | | P | B | | | | | | | | | T | E |
| ITOS / ITOS | Service Support | Problem Management | B | | | | L | B | C | | L | | P | B | | | | | | | | | T | |

| | | | CONSUMER | | | | | PROVIDER | | | | | | BROKER | | | | | | | | CARRIER | AUDITOR |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | B | C | I | O | L | B | C | I | L | R | P | B | C | I | L | aC | al | cA | cl | | |
| ITOS | Service Support | Knowledge Management | | C | | | L | B | C | | L | | P | | | | | | | | | | E |
| Information Services | ITOS | Incident Management | | | I | | L | B | | | L | | | | | | | | | | | T | |
| Information Services | Service Support | Service Events | | | | | L | B | C | | L | | P | B | | | | | | | | T | |
| S & RM | Infrastructure Protection Services | End-Point | | C | | O | | | C | | L | | P | B | | | | | | | | T | E |
| ITOS / ITOS | Service Support | Change Management & Release Management | | C | I | | | | C | I | L | | P | | | | | | | | | | |
| Infrastructure Services | Internal Infrastructure: Patch Management | Service Discovery | | C | | | | | | | | R | P | | | | | | | | | T | |
| Infrastructure Services | Internal Infrastructure: Equipment Maintenance | | | C | | | | | | | | | P | | | | | | | | | T | |
| BOSS | Data Governance | Secure Disposal of Data | | C | I | | L | | C | | L | | | | | | | | | | | | E |
| Infrastructure Services | Internal Infrastructure: Storage Services | | | C | | | L | | | | | | P | | | | | | | | | | E |

Page 169

| | | | CONSUMER | | | | | PROVIDER | | | | | | BROKER | | | | | | | | CARRIER | AUDITOR |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | B | C | I | O | L | B | C | I | L | R | P | B | C | I | L | aC | aI | cA | cI | | |
| Infrastructure Services | **Virtual Infrastructure:** Storage Virtualization | Block-Based Virtualization | | | | | L | | | | L | R | P | | | | | | | | | | |
| S & RM | Infrastructure Protection Services | End-Point | B | C | | O | | | | | L | | P | | | | | | | | | T | E |
| Infrastructure Services | **Internal Infrastructure:** Facility Security | Controlled Physical Access | | | | | L | | | | | | P | | | | | | | | | | E |
| Infrastructure Services | **Internal Infrastructure:** Facility Security | Asset Handling | | C | | | | | C | | | | P | | | | | | | | | | E |
| Infrastructure Services | **Internal Infrastructure:** Facility Security | Environmental Risk Management | | C | | | L | | | | | | P | | | | | | | | | | E |
| S & RM | InfoSec Management | Residual Risk Management | | C | I | | | | C | | L | | P | | | | | | | | | | |

| | | | CONSUMER | | | | | PROVIDER | | | | | | BROKER | | | | | | | | CARRIER | AUDITOR |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | B | C | I | O | L | B | C | I | L | R | P | B | C | I | L | aC | aI | cA | cI | | |
| BOSS BOSS BOSS | Human Resource Security | Employment Agreement, Background Screening & Employee Termination | B | | | | L | | | | L | | P | B | | | | | | | | | | E |
| BOSS BOSS BOSS | Human Resource Security | Job Descriptions, Roles and Responsibilities & Employee Code of Conduct | B | | | | | | | | L | | P | B | | | | | | | | | | E |
| BOSS | Compliance | Information Systems Regulatory Mapping | B | | | | | | C | I | L | | P | | | | | | | | | | T | E |
| BOSS | Data Governance | Data Ownership - Personnel Responsibilities/ Stewardship | | C | I | | | B | | I | L | | | | | | | | | | | | | E |
| BOSS | Data Governance | Data Classification | B | C | I | | L | B | | I | L | | | | | | | | | | | | | E |
| Information Services | BOSS | Data Classification | B | C | I | | L | B | | I | L | | | | | | | | | | | | | |
| Information Services | Data Governance | Risk Assessments | | C | | | L | B | | I | | | | | | | | | | | | | T | |
| Information Services | Risk Management | Risk Assessments | | C | | | L | B | | | | | | | | | L | | | | | | T | |
| Information Services | Risk Management | Business Impact Assessment. | B | | | O | L | B | | | L | | | | | | L | | | | | | | |

| | | | CONSUMER | | | | | PROVIDER | | | | | | BROKER | | | | | | | | CARRIER | AUDITOR |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | B | C | I | O | L | B | C | I | L | R | P | B | C | I | L | aC | aI | cA | cI | | |
| Information Services | Risk Management | Vendor - Risk Assessment (VRA) | | | | O | | B | | | L | | | | | | L | | | | | | E |
| Information Services | Risk Management | Threats Vulnerability Management Testing (TVM) | | C | I | O | | B | C | I | L | R | | | | | L | | | | | T | |
| S & RM | Governance Risk & Compliance | Policy Management | | | | O | | B | | | L | | | | | | | | | | | T | E |
| S & RM | InfoSec Management | Risk Dashboard | | | | O | | B | | | L | | P | | | | | | | | | | |
| S & RM | Threat and Vulnerability Management | Vulnerability Management & Threat Management | | | | | L | | C | I | L | | P | | | | L | aC | aI | | | | E |
| | Threat and Vulnerability Management | Penetration Testing | | | | | L | | C | | L | | P | | | | L | aC | aI | | | | E |
| S & RM | Policies and Standards | Data/ Asset Classification | | | | O | | | | | L | | P | | | | | | | | | | E |
| BOSS | Security Monitoring Services | Managed (Outsourced) Security Services | B | | | | L | | C | | L | | | | | | | | | | | | |
| BOSS | Legal Services | Contracts | B | | | | | B | | I | L | | | B | | | | | | | | | E |
| ITOS | Service Delivery | Asset Management | B | | | | | B | C | | | | P | | | | | | | | | T | |
| ITOS | Service Support | Incident Management | B | C | I | | | B | C | | L | | P | | | | | | | | | | |

| Domain | Category | Service | CONSUMER B | C | I | O | L | PROVIDER B | C | I | L | R | P | BROKER B | C | I | L | aC | aI | cA | cI | CARRIER | AUDITOR |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Application Services / Application Services | Security Knowledge Lifecycle | Security Design Patterns & Security Application Framework - ACEG | | | | | L | | C | I | L | | | | | | | | | | | | | E |
| Application Services / Application Services / Application Services | Development Processes | Self Service | | | | | L | | C | | L | | | | | | | | | | | | T | E |
| Application Services | Development Processes | Software Quality Assurance | | | | O | L | | | | L | | | | | | | | | | | | | E |
| Application Services | Integration Middleware | | | C | I | | L | | | I | L | R | | | | | | | | | | | | |
| Information Services | Service Delivery | OLA´s | | | | O | L | B | C | | | | P | | | | | | | | | | |
| Information Services | Data Governance | Non-Production Data | | | I | | | | C | I | L | | P | B | | | | | | | | | | |
| S & RM | Governance Risk & Compliance | Vendor Management | B | | | | | B | C | I | L | | P | B | | | | | | | | | | E |
| S & RM | Data Protection | Data Lifecycle Management | | | | | L | B | C | I | L | | P | | | | | | | | | | | E |
| S & RM | Policies and Standards | Technical Security Standards | | | | O | | | | | L | | P | | | | | | | | | | T | E |
| BOSS | Security Monitoring Services | Honey Pot | | C | | | L | | | | | | | | | | | | | | | | |

| | | | CONSUMER | | | | | PROVIDER | | | | | | BROKER | | | | | | | | CARRIER | AUDITOR |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | B | C | I | O | L | B | C | I | L | R | P | B | C | I | L | aC | aI | cA | cI | | |
| BOSS | Security Monitoring Services | Real Time Internetwork Defense (SCAP) | | C | I | | L | | C | I | L | | | | | | | aC | aI | | | T | |
| ITOS | Service Delivery | Information Technology Resiliency | B | | I | | | | C | I | L | | P | | | | | aC | aI | | | T | |
| Presentation Services / Presentation Services | Presentation Modality | Consumer Service Platform | | | I | | L | B | | | L | | | | | | | aC | | | | | |
| Presentation Services | Presentation Modality | Enterprise Service Platform Lower Comp: B2E, B2M, B2B, B2C, P2P | | | | | L | | | I | L | | | | | | | | | | | | |
| Presentation Services | Presentation Platform | Speech Recognition (IVR) | | | I | | L | | | I | | | | | | | | | | | | | |
| Presentation Services | Presentation Platform | Handwriting (ICR) | | | I | | L | | | I | | | | | | | | | | | | | |
| Application Services | Abstraction | | | | | | L | | | I | L | R | | | | | | | | | | | |
| Information Services | Security Monitoring | NIPS Events | | | | | L | | | I | L | | | | | | | aC | aI | | | T | |
| Information Services | Security Monitoring | DLP Events | | | I | O | L | | C | | L | | | | | | | aC | aI | | | | |
| Infrastructure Services | Internal Infrastructure: Network Services | Network Segmentation | | | | | L | | | | L | R | P | | | | | | | | | T | |

| | | | CONSUMER | | | | | PROVIDER | | | | | | BROKER | | | | | | | | CARRIER | AUDITOR |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | B | C | I | O | L | B | C | I | L | R | P | B | C | I | L | aC | aI | cA | cI | | |
| Infrastructure Services | **Virtual Infrastructure**: Desktop "Client" Virtualization | Local | | C | I | | L | | C | I | L | R | | | | | | | | | | | |
| Infrastructure Services / Infrastructure Services | **Virtual Infrastructure**: Desktop "Client" Virtualization | Remote | | C | I | | L | | C | I | L | R | | B | | | | | | | | | |
| Infrastructure Services / Infrastructure Services | **Virtual Infrastructure**: Storage Virtualization | Block-Based & File-Base Virtualization | | C | I | | L | | C | I | L | R | P | B | | | | | | | | | |
| Infrastructure Services | **Virtual Infrastructure**: Application Virtualization | Client & Server Application Streaming | | C | I | | | | | I | L | R | P | | | | | | | | | | |
| Infrastructure Services | **Virtual Infrastructure**: Virtual Workspaces | | | C | I | | L | | C | I | L | | | | | | | | | | | | |
| Infrastructure Services | **Virtual Infrastructure**: Server Virtualization | Virtual Machines (host based) | | C | I | | L | | C | I | L | R | | | | | | | | | | | |
| | | OS & TPM Virtualization | | C | I | | L | | C | I | L | R | | | | | | | | | | | |
| | | Virtual Memory | | C | I | | L | | C | I | L | R | | | | | | | | | | | |
| Infrastructure Services | **Virtual Infrastructure**: Network | Network Address Space | | C | | | L | | C | I | L | R | | | | | | | | | | T | |
| | | VLAN | | C | I | | L | | C | I | L | R | | | | | | | | | | T | |
| | | VNIC | | C | I | | L | | C | I | L | R | | | | | | | | | | T | |

Page 175

| Domain | Category | Subcategory | C:B | C:C | C:I | C:O | C:L | P:B | P:C | P:I | P:L | P:R | P:P | Br:B | Br:C | Br:I | Br:L | Br:aC | Br:aI | Br:cA | Br:cI | CARRIER | AUDITOR |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Infrastructure Services | Virtual Infrastructure: Database Virtualization | | | C | I | | | | C | I | L | R | | | | | | | | | | | |
| Infrastructure Services | Virtual Infrastructure: Mobile Device Virtualization | | | C | I | | | | C | I | L | R | | | | | | | | | | | |
| Infrastructure Services | Virtual Infrastructure: Smartcard Virtualization | | | C | I | | | | C | I | L | R | | | | | | | | | | | |
| S & RM | Privilege Management Infrastructure | Privilege Usage Management | | C | | | | | C | I | L | | | | | | | | | | | T | |
| S & RM | Infrastructure Protection Services | Network | | | | | L | | | I | L | | | | C | | | | | | | T | E |
| S & RM | Infrastructure Protection Services | Application | | | | | L | | C | I | L | | | | | | | | | | | | E |
| S & RM | Data Protection | Data Lifecycle Management | | | | | L | B | C | I | L | | P | | | | | | | | | | E |
| S & RM | Data Protection | Data Leakage Prevention | | | | | L | | C | I | L | | P | | C | | | | | | | | E |

| | | | CONSUMER | | | | | PROVIDER | | | | | | BROKER | | | | | | | | CARRIER | AUDITOR |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | B | C | I | O | L | B | C | I | L | R | P | B | C | I | L | aC | aI | cA | cI | T | E |
| S & RM | Cryptographic Services | Key Management Lower comp: Synchronous keys, Asynchronous keys | | C | | | L | | C | I | L | | | B | | | | | | | | T | E |
| S & RM | Cryptographic Services | PKI | | C | | O | L | | C | I | L | | | B | | | | | | | | T | E |
| S & RM | Cryptographic Services | Data in use (memory) Encryption | | | | | L | | C | I | L | | | | | | | | | | | | T | E |
| S & RM | Cryptographic Services | Data in Transit Encryption (Transitory, Fixed) | | | | | L | | C | I | L | | | B | | | | | | | | T | E |
| S & RM | Cryptographic Services | Data as Rest Encryption (DB, File, SAN, Desktop, Mobile) | | | | | L | | C | I | L | | | | | | | aC | | | | | | E |
| BOSS | Data Governance | Rules for Data Retention | B | C | I | | L | B | C | I | L | | | | | | | | | | | | | E |
| BOSS | Security Monitoring Services | SIEM Platform | | C | I | | L | | C | I | L | | | | | | | | | | | | T | E |
| BOSS | Security Monitoring Services | Anti-Phishing | | | | | L | B | C | I | | | | | | | | | | | | | | |
| ITOS | Service Delivery | Application Performance Monitoring | B | | | | L | B | C | I | L | | | | | | | | | | | | | |
| ITOS | Service Support | Release Management | B | C | I | | | | C | | L | | P | | | | | | | | | | | |

| | | | CONSUMER | | | | | PROVIDER | | | | | | BROKER | | | | | | | | CARRIER | AUDITOR |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | B | C | I | O | L | B | C | I | L | R | P | B | C | I | L | aC | al | cA | cl | | |
| Application Services | Programming Interfaces | Input Validation | | | | | L | | C | I | L | | | | | | | | | | | | | |
| Application Services | Security Knowledge Lifecycle | Code Samples | | | | | L | | C | | L | | | | | | | | | | | | | |
| Information Services | Data Governance | Information Leakage Metadata | | C | I | | L | | C | | L | | | | | | | | | | | | | |
| Information Services | Data Governance | Data Segregation | | C | I | | L | | C | | L | | | | | | | | | | | | | |
| Information Services | Security Monitoring | Transformation Services | | | | O | | | C | | L | | | | | | | | | | | | | |
| Information Services | Security Monitoring | Session, Application, Computer Events | | | | | L | | C | | L | | | | | | | | | | | | | |
| Information Services | | | | | | | | | | | | | | | | | | | | | | | | |
| Information Services | | | | | | | | | | | | | | | | | | | | | | | | |
| Information Services | Security Monitoring | Network Events | | | | | L | | | | | | | | | | | | | | | | T | |
| Information Services | Security Monitoring | Host Intrusion Protection Systems (HIPS) | | | I | O | L | | C | I | L | | | | | | | | | | | | | |
| Information Services | Security Monitoring | Database Events | | | | O | L | | | | L | | | | | | | | | | | | | E |
| S & RM | Infrastructure Protection Services | Server | | | | | L | | C | I | L | | P | | | | | | | | | | | |
| S & RM | Infrastructure Protection | End-Point | | | | | L | | C | I | L | | P | | | | | | | | | | T | E |

| | | | CONSUMER | | | | | PROVIDER | | | | | | BROKER | | | | | | | | CARRIER | AUDITOR |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | B | C | I | O | L | B | C | I | L | R | P | B | C | I | L | aC | aI | cA | cI | | |
| S & RM | Services | | | | | | | | | | | | | | | | | | | | | | |
| S & RM | Infrastructure Protection Services | Network | | | | | L | | C | I | L | | P | | C | | | | | | | T | E |
| S & RM | Data Protection | Data Lifecycle Management | | | | | L | B | C | I | L | | P | | | | | | | | | | E |
| S & RM | Cryptographic Services | Signature Services | | | | | L | | C | I | L | | | | | | | | | | | T | E |
| BOSS | Compliance | Contract/ Authority Maintenance | B | | | | L | B | | | L | | P | B | | | | | | | | T | E |
| BOSS | Operational Risk Management | Operational Risk Committee | B | C | | | | B | | | L | | | | | | | | | | | | E |
| BOSS | Operational Risk Management | Key Risk Indicators | B | | | | | B | | | L | | | | | | | | | | | | |
| BOSS | Security Monitoring Services | Counter Threat Management | | | | | L | | | | L | | | | | | | | | | | | |
| BOSS | Security Monitoring Services | SOC Portal | | C | I | | L | | | | | | | B | C | | | | | | | T | |
| BOSS | Security Monitoring Services | Branding Protection | B | | | | L | B | | | | | | | | | | | | | | | E |
| ITOS | IT Operations | DRP | B | | I | | | | C | I | L | | P | B | C | | | | | | | | E |
| ITOS / ITOS | IT Operations | IT Governance | B | C | I | | L | | C | | L | | P | B | | | | | | | | | - |
| ITOS / ITOS | IT Operations | PMO | B | | | | | | C | I | | | P | B | | | | | | | | | E |

| Category | Sub | Process | CONSUMER | | | | | PROVIDER | | | | | | BROKER | | | | | | | | CARRIER | AUDITOR |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | B | C | I | O | L | B | C | I | L | R | P | B | C | I | L | aC | al | cA | cl | | |
| ITOS | | | | | | | | | | | | | | | | | | | | | | | |
| ITOS | IT Operations | Portfolio Management | B | C | I | | L | | C | | | | P | | | | | | | | | | |
| ITOS | Service Delivery | Service Level Management | B | | | | | B | C | I | L | | | | | | | | | | | T | E |
| ITOS | Service Delivery | Asset Management | B | C | I | | | B | C | | | | | | | | | | | | | | |
| ITOS | Service Support | Problem Management & Knowledge Management | B | C | | | | B | C | | L | | P | | | | | | | | | T | |
| Information Services | Service Delivery | Contracts | B | | | | | B | C | | | | | B | | | | | | | | | |
| Information Services | ITOS | Program Management (PMO), Strategy & Roadmap | | | | O | | | C | | | | | B | | | | | | | | | |
| Information Services | ITOS | Knowledge & Service Management | | | | O | | | C | | L | | | B | | | | | | | | | |
| Information Services | BOSS | Risk Assessments | | | | O | | B | | | | | | B | | | | | | | | T | |

| Category | Domain | Function | CONSUMER B | C | I | O | L | PROVIDER B | C | I | L | R | P | BROKER B | C | I | L | aC | aI | cA | cI | CARRIER | AUDITOR |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Information Services | BOSS | Process Ownership | B | | | O | | B | | | | | | | | | | | | | | | |
| Information Services | BOSS | Business Strategy | B | | | O | | B | | | | | | | | | | | | | | | |
| Information Services | Service Support | Knowledge Repository | | C | | O | L | | | | | | P | B | | | | | | | | | |
| Information Services | Risk Management | Governance, Risk management, Compliance (GRC) | B | | | O | L | B | | | L | | | | | | | | | | | | E |
| Information Services | Risk Management | Disaster Recovery (DR) & Business Continuity (BC) Plans | B | | | O | L | B | | | L | | | B | | | | | | | | T | |
| Infrastructure Services | Internal Infrastructure: Patch Management | Compliance Monitoring | B | C | | | L | | C | | | R | P | B | | | | | | | | T | |
| S & RM | Governance Risk & Compliance | IT Risk Management | | | | | | | | | L | | P | B | | | | | | | | T | E |
| S & RM | InfoSec Management | Risk Portfolio Management | | | | | | | | | | | P | B | | | | | | | | | |
| S & RM | Privilege Management Infrastructure | Authorization Services | | C | | O | | | C | I | L | | | | C | I | | | | | | | |
| S & RM | Policies and Standards | Information Security Polices | | | | O | | | C | | | | P | | | | | | | | | | E |

## 13 ANNEX F: ECOSYSTEM ORCHESTRATION - SECURITY INDEX SYSTEM

### 13.1 USE CASE SUMMARY

| Services Covered | Featured Deployment and Service Models: |
|---|---|
| • Broker cloud secure service provisioning<br>• Broker cloud secure service status and metrics<br>• Broker cloud secure service control and management<br>• Identity management between cloud broker and cloud service provider<br>• Continuous monitoring status between cloud broker and cloud service provider<br>• Broker based identity and credential management integration<br>• Broker based secure service orchestration<br>• Broker based integrated secure service status and metrics<br>• Broker cloud secure service control and management<br>• Broker cloud secure service arbitrage<br>• Broker-based technical integration with CSPs returned in aggregation (minimum requirement)<br>• Broker-based business integration with CSP's for secure account creation and credential acquisition (advanced capability)<br>• Broker based arbitrage models capable of approximating cloud consumer requirements to a degree that automated secure provisioning is acceptable (advanced capability)<br>• Broker based ability to perform full or human-assisted workload transition from CSP to CSP (advanced capability) | • All Deployment Models<br>• All Service Models |

| Actors: | Systems |
|---|---|
| • Cloud Consumer<br>• A marketplace or ecosystem of at least two and typically many cloud service providers<br>• Cloud Broker | • Cloud broker secure provisioning system<br>• Cloud broker continuous monitoring system<br>• Cloud broker identity management<br>• Cloud broker APIs to each cloud service provider<br>• Cloud service provider identity management, provisioning and monitoring systems, secure accessed by broker<br>• Cloud broker identity management system with cloud consumer-facing integration capabilities<br>• Cloud broker secure orchestration system with Cross-CSP secure orchestration capabilities<br>• Cloud broker based continuous monitoring offering an integrated view across multiple CSP's<br>• Cloud broker based secure reporting offering an integrated view across multiple CSP's<br>• Cloud broker model for gathering cloud consumer business, technical and policy/security parameters<br>• Cloud broker model for rating and ranking CSP capabilities in a consistent and meaningful manner<br>• Cloud broker system to deliver rankings to cloud consumers<br>• Business transaction systems between broker and CSPs<br>• Automated service selection systems between broker and cloud consumers |

**Notable Services:**

Broker to CSP secure business interfaces

Combined cloud secure service business and technical brokerage

Advanced arbitrage and decision support systems

Cross-CSP services for automated or semi-automated workload migration

**Dependencies:**

- Secure provisioning, continuous monitoring and management capabilities for all CSPs are limited by the broker capabilities and interface
- Secure provisioning, continuous monitoring and management capabilities for a given CSP are limited by the underlying CSP API and capabilities
- Broker-side services implementing cited enhancements
- Cloud consumer identity management systems capable of integrating with the broker-based identity management capability
- Cloud consumer technical staff capabilities to specify orchestration using broker tools
- Means to harvest CSP secure capabilities, secure policies and costs in a consistent manner
- CSP and Broker automated secure business interfaces
- Standards sufficient to support workload migration across CSPs
- Advanced decision or decision support systems to drive technical brokerage from arbitrage

**Assumptions:**

- Consumer has a primary financial and secure service relationship with each cloud service provider. Broker role manages but does not own the relationship with the cloud service provider in this use case.
- Consumer has accepted risks of broker-based secure access to CSPs
- Broker may be in cloud, virtual or traditional environment. Cloud service broker refers to its role, not its mode of implementation
- Consumer has an identity and credentials management (ICAM) system in place which is capable of integrating with broker ICAM
- Consumer has accepted risks of ICAM integration
- Consumer has technical capability to carry out ICAM integration with broker
- Broker has secure access to public and/or private CSP secure capabilities, secure policies and costs
- Broker has no operational relationship with CSPs in the scope of this use case. Such relationships may exist outside the scope of this case.
- Broker has developed a conceptual model and technical implementation to meaningfully gather and apply rankings to harvested CSP information
- Consumer has a primary financial and secure service relationship with the cloud broker but does not necessarily have a business relationship with any particular CSP at any point in time. Consumer to CSP business relationships fall outside the scope of this use case.
- CSP and Broker automated secure business interfaces
- Standards sufficient to support workload migration across CSPs
- Advanced decision or decision support systems to drive technical brokerage from arbitrage

## 13.2 SECURITY INDEX SYSTEM

| | | | | | Security Index | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | **C** | **I** | **A** | **Ag** |
| **BOSS** | Compliance | Intellectual Property Protection | | AC | 2.00 | 2.00 | 2.00 | 6.00 |
| **BOSS** | Data Governance | Handling/ Labeling/ Security Policy | | AC | 3.00 | 2.00 | 1.00 | 6.00 |
| **BOSS** | Data Governance | Clear Desk Policy | | AC | 1.00 | 0.00 | 1.00 | 2.00 |
| **BOSS** | Data Governance | Rules for Information Leakage Prevention | | AC | 2.00 | 3.00 | 2.00 | 7.00 |
| **BOSS** | Human Resource Security | Employee Awareness | | AT | 2.00 | 3.00 | 2.00 | 7.00 |
| **BOSS** | Security Monitoring Services | Market Threat Intelligence | | AT | 1.00 | 1.00 | 1.00 | 3.00 |
| **BOSS** | Security Monitoring Services | Knowledge Base | | AT | 1.00 | 2.00 | 2.00 | 5.00 |
| **BOSS** | Compliance | Audit Planning | | AU | 2.00 | 2.00 | 2.00 | 6.00 |
| **BOSS** | Compliance | Internal Audits | | AU | 2.00 | 2.00 | 2.00 | 6.00 |
| **BOSS** | Security Monitoring Services | Event Mining | | AU | 2.00 | 2.00 | 2.00 | 6.00 |
| **BOSS** | Security Monitoring Services | Event Correlation | | AU | 2.00 | 3.00 | 2.00 | 7.00 |
| **BOSS** | Security Monitoring Services | Email Journaling | | AU | 2.00 | 3.00 | 2.00 | 7.00 |
| **BOSS** | Security Monitoring Services | User Behaviors and Profile Patterns | | AU | 3.00 | 2.00 | 2.00 | 7.00 |
| **BOSS** | Legal Services | E-Discovery | | AU | 1.00 | 2.00 | 2.00 | 5.00 |
| **BOSS** | Legal Services | Incident Response Legal Preparation | | AU | 1.00 | 3.00 | 1.00 | 5.00 |
| **BOSS** | Internal Investigations | Forensic Analysis | | AU | 1.00 | 1.00 | 1.00 | 3.00 |
| **BOSS** | Internal Investigations | e-Mail Journaling | | AU | 2.00 | 3.00 | 2.00 | 7.00 |
| **BOSS** | Compliance | Independent Audits | | CA | 1.00 | 2.00 | 2.00 | 5.00 |
| **BOSS** | Compliance | Third Party Audits | | CA | 1.00 | 2.00 | 2.00 | 5.00 |
| **BOSS** | Operational Risk Management | Business Impact Analysis | | CP | 0.00 | 2.00 | 4.00 | 6.00 |
| **BOSS** | Operational Risk Management | Business Continuity | | CP | 0.00 | 1.00 | 2.00 | 3.00 |
| **BOSS** | Operational Risk Management | Crisis Management | | IR | 1.00 | 2.00 | 1.00 | 4.00 |
| **BOSS** | Operational Risk Management | Risk Management Framework | | IR | 1.00 | 2.00 | 2.00 | 5.00 |

| BOSS | Operational Risk Management | Independent Risk Management | | IR | 1.00 | 2.00 | 2.00 | 5.00 |
|------|------|------|------|------|------|------|------|------|
| **BOSS** | Security Monitoring Services | Database Monitoring | | IR | 2.00 | 3.00 | 3.00 | 8.00 |
| **BOSS** | Security Monitoring Services | Application Monitoring | | IR | 2.00 | 3.00 | 3.00 | 8.00 |
| **BOSS** | Security Monitoring Services | End-Point Monitoring | | IR | 2.00 | 3.00 | 3.00 | 8.00 |
| **BOSS** | Security Monitoring Services | Cloud Monitoring | | IR | 2.00 | 3.00 | 3.00 | 8.00 |
| **BOSS** | Data Governance | Secure Disposal of Data | | MP | 3.00 | 3.00 | 3.00 | 9.00 |
| **BOSS** | Human Resource Security | Employee Termination | | PS | 2.00 | 3.00 | 2.00 | 7.00 |
| **BOSS** | Human Resource Security | Employment Agreements | | PS | 2.00 | 2.00 | 2.00 | 6.00 |
| **BOSS** | Human Resource Security | Background Screening | | PS | 2.00 | 2.00 | 2.00 | 6.00 |
| **BOSS** | Human Resource Security | Job Descriptions | | PS | 1.00 | 1.00 | 1.00 | 3.00 |
| **BOSS** | Human Resource Security | Roles and Responsibilities | | PS | 1.00 | 1.00 | 1.00 | 3.00 |
| **BOSS** | Human Resource Security | Employee Code of Conduct | | PS | 2.00 | 2.00 | 2.00 | 6.00 |
| **BOSS** | Compliance | Information Systems Regulatory Mapping | | RA | 1.00 | 1.00 | 1.00 | 3.00 |
| **BOSS** | Data Governance | Data Ownership - Personnel Responsibilities/ Stewardship | | RA | 3.00 | 3.00 | 3.00 | 9.00 |
| **BOSS** | Data Governance | Data Classification | | RA | 3.00 | 1.00 | 1.00 | 5.00 |
| **BOSS** | Security Monitoring Services | Managed (Outsourced) Security Services | | SA | 1.00 | 1.00 | 1.00 | 3.00 |
| **BOSS** | Legal Services | Contracts | | SA | 3.00 | 3.00 | 3.00 | 9.00 |
| **BOSS** | Security Monitoring Services | Honey Pot | | SC | 2.00 | 1.00 | 2.00 | 5.00 |
| **BOSS** | Security Monitoring Services | Real Time Internetwork Defense (SCAP) | | SC | 3.00 | 3.00 | 3.00 | 9.00 |
| **BOSS** | Data Governance | Rules for Data Retention | | SI | 1.00 | 2.00 | 3.00 | 6.00 |
| **BOSS** | Security Monitoring Services | SIEM Platform | | SI | 3.00 | 3.00 | 3.00 | 9.00 |
| **BOSS** | Security Monitoring Services | Anti Phishing | | SI | 2.00 | 2.00 | 2.00 | 6.00 |
| **BOSS** | Compliance | Contract/ Authority Maintenance | | PM | 2.00 | 2.00 | 2.00 | 6.00 |
| **BOSS** | Operational Risk Management | Operational Risk Committee | | PM | 1.00 | 2.00 | 1.00 | 4.00 |
| **BOSS** | Operational Risk Management | Key Risk Indicators | | PM | 1.00 | 2.00 | 1.00 | 4.00 |
| **BOSS** | Security Monitoring Services | Counter Threat Management | | PM | 1.00 | 1.00 | 1.00 | 3.00 |
| **BOSS** | Security Monitoring Services | SOC Portal | | PM | 1.00 | 1.00 | 1.00 | 3.00 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **BOSS** | Security Monitoring Services | Branding Protection | | PM | 2.00 | 3.00 | 3.00 | 8.00 |
| **ITOS** | IT Operations | Resource Management | Segregation of duties | AC | 1.00 | 1.00 | 2.00 | 4.00 |
| **ITOS** | IT Operations | Resource Management | Contractors | AC | 1.00 | 1.00 | 2.00 | 4.00 |
| **ITOS** | Service Delivery | Information Technology Resiliency | Resiliency Analysis | AU | 1.00 | 0.00 | 2.00 | 3.00 |
| **ITOS** | Service Delivery | Information Technology Resiliency | Capacity Planning | AU | 1.00 | 2.00 | 3.00 | 6.00 |
| **ITOS** | Service Support | Configuration Management | Automated Asset Discovery | AU | 2.00 | 1.00 | 1.00 | 4.00 |
| **ITOS** | Service Support | Problem Management | Event Classification | AU | 1.00 | 2.00 | 2.00 | 5.00 |
| **ITOS** | Service Support | Problem Management | Root Cause Analysis | AU | 2.00 | 2.00 | 1.00 | 5.00 |
| **ITOS** | IT Operations | Portfolio Management | Maturity Model | C M | 1.00 | 1.00 | 2.00 | 4.00 |
| **ITOS** | Service Delivery | Asset Management | Change Back | C M | 1.00 | 1.00 | 1.00 | 3.00 |
| **ITOS** **ITOS** | Service Support Service Support | Configuration Management Configuration Management | Software Management | C M | 1.00 | 1.00 | 2.00 | 4.00 |
| | | | Configuration Management | C M | 2.00 | 3.00 | 3.00 | 8.00 |
| **ITOS** | Service Support | Configuration Management | Physical Inventory | C M | 1.00 | 1.00 | 2.00 | 4.00 |
| **ITOS** | Service Support | Knowledge Management | Benchmarking | C M | 1.00 | 2.00 | 1.00 | 4.00 |
| **ITOS** | Service Support | Knowledge Management | Security Job Aids | C M | 1.00 | 2.00 | 1.00 | 4.00 |
| **ITOS** | Service Support | Knowledge Management | Security FAQ | C M | 1.00 | 2.00 | 1.00 | 4.00 |
| **ITOS** | Service Support | Change Management | Service Provisioning | C M | 1.00 | 2.00 | 1.00 | 4.00 |
| **ITOS** | Service Support | Change Management | Approval Workflow | C M | 1.00 | 2.00 | 1.00 | 4.00 |
| **ITOS** | Service Support | Change Management | Change Review Board | C M | 1.00 | 2.00 | 2.00 | 5.00 |
| **ITOS** | Service Support | Change Management | Planned Changes | C M | 1.00 | 1.00 | 2.00 | 4.00 |

| ITOS | Service Support | Release Management | Version Control | C M | 1.00 | 3.00 | 2.00 | 6.00 |
|------|-----------------|--------------------|--------------------|-----|------|------|------|------|
| ITOS | Service Support | Release Management | Source Code Management | C M | 1.00 | 3.00 | 4.00 | 8.00 |
| ITOS | IT Operations | DRP | Plan Management | CP | 0.00 | 2.00 | 3.00 | 5.00 |
| ITOS | Service Support | Configuration Management | Capacity Planning | CP | 0.00 | 2.00 | 3.00 | 5.00 |
| ITOS | Service Support | Incident Management | Security Incident Reponse | IR | 2.00 | 3.00 | 3.00 | 8.00 |
| ITOS | Service Support | Incident Management | Automated Ticketing | IR | 2.00 | 2.00 | 2.00 | 6.00 |
| ITOS | Service Support | Incident Management | Ticketing | IR | 2.00 | 2.00 | 2.00 | 6.00 |
| ITOS | Service Support | Incident Management | Cross Cloud Security Incident Response | IR | 2.00 | 3.00 | 3.00 | 8.00 |
| ITOS | Service Support | Problem Management | Trend Analysis | IR | 1.00 | 2.00 | 2.00 | 5.00 |
| ITOS | Service Support | Problem Management | Orphan Incident Management | IR | 1.00 | 2.00 | 2.00 | 5.00 |
| ITOS | Service Support | Knowledge Management | Trend Analysis | IR | 1.00 | 1.00 | 1.00 | 3.00 |
| ITOS | Service Support | Change Management | Emergency Changes | MA | 2.00 | 2.00 | 3.00 | 7.00 |
| ITOS | Service Support | Release Management | Scheduling | MA | 2.00 | 2.00 | 3.00 | 7.00 |
| ITOS | Service Delivery | Asset Management | Service Costing (Internal) | SA | 1.00 | 1.00 | 1.00 | 3.00 |
| ITOS | Service Support | Incident Management | Self-Service | SA | 3.00 | 2.00 | 3.00 | 8.00 |
| ITOS | Service Delivery | Information Technology Resiliency | Availability Managemetn | SC | 2.00 | 2.00 | 3.00 | 7.00 |
| ITOS | Service Delivery | Application Performance Monitoring | | SI | 2.00 | 2.00 | 1.00 | 5.00 |
| ITOS | Service Support | Release Management | Testing | SI | 1.00 | 2.00 | 3.00 | 6.00 |
| ITOS | Service Support | Release Management | Build | SI | 1.00 | 2.00 | 3.00 | 6.00 |
| ITOS | IT Operations | DRP | Test Management | PM | 1.00 | 3.00 | 1.00 | 5.00 |
| ITOS | IT Operations | IT Governance | Architecture Governance | PM | 1.00 | 2.00 | 1.00 | 4.00 |
| ITOS | IT Operations | IT Governance | Standards and Guidelines | PM | 1.00 | 2.00 | 1.00 | 4.00 |
| ITOS | IT Operations | PMO | Program Mngmt | PM | 1.00 | 1.00 | 1.00 | 3.00 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **ITOS** | IT Operations | PMO | Project Mgnmt | PM | 1.00 | 1.00 | 1.00 | 3.00 |
| **ITOS** | IT Operations | PMO | Remediation | PM | 1.00 | 2.00 | 1.00 | 4.00 |
| **ITOS** | IT Operations | Portfolio Management | Roadmap | PM | 1.00 | 1.00 | 1.00 | 3.00 |
| **ITOS** | IT Operations | Portfolio Management | Astrategy Alignment | PM | 1.00 | 1.00 | 1.00 | 3.00 |
| **ITOS** | Service Delivery | Service Level Management | Objectives | PM | 2.00 | 2.00 | 2.00 | 6.00 |
| **ITOS** | Service Delivery | Service Level Management | OLAs | PM | 2.00 | 2.00 | 2.00 | 6.00 |
| **ITOS** | Service Delivery | Service Level Management | Internal SLAs | PM | 2.00 | 2.00 | 2.00 | 6.00 |
| **ITOS** | Service Delivery | Service Level Management | External SLAs | PM | 2.00 | 2.00 | 2.00 | 6.00 |
| **ITOS** | Service Delivery | Service Level Management | Vendor Management | PM | 2.00 | 2.00 | 2.00 | 6.00 |
| **ITOS** | Service Delivery | Service Level Management | Service Dashboard | PM | 1.00 | 1.00 | 1.00 | 3.00 |
| **ITOS** | Service Delivery | Asset Management | Operational Budgeting | PM | 1.00 | 1.00 | 1.00 | 3.00 |
| **ITOS** | Service Delivery | Asset Management | Investment Budgeting | PM | 1.00 | 1.00 | 1.00 | 3.00 |
| **ITOS** | Service Support | Problem Management | Problem Resolutions | PM | 1.00 | 2.00 | 1.00 | 4.00 |
| **ITOS** | Service Support | Knowledge Management | Best Practices | PM | 1.00 | 2.00 | 1.00 | 4.00 |
| **Presentation Services** | Presentation Modality | Consumer Service Platform | Social Media | AC | 1.00 | 1.00 | 1.00 | 3.00 |
| **Presentation Services** | Presentation Modality | Consumer Service Platform | Collaboration | AC | 1.00 | 1.00 | 1.00 | 3.00 |
| **Presentation Services** | Presentation Modality | Consumer Service Platform | E-Mail | AC | 1.00 | 1.00 | 1.00 | 3.00 |
| **Presentation Services** | Presentation Modality | Enterprise Service Platform | B2M | AC | 1.00 | 1.00 | 1.00 | 3.00 |
| **Presentation Services** | Presentation Modality | Enterprise Service Platform | B2B | AC | 1.00 | 1.00 | 1.00 | 3.00 |
| **Presentation Services** | Presentation Modality | Enterprise Service Platform | B2C | AC | 1.00 | 1.00 | 1.00 | 3.00 |
| **Presentation Services** | Presentation Modality | Enterprise Service Platform | P2P | AC | 1.00 | 1.00 | 1.00 | 3.00 |
| **Presentation Services** | Presentation Platform | End-Points | Mobile Devices | AC | 3.00 | 1.00 | 3.00 | 7.00 |
| **Presentation Services** | Presentation Platform | End-Points | Fixed Devices | AC | 3.00 | 1.00 | 3.00 | 7.00 |

| Presentation Services | Presentation Platform | End-Points | Desktops | AC | 3.00 | 1.00 | 3.00 | 7.00 |
|---|---|---|---|---|---|---|---|---|
| **Presentation Services** | Presentation Platform | End-Points | Portable Devices | AC | 3.00 | 1.00 | 3.00 | 7.00 |
| **Presentation Services** | Presentation Platform | End-Points | Medical Devices | AC | 3.00 | 1.00 | 3.00 | 7.00 |
| **Presentation Services** | Presentation Platform | End-Points | Smart Appliances | AC | 3.00 | 3.00 | 3.00 | 9.00 |
| **Presentation Services** | Presentation Modality | Consumer Service Platform | Search | SC | 1.00 | 1.00 | 2.00 | 4.00 |
| **Presentation Services** | Presentation Modality | Consumer Service Platform | e-Readers | SC | 1.00 | 1.00 | 2.00 | 4.00 |
| **Presentation Services** | Presentation Modality | Enterprise Service Platform | B2E | SC | 1.00 | 1.00 | 2.00 | 4.00 |
| **Presentation Services** | Presentation Platform | Speech Recognition (IVR) | | SC | 1.00 | 2.00 | 2.00 | 5.00 |
| **Presentation Services** | Presentation Platform | Handwriting (ICR) | | SC | 1.00 | 2.00 | 2.00 | 5.00 |
| **Application Services** | Security Knowledge Lifecycle | Attack Patterns | | C M | 2.00 | 2.00 | 2.00 | 6.00 |
| **Application Services** | Connectivity & Delivery | | | C M | 1.00 | 2.00 | 4.00 | 7.00 |
| **Application Services** | Security Knowledge Lifecycle | Secuirty Design Patterns | | SA | 2.00 | 2.00 | 2.00 | 6.00 |
| **Application Services** | Security Knowledge Lifecycle | Security Application Framework - ACEGI | | SA | 3.00 | 3.00 | 3.00 | 9.00 |
| **Application Services** | Development Processes | Self Service | Security Code Review | SA | 3.00 | 3.00 | 3.00 | 9.00 |
| **Application Services** | Development Processes | Self Service | Application Vulnerability Scanning | SA | 3.00 | 3.00 | 3.00 | 9.00 |
| **Application Services** | Development Processes | Self Service | Stress Volume Testing | SA | 2.00 | 2.00 | 3.00 | 7.00 |
| **Application Services** | Development Processes | Software Quality Assurance | | SA | 2.00 | 3.00 | 2.00 | 7.00 |
| **Application Services** | Integration Middleware | | | SA | 1.00 | 2.00 | 1.00 | 4.00 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Application Services** | Abstraction | | | SC | 0.00 | 0.00 | 2.00 | 2.00 |
| **Application Services** | Programming Interfaces | Input Validation | | SI | 4.00 | 4.00 | 4.00 | 12.00 |
| **Application Services** | Security Knowledge Lifecycle | Code Samples | | SI | 2.00 | 2.00 | 2.00 | 6.00 |
| **Information Services** | BOSS | Audit Findings | | AU | 2.00 | 2.00 | 2.00 | 6.00 |
| **Information Services** | Security Monitoring | eDiscovery Events | | AU | 1.00 | 2.00 | 1.00 | 4.00 |
| **Information Services** | Reporting Services | Dashboard | | CA | 1.00 | 1.00 | 1.00 | 3.00 |
| **Information Services** | Reporting Services | Data Mining | | CA | 1.00 | 1.00 | 1.00 | 3.00 |
| **Information Services** | Reporting Services | Reporting Tools | | CA | 1.00 | 2.00 | 2.00 | 5.00 |
| **Information Services** | Reporting Services | Business Intelligence | | CA | 1.00 | 1.00 | 1.00 | 3.00 |
| **Information Services** | ITOS | Problem Management | | CA | 2.00 | 2.00 | 2.00 | 6.00 |
| **Information Services** | Service Delivery | Service Catalog | | C M | 0.00 | 1.00 | 0.00 | 1.00 |
| **Information Services** | Service Delivery | SLA´s | | C M | 1.00 | 2.00 | 1.00 | 4.00 |
| **Information Services** | ITOS | CMDB | | C M | 3.00 | 4.00 | 4.00 | 11.00 |
| **Information Services** | ITOS | Change Management | | C M | 2.00 | 3.00 | 3.00 | 8.00 |
| **Information Services** | Service Support | Configuration Rules (Metadata) | | C M | 2.00 | 2.00 | 2.00 | 6.00 |
| **Information Services** | Service Support | Configuration Management Database (CMDB) | | C M | 2.00 | 3.00 | 3.00 | 8.00 |
| **Information Services** | Service Support | Change Logs | | C M | 2.00 | 3.00 | 3.00 | 8.00 |
| **Information Services** | Security Monitoring | Compliance Monitoring | | C M | 2.00 | 3.00 | 3.00 | 8.00 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Information Services** | Security Monitoring | Privilege Usage Events | | C M | 3.00 | 3.00 | 3.00 | 9.00 |
| **Information Services** | Service Delivery | Recovery Plans | | CP | 0.00 | 3.00 | 4.00 | 7.00 |
| **Information Services** | BOSS | GR Data (Employee & contractors) | | IA | 1.00 | 3.00 | 2.00 | 6.00 |
| **Information Services** | Security Monitoring | Authorization Events | | IA | 3.00 | 2.00 | 3.00 | 8.00 |
| **Information Services** | Security Monitoring | Authentication Events | | IA | 3.00 | 2.00 | 3.00 | 8.00 |
| **Information Services** | Security Monitoring | ACL´s | | IA | 3.00 | 3.00 | 3.00 | 9.00 |
| **Information Services** | Security Monitoring | CRL´s | | IA | 3.00 | 3.00 | 3.00 | 9.00 |
| **Information Services** | User Directory Services | Active Directory Services | | IA | 3.00 | 3.00 | 4.00 | 10.00 |
| **Information Services** | User Directory Services | LDAP Repositories | | IA | 3.00 | 3.00 | 4.00 | 10.00 |
| **Information Services** | User Directory Services | X.500 Repositories | | IA | 3.00 | 3.00 | 4.00 | 10.00 |
| **Information Services** | User Directory Services | DBMS Repositories | | IA | 3.00 | 3.00 | 4.00 | 10.00 |
| **Information Services** | User Directory Services | Registry Services | | IA | 3.00 | 3.00 | 4.00 | 10.00 |
| **Information Services** | User Directory Services | Location Services | | IA | 3.00 | 3.00 | 4.00 | 10.00 |
| **Information Services** | User Directory Services | Federated Services | | IA | 3.00 | 4.00 | 4.00 | 11.00 |
| **Information Services** | User Directory Services | Virtual Directory Services | | IA | 3.00 | 3.00 | 4.00 | 10.00 |
| **Information Services** | User Directory Services | Meta Directory Services | | IA | 3.00 | 3.00 | 4.00 | 10.00 |
| **Information Services** | ITOS | Incident Management | | IR | 2.00 | 3.00 | 3.00 | 8.00 |
| **Information Services** | Service Support | Service Events | | IR | 2.00 | 3.00 | 3.00 | 8.00 |

Page 193

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Information Services** | BOSS | Data Classification | | RA | 3.00 | 1.00 | 1.00 | 5.00 |
| **Information Services** | Data Governance | Risk Assessments | | RA | 1.00 | 2.00 | 2.00 | 5.00 |
| **Information Services** | Risk Management | Risk Assessments | | RA | 1.00 | 2.00 | 2.00 | 5.00 |
| **Information Services** | Risk Management | Business Impact Assessment. | | RA | 1.00 | 2.00 | 2.00 | 5.00 |
| **Information Services** | Risk Management | VRA | | RA | 1.00 | 2.00 | 2.00 | 5.00 |
| **Information Services** | Risk Management | TVM | | RA | 1.00 | 1.00 | 1.00 | 3.00 |
| **Information Services** | Service Delivery | OLA´s | | SA | 1.00 | 3.00 | 1.00 | 5.00 |
| **Information Services** | Data Governance | Non-Production Data | | SA | 1.00 | 1.00 | 1.00 | 3.00 |
| **Information Services** | Security Monitoring | NIPS Events | | SC | 3.00 | 3.00 | 3.00 | 9.00 |
| **Information Services** | Security Monitoring | DLP Events | | SC | 3.00 | 2.00 | 3.00 | 8.00 |
| **Information Services** | Data Governance | Information Leakage Metadata | | SI | 3.00 | 2.00 | 2.00 | 7.00 |
| **Information Services** | Data Governance | Data Segregation | | SI | 3.00 | 3.00 | 3.00 | 9.00 |
| **Information Services** | Security Monitoring | Transformation Services | | SI | 1.00 | 3.00 | 3.00 | 7.00 |
| **Information Services** | Security Monitoring | Session Events | | SI | 1.00 | 3.00 | 3.00 | 7.00 |
| **Information Services** | Security Monitoring | Application Events | | SI | 1.00 | 3.00 | 3.00 | 7.00 |
| **Information Services** | Security Monitoring | Network Events | | SI | 1.00 | 3.00 | 3.00 | 7.00 |
| **Information Services** | Security Monitoring | Computer Events | | SI | 1.00 | 3.00 | 3.00 | 7.00 |
| **Information Services** | Security Monitoring | Host Intrusion Protection Systems (HIPS) | | SI | 1.00 | 3.00 | 3.00 | 7.00 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Information Services** | Security Monitoring | Database Events | | SI | 1.00 | 3.00 | 3.00 | 7.00 |
| **Information Services** | Service Delivery | Contracts | | PM | 1.00 | 2.00 | 1.00 | 4.00 |
| **Information Services** | ITOS | PMO | | PM | 1.00 | 1.00 | 1.00 | 3.00 |
| **Information Services** | ITOS | Strategy | | PM | 1.00 | 1.00 | 1.00 | 3.00 |
| **Information Services** | ITOS | Roadmap | | PM | 1.00 | 1.00 | 1.00 | 3.00 |
| **Information Services** | ITOS | Knowledge Management | | PM | 1.00 | 1.00 | 1.00 | 3.00 |
| **Information Services** | ITOS | Service Management | | PM | 1.00 | 1.00 | 1.00 | 3.00 |
| **Information Services** | BOSS | Risk Assessments | | PM | 1.00 | 2.00 | 1.00 | 4.00 |
| **Information Services** | BOSS | Process Ownership | | PM | 1.00 | 2.00 | 1.00 | 4.00 |
| **Information Services** | BOSS | Business Strategy | | PM | 1.00 | 1.00 | 2.00 | 4.00 |
| **Information Services** | Service Support | Knowledge Repository | | PM | 1.00 | 1.00 | 1.00 | 3.00 |
| **Information Services** | Risk Management | GRC | | PM | 1.00 | 2.00 | 1.00 | 4.00 |
| **Information Services** | Risk Management | DR & BC Plans | | PM | 1.00 | 2.00 | 2.00 | 5.00 |
| **Infrastructure Services** | Virtual Infrastructure: Storage Virtualization | Block-Based Virtualization | Network-Based | AC | 0.00 | 3.00 | 1.00 | 4.00 |
| **Infrastructure Services** | **Internal Infrastructure:** Network Services | Authoritative Time Source | | AU | 1.00 | 3.00 | 1.00 | 5.00 |
| **Infrastructure Services** | **Internal Infrastructure:** Servers | | | CM | 0.00 | 0.00 | 0.00 | 0.00 |
| **Infrastructure Services** | **Internal Infrastructure:** Availability Services | | | CP | 0.00 | 0.00 | 3.00 | 3.00 |
| **Infrastructure Services** | **Internal Infrastructure**: Patch Management | Service Discovery | | MA | 1.00 | 1.00 | 1.00 | 3.00 |

| Infrastructure Services | Internal Infrastructure: Equipment Maintenance | | | MA | 0.00 | 0.00 | 0.00 | 0.00 |
|---|---|---|---|---|---|---|---|---|
| Infrastructure Services | Internal Infrastructure: Storage Services | | | MP | 0.00 | 0.00 | 2.00 | 2.00 |
| Infrastructure Services | Virtual Infrastructure: Storage Virtualization | Block-Based Virtualization | Storage Device-Based | MP | 0.00 | 2.00 | 3.00 | 5.00 |
| Infrastructure Services | Internal Infrastructure: Facility Security | Controlled Physical Access | Barriers | PE | 1.00 | 1.00 | 3.00 | 5.00 |
| Infrastructure Services | Internal Infrastructure: Facility Security | Controlled Physical Access | Security Patrols | PE | 1.00 | 1.00 | 3.00 | 5.00 |
| Infrastructure Services | Internal Infrastructure: Facility Security | Controlled Physical Access | Electronic Surveillance | PE | 1.00 | 1.00 | 3.00 | 5.00 |
| Infrastructure Services | Internal Infrastructure: Facility Security | Controlled Physical Access | Physical Authentication | PE | 1.00 | 1.00 | 3.00 | 5.00 |
| Infrastructure Services | Internal Infrastructure: Facility Security | Asset Handling | Data | PE | 1.00 | 2.00 | 3.00 | 6.00 |
| Infrastructure Services | Internal Infrastructure: Facility Security | Asset Handling | Storage | PE | 1.00 | 2.00 | 3.00 | 6.00 |
| Infrastructure Services | Internal Infrastructure: Facility Security | Asset Handling | Hardware | PE | 1.00 | 2.00 | 3.00 | 6.00 |
| Infrastructure Services | Internal Infrastructure: Facility Security | Environmental Risk Management | Physical Security | PE | 1.00 | 1.00 | 3.00 | 5.00 |
| Infrastructure Services | Internal Infrastructure: Facility Security | Environmental Risk Management | Equipment Location | PE | 1.00 | 1.00 | 3.00 | 5.00 |
| Infrastructure Services | Internal Infrastructure: Facility Security | Environmental Risk Management | Power Redundancy | PE | 1.00 | 1.00 | 3.00 | 5.00 |
| Infrastructure Services | Internal Infrastructure: Network Services | Network Segmentation | | SC | 1.00 | 2.00 | 3.00 | 6.00 |
| Infrastructure Services | Virtual Infrastructure: Desktop "Client" Virtualization | Local | | SC | 0.00 | 0.00 | 2.00 | 2.00 |
| Infrastructure Services | Virtual Infrastructure: Desktop "Client" Virtualization | Remote | Session-Based | SC | 0.00 | 0.00 | 2.00 | 2.00 |
| Infrastructure Services | Virtual Infrastructure: Desktop "Client" Virtualization | Remote | VM-Based (VDI) | SC | 0.00 | 0.00 | 2.00 | 2.00 |
| Infrastructure Services | Virtual Infrastructure: Storage Virtualization | Block-Based Virtualization | Host-Based | SC | 0.00 | 0.00 | 2.00 | 2.00 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Infrastructur e Services** | **Virtual Infrastructure:** Storage Virtualization | File-Based virtualization | | SC | 0.00 | 1.00 | 3.00 | 4.00 |
| **Infrastructur e Services** | **Virtual Infrastructure:** Application Virtualization | Client Application Streaming | | SC | 1.00 | 1.00 | 3.00 | 5.00 |
| **Infrastructur e Services** | **Virtual Infrastructure:** Application Virtualization | Server Application Streaming | | SC | 1.00 | 1.00 | 3.00 | 5.00 |
| **Infrastructur e Services** | **Virtual Infrastructure**: Virtual Workspaces | | | SC | 0.00 | 0.00 | 0.00 | 0.00 |
| **Infrastructur e Services** | **Virtual Infrastructure:** Server Virtualization | Virtual Machines (host based) | Full | SC | 0.00 | 0.00 | 2.00 | 2.00 |
| **Infrastructur e Services** | **Virtual Infrastructure:** Server Virtualization | Virtual Machines (host based) | Paravirtualization | SC | 0.00 | 0.00 | 2.00 | 2.00 |
| **Infrastructur e Services** | **Virtual Infrastructure:** Server Virtualization | Virtual Machines (host based) | Hardware-Assisted | SC | 0.00 | 0.00 | 2.00 | 2.00 |
| **Infrastructur e Services** | **Virtual Infrastructure:** Server Virtualization | OS Virtualization | | SC | 0.00 | 0.00 | 2.00 | 2.00 |
| **Infrastructur e Services** | **Virtual Infrastructure:** Server Virtualization | TPM Virtualization | | SC | 0.00 | 0.00 | 2.00 | 2.00 |
| **Infrastructur e Services** | **Virtual Infrastructure:** Server Virtualization | Virtual Memory | | SC | 0.00 | 0.00 | 2.00 | 2.00 |
| **Infrastructur e Services** | **Virtual Infrastructure:** Network | Network Address Space | IPv4 | SC | 0.00 | 0.00 | 2.00 | 2.00 |
| **Infrastructur e Services** | **Virtual Infrastructure:** Network | Network Address Space | IPv6 | SC | 0.00 | 0.00 | 2.00 | 2.00 |
| **Infrastructur e Services** | **Virtual Infrastructure:** Network | VLAN | | SC | 0.00 | 1.00 | 3.00 | 4.00 |
| **Infrastructur e Services** | **Virtual Infrastructure:** Network | VNIC | | SC | 0.00 | 1.00 | 3.00 | 4.00 |
| **Infrastructur e Services** | **Virtual Infrastructure:** Database Virtualization | | | SC | 0.00 | 0.00 | 2.00 | 2.00 |
| **Infrastructur e Services** | **Virtual Infrastructure**: Mobile Device Virtualization | | | SC | 0.00 | 0.00 | 2.00 | 2.00 |
| **Infrastructur e Services** | **Virtual Infrastructure:** Smartcard Virtualization | | | SC | 0.00 | 0.00 | 2.00 | 2.00 |
| **Infrastructur e Services** | **Internal Infrastructure**: Patch Management | Compliance Monitoring | | PM | 1.00 | 2.00 | 1.00 | 4.00 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| S & RM | Privilege Management Infrastructure | Privilege Usage Management | Privilege Usage Gateway | AC | 3.00 | 3.00 | 3.00 | 9.00 |
| S & RM | Infrastructure Protection Services | Server | White Listing | AC | 3.00 | 1.00 | 2.00 | 6.00 |
| S & RM | Infrastructure Protection Services | Server | Host Firewall | AC | 3.00 | 2.00 | 3.00 | 8.00 |
| S & RM | Infrastructure Protection Services | End-Point | Host Firewall | AC | 3.00 | 2.00 | 3.00 | 8.00 |
| S & RM | Infrastructure Protection Services | End-Point | Content Filtering | AC | 3.00 | 1.00 | 2.00 | 6.00 |
| S & RM | | End-Point | White Listing | AC | 3.00 | 2.00 | 3.00 | 8.00 |
| S & RM | Infrastructure Protection Services | Network | Content Filtering | AC | 3.00 | 1.00 | 2.00 | 6.00 |
| S & RM | | Network | Firewall | AC | 3.00 | 3.00 | 4.00 | 10.00 |
| S & RM | Infrastructure Protection Services | Network | Black Listing Filtering | AC | 3.00 | 1.00 | 2.00 | 6.00 |
| | Infrastructure Protection Services Infrastructure Protection Services | Application | Application Firewall | AC | 3.00 | 3.00 | 4.00 | 10.00 |
| S & RM | Infrastructure Protection Services | Application | Secure Collaboration | AC | 3.00 | 2.00 | 3.00 | 8.00 |
| S & RM | | Application | Real Time Filtering | AC | 3.00 | 2.00 | 3.00 | 8.00 |
| S & RM | Infrastructure Protection Services | Data Lifecycle Management | Meta data Control | AC | 3.00 | 1.00 | 1.00 | 5.00 |
| S & RM | Data Protection Data Protection | Data Lifecycle Management | Data Seeding | AC | 2.00 | 0.00 | 1.00 | 3.00 |
| S & RM | Data Protection | Intellectual Property Prevention | Digital Rights Management | AC | 3.00 | 1.00 | 2.00 | 6.00 |
| S & RM | Policies and Standards | Role Based Awareness | | AC | 2.00 | 2.00 | 2.00 | 6.00 |
| S & RM | Governance Risk & Compliance | Technical Awareness and Training | | AT | 2.00 | 2.00 | 2.00 | 6.00 |
| S & RM | Governance Risk & Compliance | Compliance Management | | AU | 1.00 | 2.00 | 1.00 | 4.00 |
| S & RM | Governance Risk & Compliance | Audit Management | | AU | 1.00 | 1.00 | 1.00 | 3.00 |
| S & RM | Threat and Vulnerability Management | Compliance Testing | Databases | AU | 3.00 | 3.00 | 3.00 | 9.00 |

| S & RM | Threat and Vulnerability Management | Compliance Testing | Servers | AU | 3.00 | 3.00 | 3.00 | 9.00 |
|---|---|---|---|---|---|---|---|---|
| S & RM | Policies and Standards | Best Practices & Regulatory correlation | | CA | 2.00 | 2.00 | 2.00 | 6.00 |
| S & RM | InfoSec Management | Capability Mapping | | C M | 0.00 | 2.00 | 3.00 | 5.00 |
| S & RM | Infrastructure Protection Services | End-Point | Inventory Control | C M | 1.00 | 2.00 | 1.00 | 4.00 |
| S & RM | Data Protection | Intellectual Property Prevention | Intellectual Property | C M | 1.00 | 2.00 | 1.00 | 4.00 |
| S & RM | Policies and Standards | Operational Security Baselines | | C M | 1.00 | 2.00 | 2.00 | 5.00 |
| S & RM | Policies and Standards | Job Aid Guidelines | | C M | 1.00 | 2.00 | 1.00 | 4.00 |
| S & RM | Privilege Management Infrastructure | Identity Management | Domain Unique Identifier | IA | 3.00 | 4.00 | 3.00 | 10.00 |
| S & RM | Privilege Management Infrastructure | Identity Management | Federated IDM | IA | 3.00 | 4.00 | 3.00 | 10.00 |
| S & RM | Privilege Management Infrastructure | Identity Management | Identity Provisioning | IA | 3.00 | 4.00 | 3.00 | 10.00 |
| S & RM | Privilege Management Infrastructure | Identity Management | Attribute Provisioning | IA | 3.00 | 3.00 | 3.00 | 9.00 |
| S & RM | Privilege Management Infrastructure | Authorization Services | Policy Enforcement | IA | 2.00 | 3.00 | 2.00 | 7.00 |
| S & RM | Privilege Management Infrastructure | Authorization Services | Policy definition | IA | 2.00 | 3.00 | 2.00 | 7.00 |
| S & RM | Privilege Management Infrastructure | Authorization Services | Principal Data Mngmnt | IA | 2.00 | 3.00 | 2.00 | 7.00 |
| S & RM | Privilege Management Infrastructure | Authorization Services | XACML | IA | 2.00 | 2.00 | 2.00 | 6.00 |
| S & RM | Privilege Management Infrastructure | Authorization Services | Role Management | IA | 2.00 | 3.00 | 2.00 | 7.00 |
| S & RM | Privilege Management Infrastructure | Authorization Services | Obligation | IA | 2.00 | 2.00 | 2.00 | 6.00 |
| S & RM | Privilege Management Infrastructure | Authorization Services | Out of the Box (OTB) autZ | IA | 3.00 | 4.00 | 3.00 | 10.00 |

Page 199

| S & RM | Privilege Management Infrastructure | Authentication Services | SAML Token | IA | 3.00 | 3.00 | 3.00 | 9.00 |
|--------|-------------------------------------|-------------------------|------------|----|------|------|------|------|
| S & RM | Privilege Management Infrastructure | Authentication Services | Risk Based Auth | IA | 3.00 | 3.00 | 3.00 | 9.00 |
| S & RM | Privilege Management Infrastructure | Authentication Services | Multifactor | IA | 3.00 | 3.00 | 3.00 | 9.00 |
| S & RM | Privilege Management Infrastructure | Authentication Services | OTP | IA | 3.00 | 3.00 | 3.00 | 9.00 |
| S & RM | Privilege Management Infrastructure | Authentication Services | Smart Card | IA | 3.00 | 3.00 | 3.00 | 9.00 |
| S & RM | Privilege Management Infrastructure | Authentication Services | Password Management | IA | 3.00 | 3.00 | 3.00 | 9.00 |
| S & RM | Privilege Management Infrastructure | Authentication Services | Biometrics | IA | 3.00 | 3.00 | 3.00 | 9.00 |
| S & RM | Privilege Management Infrastructure | Authentication Services | Network Authentication | IA | 3.00 | 3.00 | 3.00 | 9.00 |
| S & RM | Privilege Management Infrastructure | Authentication Services | Single Sign On | IA | 3.00 | 3.00 | 3.00 | 9.00 |
| S & RM | Privilege Management Infrastructure | Authentication Services | WS-Security | IA | 3.00 | 3.00 | 3.00 | 9.00 |
| S & RM | Privilege Management Infrastructure | Authentication Services | Middleware Auth | IA | 3.00 | 3.00 | 3.00 | 9.00 |
| S & RM | Privilege Management Infrastructure | Authentication Services | Identity Verification | IA | 3.00 | 3.00 | 3.00 | 9.00 |
| S & RM | Privilege Management Infrastructure | Authentication Services | Out-of-The-Box (OTB) Auth | IA | 2.00 | 2.00 | 2.00 | 6.00 |
| S & RM | Privilege Management Infrastructure | Privilege Usage Management | Keystroke/Session Logging | IA | 3.00 | 2.00 | 3.00 | 8.00 |
| S & RM | Privilege Management Infrastructure | Privilege Usage Management | Password Vaulting | IA | 4.00 | 3.00 | 3.00 | 10.00 |
| S & RM | Threat and Vulnerability Management | Compliance Testing | Network Authentication | IA | 2.00 | 3.00 | 2.00 | 7.00 |
| S & RM | Infrastructure Protection Services | End-Point | Forensic Tools | IR | 2.00 | 2.00 | 2.00 | 6.00 |
| S & RM | Infrastructure Protection Services | End-Point | Media Lockdown | MP | 1.00 | 2.00 | 3.00 | 6.00 |
| S & RM | InfoSec Management | Residual Risk Management | | PL | 2.00 | 2.00 | 2.00 | 6.00 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| S & RM | Governance Risk & Compliance | Policy Management | Exceptions | RA | 1.00 | 2.00 | 1.00 | 4.00 |
| S & RM | Governance Risk & Compliance | Policy Management | Self-Assessment | RA | 1.00 | 2.00 | 1.00 | 4.00 |
| S & RM | InfoSec Management | Risk Dashboard | | RA | 1.00 | 1.00 | 1.00 | 3.00 |
| S & RM | Threat and Vulnerability Management | Vulnerability Management | application | RA | 3.00 | 3.00 | 3.00 | 9.00 |
| S & RM | Threat and Vulnerability Management | Vulnerability Management | Infrastructure | RA | 3.00 | 3.00 | 3.00 | 9.00 |
| S & RM | Threat and Vulnerability Management | Vulnerability Management | DB | RA | 3.00 | 3.00 | 3.00 | 9.00 |
| S & RM | Threat and Vulnerability Management | Penetration Testing | Infernal | RA | 2.00 | 2.00 | 2.00 | 6.00 |
| S & RM | Threat and Vulnerability Management | Penetration Testing | External | RA | 3.00 | 3.00 | 3.00 | 9.00 |
| S & RM | Threat and Vulnerability Management | Threat Management | Source Code Scanning | RA | 2.00 | 2.00 | 2.00 | 6.00 |
| S & RM | Threat and Vulnerability Management | Threat Management | Risk Taxonomy | RA | 2.00 | 2.00 | 2.00 | 6.00 |
| S & RM | Policies and Standards | Data/ Asset Classification | | RA | 1.00 | 2.00 | 2.00 | 5.00 |
| S & RM | Governance Risk & Compliance | Vendor Management | | SA | 1.00 | 2.00 | 1.00 | 4.00 |
| S & RM | Data Protection | Data Lifecycle Management | Life cycle management | SA | 1.00 | 3.00 | 1.00 | 5.00 |
| S & RM | Policies and Standards | Technical Security Standards | | SA | 1.00 | 1.00 | 1.00 | 3.00 |
| S & RM | Privilege Management Infrastructure | Privilege Usage Management | Resource Protection | SC | 4.00 | 3.00 | 3.00 | 10.00 |
| S & RM | Infrastructure Protection Services | Network | Deep Packet Inspection (DPI) | SC | 1.00 | 3.00 | 2.00 | 6.00 |
| S & RM | Infrastructure Protection Services | Network | Wireless Protection | SC | 1.00 | 2.00 | 3.00 | 6.00 |
| S & RM | Infrastructure Protection Services | Network | Link Layer Network security | SC | 1.00 | 2.00 | 3.00 | 6.00 |
| S & RM | Infrastructure Protection Services | Application | XML Appliance | SC | 1.00 | 1.00 | 2.00 | 4.00 |
| S & RM | Infrastructure Protection Services | Application | Secure Messaging | SC | 4.00 | 3.00 | 3.00 | 10.00 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **S & RM** | Data Protection | Data Lifecycle Management | Data De-Identification | SC | 4.00 | 1.00 | 3.00 | 8.00 |
| **S & RM** | Data Protection | Data Lifecycle Management | Data Masking | SC | 4.00 | 1.00 | 3.00 | 8.00 |
| **S & RM** | Data Protection | Data Lifecycle Management | Data Tagging | SC | 4.00 | 1.00 | 3.00 | 8.00 |
| **S & RM** | Data Protection | Data Lifecycle Management | Data Obscuring | SC | 4.00 | 1.00 | 3.00 | 8.00 |
| **S & RM** | Data Protection | Data Leakage Prevention | Data Discovery | SC | 3.00 | 3.00 | 3.00 | 9.00 |
| **S & RM** | Data Protection | Data Leakage Prevention | Network (Data in Transit) | SC | 3.00 | 1.00 | 2.00 | 6.00 |
| **S & RM** | Data Protection | Data Leakage Prevention | End-Point (data in Use) | SC | 3.00 | 1.00 | 2.00 | 6.00 |
| **S & RM** | Data Protection | Data Leakage Prevention | Server (data at Rest) | SC | 3.00 | 1.00 | 2.00 | 6.00 |
| **S & RM** | Cryptographic Services | Key Management | Symmetric Keys | SC | 2.00 | 3.00 | 2.00 | 7.00 |
| **S & RM** | Cryptographic Services | Key Management | Asymmetric Keys | SC | 2.00 | 3.00 | 2.00 | 7.00 |
| **S & RM** | Cryptographic Services | PKI | | SC | 3.00 | 3.00 | 3.00 | 9.00 |
| **S & RM** | Cryptographic Services | Data in use (memory) Encryption | | SC | 3.00 | 3.00 | 3.00 | 9.00 |
| **S & RM** | Cryptographic Services | Data in Transit Encryption (Transitory, Fixed) | | SC | 3.00 | 3.00 | 3.00 | 9.00 |
| **S & RM** | Cryptographic Services | Data as Rest Encryption (DB, File, SAN, Desktop, Mobile) | | SC | 3.00 | 3.00 | 3.00 | 9.00 |
| **S & RM** | Infrastructure Protection Services | Server | Anti-virus | SI | 3.00 | 3.00 | 3.00 | 9.00 |
| **S & RM** | Infrastructure Protection Services | Server | HIPS/HIDS (Intrusion Protection /Detection) | SI | 3.00 | 3.00 | 3.00 | 9.00 |
| **S & RM** | Infrastructure Protection Services | End-Point | Anti-Virus, Anti-Spam, Anti-Malware | SI | 3.00 | 3.00 | 3.00 | 9.00 |
| **S & RM** | Infrastructure Protection Services | End-Point | HIPS/HIDS (Intrusion Protection /Detection) | SI | 3.00 | 3.00 | 3.00 | 9.00 |
| **S & RM** | Infrastructure Protection Services | End-Point | Hardware Based trusted Assets | SI | 2.00 | 2.00 | 1.00 | 5.00 |
| **S & RM** | Infrastructure Protection Services | Network | NIPS/NIDS | SI | 1.00 | 3.00 | 1.00 | 5.00 |
| **S & RM** | Data Protection | Data Lifecycle Management | eSignature | SI | 3.00 | 3.00 | 3.00 | 9.00 |
| **S & RM** | Cryptographic Services | Signature Services | | SI | 3.00 | 4.00 | 3.00 | 10.00 |
| **S & RM** | Governance Risk & Compliance | IT Risk Management | | PM | 1.00 | 2.00 | 1.00 | 4.00 |

| S & RM | InfoSec Management | Risk Portfolio Management | | PM | 1.00 | 2.00 | 1.00 | 4.00 |
| S & RM | Privilege Management Infrastructure | Authorization Services | Policy Management | PM | 3.00 | 3.00 | 3.00 | 9.00 |

## 13.3 ASIS HEAT MAP