

NIST

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

Working Document

NIST Cloud Computing Security Reference Architecture

*NIST Cloud Computing Security Working Group
NIST Cloud Computing Program
Information Technology Laboratory*

This page left intentionally blank

DRAFT

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.

DISCLAIMER

This document has been prepared by the National Institute of Standards and Technology (NIST) and describes standards research in support of the NIST Cloud Computing Program.

Certain commercial entities, equipment, or material may be identified in this document in order to describe a concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that these entities, materials, or equipment are necessarily the best available for the purpose.

Acknowledgements

Dr. Michaela Iorga, Chair of the NIST Cloud Computing Security Working Group (NCC SWG) and editor of this document gratefully acknowledges and appreciates the broad contributions from members of the NCC SWG. The following contributors¹ and internal reviewers that accepted to be publically acknowledged in this document are only very few of the members that participated in this effort. The list (in alphabetic order by last name), will be updated when we receive more confirmations form our members.

CONTRIBUTORS:

Wayne W. Armour, independent consultant
Nadeem Bukhari, Kinamik Data Integrity
Kyle Coble, Department of Homeland Security
Pw Carey, consultant, Compliance Partners, LLC
Muhammad F. Islam, PhD candidate, GWU, senior consultant, Booz Allen Hamilton, Inc.
Jerry Kickenson, SWIFT
Juanita Koilpillai, CTO, Electrosoft Services, Inc.
Prabha Kumar, PhD., Technical Director, DoD CIO/Cybersecurity
Nancy M. Landreville, PhD., EmeSec (contractor for the Dep. of VA), Professor, UMD
Anne L. Lee, PhD., Chief Eng., Sys. Arch., U.S. Air Force, Space and Missile Sys. Center
Cheng-Yin Lee, independent consultant
Chan Lim, Technical Architect, IBM
Keyun Ruan, PhD., University. College Dublin, EADS N.V., XENSIX Inc.
Michael A. Salim, CTO, American Data Technology, Inc.
Ken E. Stavinoha, PhD., Cisco Systems

INTERNAL REVIEWERS:

Wayne W. Armour, independent consultant
Jerry Kickenson, SWIFT
Juanita Koilpillai, CTO, Electrosoft Services, Inc.
Michael A. Salim, CTO, American Data Technology, Inc.
Ken E. Stavinoha, PhD., Cisco Systems

NOTE: All views expressed in this document by our contributors are their personal opinions and not that of the organizations they represent.

Appendix A lists the SWG active members that provided subject-matter expertise during our meeting, for particular areas discussed in this document and accepted to be publically acknowledged

¹ A member of the NCC SWG that dedicated substantial time, on a regular basis, to the research and development of this document.

Table of Contents

EXECUTIVE SUMMARY	9
1 INTRODUCTION	10
1.1 BACKGROUND.....	10
1.2 OBJECTIVES	10
1.3 STRUCTURE OF THE DOCUMENT	12
1.4 USING THE DOCUMENT	13
2 SECURITY REFERENCE ARCHITECTURE: OVERVIEW.....	15
2.1 RISK MANAGEMENT	16
2.2 ASSUMPTIONS AND CLARIFICATIONS	21
2.2.1 <i>Cloud Consumer</i>	23
2.2.2 <i>Cloud Provider</i>	23
2.2.2.1 <i>Intermediary Cloud Provider Example</i>	24
2.2.3 <i>Cloud Broker</i>	25
2.2.3.1 <i>Differentiating Business and Technical Broker Services</i>	25
2.2.3.2 <i>A Cloud Brokerage Example</i>	26
2.2.4 <i>Cloud Carrier</i>	27
2.2.5 <i>Cloud Auditor</i>	28
2.2.6 <i>Cloud Ecosystem</i>	29
2.2.7 <i>Security Conservation Principle</i>	30
2.3 OUR APPROACH.....	31
3 SECURITY REFERENCE ARCHITECTURE: SECURITY COMPONENTS	34
4 SECURITY REFERENCE ARCHITECTURE: DATA ANALYSIS METHODOLOGY	36
4.1 DATA COLLECTION.....	36
4.2 DATA AGGREGATION AND VALIDATION	37
4.3 DERIVING THE SECURITY RESPONSIBILITIES FOR INTERMEDIARY PROVIDER AND TECHNICAL BROKER.....	38
4.4 MAPPING SECURITY COMPONENTS TO SECURITY CONTROL FAMILIES	40
4.5 EMPIRICAL DATA ANALYSIS AND THE GENERIC HEAT MAP	41
5 SECURITY REFERENCE ARCHITECTURE: FORMAL MODEL.....	44
5.1 THE FORMAL MODEL OVERVIEW	44
5.2 CONSUMER - ARCHITECTURAL COMPONENTS.....	47
5.2.1 <i>Secure Cloud Consumption Management</i>	49
5.2.1.1 <i>Secure Business Support</i>	50
5.2.1.2 <i>Secure Configuration</i>	50
5.2.1.3 <i>Secure Portability and Interoperability</i>	51
5.2.1.4 <i>Secure Organizational Support</i>	52
5.2.2 <i>Secure Cloud Ecosystem Orchestration</i>	52
5.2.2.1 <i>Secure Functional Layer</i>	53
5.3 PROVIDER – ARCHITECTURAL COMPONENTS.....	54
5.3.1 <i>Secure cloud Ecosystem Orchestration</i>	56
5.3.1.1 <i>Secure Deployment and Service Layer</i>	57
5.3.1.2 <i>Secure Resource Abstraction and Control Layer</i>	58
5.3.1.3 <i>Secure Physical Resource Layer</i>	59
5.3.2 <i>Secure Cloud Service Management</i>	59
5.3.2.1 <i>Secure Provisioning and Configuration</i>	61
5.3.2.2 <i>Secure Portability and Interoperability</i>	62
5.3.2.3 <i>Secure Business Support</i>	63
5.4 BROKER – ARCHITECTURAL COMPONENTS.....	64
5.4.1 <i>Technical Broker</i>	66

5.4.2	<i>Business Broker</i>	68
5.4.3	<i>Secure Cloud Ecosystem Orchestration</i>	69
5.4.3.1	<i>Secure Service Layers</i>	70
5.4.4	<i>Secure Service Aggregation</i>	71
5.4.5	<i>Secure Cloud Service Management</i>	72
5.4.5.1	<i>Secure Portability and Interoperability</i>	73
5.4.5.2	<i>Secure Provisioning and Configuration</i>	73
5.4.5.3	<i>Secure Business Support</i>	74
5.4.6	<i>Secure Service Intermediation</i>	74
5.4.7	<i>Secure Service Arbitrage</i>	75
5.5	CARRIER – ARCHITECTURAL COMPONENTS	75
5.6	AUDITOR – ARCHITECTURAL COMPONENTS	77
6	SECURITY REFERENCE ARCHITECTURE: A METHODOLOGY OF ORCHESTRATING A CLOUD ECOSYSTEM	80
6.1	ORCHESTRATION METHODOLOGY OVERVIEW	80
6.2	CLOUD ECOSYSTEM ORCHESTRATION USE CASE	81
6.2.1	<i>Use Case Description</i>	81
6.2.2	<i>Cloud Solution Analysis and High-Level Design</i>	82
6.2.3	<i>Risk Assessment Overview</i>	86
6.2.4	<i>Cloud Ecosystem High-Level Architecture</i>	89
6.2.5	<i>Service Agreement Overview</i>	89
7	SECURITY REFERENCE ARCHITECTURE: CLOUD DEPLOYMENT MODES	92
8	GLOSSARY AND ACRONYMS	93
9	REFERENCES	95
APPENDIX A: ACTIVE MEMBERS		97
10	ANNEX A: TRUSTED COMPUTING INITIATIVE REFERENCE ARCHITECTURE	98
11	ANNEX B: MAPPING TO SP 800-53 SECURITY CONTROL FAMILIES	99
12	ANNEX C: GENERIC HEAT MAP	100
13	ANNEX D: AGGREGATED DATA	101
13.1	ACTORS-BASED DATA AGGREGATION	101
13.2	SERVICE-BASED ECOSYSTEM-LEVEL DATA AGGREGATION	124
14	ANNEX E: MAPPING OF THE ARCHITECTURAL COMPONENTS	151
15	ANNEX F: ECOSYSTEM ORCHESTRATION - SECURITY INDEX SYSTEM	175
15.1	USE CASE SUMMARY	175
15.2	SECURITY INDEX SYSTEM	179
15.3	ASIS HEAT MAP	197

List of Figures

FIGURE 1: NIST CLOUD COMPUTING SECURITY REFERENCE ARCHITECTURE APPROACH.....	16
FIGURE 2: RISK MANAGEMENT FRAMEWORK (NIST SPECIAL PUBLICATION 800-37 REV 1).....	18
FIGURE 3: COMPOSITE CLOUD ECOSYSTEM SECURITY ARCHITECTURE	22
FIGURE 4: INTERMEDIARY CLOUD PROVIDER EXAMPLE	24
FIGURE 5: CLOUD BROKER EXAMPLE	27
FIGURE 6: EXAMPLE OF SERVICES AVAILABLE TO A CLOUD CONSUMER (NIST SP 500-292)	29
FIGURE 7: SECURITY CONSERVATION PRINCIPLE (ORIGINAL GRAPHIC FROM NIST SP 800-144).....	31
FIGURE 8: SECURITY REFERENCE ARCHITECTURE CONSTRUCTS AND INSTANCES	32
FIGURE 9: SECURITY COMPONENTS OVERVIEW	34
FIGURE 10: SECURITY COMPONENTS OVERVIEW	37
FIGURE 11: SECURITY COMPONENTS FOR TECHNICAL BROKER & INTERMEDIARY PROVIDER.....	39
FIGURE 12: LEGEND OF THE GENERIC HEAT MAP	43
FIGURE 13: NIST CLOUD COMPUTING REFERENCE ARCHITECTURE (UPDATED).....	44
FIGURE 14: FORMAL MODEL – SECURITY REFERENCE ARCHITECTURE	46
FIGURE 15: SRA – CLOUD CONSUMER.....	48
FIGURE 16: SECURE CLOUD ECOSYSTEM ORCHESTRATION.....	53
FIGURE 17: SECURE FUNCTIONAL LAYERS.....	53
FIGURE 18: SRA – CLOUD PROVIDER	55
FIGURE 19: SECURE SERVICE ORCHESTRATION – STACK DIAGRAM.....	56
FIGURE 20: SECURE DEPLOYMENT AND SERVICE LAYERS	57
FIGURE 21: SECURE RESOURCE ABSTRACTION AND PHYSICAL RESOURCE LAYERS	58
FIGURE 22: SECURE CLOUD SERVICE MANAGEMENT – STACK DIAGRAM.....	60
FIGURE 23: SRA – CLOUD BROKER	64
FIGURE 24: CLOUD BROKER – ARCHITECTURAL COMPONENTS	66
FIGURE 25: TECHNICAL BROKER – ARCHITECTURAL COMPONENTS	67
FIGURE 26: BUSINESS BROKER – ARCHITECTURAL COMPONENTS	69
FIGURE 27: SECURE CLOUD ECOSYSTEM ORCHESTRATION – BROKER STACK DIAGRAM	70
FIGURE 28: SECURE CLOUD SERVICE MANAGEMENT – BROKER STACK DIAGRAM	72
FIGURE 29: SRA – CLOUD CARRIER	76
FIGURE 30: SRA – CLOUD AUDITOR.....	77
FIGURE 30: SRA – CLOUD AUDITOR	79
FIGURE 31: SECURE CLOUD ECOSYSTEM ORCHESTRATION – ACTORS INTERACTIONS.....	80
FIGURE 32: NIST RISK MANAGEMENT FRAMEWORK AND THE FEDRAMP A&A PROCESS.....	88
FIGURE 33: SERVICE AGREEMENT MIND MAP	90

List of Tables

TABLE 1: SRA DATA COLLECTION FORM WITH THE SET OF SECURITY COMPONENTS 35
TABLE 2: TCI REFERENCE ARCHITECTURE - DOMAINS AND SERVICE LAYERS 40
TABLE 3: NIST 800-53 CONTROL FAMILIES – ASSIGNED COLOR CODES 41
TABLE 4: SECURITY COMPONENT - VECTOR GENERATION 42
TABLE 5: SECURITY INDEXES SYSTEM 84
TABLE 6: CLOUD ACTORS’ ARCHITECTURAL COMPONENTS 151

DRAFT

EXECUTIVE SUMMARY

NIST, along with other agencies, was tasked with a key role and specific activities aimed at accelerating the adoption of cloud computing, including the delivery of the NIST Technology Roadmap and the publication of other Special Publications that address the reference architecture, definitions and security aspects 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, *Cloud Computing Reference Architecture*
- NIST SP 500-293, *US Government Cloud Computing Technology Roadmap Volume I, 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)* and

This document was developed as a collective effort of 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 I, High-Priority requirements to Further USG Agency Cloud Computing Adoption* which highlights the concerns around the protection and control of cloud *Consumer* data. This document introduces the NIST Cloud Computing Security Reference Architecture, providing a comprehensive formal model derived as security overlay to the NIST Special Publication 500-292: *NIST Cloud Computing Reference Architecture*, an associated set of *security components* and a methodology of using the formal model and the *security components* in orchestrating a secure cloud Ecosystem by applying the Risk Management Framework described in NIST SP 800-37: “*Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*”.

The emphasis of this document is on a risk based approach to derive responsibility for implementing controls for each cloud Actor involved in the life cycle of the cloud Ecosystem. 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*. The 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

1.1 BACKGROUND

The National Institute of Standards and Technology (NIST) has been designated by the Federal Chief Information Officer with the technical leadership for US government (USG) agency efforts related to the adoption and development of cloud computing standards. The goal is to accelerate the federal government's adoption of *secure* and effective cloud computing to reduce costs and improve services. The NIST strategy is to build a USG Cloud Computing Technology Roadmap which focuses on the highest priority USG cloud computing security, interoperability and portability requirements, and to 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 review the security related issues 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 the SP 500-292: NIST Reference Architecture (RA) with a formal model and identifies the core-set of *security components* recommended to be implemented 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 for ensuring a consistent approach in identifying the security requirements the procurement offices should identify and address in order to acquire a cloud service with a similar or higher security level than the original data center.

1.2 OBJECTIVES

In the cloud computing model, the primary focus is on the economic posture that provides higher quality and faster services at a lower cost to the users. In the traditional IT service delivery model, there is a large emphasis on procuring, maintaining and operating the necessary hardware and related infrastructure. However, the migration of the agency's operations to a cloud computing environment does not inherently provide for the same level of security and compliance as mandated for the USG agencies. The ability to comply with any business, regulatory, operational or security requirements is a direct result of the service and deployment model adopted by the agency and the architecture, deployment and management of the resources in scope.

Understanding the relationships and inter-dependencies between the cloud computing deployment methods and the different service models is critical to understanding the cloud computing security risks. The differences in methods and responsibilities for securing the different cloud service models and deployment methods are challenging endeavors for the consumers that need to perform a thorough risk assessment and to accurately identify the security controls necessary for maintaining the security of agency's information and to preserve the security level of the agency's operations post migration to the cloud.

The purpose of this document is to define a Security Reference Architecture – a framework that:

- identifies a core-set of *security components* that can be implemented in a Cloud Computing 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 model and elected service type;
- defines a security-centric formal architectural model that adds a security layer to the current NIST Reference Architecture defined in the SP 500-292;
- provides several approaches for analyzing the aggregated data; and
- presents an example of securely orchestrating a Cloud Ecosystem for a unified messaging system migrated to a Public SaaS cloud by introducing a Security Index System for the confidentiality, integrity and availability of each component in the process of prioritizing the implementation of the core-set of *security components*..

The information provided in this document is presented in a manner that is familiar to federal stakeholders – i.e. referencing the NIST SP 800-53 control families and to private sector offering cloud services – i.e. leveraging on the Cloud Security Alliance’s Trusted Computed Initiative – Reference Architecture (see <https://research.cloudsecurityalliance.org/tci/>).

The NIST Security Reference Architecture is an elastic, dynamic framework layered over the NIST Reference Architecture and taking in consideration:

1. The cloud computing service models: IaaS, PaaS, SaaS;
2. The cloud deployment methods: Public, Private, Community, Hybrid;
3. The NIST RA’s defined actors: Consumer, Provider, Broker, Carrier, Auditor

The five actors are collaborating parties building a fully functional, secured cloud ecosystem. Cloud Consumer performs a security and risk assessment for each use case of data migrated to the cloud and by electing the cloud deployment model and the service model, the Consumer identifies the cloud ecosystem model and the corresponding instance of the Security Reference Architecture model that best suits the agency’s needs in terms of functionality, cost, and security capabilities.

By leveraging on the NIST Cloud Computing Security Reference Architecture, agencies reduce cost by avoiding duplication of efforts. For example, a Cloud Consumer electing a Public IaaS cloud service for their data migrated to the cloud may start with the Security Reference Architecture model described in this document and adopt the set of *security components* identified for the Public IaaS instance of the Security Reference Architecture model.

The Security Reference Architecture document is not a comprehensive guide of security requirements for all possible instances of cloud-type, data, and service-model. The NIST Security Reference Architecture document aims to identify only a core-set of *security components* that

should be implemented by each Cloud *Actor* defined in the NIST Reference Architecture specification.

1.3 STRUCTURE OF THE DOCUMENT

This document is organized into seven sections supported by six annexes which present the reader with a logical and, when necessary, step-wise approach to evaluating cloud based services using a Risk Management Framework approach.

The first section deals with the introduction to the document and its proposed use by cloud Actors.

The second section presents a comprehensive overview of the Security Reference Architecture, of the Risk Management Framework (RMF) as outlined in NIST Special Publication 800-37, and presents the assumptions and clarifications regarding the cloud Actors' roles and responsibilities adopted for the purpose of this document.

The third section introduces the core-set of *security components* derived from the Cloud Security Alliance's Trusted Computing Initiative Reference Architecture.

The fourth section outlines the data analysis methodology used to populate the responsibility matrix by Actor which assigns accountability for implementing each *security component*. This section discusses data collection, aggregation and validation as initial steps of the data analysis methodology, and maps the derived *security components* from the matrix to the NIST SP 800-53 security control families. The data analysis methodology is completed by illustrating the generation of a heat map for particular cloud deployment models (e.g. Public cloud) which highlights the level of control exerted by the Actors.

The fifth section introduces the NIST Security Architecture formal model and discusses the architectural components the formal model for each cloud Actor.

The sixth section describes the orchestration a secure cloud Ecosystem as defined by those interactions between the cloud *Actors* for implementing and integrating the *security components*. To better illustrate the interaction 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 orchestrate a secure cloud Ecosystem, and to determine the high-level cloud architecture that meets the cloud Consumer's security requirements. The section concludes with the negotiation of the contractual terms and agreements of Service Level Agreements (SLA).

The seventh section is currently a place holder for the final discussion of the cloud deployment modes.

Annex A depicts a set of *security components* and how to use it for a particular cloud model is introduced in detail in Section 3.

Annex B depicts the mapping or pairing of the *security components* to the NIST 800-53 security control families using the color code presented in Table 3.

Annex C is the Generic Heat Map of Actor responsibilities for implementing security controls

Annex D is the Data Aggregation table which indicates 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-Base Ecosystem-Level.

Annex E of this document presents a matrix that maps the high-level security components, and with them the SP 800-53 security control families, to the architectural components and sub-components defined for each cloud Actor.

Annex F presents the SIS for the CIA security triad and the ASIS used to prioritize the *security components* for the Unified Messaging System use case. The SIS example given in this document is not provided as guidance for any UMS migration to the cloud

1.4 USING THE DOCUMENT

Federal agencies may use the information presented in this document by following the steps presented below:

- **Describe** the service that should be migrated to the cloud,
- **Identify** the necessary capabilities,
- **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 the 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 FIPS 199 and FIPS 200, respectively.

Note: As defined in the Federal Information Processing Standard (FIPS) 200, a *low-impact system* is an information system in which all three of the security objectives are low. A *moderate-impact system* is an information system in which at least one of the security objectives is moderate and no security objective is greater than moderate. And finally, a *high-impact system* is an information system in which at least one security objective is high.

- **Analyze and select** the most appropriate instance of a cloud Ecosystem by identifying the cloud composite architecture such as the cloud deployment model and the cloud service type:
 - 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.
- **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 (a.k.a. system migrated to the cloud) by:
 - Identifying and customizing the core-set of *security components* to the assessed impact level of the system migrated to the cloud by applying a Security Index System as introduced in Section 6 below;
 - Identifying the NIST SP 800-53 security controls necessary to be implemented for each security component;
 - Applying scoping considerations to the remaining baseline *security components* and associated controls;
 - Identifying, when necessary, additional compensating *security components* and security controls;
 - Assigning specific values to organization-defined security parameters via explicit assignment and selection statements;
 - Supplementing baselines with additional *security components* and control enhancements, if needed; and
 - Providing additional specification information for *security components* implementation.

A more concrete example of how a new cloud Ecosystem for a Unified Messaging System can be orchestrated by leveraging the information presented in this document is provided in Section 6.2 below.

2 SECURITY REFERENCE ARCHITECTURE: OVERVIEW

The U.S. Chief Information Officer Vivek Kundra emphasizes in the “Federal Cloud Computing Strategy” (Feb 8, 2011) 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.*”

The approach to securing the cloud 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 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 Cloud Security 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 the cloud characteristics such as:

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

The above-listed cloud computing characteristics often present to an agency different security risks than the traditional information technology solutions, altering the agency’s security posture. To preserve the post-migration security level of their data in the Cloud, agencies need to identify all cloud-specific risk-adjusted security controls or components in advance and request from the cloud Providers through contractual means and Service Level Agreements (SLAs) to have all identified security components and controls fully and accurately implemented.

In this document we present the NIST Cloud Computing Security Reference Architecture (SRA) formal model derived from the NIST Special Publication 500-292: NIST Cloud Computing Reference Architecture, an associated set of security components and a methodology of using the formal model and the security components to orchestrate a secure cloud Ecosystem. To identify the set of security components we leveraged the Cloud Security Alliance (CSA) Trusted Computing Initiative - Reference Architecture (TCI-RA). Figure 1 below depicts the NIST Cloud Computing Security Reference Architecture approach described in detail in this document.

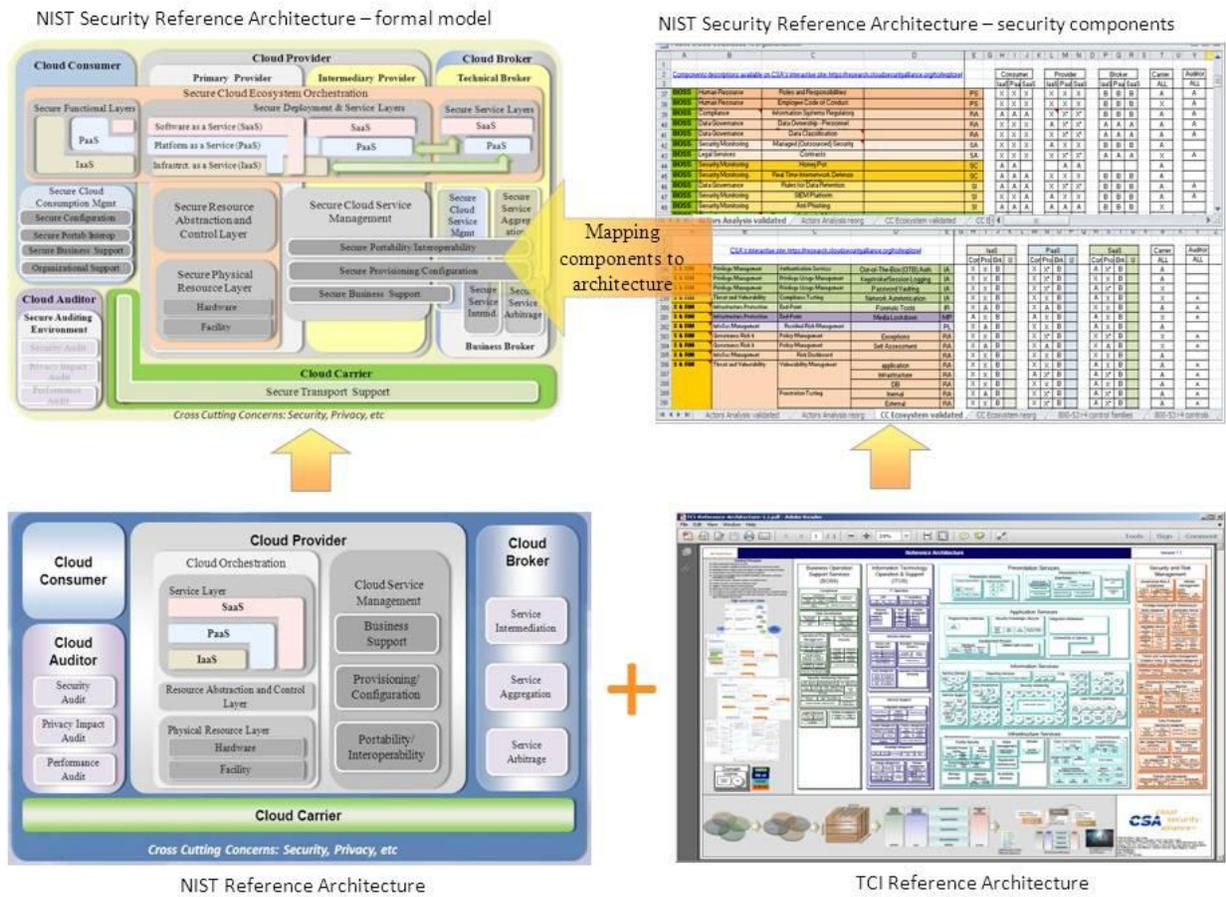


Figure 1: NIST Cloud Computing Security Reference Architecture Approach

2.1 RISK MANAGEMENT

The Federal CIO’s “Federal Cloud Computing Strategy” also stresses that “*Federal Government IT programs have a wide range of security requirements. Federal Information Security Management Act (FISMA) requirements include: compliance with Federal Information Processing Standards agency specific policies; Authorization to Operate requirements; and vulnerability and security event monitoring, logging, and reporting. It is essential that the decision to apply a specific cloud computing model to support mission capability considers these requirements. Agencies have the responsibility to ensure that a safe, secure cloud solution is available to provide a prospective IT service, and should carefully consider agency security needs across a number of dimensions*”.

The NIST 500-293: “U.S Government Cloud Computing Technology Roadmap (Vol. 1)” identifies in the 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*.

The assurance or confidence that the risk from 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.

The correct implementation of the security controls implemented by the cloud Provider or cloud Broker should be tested during an Assessment and Authorization (A&A) process for cloud Ecosystems in a similar way any other federal information system is assessed and authorized for compliance with the Federal Information Security Management Act (FISMA) of 2002, H.R. 2458, Title III – *Information Security* and of the Office of Management and Budget (OMB) Circular A-130, Section 8b (3), *Securing Agency Information Systems*. FISMA and OMB policy requires cloud Providers that handle federal information or operating information systems on behalf of the federal government 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 Risk Management Framework and associated NIST security standards, special publications and guidelines.

The Risk Management Framework provides a structured, yet flexible approach for managing the portion of risk resulting from the incorporation of information systems into the mission and business processes of the organization.

Consumers can require cloud Providers to implement all steps in the Risk Management Framework described in NIST SP 800-37: *"Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach"*, Revision 1, with the exception of the security authorization step, which remains an inherent federal responsibility that is directly linked to the management of risk related to the use of cloud services.

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standard framework for assessing and authorizing cloud Providers using a standardized approach to security assessment, authorization, and continuous monitoring. The Federal Risk and Authorization Management Program (FedRAMP) maintains an online site with requirements, templates, and supporting materials for agencies and cloud vendors at <http://www.FedRAMP.gov>. US Government agencies are required to accept only cloud Providers successfully assess and authorized (A&A) by the FedRAMP. FedRAMP process assess if a cloud Provider adheres to the minimum security requirements and implements the identified security controls for low and moderate impact level systems.

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. Security risk is addressed by incorporating the Risk Management Framework (RMF) as part of 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 Service Level Agreements (SLAs) which are intrinsic parts of the Service Agreements (SA) between the cloud Consumer and cloud Provider and/or Broker. Contractual terms should include, for example, 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 Section 6.2 of this document.

Agencies may require cloud Providers to implement all steps in the RMF except the security authorization step (see Figure 1), which remains an inherent Federal responsibility directly linked to managing the information security risk related to the use of external information system services.

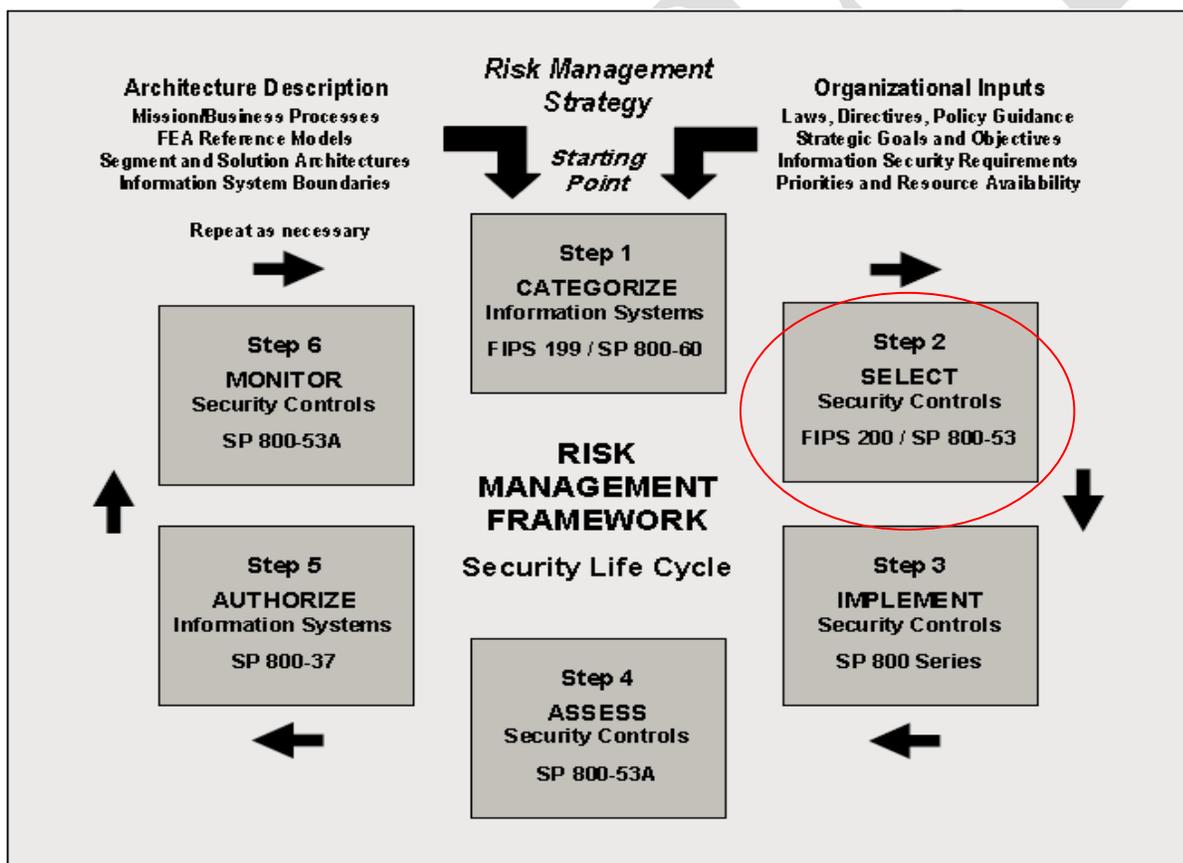


Figure 2: Risk Management Framework (NIST Special Publication 800-37 Rev 1)

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

of helpful online documentation for agencies, including a best practices guide for Creating Effective Cloud Computing Contracts for the Federal Government.

US Government cloud Consumers should require cloud Providers and Brokers to present appropriate evidence that demonstrates their compliance with the RMF in protecting Federal information. While the framework provides steps for the life-cycle of information security, this document is primarily focused on Step 2 of the RMF shown below.

The Risk Management Framework (RMF), illustrated in Figure 2 above, 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.

The Risk Management Framework's steps include:

Step 1: Categorize the information system and the information processed, stored, and transmitted by that system based on an impact analysis. [FIPS 199](#) provides security categorization guidance for non-national security systems. [NIST Special Publication 800-60](#) provides implementation guidance on the assignment of security categories to information and information systems. [Committee on National Security Systems \(CNSS\) Instruction 1253](#) provides similar guidance for national security systems.

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](#) provides the minimum security controls defined in the low, moderate, and high security control baselines. [NIST Special Publication 800-53](#) provides security control selection guidance for non-national security systems. [Committee on National Security Systems \(CNSS\) Instruction 1253](#) provides similar guidance for national security systems.

Step 3: Implement the security controls and describe how the controls are employed within the information system and its environment of operation. [NIST Special Publication 800-70](#) (Revision 2) 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 Special Publication 800-53A](#) provides security control assessment procedures for security controls defined in [NIST Special Publication 800-53](#).

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 Special Publication 800-37 Revision 1](#) provides guidance on authorizing 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 Special Publication 800-37 Revision 1](#) 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 operated status. [NIST Special Publication 800-53A](#) provides continuous monitoring guidance for the security controls defined in [NIST Special Publication 800-53](#).

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

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. Step 2 of the Risk Management Framework depicted in Figure 2 requires agencies to perform three tasks to accomplish the proper selection of security controls. Those tasks include:

TASK 2-1: Identify the security controls that are provided by the organization as common controls for organizational information systems and document the controls in a security plan (or equivalent document).

TASK 2-2: Select the security controls for the information system and document the controls in the security plan.

TASK 2-3: Develop a strategy for the continuous monitoring of security control effectiveness and any proposed or actual changes to the information system and its environment of operation.

As previously mentioned, this document is focused on task 2.1, which requires the agency to identify the proper *security components* and associated security controls using five security indexes to assess the confidentiality, integrity and availability of systems and data migrated to the cloud. 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 provides information to agencies in terms of each cloud *Actor's* responsibilities, for each cloud deployment model and service type, in applying each identified *security component* as outlined in this document.

For example, a Consumer planning the migration of their particular agency's data to a Public cloud may, upon completion of the risk assessment analysis, follow the steps presented in Section 1.4 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 migrated to the cloud.

Based upon the deployment model and the service type elected, the agency would retain and take 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 and may require in the SLA and other appropriate contractual documents, from the IaaS Provider to implement the *security components* identified in the NIST Security Reference Architecture for a Provider of a Public IaaS, augmented with use-case specific supplemental *security components* and controls.

The RMF also works hand-in-hand with the National Strategy for Trusted Identities in Cyberspace (NSTIC) Identity Ecosystem as it develops. This Identity Ecosystem is 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. NSTIC is actively working across industry, academia, and government to raise the level of trust associated with identities involved in online transactions.

2.2 ASSUMPTIONS AND CLARIFICATIONS

This section is provided to bring clarifications to the roles and responsibilities of the cloud Actors described in the NIST Cloud Computing Reference Architecture (NIST SP 500-292) and to list the assumptions made regarding their core operational responsibilities that have associated security requirements.

To facilitate the discussion, we present in Figure 3 a composite cloud Ecosystem Security Architecture that graphically depicts the cloud *Actors* involved in orchestrating a cloud Ecosystem. We present different possible compositions for each cloud service type.

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 the data within the cloud is assigned by the NIST SP 500-292: NIST Cloud Computing Reference Architecture document to the cloud Provider, leaving the cloud Carrier with the role and responsibility of securely transporting the data in transit from the end-user to and from the Cloud. Additional assumptions and clarifications are provided in the following sub-sections for each cloud *Actor*.

It is important to note that the diagram is not representing the cloud Carrier involved in the cloud Ecosystem because the service provided by the Carrier, the data transport, can be done using different vehicles from dedicated communication channels to the open Internet that involves 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.

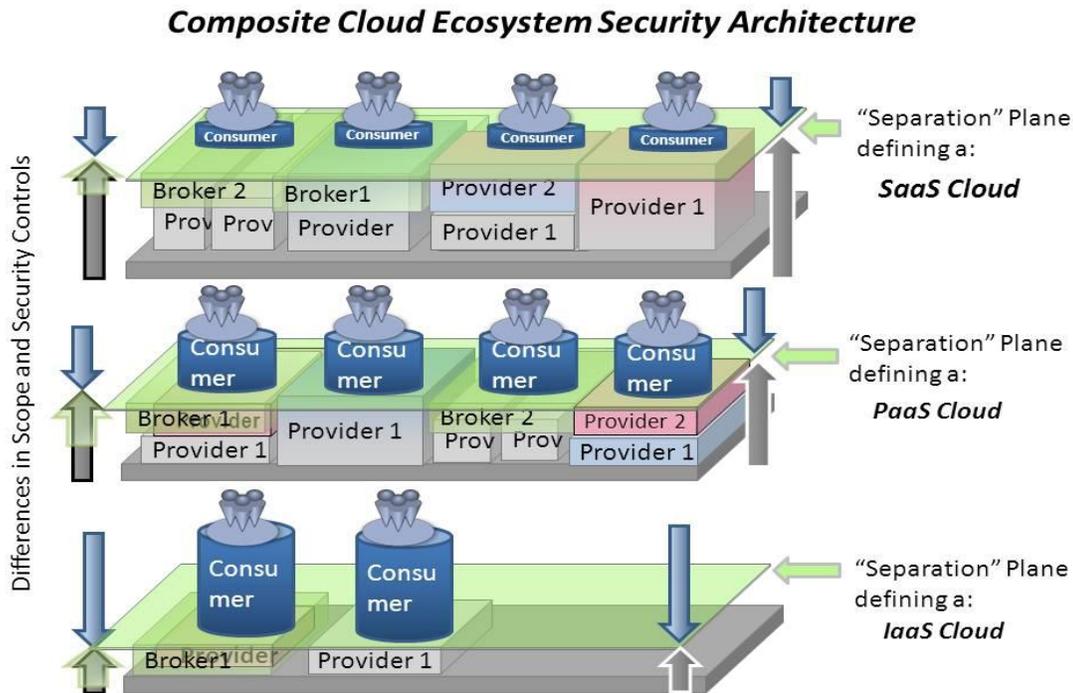


Figure 3: Composite Cloud Ecosystem Security Architecture

In a cloud Ecosystem that serves the needs of the US Government, it is the Consumer's (Federal agency) responsibility to determine, based upon the risk analysis performed, what is the full set of security controls that must be mandated and implemented to secure the operations and the data migrated to the cloud. It is 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 used. The Consumer is also responsible to implement the security controls identified as necessary to be implemented by the Consumer. The union of all subsets of security controls must result in a set of controls that fully secure the cloud ecosystem.

It is the role 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 Analysis, Risk Assessments, Vulnerability Assessments, Business Continuity Plans, Disaster Recovery Plans
- Physical and Environmental Security Policy, User Account Termination Procedures, Contingency Plan, including test protocols, Incident Reporting and Response Plan, including test protocols, Emergency Response Plan, Facility Layout

- Compliance with National and International/Industry Standards on Security
- Visual Walk-Through Inspection of the Provider's facility, Security Infrastructure, Human Resources, Physical Security, Environmental Security
- Restoration plan incorporating and quantifying the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for services.
- Transparency into the security posture of the cloud Providers, Brokers and Carriers.

2.2.1 CLOUD CONSUMER

A Cloud Consumer is the person or organization that maintains a business relationship with, and uses service 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, sets up service contracts with the cloud Provider directly or using a cloud Broker's services and before effectively using the service. Carrier services may be separately set up by the Consumer, or be integrated into the service offered by the cloud Provider or 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 fulfilled by a cloud Provider and/or cloud Broker.

If the cloud Consumer is a US Government agency, the migration of any operations to the Cloud does not void the mandate of compliance to the Federal Information Security Management Act (FISMA) of 2002, H.R. 2458, Title III – *Information Security* and of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), *Securing Agency Information Systems*, depending upon which services or applications are migrated to the Cloud. Therefore, the Consumers are ultimately accountable for the security and privacy of data held by a cloud Provider on their behalf, and are required to identify the set of security controls that should be implemented to protect data. The security controls should then be implemented by the cloud Consumer, cloud Provider, cloud Carrier and cloud Broker when 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.

2.2.2 CLOUD PROVIDER

A Cloud Provider is an entity responsible for making a service available to Cloud Consumers. A Cloud Provider acquires and manages the computing infrastructure required for providing the services, runs the cloud software that provides the services, and makes arrangement to deliver the cloud services to the Cloud Consumers through network access.

A Cloud Provider’s activities can be described in five major areas; a cloud Provider conducts its activities in the areas of service deployment, service orchestration, cloud service management, security, and 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 additional layer of functionality in a transparent way (see Section 2.2.3 for more information). Figure 2 above depicts the two major types of Providers, as identified in the NIST RA:

1. Primary Provider (labeled “Provider 1” in the Cloud Composite Architecture - Figure 2);
2. Intermediary Provider (labeled “Provider 2” in the Cloud Composite Architecture - Figure 2).

2.2.2.1 INTERMEDIARY CLOUD PROVIDER EXAMPLE

An Intermediary Provider has the capability to interact with other cloud Providers without offering visibility or transparency into who are the Primary Providers. Intermediary Provider uses the Primary Provider as invisible components of its own service, which it presents to the customer as an integrated offering. From a security perspective, all security services and components required of a Cloud Provider is also required of an intermediary Cloud Provider.

Figure 4 below shows a simple example of an Intermediary Provider interaction.

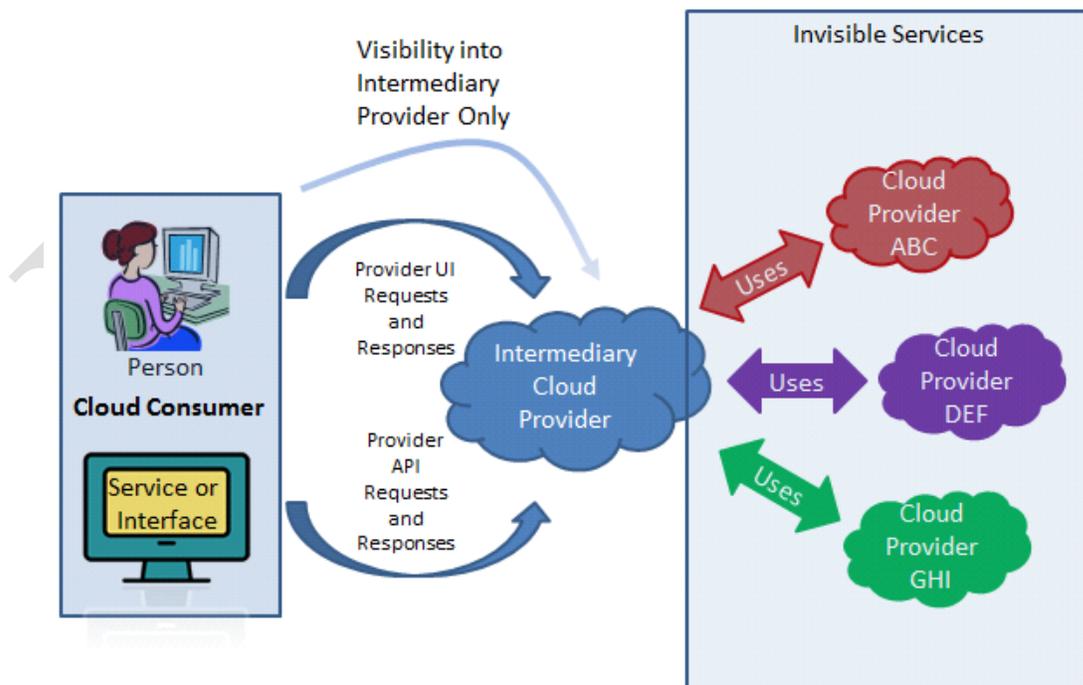


Figure 4: Intermediary Cloud Provider Example

2.2.3 CLOUD BROKER

The NIST Cloud Computing Reference Architecture document, NIST SP 500-292, 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. As cloud computing evolves, the integration of cloud services can be too complex for cloud consumers to manage. 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, become the ability to provide a single consistent interface to multiple differing Providers, whether the interface is for business or technical purposes, and the *transparency* into the process of who is providing the services in the background.

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, but rather indicates that the cloud Broker, in addition to providing extra functionality, allows the cloud Consumer to have particular level of information into the cloud Provider services, and, when necessary, direct communication with the Provider, in the orchestration of the cloud Ecosystem and during operational process. Herein, this is referred to as the “*transparency* into the process of who is providing the cloud services in the background”, as noted above.

In general, cloud Brokers provide services in three categories:

- **Aggregation:** A cloud broker combines and integrates multiple services into one or more new services. The broker provides data integration and ensures the secure data movement 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 agencies depending on 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.

The purpose of this section is to bring clarity to the definition provided by in NIST SP 500-292, to give a better understanding of the roles and types of services that a cloud Broker may provide to cloud Consumers, and to distinguish the differences between a cloud Broker and a cloud Provider.

2.2.3.1 DIFFERENTIATING BUSINESS AND TECHNICAL BROKER SERVICES

An organization that acts as a cloud Broker may provide the following services:

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

A cloud Broker that only provides business and relationship services, plays the role of a Business Broker and does not have any contact with the cloud Consumer's data migrated to the cloud, with the Consumer's operational processes in the cloud or Consumer-based cloud artifacts such as images, volumes or firewalls.

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

A cloud Broker provides a single interface across multiple cloud service Providers. Furthermore, a Cloud Broker will always allow the cloud Consumer to have a particular level of transparency and interaction if necessary, into whom the target cloud Providers are. Combinations of technical and business brokerage can be carried out by the same entity.

A cloud Broker will always allow the cloud Consumer a particular level of transparency into the identity of the target cloud Providers. An entity that offers additional layers of functionality without allowing for transparency into their underlying cloud Providers will be considered an intermediary cloud Provider and not a cloud Broker.

In Figure 3 above, the composite cloud Ecosystem architecture exhibits the three different types of cloud services that are available to Consumers. There is a particular emphasis on the delineation of transparency and aggregation between a cloud Technical Broker (Broker 2 in Figure 3) and Intermediary Provider.

2.2.3.2 A CLOUD BROKERAGE EXAMPLE

Figure 5 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 are fulfilled:

- Aggregation - the cloud Consumer deals with multiple providers through a single broker interface.
- Transparency - the cloud Consumer retains visibility into the cloud service providers they use through the broker, either through the broker or directly.

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

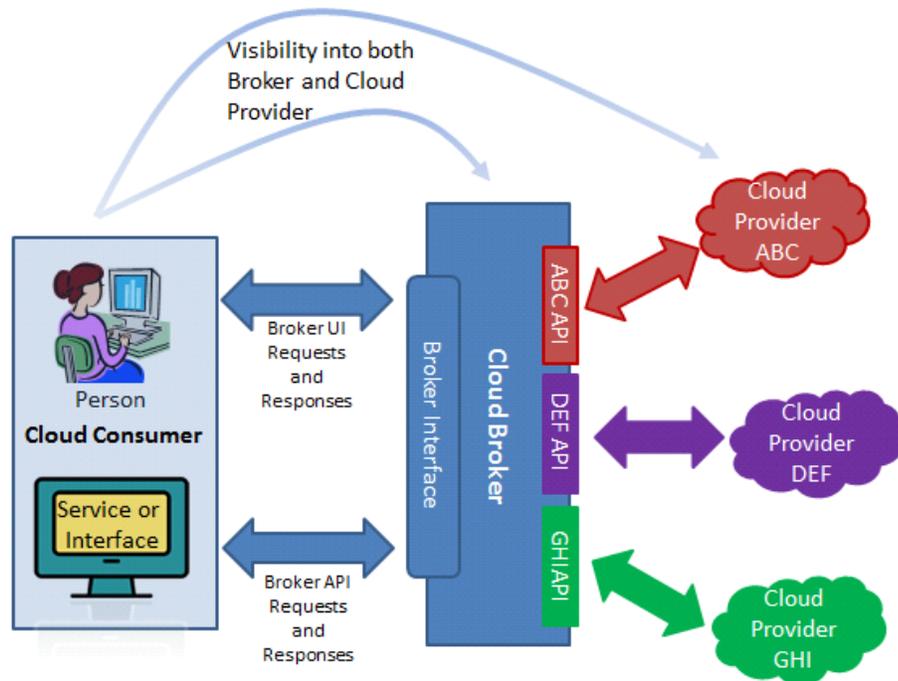


Figure 5: Cloud Broker Example

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.

2.2.4 CLOUD CARRIER

A cloud Carrier acts as an intermediary that provides connectivity and transport of cloud services between cloud Consumers and cloud Providers. Cloud Carriers provide access to Consumers through network, telecommunication and other access devices. For example, cloud Consumers can obtain cloud services through network access 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, where 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 services consistent with the level of SLAs offered to cloud Consumers, and may require the cloud Carrier to provide dedicated and secure connections between cloud Consumers and cloud Providers.

The security concerns of the Carrier role included consideration for the exposures and threats that would be present in the transmission of data to and from a cloud structure. Though it would be nice to think of that as a closed system, due to the evolutionary nature of the Internet and the development over time of methods for signal transmission, there are inherent vulnerabilities. Security breaches at these juncture and insertion points present a challenging problem for the consideration of security in a cloud or non-cloud transmissions for Carriers. For these reasons the Carrier was attributed with security control points that span of the systems they manage, but also included testing and risk management of those preventative tasks that would be expected to reduce such vulnerabilities. Dedicated lines between communication endpoints can be offered by carriers, including interstate and international dedicated lines.

Based on the NIST Reference Architecture description of the Carrier's roles and the above clarifications, we concluded that the Carrier's security responsibilities do not vary with the type of service model selected for the cloud ecosystem.

2.2.5 CLOUD AUDITOR

A cloud Auditor is a party that can conduct independent assessment of cloud services, information system operations, performance, privacy impact and security of the various cloud service types and deployment models. A cloud Auditor performs an independent examination of cloud service controls with the intent to express an opinion thereon. Audits verify conformance to standards through review of objective evidence. A cloud Auditor can evaluate the services provided by a cloud Provider in terms of security controls, privacy impact, performance, etc.

Security controls are the management, operational, and technical safeguards or countermeasures employed within an organizational information system to protect the confidentiality, integrity, and availability of the system and its information. For IT or IS security auditing, 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 the 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 Security Reference Architecture document acknowledges the importance of the auditing process, the complexity of an audit and the wide variation of the audited targets, the document restricts the analysis of the cloud Actor from the security perspective only to the set of the 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 their report findings 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.

2.2.6 CLOUD ECOSYSTEM

In the cloud computing Ecosystem, the cloud Consumer has three different service models to choose from: Infrastructure as a Service, Platform as a Service, and Software as a Service.

Figure 6 below presents some examples of cloud services available to a cloud Consumer (For more details, see SP 500-292: NIST Cloud Computing Reference Architecture, Appendix B: Examples of Cloud Services).

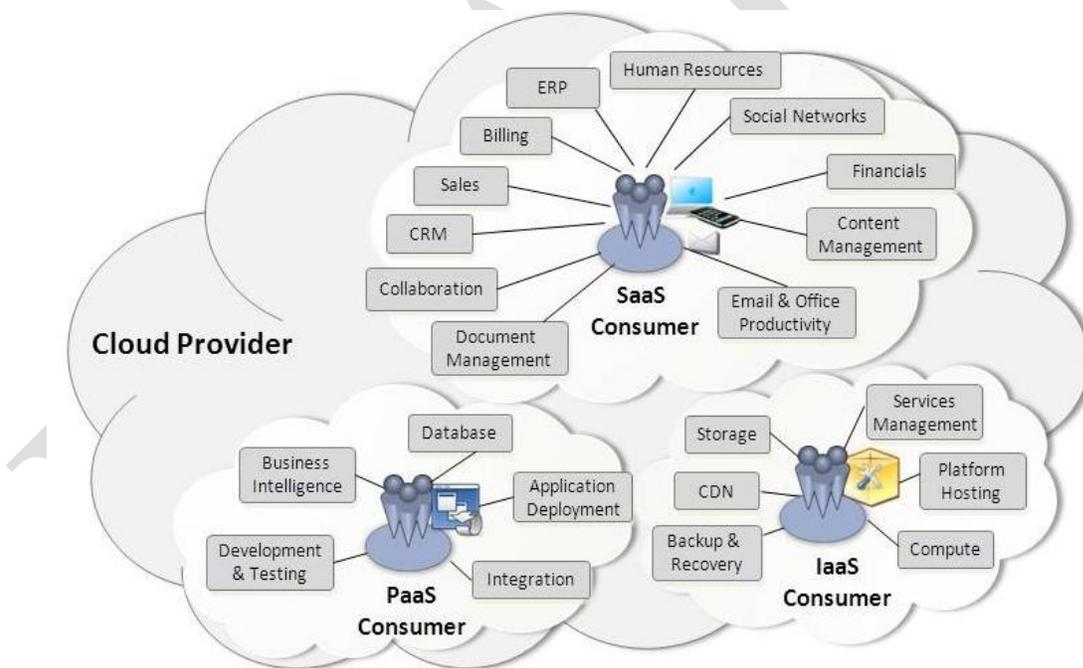


Figure 6: Example of Services Available to a Cloud Consumer (NIST SP 500-292)

As mentioned previously 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. When selected

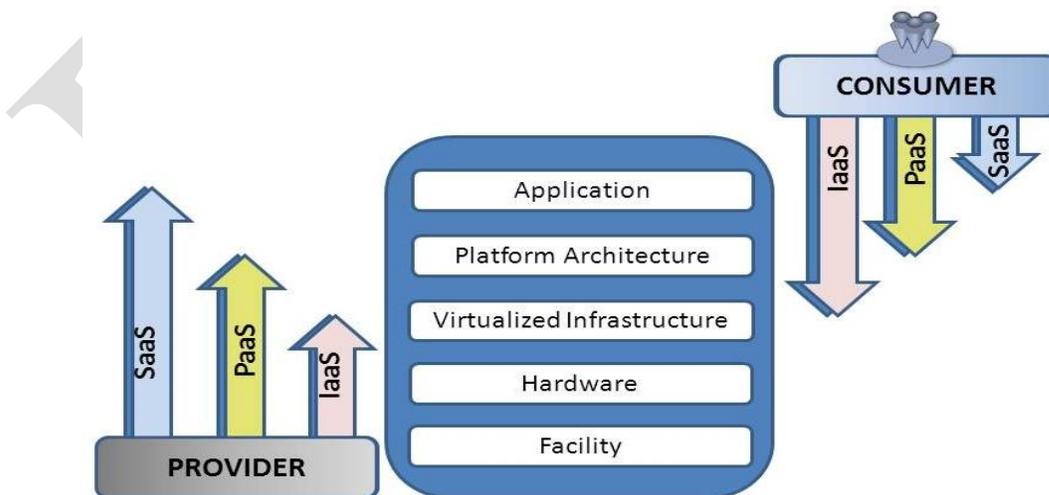
security components and controls cannot be directly implemented by the Consumer, then a shared responsibility for implementation exists with the cloud Provider and cloud Technical Broker even though components and controls specification and oversight accountability ultimately rests with the cloud Consumer.

2.2.7 SECURITY CONSERVATION PRINCIPLE

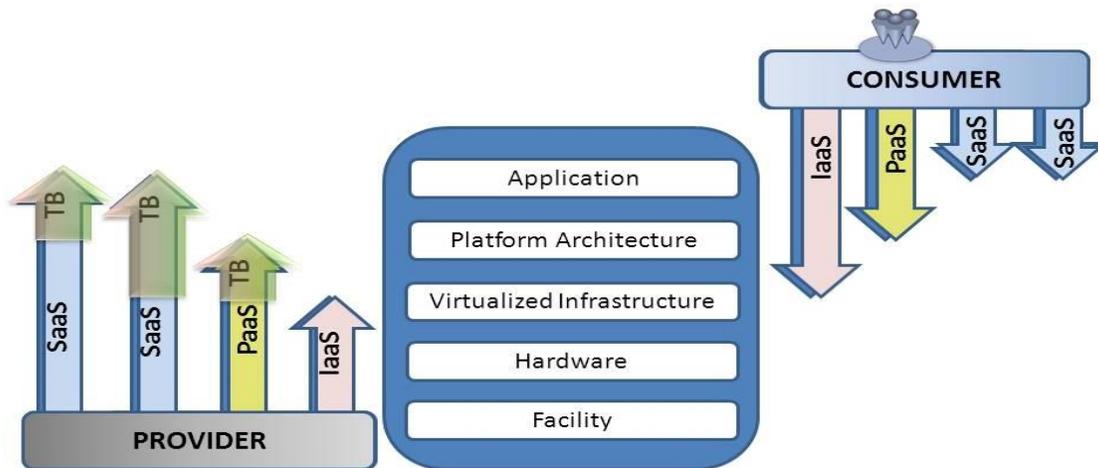
Figure 7 below graphically depicts the *Security Conservation Principle* for the cloud Ecosystem. The main idea behind this principle is that, for a particular service migrated to the cloud, the super set of *security components* and controls necessary to be implemented cumulatively by all cloud *Actors* involved in the Ecosystem is invariant with the cloud model and service type. For the sake of brevity diagram a) in Figure 7 identifies only the major cloud *Actors*: Consumer and Provider, so we highlight the shifting of the responsibility on implementing particular security components from the Consumer to the Provider as the scope shifts from IaaS to PaaS and SaaS cloud service types while the cumulative set or components remains invariant.

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 7 illustrates the same concept with random examples of technical Broker functionality added.

The two diagrams below also indicate that the cloud Consumer’s responsibility of implementing *security components* is higher for an IaaS service type and decreases for a PaaS service type reaching minimum for a SaaS service type, while for the cloud Provider and Broker combined, the responsibility of implementing *security components* increases rapidly from IaaS to PaaS and SaaS respectively.



a)



Legend: TB = cloud technical Broker

b)

Figure 7: Security Conservation Principle (original graphic from NIST SP 800-144)

2.3 OUR APPROACH

The NIST Cloud Computing Security Reference Architecture (NCC-SRA) defined in this document is developed using a three dimensional approach using the following constructs:

- The three types of service models defined in the NIST Reference Architecture: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS);
- The four types of deployment models defined in the NIST Reference Architecture: Public, Private, Hybrid, and Community;
- The five Actors defined in the NIST Reference Architecture: Provider, Consumer, Broker, Carrier and Auditor; and

As introduced in Section 2 and Figure 1 above, the NCC-SRA provides a formal model, a set of security components and a methodology of using this information to orchestrate a secure cloud Ecosystem. The NCC-SRA formal model was derived from the NIST Cloud Computing Reference Architecture (NIST SP 500-292) and it is described in detail in Section 4.

The NCC-SRA also provides a set of *security components* deemed important in securing the data and the operations of a cloud computing Ecosystem. In defining this set we leverage the Cloud Security Alliance's (CSA) Trusted Cloud Initiative Reference Architecture (TCI-RA) shown in

Annex A. The set of *security components* and how to use it for a particular cloud model is introduced in detail in Section 3.

The NCC-SRA is presented using a cloud Ecosystem that can be constructed employing any of the twelve instances of the model defined by all possible combinations of the four deployment methods with the three service models. The twelve instances of the cloud architectures addressed in this document are:

- 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.

Figure 8 below provides a graphical representation of the NCC-SRA three-dimensional approach that leads to the twelve instances for which data is collected, then aggregated and analyzed for each cloud type.

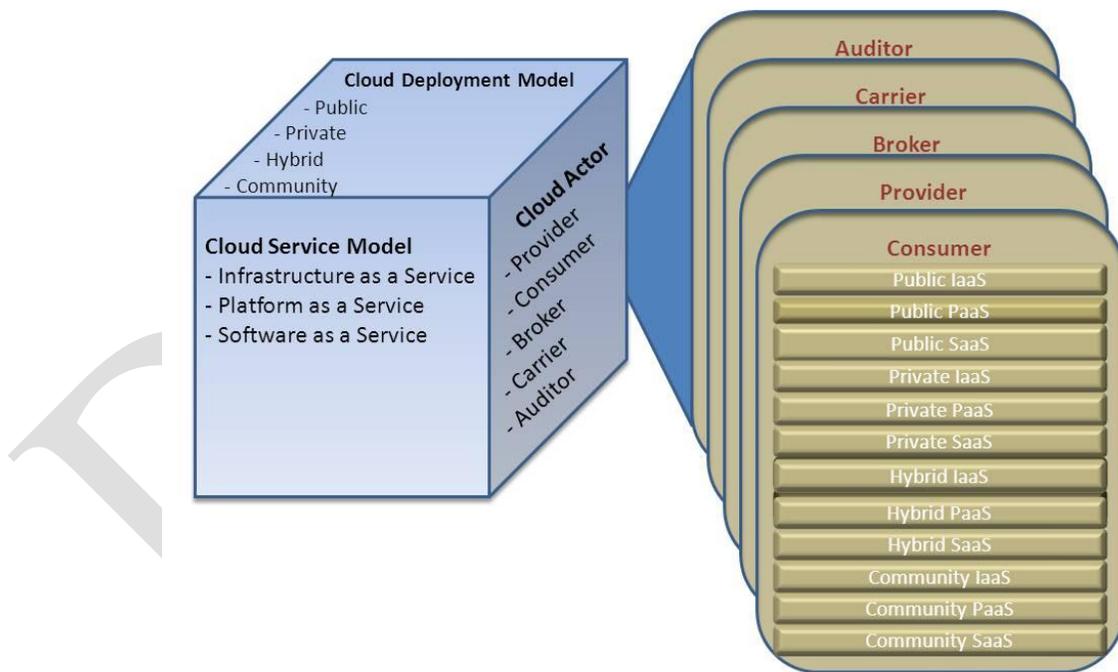


Figure 8: Security Reference Architecture Constructs and Instances

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 is then validated and aggregated Actor-centric and Ecosystem-type-centric to illustrate the core set of *security components* from the cloud *Actor* perspective, highlighting the shifting of responsibilities with the service type model, or 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 Section 5.

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 type with a set of *architectural components* to which the *security components* are mapped to, we aim to aid an organization that elects to migrate one or more of their 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.

DRAFT

3 SECURITY REFERENCE ARCHITECTURE: SECURITY COMPONENTS

Leveraging the Cloud Security Alliance’s Trusted Computing Initiative - Reference Architecture (shown in Annex A), we extracted all capabilities presented in the TCI-RA, preserving the path to the root-domains (e.g. Business Operation Support Service-BOSS, Information Technology Operation Support-ITOS, etc.) and generated a set of 346 *security components*.

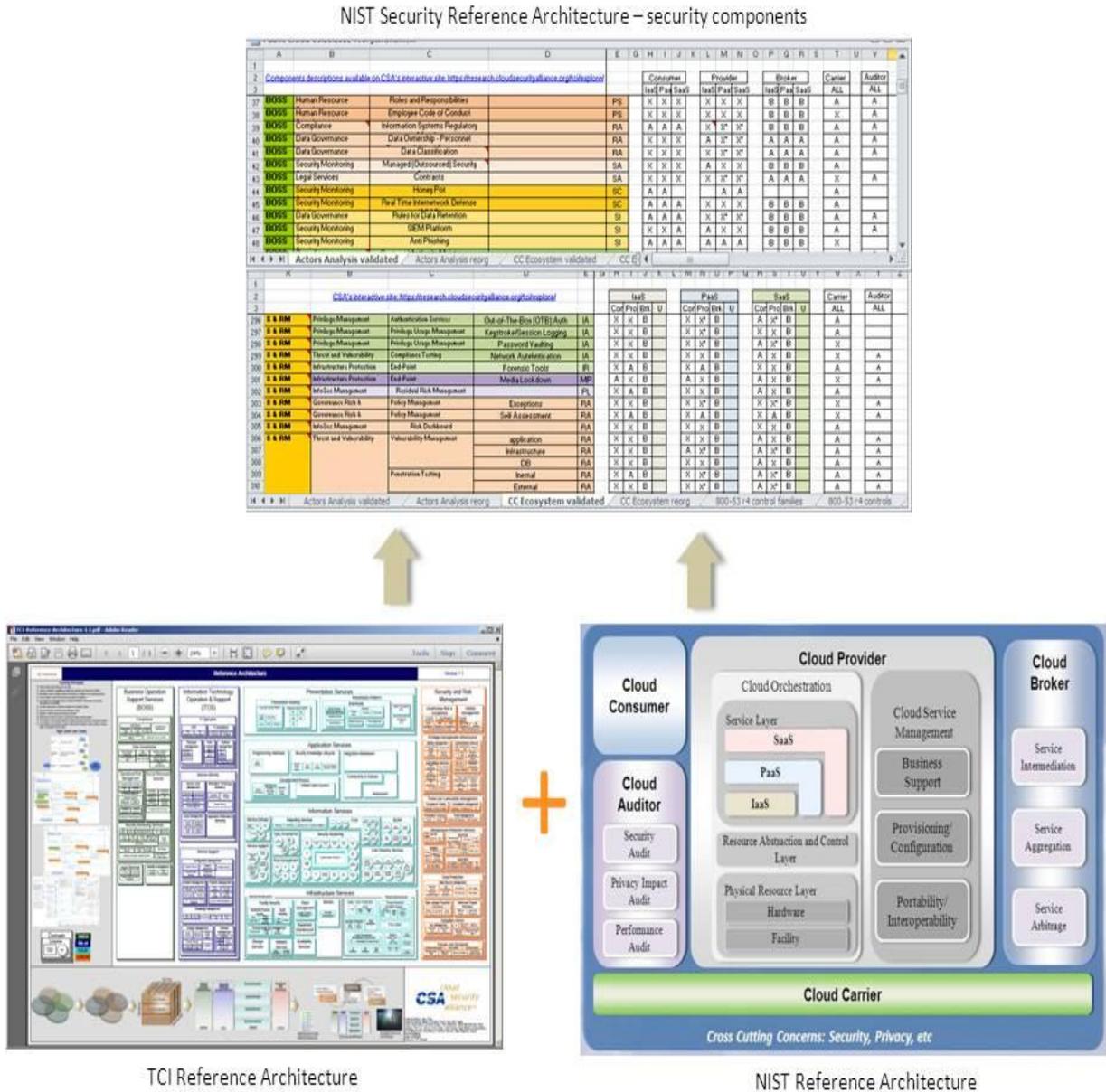


Figure 9: Security Components Overview

The *security components* were captured in data collection forms like the one depicted in Table 1 below. There is one data collection form (bottom tabs in Table 1) for each of the twelve possible instances of a cloud Ecosystem as described in Section 2.3.

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		
BOSS	Compliance	Audit Planning								
BOSS	Compliance	Independent Audits								
BOSS	Compliance	Third Party Audits								
BOSS	Compliance	Internal Audits								
BOSS	Compliance	Contract/ Authority Maintenance								
BOSS	Compliance	Information Systems Regulatory Mapping								
BOSS	Compliance	Intellectual Property Protection								
BOSS	Data Governance	Data Ownership/ Stewardship								
BOSS	Data Governance	Data Classification								
Information Technology	IT Operations	DRP	Plan Management							
Information Technology	IT Operations	DRP	Test Management							
Information Technology	IT Operations	IT Governance	Architecture Governance							
Information Technology	IT Operations	IT Governance	Standards and Guidelines							
Information Technology	IT Operations	Resource Management	Segregation of duties							
Information Technology	IT Operations	Resource Management	Contractors							

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

Collected data was then aggregated, validated and processed for each of the cloud deployment modes (e.g. Public, private, etc.) as part of the data analysis methodology presented in the next section.

4 SECURITY REFERENCE ARCHITECTURE: DATA ANALYSIS METHODOLOGY

4.1 DATA COLLECTION

The data collection effort was focused on populating this model with the applicability of the *security component* for a given cloud instance. Accordingly, each blank cell under each cloud *Actor* heading was marked with ‘X’, ‘A’, ‘B’, or left blank to indicate the following:

- The ‘X’ means the *security component* should be implemented by the *Actor* to secure the functionality and Consumer’s data migrated to the Cloud.
- The ‘A’ means the *security component* should be implemented internally, independent of the Consumer’s data, for administrative or best-practice reasons.
- ‘B’ means a *security component* that is implemented to secure the cloud computing business oriented service (B is specific to Business Brokers only) and emphasizes that the Business Broker only provides business and relationship services, plays the role of a Business Broker and does not have any contact with the cloud Consumer’s data migrated to the cloud.
- A blank cell means 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 (see the interactive site at <https://research.cloudsecurityalliance.org/tci/explore/>) were used to better determine the applicability of the *security component* to the given cloud instance for each cloud *Actor*.

The purpose of the marking as such is to provide a resource for the cloud Consumer to reference when needed to identify *security components* that are applicable to a particular cloud service type. Many of the *security components* are common and should be considered by all cloud *Actors* (organizations) in their internal operations as well as in service-offering operations.

The cloud Consumer is always accountable for ensuring an effective control environment and cannot relinquish accountability. If a *security component* is applicable, the Consumer is accountable for identifying that *security component* and is responsible for requesting the implementation of the component through contractual means when the component’s implementation is outsourced to another cloud *Actor* involved in setting the cloud Ecosystem. For some *security components* in certain cloud service types, the cloud Consumer is both accountable and responsible.

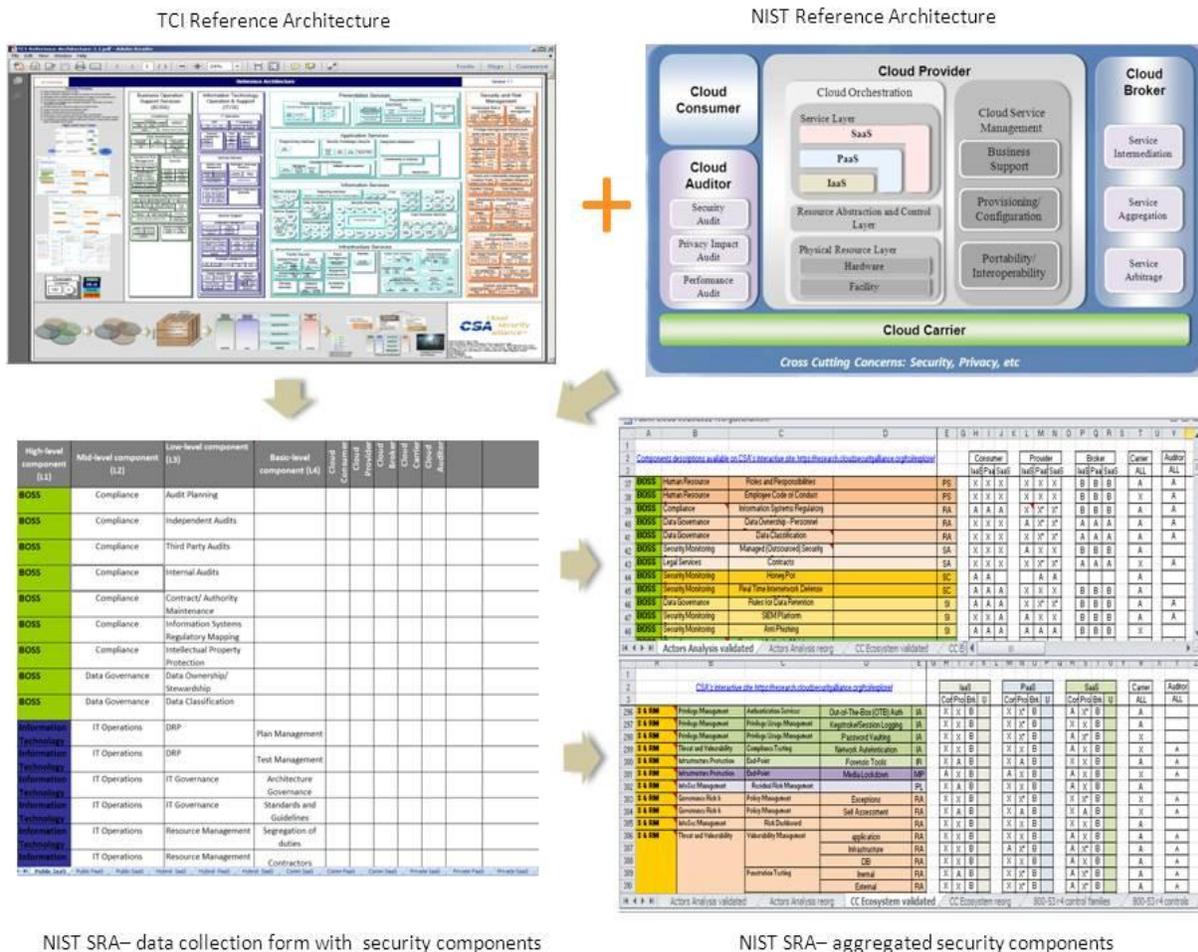
Providers and Technical Brokers of cloud services are responsible for certain *security components* based on their actor role as well as the cloud service type offered. The objective of the data matrixes is to identify which *Actor* is responsible to implement the identified security components for a particular use case of service migrated to the Cloud for each of the cloud Ecosystem instances. As indicated by the data sets, there are areas in which the responsibility may reside with multiple cloud *Actors* depending on the specifics of the *security component* and the particular use case.

4.2 DATA AGGREGATION AND VALIDATION

The data collected for each instance of a cloud Ecosystem as described in section 3.2, is aggregated, for each deployment mode (e.g. Public Cloud, Private Cloud, etc.) to facilitate data validation using the *Security Conservation Principle* defined above in section 2.2.7.

Data aggregation allows for a better understanding of the data dynamics with the shifting in the responsibilities on implementing the core-set of *security components* among cloud *Actors* when the cloud service type changes from IaaS to PaaS and SaaS.

Figure 10 below captures graphically the derivation of the *security components*, data collection process and the two types of data aggregation used to analyze the set of security components for each type of cloud deployment model (e.g. Public, Private, etc.)



NIST SRAC- data collection form with security components

NIST SRAC- aggregated security components

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 type of service (IaaS, PaaS and SaaS), is gathered on one matrix in adjacent columns (e.g. see Annex D, section 11.1 for a Public cloud deployment mode) to highlight the level of control the cloud *Actor* has over the implementation of each *security component* and how this level increases or diminishes with the service type.

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 (e.g. see Annex D, section 11.2 for a Public cloud deployment mode) to highlight the shared responsibilities among Actors involved in constructing and securing the cloud Ecosystem on implementing the identified *security components*. This type of aggregation also highlights the *Security Conservation Principle*.

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 of implementing *security components* is higher for an IaaS service type and decreases for a PaaS service type reaching minimum for a SaaS service type, while for the cloud Provider and Broker combined, the responsibility of implementing *security components* increases rapidly from IaaS to PaaS and SaaS respectively.
2. In the Ecosystem-centric aggregation type, the cumulative set of security components implemented by all Actors involved in the cloud Ecosystem remains invariant with the shift of service type from IaaS to PaaS and SaaS.

It is important to note that based on the SP 500-292 definitions of the cloud Carrier and its unique role of securing the data transport from the Consumer to the entry point in the cloud, the data collected for this *Actor* does not vary with the cloud service type (IaaS, PaaS or SaaS) for a particular cloud deployment mode (e.g. Public, Private, etc.). All other transport roles and responsibilities within the cloud are attributed to the cloud Provider.

Moreover, since for a cloud Auditor the NCC-SRA is only addressing the core set of *security components* necessary to be implemented to secure the *Actor's* auditing environment, the data collected was also invariant with the cloud service type and deployment mode.

4.3 DERIVING THE SECURITY RESPONSIBILITIES FOR INTERMEDIARY PROVIDER AND TECHNICAL BROKER

The overall core-set of *security components* that a Technical Broker (TB) or an Intermediary Provider (IP) should analyze and implement, (in addition to the baseline set all cloud Actors should

implement), to secure the Consumer’s data and the operations of the Cloud, can be determined following the next 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 the Annex D the Primary Provider set 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 graphically represents the approach listed above.

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

Example:

$$SC(IP)_{SaaS} = SC(PP)_{SaaS} - SC(PP)_{PaaS}, \text{ where } "X" = "S", "Y" = "P"$$

$$SC(TB)_{PaaS} = SC(PP)_{PaaS} - SC(PP)_{IaaS}, \text{ where } "X" = "P", "Y" = "I"$$

Legend:

SC – set of Security Components

PP – Primary Provider

IP – Intermediary Provider

TB – Technical Broker

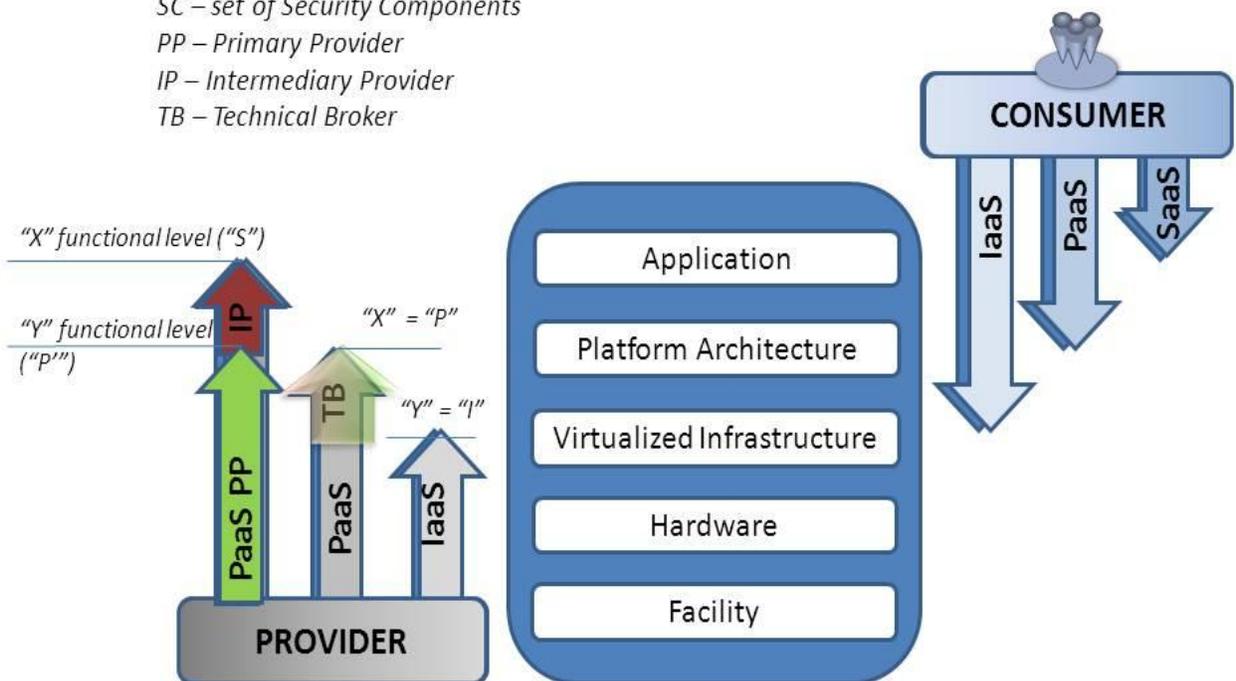


Figure 11: Security Components for Technical Broker & Intermediary Provider

4.4 MAPPING SECURITY COMPONENTS TO SECURITY CONTROL FAMILIES

NIST SP 500-293 Volume II (draft) identifies the *need for clarification of security control roles and responsibilities* as a challenging security requirement. To address these issues we provide a data mapping between the *security components* identified in our Security Reference Architecture and the NIST 800-53 security control families. To this end, the mapping between the *security components* and the SP 800-53 security controls is necessary to set a common ground for government cloud Consumers and the cloud Providers and Brokers coming from the private sector. By providing in this document the framework to achieve a clear attribution of the mapping between the *security component* and the 800-53 security controls through the mapping to the security control families, this document aims to come one step closer towards identifying the cloud Actors’ roles and responsibilities in implementing these security components and controls.

This section outlines the process used to map the *security components* to the security control families of NIST SP 800-53: “*Security and Privacy Controls for Federal Information Systems and Organizations*”.

To accomplish the mapping or pairing of the *security components* to the NIST 800-53 control families we leveraged the definitions provided by CSA for their capabilities of the TCI Reference Architecture available at <https://research.cloudsecurityalliance.org/tci/explore/> as also definitions for NCC-SRA *security components*. The mapping or assignment of the *security components* to one of the eighteen families of security controls identified in the NIST SP 800-53 was done by finding the security control family that best fits the *security component*. It is important to note that this mapping is not based upon particular security controls defined in the NIST SP 800-53 since for each *security component* there are multiple SP 800-53 security controls, often belonging to different families that could be applied to insure the correct implementation of a *security component*.

In the data collection forms presented in Section 3.1, the NCC-SRA *security components* carried on the three root-domains and service layers identified by the TCI Reference Architecture capabilities (see also Table 2 below). The eighteen security control families identified in the NIST SP 800-53 (Rev. 4) are listed in the Table 3 below. Annex B depicts the mapping or pairing of the *security components* to the NIST 800-53 security control families using the color code presented in Table 3.

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

Table 2: TCI Reference Architecture - Domains and Service Layers

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

Table 3: NIST 800-53 Control Families – Assigned Color Codes

Cloud Consumers can quickly reference Annex B below to identify the appropriate *security component*-security control family pair 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 represented in dark blue shade.

4.5 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, Section 13.2 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 type elected by Consumer. Such a heat map highlights the *security components* that are under Consumer’s responsibility versus the ones that can only be addressed by the Provider and/or Broker when applicable. Such a heat map represents in “hot” colors the *security components* where the cloud Consumer loses the ability to manage the security controls for the component. 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 (the “hot” and “warm” components) that should be specified in SLAs and contracts with cloud Providers, Brokers and Carriers.

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, Section 11.2 for a public cloud), for all three service types (highlighted cells below in the Table 4 sample) and format the data as a vector.

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]

Table 4: Security Component - Vector Generation

In the example above, the vector (XA, XA, AX) shown in Table 4 means that for this *security component*, the Consumer has an “X”, for IaaS, “X” for PaaS, and “A” for SaaS. For the same vector (XA, XA, AX), indicates that the cloud Provider has an “A” for IaaS, “A” for PaaS, and X SaaS respectively.

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 in implementing the security 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 secure the component for the particular service type in discussion. However, if the Provider has an X while the Consumer has an A for a *security component*, it means that the Provider has full responsibility of implementing the security controls associated necessary to secure the component.

If we quantify the amount of control a Consumer is transferring to the Provider, and assign numerical values: XA => 0, XX => 0.5 and AX => 1 to the vector’s components, then we can order these values in the following way: XA < XX < AX, where the higher value (AX) shows the case where the consumer has the least control over the implementation of the *security components* and has to negotiate with the Provider the component’s secure implementation. A heat map of this subset of values would show:

- XA as a “cool” color (blue) because the Consumer has total control over the implementation of the *security component*, and
- AX as a “hot” color to indicate that the Consumer needs to negotiate with the Provider the implementation of the *security component*.

If we extrapolate this approach to all three service levels (IaaS, PaaS, and SaaS) then we obtain the partial ordering shown in the legend below in Figure 12. The total value of the vector obtained by summing the three numerical values of its components, is then associated with a color as indicated in the legend below (Figure 12), and represented in the generic heat map.

The exception is just the least responsibility vector (AA AA AA) and the vector derived from empty cells.

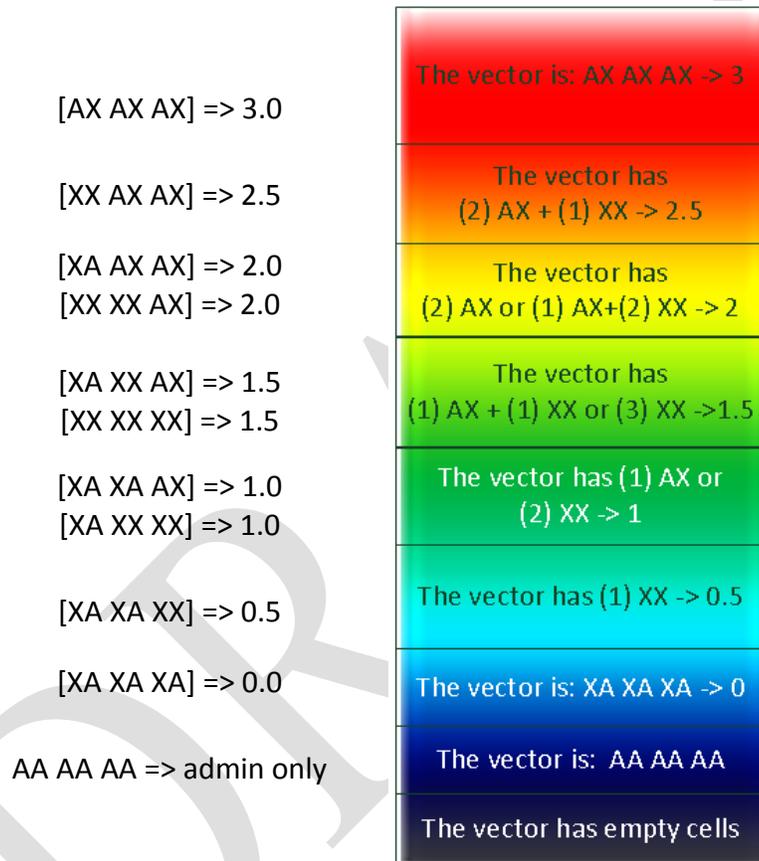


Figure 12: Legend of the Generic Heat Map

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 Generic Heat Maps can be generated for all other types of clouds (e.g. Private, Hybrid, etc.)

5 SECURITY REFERENCE ARCHITECTURE: FORMAL MODEL

5.1 THE FORMAL MODEL OVERVIEW

Leveraging the cloud computing architectural model presented in the SP 500-292 document, the NIST Reference Architecture (NIST RA) reproduced in Figure 13 below with latest updates included, we derived the NIST Cloud Computing Security Reference Architecture formal model (Figure 14). 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 associates SP 800-53 security controls, as found necessary. It is important to reiterate that even though SRA only maps the *security components* to SP 800-53 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 use-case migrated to the cloud.

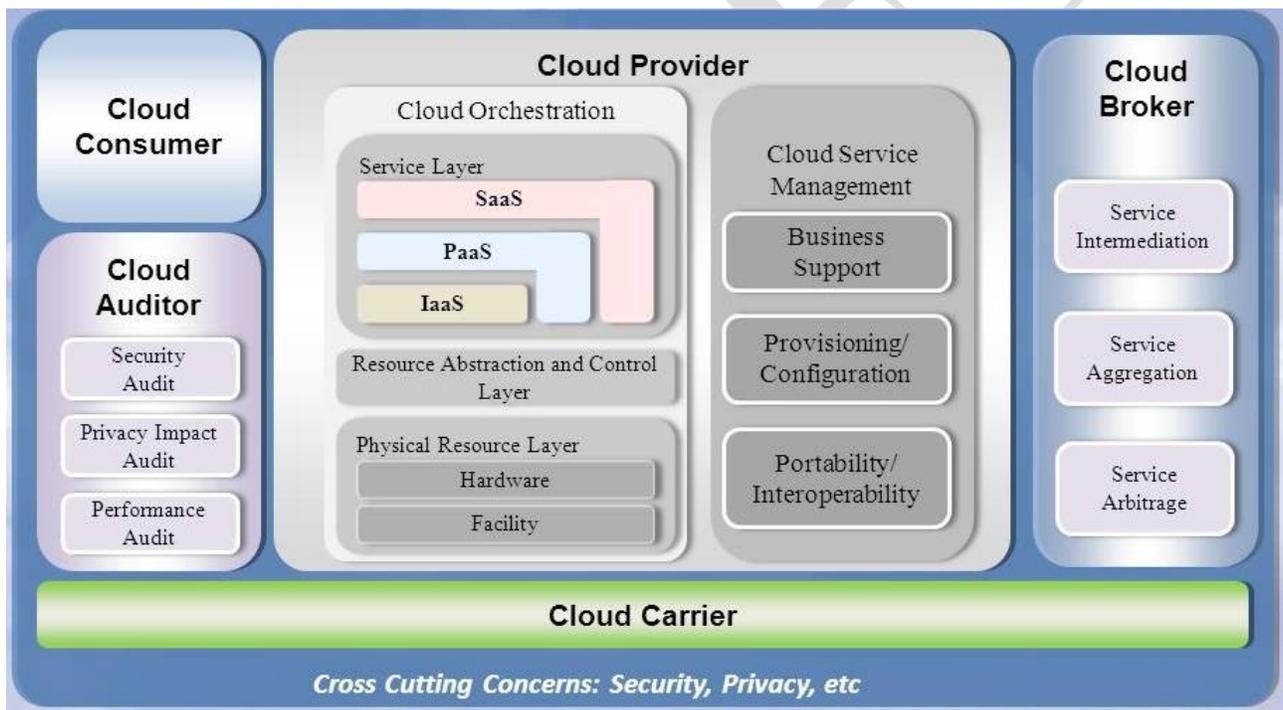


Figure 13: NIST Cloud Computing Reference Architecture (updated)

The SRA formal model presented in Figure 14 below depicts, in a layered representation, the cloud Actors on the background and the security *architectural components* defined for each Actor, in the foreground with the *architectural components* and sub-components stretched across multiple Actors when Actors could satisfy 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 and 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 Consumer also 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.

The hierarchical list of all *architectural components* and sub-components 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.

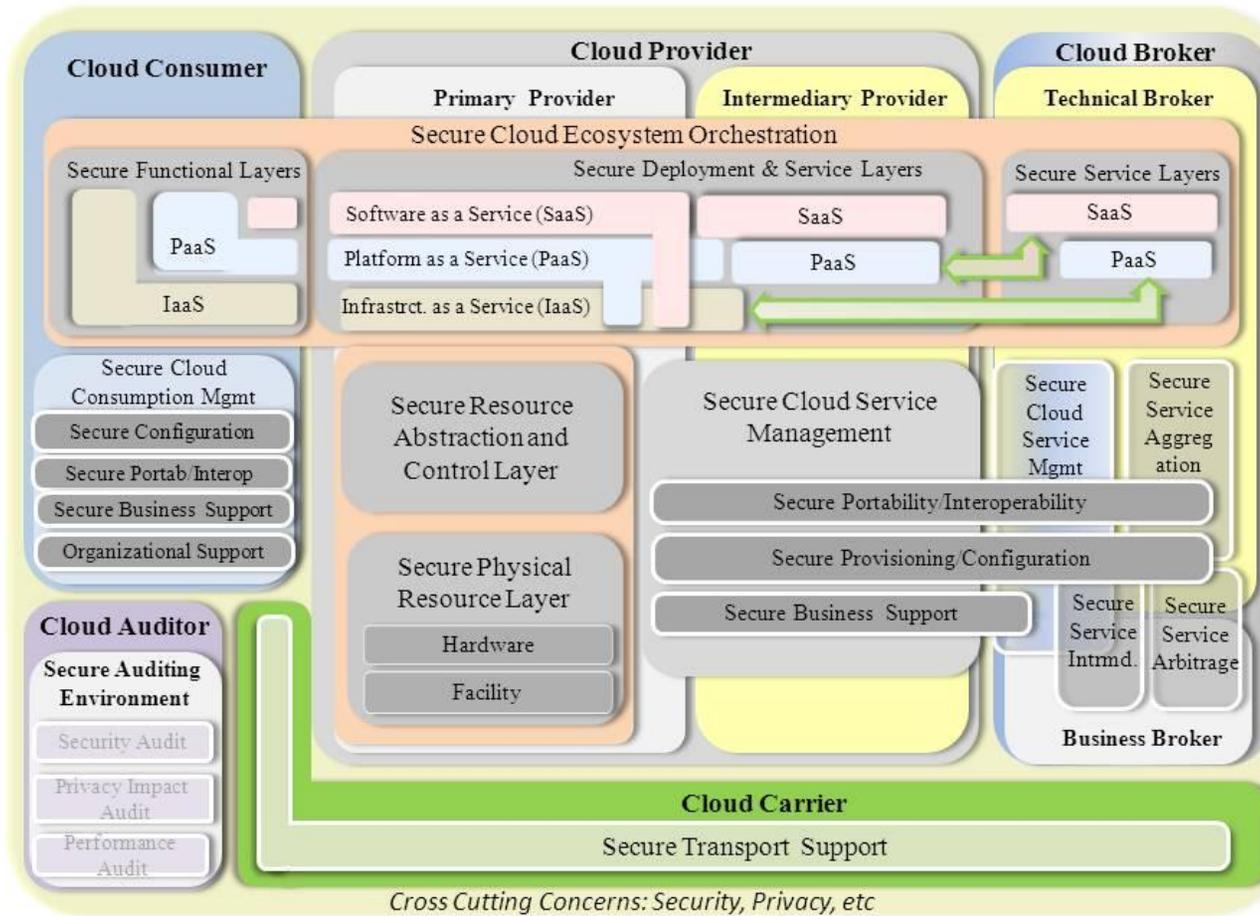


Figure 14: Formal Model – Security Reference Architecture

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.

In the next sections, the *architectural components* and sub-components are introduced and discussed for each cloud *Actor*.

Annex E of this document presents a matrix that maps the high-level *security components*, and with them the SP 800-53 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.

5.2 CONSUMER - ARCHITECTURAL COMPONENTS

The NIST Reference Architecture document (SP 500-292) identifies the Provider’s and Broker’s *architectural components* based on the areas in which the cloud *Actors* conduct their activities. However, the document lacks an introduction and analysis of the Consumer’s *architectural*

components. Therefore, the *architectural components* identified in this document are first introduced and do not map to any NIST RA component. The Consumer’s *architectural components* we identified are complementing 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

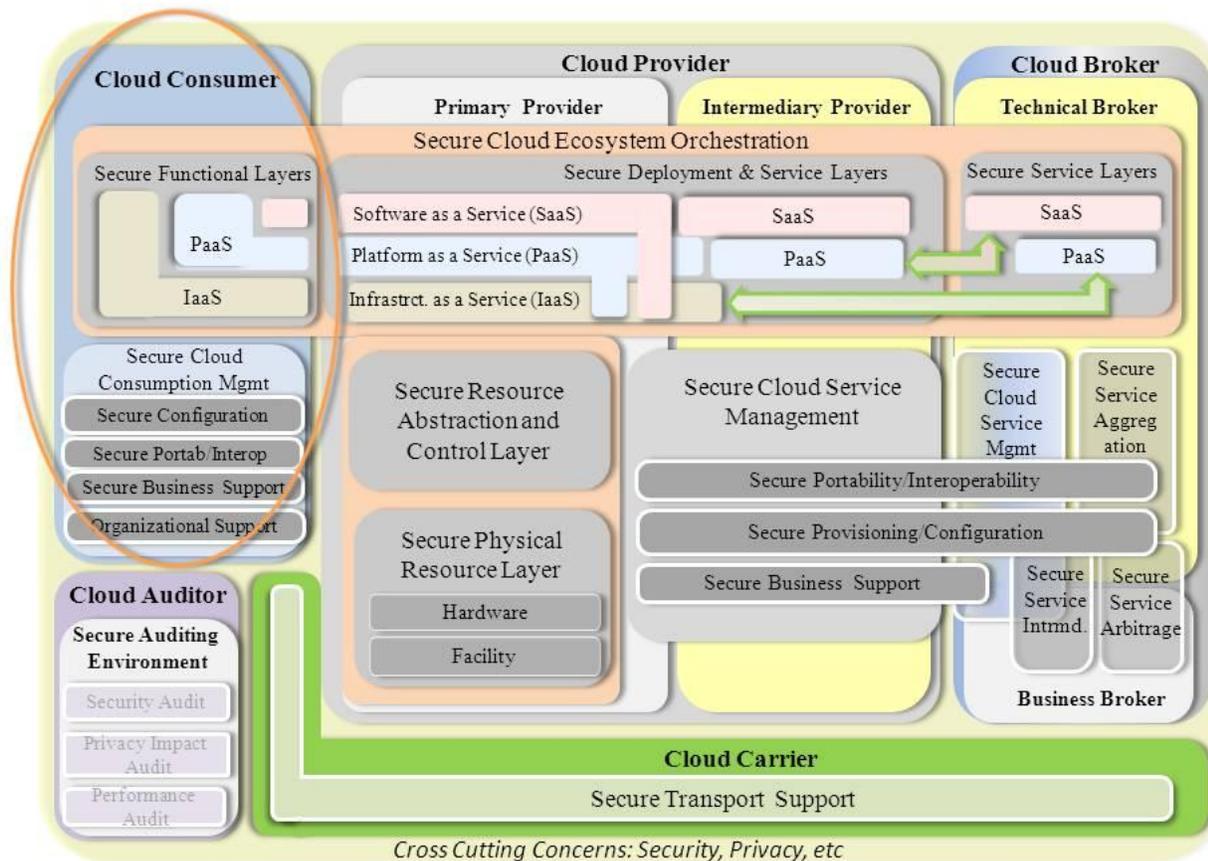


Figure 15: SRA – Cloud Consumer

In the following subsections we will discuss each cloud Consumer's *architectural component*.

5.2.1 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);

which leads to the following main architectural sub-components:

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

These four architectural sub-components (listed above) are discussed in detail in the next subsections.

One of the challenges cloud Consumers are facing when moving applications and data to the cloud is ensuring that the Risk Management Framework is applied properly and the near real time-time risk management and ongoing information system authorization meets the agency's needs through a robust *continuous monitoring* process (see NIST SP 800-37 for more details). In a cloud Ecosystem, the *continuous monitoring* activities become a shared responsibility among cloud *Actors* involved in the cloud Ecosystem. Without shared agreements and well-structured, cost-effective automation process that ensures 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). For example, OS images used by the cloud Providers 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 as SCAP, cloud Actors can collaborate on the ability to check security policy compliance, vulnerability of OS images, and measure deviations from required configuration settings. Additionally, cloud Consumers can gain measurable data to map to high-level NIST SP 800-53 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. NIST maintains a list of SCAP-validated products at:

<http://nvd.nist.gov/scaproducts.cfm>.

In Annex E we present all the high-level SRA *security components* and their mapping to each of the *architectural component* and *sub-component* defined for a cloud Consumer, next to similar mappings for Provider, Broker, Carrier and Auditor.

5.2.1.1 SECURE BUSINESS SUPPORT

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, setup/negotiate/close/terminate 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 Agency'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 component* of a cloud Consumer, the *Secure Business Support* architectural component is coded "B" under the "Consumer" section of the table.

5.2.1.2 SECURE CONFIGURATION

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 regulations (e.g. NIST SP 800-53, NIST SP 800-37, FIPS 199, etc.) as well as requirements set forth in the Service Level Agreement. 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 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, to ensure 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, and active user accounts). Securely managing metering means that cloud Providers implement specific internal controls to ensure that storage can be encrypted, processing can be sand-boxed, abnormal bandwidth usage can be reported, user account management is compliance with security policies of the consumer.
- *Service Level Agreement Management*: encompassing the SLA contract definitions (basic schema with the QoS parameters), SLA monitoring and SLA enforcement according to defined policies. In the context of secure configuration, the SLA's will need to provide ample visibility in order to ensure compliance with secure configuration management mandates as defined in NIST 800-53.

Annex E provides the high-level SRA *security components* mapped to the *architectural component* of a cloud Consumer, the *Secure Configuration* is coded "C" under the "Consumer" section of the table.

5.2.1.3 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 implemented risk mitigating measures are commensurable with the data security and privacy requirements and necessary protection level. The *security components* mapped to this architectural subcomponent are providing 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 along multiple cloud Ecosystems through a secure and unified management interface. Requirements for secure portability and interpretability vary based on cloud service type adopted. System

maintenance time and disruptions should be kept by the Providers and Brokers at an acceptable minimum level as agreed in the Service Level Agreements.

In Annex E that provides the high-level SRA *security components* mapped to the *architectural component* of a cloud Consumer, the *Secure Portability/Interoperability* is coded “I” under the “Consumer” section of the table.

5.2.1.4 SECURE ORGANIZATIONAL SUPPORT

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 following *security components*: Compliance Management, Audit Management under Governance Risk & Compliance; and Technical Security Standards, Best Practice & Regulatory Correlation, and Information Security Policies under Policies and Standards, to mention only few as an example, are organizational processes mapped to the *Secure Organizational Support (O)* architectural sub-component.

In Annex E that provides the high-level SRA *security components* mapped to the *architectural component* of a cloud Consumer, the *Secure Organizational Support* is coded “O” under the “Consumer” section of the table.

5.2.2 SECURE CLOUD ECOSYSTEM ORCHESTRATION

The NIST Reference Architecture document (SP 500-292) describes the *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, the cloud *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 type and deployment model.

In the SRA we expand on the generic stack diagram (Figure 15 of the SP 500-292) 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) and extrapolate the cloud Provider’s *Service Layer* to construct the SRA’s *Secure Service Layer* architectural sub-component for the Provider and Technical Broker and the *Secure Functional*

Layer architectural sub-component for the Consumer (see Figure 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 the cloud service type adopted.

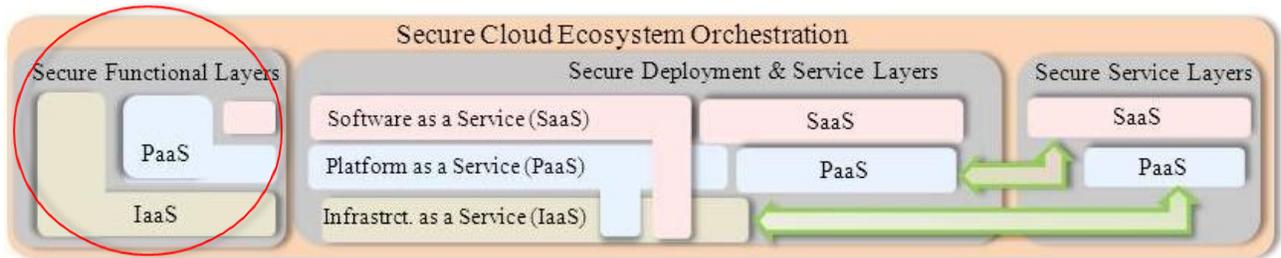


Figure 16: Secure Cloud Ecosystem Orchestration

A cloud Consumer may only secure its interface to the cloud service and the functional layers above this interface in the functionality stack, relying on cloud Provider or cloud Technical Broker to secure the service layers below the service interface.

5.2.2.1 SECURE FUNCTIONAL LAYER

The set of *security components* a cloud Consumer implements to secure the cloud *Functional Layer* depends upon the particular type of cloud service used (IaaS, PaaS and SaaS) and it is intrinsically correlated with the sets of *security components* implemented by the other cloud Actors involved in the construct of the cloud Ecosystem.

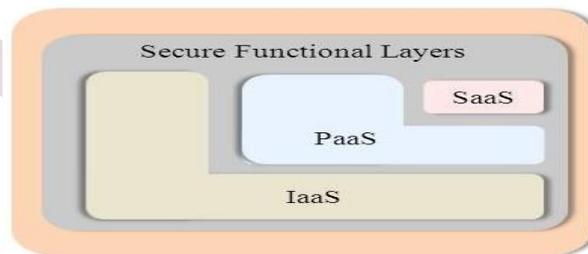


Figure 17: Secure Functional Layers

In an IaaS cloud ecosystem, a cloud Consumer uses the provisioned infrastructure and computing resources, such as a virtual computer, for their fundamental computing needs and has access to more fundamental forms of computing resources, has more control over the software components in an application stack, including the OS and network.

In a PaaS cloud Ecosystem, a cloud Consumer has control over the applications and possibly some the hosting environment settings, but has no or limited access to the infrastructure underlying the platform such as network, servers, operating systems (OS), or storage.

In a SaaS cloud Ecosystem, a cloud Consumer has much less control than in PaaS and SaaS cloud Ecosystems since the cloud Consumer has only limited administrative control of the applications used.

For example, in an IaaS cloud Ecosystem, a Consumer may secure the Infrastructure Protection Service - Server Firewall security component but may secure the Infrastructure Protection Service - Endpoint Firewall for all types of cloud (IaaS, PaaS and SaaS). However, a cloud Consumer would be unable to use its own Server Firewall for securing a PaaS or SaaS cloud. Instead, the cloud Consumer needs to rely on the cloud Provider Server Firewall services and therefore should make sure the desired level of protection is clearly stipulated in the Service Level Agreement.

In Annex E that provides the high-level *security components* mapped to the *architectural component* of a cloud Consumer, the *Secure Functional Layer* architectural sub-component is coded “L” under the “Consumer” section of the table.

5.3 PROVIDER – ARCHITECTURAL COMPONENTS

The NIST Reference Architecture document (NIST SP 500-292) identifies the RA’s architectural components based on the areas a cloud Provider conducts its activities, as follows: *service deployment, service orchestration, cloud service management, security, and privacy*. Since the *security* is a cross cutting concern same with *privacy, data content managements, SLA, etc.*, the Security Reference Architecture’s formal model (Figure 14) is interlacing the Provider’s *security* activities at all levels and across all Provider’s areas of responsibilities, embedding the security in all architectural components pertaining to the cloud Provider. Additionally, the cloud deployment is perceived as part of the cloud Ecosystem orchestration, being directly correlated with the services offered by a cloud Provider. Therefore, the Security Reference Architecture formal model defines, for a cloud Provider, the following architectural components and sub-components:

- 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) – applicable only to a Primary Provider,
 - Secure Resource Abstraction and Control Layer (Hardware & Facility) – applicable only to a Primary Provider,
 - Secure Deployment & Service Layers.

Figure 18 below highlights the cloud Provider in the Secure Reference Architecture formal model diagram, emphasizing the two types of Providers: primary and intermediary Provider, and graphically representing the architectural components pertaining to the two of them.

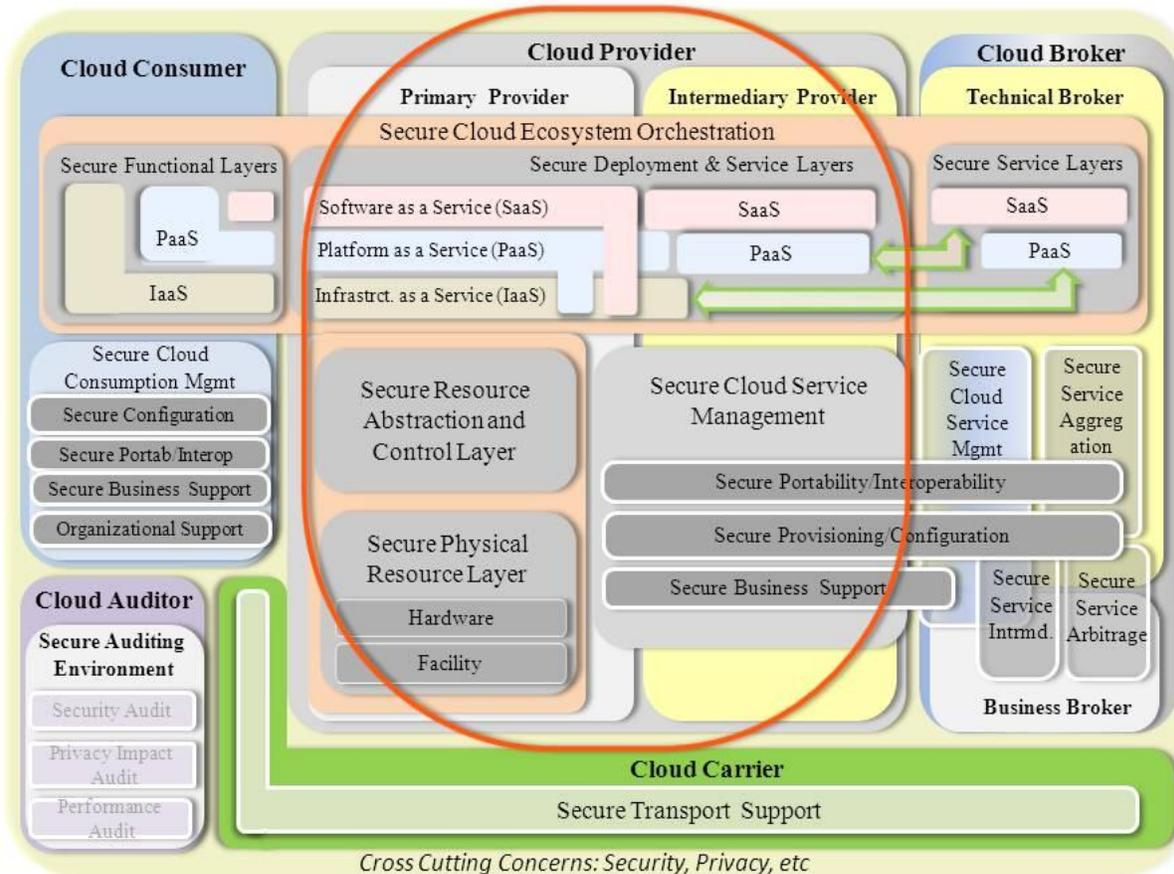


Figure 18: SRA – Cloud Provider

A primary Provider may deliver services to a cloud Consumer directly, through a Technical Broker or partner with an Intermediary Provider. An intermediary Provider delivers services to 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 some *security components* and controls as a primary Provider, and needs to coordinate among multiple Providers in order to implement these *security components* and controls.

5.3.1 SECURE CLOUD ECOSYSTEM ORCHESTRATION

The NIST Reference Architecture document (NIST SP 500-292) describes the *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 (Figure 13 above, in Section 5.1) 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 types of services a Provider can offer (IaaS, PaaS and SaaS),
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 and
3. the *physical resource layer* that includes all the physical computing resources such as hardware resources, (CPU and memory), networks (routers, firewalls, switches, network links and interfaces), storage components (hard disks) and any other physical computing infrastructure elements.

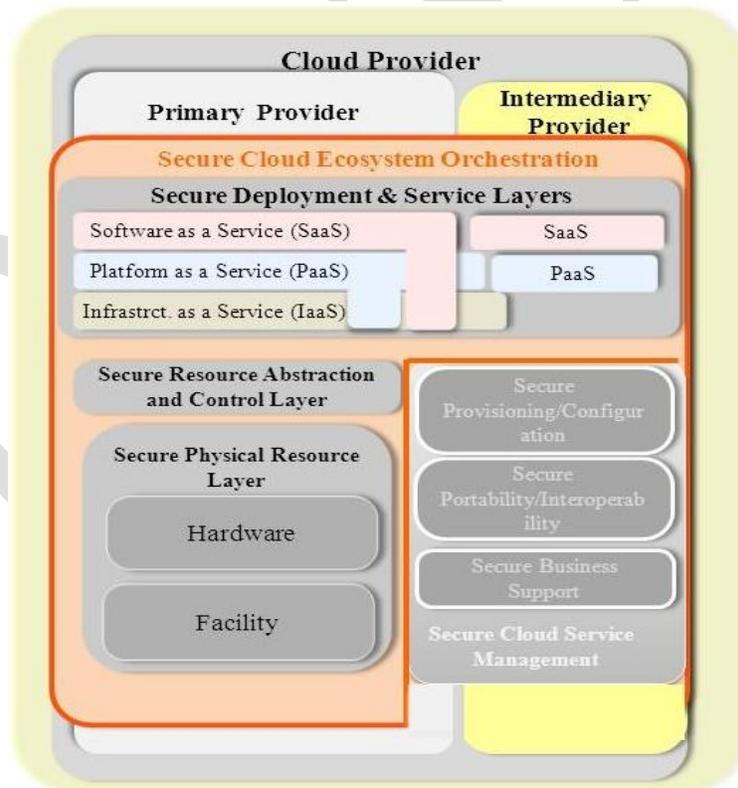


Figure 19: Secure Service Orchestration – Stack Diagram

Figure 19 above expands upon the NIST RA diagram (Figure 13, above) and identifies the architectural component that identifies the secure cloud service orchestration for Providers as the *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,
- Secure Resource Abstraction and Control Layer,
- Secure Physical Resource Layer.

All three layers are discussed in more detail in the next three subsections.

5.3.1.1 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 (e.g. IaaS, PaaS and SaaS) and the cloud deployment model (e.g. Public, Private, etc.). For each of the twelve instances of cloud Ecosystems, the set of *security components* a Provider 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 20: Secure Deployment and Service Layers

For an IaaS cloud Ecosystem, a cloud Provider acquires the physical computing resources underlying the service, including the servers, networks, storage and hosting infrastructure. The cloud Provider runs the cloud software necessary to makes 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.

For 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 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 process of their service migrated to the cloud. Such tools could be integrated development environments (IDEs), development version 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 in managing and controlling the applications and the infrastructure.

Regardless of the cloud Ecosystem offered, a cloud Provider has always control over the physical hardware and cloud software that makes the provisioning of these infrastructure services possible, for example, the physical servers, network equipment, storage devices, host OS and hypervisors for virtualization.

In Annex E that provides the high-level *security components* mapped to the *architectural component* of a cloud Provider, the *Secure Service Layer* architectural component is coded “L” under the “Provider” section of the table.

5.3.1.2 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 the physical computing resources through software abstraction. Examples of resource abstraction components include software elements such as hypervisors, virtual machines, virtual data storage, and other computing resource abstractions. The resource abstraction needs 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.

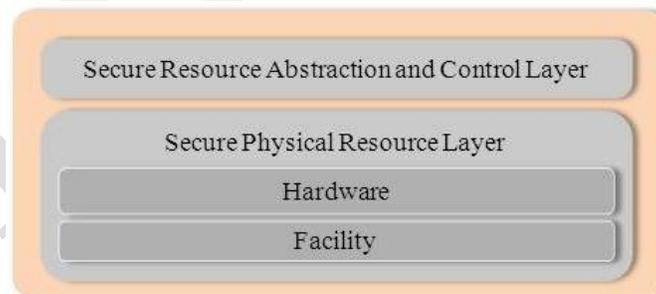


Figure 21: Secure Resource Abstraction and Physical Resource Layers

Figure 21 above expands upon the NIST RA (Figure 13, above) and 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 are accessing 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 insuring minimal interactions between layers and independence of the lower layers functionality from the functionality of upper layers.

In a cloud Ecosystem, applying the Risk Management Framework on behalf of a US Government cloud Consumer and providing *continuous monitoring* becomes a shared responsibility 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 Section 5.2.1, 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 the Security Content Automation Protocol (SCAP).

In Annex E that provides the high-level *security components* mapped to the *architectural component* of a cloud Provider, the *Secure Resource Abstraction and Control Layer* architectural component is coded “R” under the “Provider” section of the table.

5.3.1.3 SECURE PHYSICAL RESOURCE LAYER

The *Secure Physical Resource Layer* (Figure 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.

In Annex E that provides the high-level *security components* mapped to the *architectural component* of a cloud Provider, the *Secure Physical Resource Layer* architectural component is coded “P” under the “Provider” section of the table.

5.3.2 SECURE CLOUD SERVICE MANAGEMENT

NIST Reference Architecture document 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:

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

Figure 22 below expands upon the NIST RA diagram (Figure 13, above) and 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, the secure cloud management is a service that both, Primary and Intermediary Providers offer.

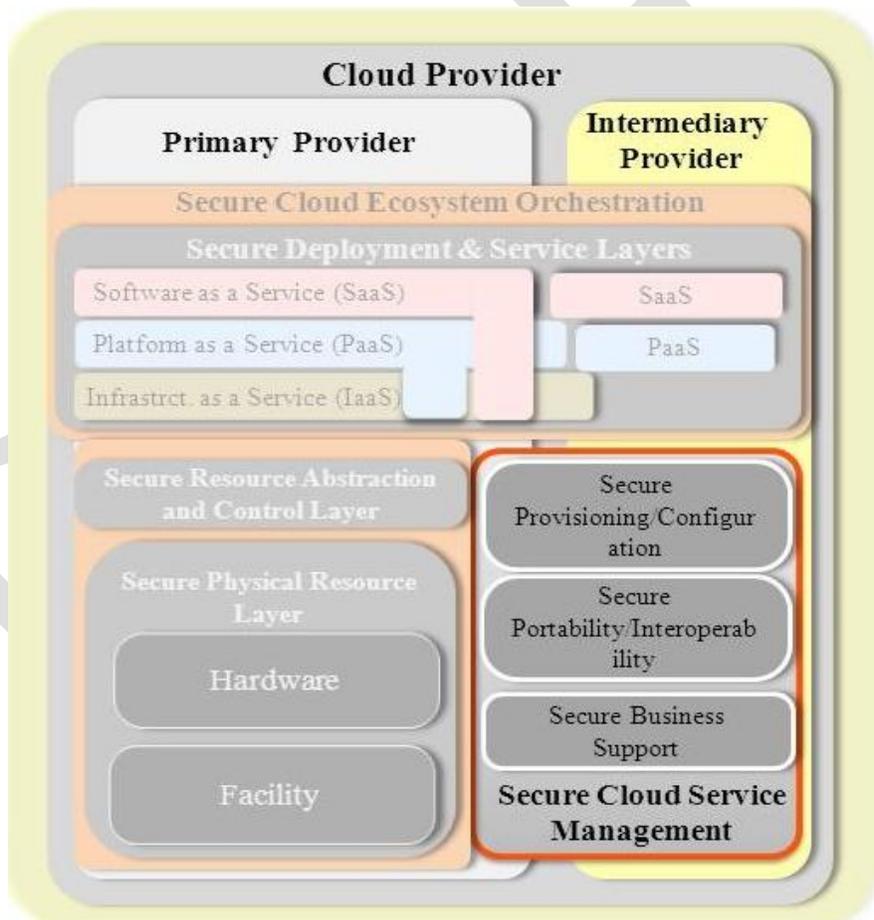


Figure 22: Secure Cloud Service Management – Stack Diagram

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 Section 5.2.1

The following sub-sections focus on the architectural sub-components corresponding to the *Secure Service Management* activities offered by Primary and Intermediary Providers.

5.3.2.1 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 the Service Level Agreements.

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 capabilities 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 the requested services, 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) attacks² due to malicious exhaustive requests for services or bandwidth or to unauthorized deployments of malicious systems.

² 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. The DoS or DDoS attack can also cause the computing platform to slow down responses due to server overload with massive non-legitimate traffics. Since cloud computing has the ability to rapidly provision computing resources and to detect whether there may be 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 attack is one kind of DoS causing saturation of computing resources, such as bandwidth, storage, or processor time. The flooding attack also interrupts the configuration/routing information. In cloud computing, there are two basic types of flooding attacks identified by Z. Xiao & Y. Xiao (2012):

- 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.

- *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 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, and active user accounts). Metering capability needs to be protected and not be tampered with. Sufficient evidence of these protections will support Consumers with their monitoring requirements and mandates.
- *SLA management*: Encompassing the SLA contract definition (basic schema with the QoS parameters), SLA monitoring and SLA enforcement according to defined security policies.

In Annex E that provides the high-level *security components* mapped to the *architectural component* of a cloud Provider, the *Secure Provisioning and Configuration* architectural component is coded "C" under the "Provider" section of the table.

5.3.2.2 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 set by cloud Consumer security requirements. System maintenance time and disruptions should be kept at an acceptable minimum level as agreed in the Service Level Agreements. 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 interpretability vary based on cloud service type adopted.

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 capability. The first example may be as simple as performing data extractions and backing it up in a standard format. The second example may need to first capture virtual machine images and then migrate that to one or more new cloud Providers who may use different virtualization technologies. Configurations based upon 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 all security controls operational during migration.

In Annex E that provides the high-level *security components* mapped to the *architectural component* of a cloud Provider, the *Secure Portability and Interoperability* architectural component is coded “I” under the “Provider” section of the table.

5.3.2.3 SECURE BUSINESS SUPPORT

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 business operations that are client-facing and supports 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 are adequately implementing the *security components* and controls that fall under their responsibility, and that the risks and the liability are appropriately addressed.

All business support responsibilities are shared by all Providers (Primary and Intermediary) once they are identified and captured in the contracts with the cloud Consumer. For example, some of the Providers’ business support responsibilities, to enumerate only few, are as follows:

- *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. based upon security policies of the Consumer.
- *Contract management*: Manage service contracts, setup/negotiate/close/terminate contract, etc. to include supplying information that supports security auditing and reporting requirements of the Consumer.
- *Inventory Management*: Set up and manage service catalogs, etc. in a secure manner so as not to be tampered with.
- *Accounting and Billing*: Manage customer billing information, send billing statements, process received payments, track invoices, etc. to ensure fraudulent activities are tracked and corrected efficiently.
- *Reporting and Auditing*: Monitor users’ operations, generate reports, etc., to support security auditing and monitoring 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. without violating Consumer protections as afforded to them by the law.

In Annex E that provides the high-level *security components* mapped to the *architectural component* of a cloud Provider, the *Secure Business Support* architectural component is coded “B” under the “Provider” section of the table.

5.4 BROKER – ARCHITECTURAL COMPONENTS

Section 2.2.3 brings clarifications to the role of the cloud Broker defined in the NIST Cloud Computing Reference Architecture document, NIST SP 500-292. 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.

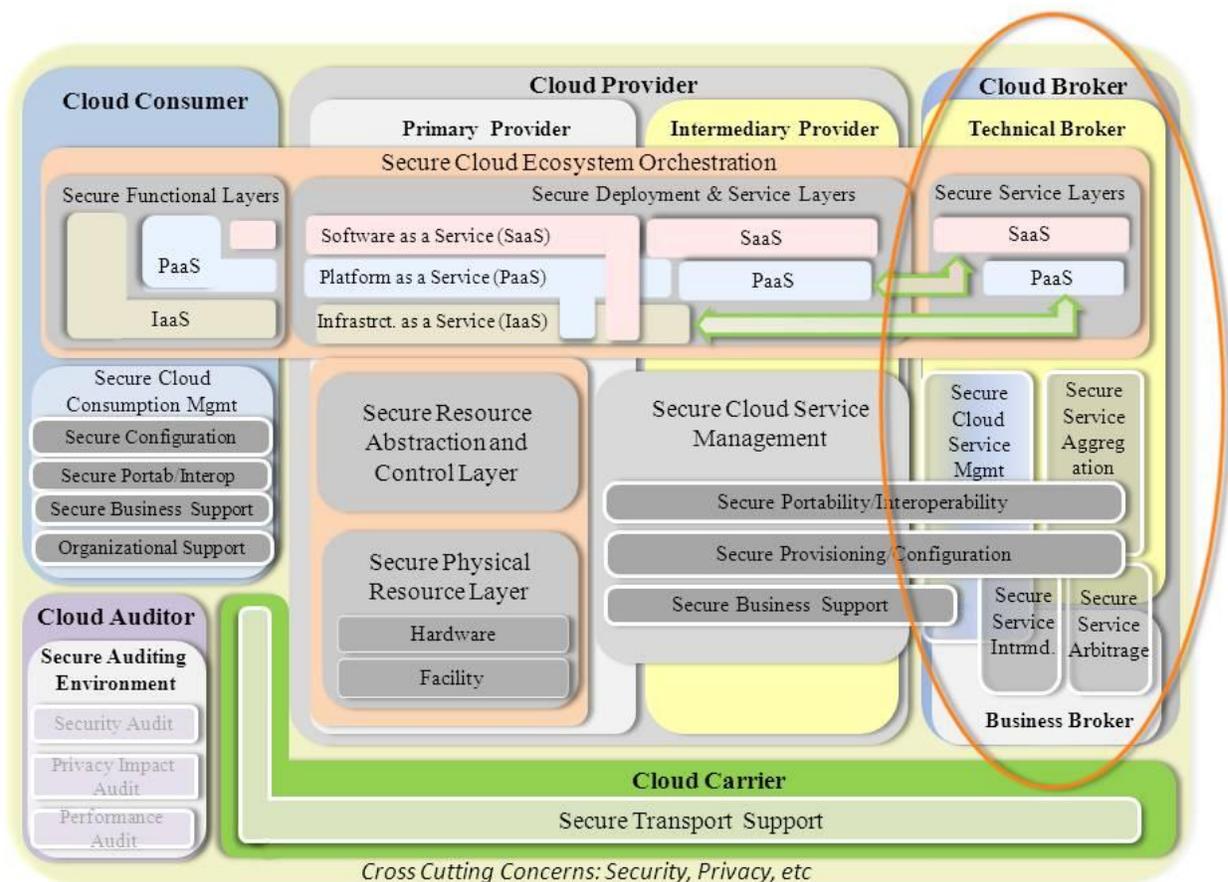


Figure 23: SRA – Cloud Broker

In general, a cloud Broker can render services that can be divided in five categories. Four of those are corresponding to the four services identify in the NIST RA document for the Broker 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. The five architectural components defined for a cloud Broker are listed below:

- *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 data movement between the cloud consumer and multiple cloud providers based upon the security policies of the Consumer. The cloud *Secure Service Aggregation* can be described from the perspective of the:
 - portability and interoperability technical requirements, and
 - 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, for example, can 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. The improvement can be managing access to cloud services, identity management, performance reporting, enhanced security, etc. while ensuring the security policies of the Consumer are maintained.
- *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. The cloud *Service Management* can be described from the perspective of the:
 - business support requirements,
 - provisioning and configuration business requirements, and
 - 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 mode (e.g Private, Public, etc.) and service type (PaaS or SaaS).

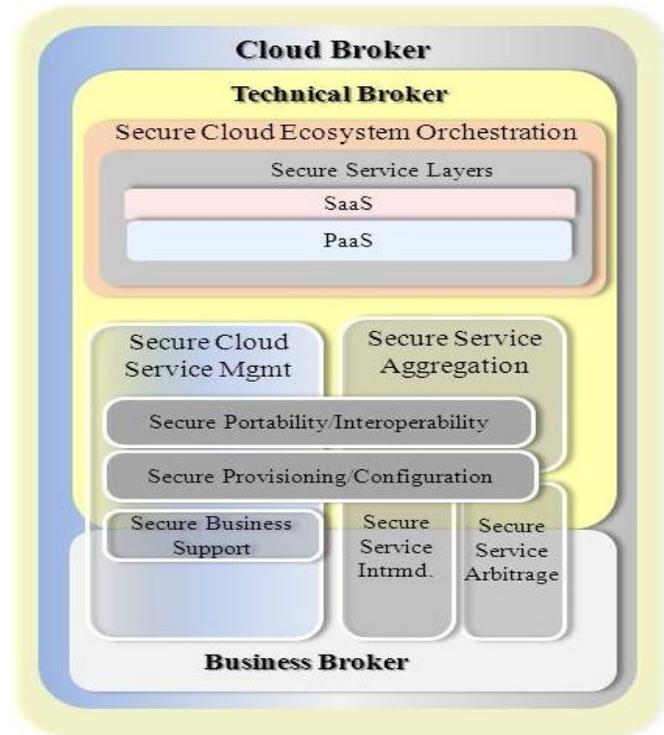


Figure 24: Cloud Broker – Architectural Components

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 address. Additional information of how to extract the Technical Broker’s set of security components is detailed in Section 4.3.

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-Base 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 migrated to the cloud.

5.4.1 TECHNICAL BROKER

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

As we emphasized earlier in Section 2.2.3, 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 such that they 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 Figure 23) 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* architectural component. Since an Intermediary Provider is not aggregating services but rather embedding services offered by a Primary Provider, repackaging and reselling them, the business and technical aspects of the activity cannot be separately identified. However, the overall set of *security components* that would 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.

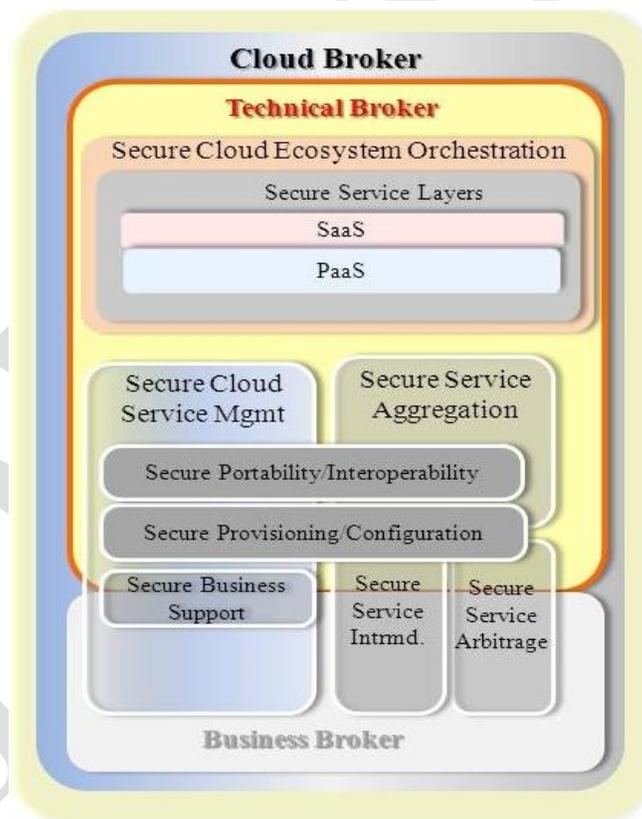


Figure 25: Technical Broker – Architectural Components

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

compose to deliver their services. The overall set of architectural components and their sub-components is:

- Secure Service Aggregation,
 - Secure Portability/Interoperability (technical aspects),
 - Secure Provisioning/Configuration (technical aspects);
- Secure Service Management
 - Secure Provisioning/Interoperability (management aspects)
 - Secure Provisioning/Configuration (management aspects),
 - Secure Business Support.
- Secure Service Intermediation,
 - Secure Provisioning/Configuration (technical aspects);
- Secure Service Arbitrage
 - Secure Provisioning/Configuration (technical aspects);
- Secure Cloud Ecosystem Orchestration
 - Secure Service Layer (technical aspects).

5.4.2 BUSINESS BROKER

Section 2.2.3 described the Business Broker as providing services such as business and relationship support services (arbitrage and business intermediation). A cloud Broker that only provides business and relationship services, plays the role of a Business Broker and does not have any contact with the cloud Consumer's data migrated to the cloud, with the Consumer's operational processes in the cloud or Consumer-based cloud artifacts such as images, volumes or firewalls.

Figure 26 depicts the Business Broker role in providing security services within the Security Reference Architecture.

The diagram illustrates the three *transparent* architectural components that represent the three types of activities a Business Broker may compose to deliver their services. The graphical transparency depicts the operational transparency into the cloud Providers a cloud Broker is required to ensure. The architectural components and their sub-components are:

- Secure Service Management
 - Secure Business Support.
- Secure Service Intermediation,
 - Secure Provisioning/Configuration (business aspects);
- Secure Service Arbitrage
 - Secure Provisioning/Configuration (business aspects);

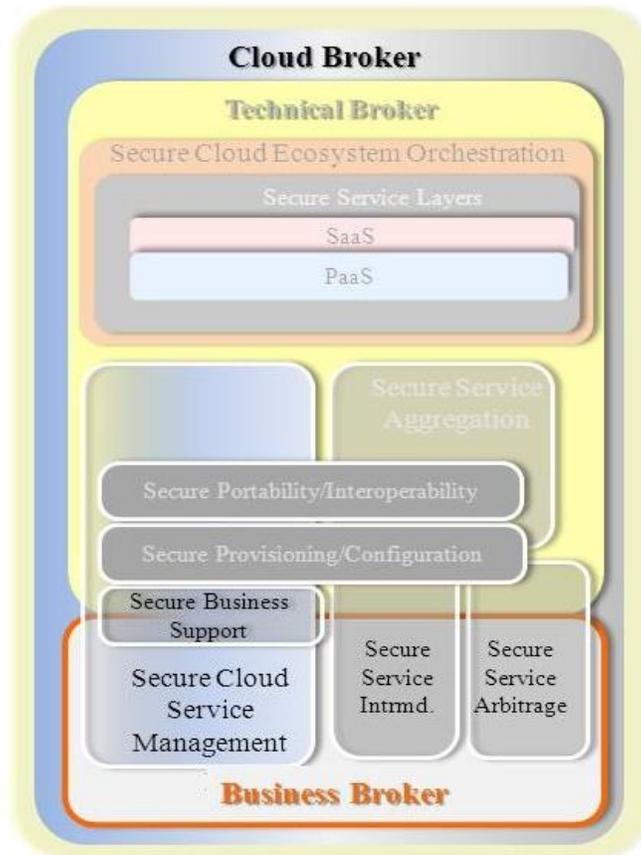


Figure 26: Business Broker – Architectural Components

For the sake of brevity, in the following section we discuss 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 sections 5.4.1.

5.4.3 SECURE CLOUD ECOSYSTEM ORCHESTRATION

The set of *security components* a cloud Broker can implement to secure the *Cloud Ecosystem Orchestration* depends upon the particular type of cloud service offered (e.g. PaaS, SaaS, etc.) and the cloud deployment model (e.g. Public, Private, etc.). 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 (SP 500-292, Figure 15) and 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 the *Secure Cloud Ecosystem Orchestration*.

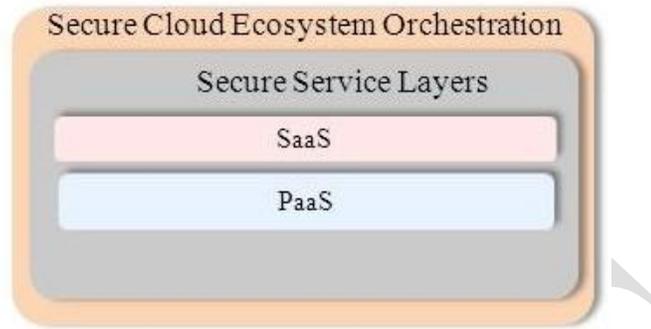


Figure 27: Secure Cloud Ecosystem Orchestration – Broker Stack Diagram

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

5.4.3.1 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 (e.g. IaaS, PaaS and SaaS) can stand by themselves 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 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 process of their service migrated to the cloud. Such tools could be integrated development environments (IDEs), development version of cloud software, software development kits (SDKs), or deployment and management tools, along with tools and processes that secures such aggregation.

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 the aggregated services offered by the Providers so that the services are provisioned to cloud Consumers at the expected service levels and met all identified security requirements,. The technical Brokers offering SaaS cloud Ecosystems assume most of the responsibilities in managing and controlling securely the applications.

A technical Broker does not participate in implementing *security components* and controls for the *Resource Abstraction and Control Layer* and the *Physical Resource Layer*.

In Annex E that provides the high-level *security components* mapped to the *architectural component* of a cloud Broker, the *Secure Service Layer* architectural component is coded “L” under the “Broker” section of the table.

5.4.4 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 data movement between the cloud consumer and multiple cloud Providers.

The *Secure Service Aggregation* architectural component addresses the technical Broker’s responsibilities of ensuring that all data, including service requests and responses to and from cloud Providers, maintain the required levels of confidentiality, integrity and availability, and appropriate levels of availability for the Consumer to underlying Providers is met as per Consumer’s security requirements stated in the contract and SLA. As a service aggregator, the technical Broker only supports Consumer’s data in transit and 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 Sections 4.3). The technical differences consist in 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 facing interface and the Broker-Provider(s) facing interface.

Two architectural subcomponents were identified for the Secure Service Aggregation:

- Secure Provisioning and Configuration – coded “aC” in Annex E under “Broker”
- Secure Portability and Interoperability – coded “aI” in Annex E under “Broker”

For a technical Broker, the security requirements for provisioning and configuring particular functionality offered to cloud Consumers are in principal similar to the security requirements a cloud Provider has for securing similar functionality (see sub-Section 5.3.2.1 for Provider for additional information).

In the same way, the security requirements a technical Broker should meet to ensure secure portability and interoperability are similar to the ones a cloud Provider has to satisfy to secure similar provisioned functionality (see sub-Section 5.3.2.2).

In Annex E that provides the high-level *security components* mapped to the *architectural component* of a cloud Broker, the *Secure Service Aggregation* architectural component is basically comprise of the sum between the *Secure Provisioning and Configuration* (aC) mapping and *Secure Portability and Interoperability* “aI” under the “Broker” section of the table.

5.4.5 SECURE CLOUD SERVICE MANAGEMENT

NIST Reference Architecture document describes the 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 and 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 perspectives 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 the cloud services:

- Secure Portability and Interoperability,
- Secure Provisioning and Configuration, and
- Secure Business Support.

5.4.5.1 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 set by cloud Consumer requirements. System maintenance time and disruptions should be kept at an acceptable minimum level as agreed in the Service Level Agreements. Brokers 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 interpretability vary based on cloud service type adopted.

In Annex E that provides the high-level *security components* mapped to the *architectural component* of a cloud Broker, the *Secure Portability and Interoperability* architectural subcomponent is coded “I” under the “Broker” section of the table.

5.4.5.2 SECURE PROVISIONING AND CONFIGURATION

The *Secure Provisioning and Configuration* architectural subcomponent 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 configuration and provisioning could address areas such as:

- *Rapid provisioning*: Automatically deploying cloud capabilities 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 bases upon updated security configuration requirements from 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, and 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 QoS parameters), SLA monitoring and SLA enforcement according to defined security policies.

In Annex E that provides the high-level *security components* mapped to the *architectural component* of a cloud Broker, the *Secure Provisioning and Configuration* architectural subcomponent is coded “C” under the “Broker” section of the table.

5.4.5.3 SECURE BUSINESS SUPPORT

The *Secure Business Support* architectural subcomponent entails the set of business-related services and supporting processes offered to Customers and it includes the *security components* used to run business operations that support the Broker’s role of enabling business support to 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.

In Annex E that provides the high-level *security components* mapped to the *architectural component* of a cloud Broker, the *Secure Business Support* architectural component is coded “B” under the “Broker” section of the table.

5.4.6 SECURE SERVICE INTERMEDIATION

A cloud Broker may enhance a given service by improving specific capability 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 addresses the Broker’s responsibilities of ensuring that all added capabilities to existing cloud services offered by Providers maintain the

required levels of confidentiality, integrity and availability, and that the Consumer’s requirements stated in the contract and/or SLA are met.

The *security components* 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 800-53 Identification and Authentication control family, while System and Communications Protection may be a lesser priority, since cloud Consumer’s data migrated to the cloud is not transiting the Broker’s cloud system. However, the difference is only one of emphasis since even for 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.

5.4.7 SECURE SERVICE ARBITRAGE

The *Secure Service Arbitrage* architectural component is, in principal, 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 his cloud Consumers. To do so, the cloud Broker can, for example, use a credit-scoring service to select the Provider(s) with the best score.

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, while the level of confidentiality, integrity and availability required by the Consumer in the contract and/or SLA are met.

In Annex E that provides the high-level SRA *security components* mapped to the *architectural component* of a cloud Broker, the *Secure Service Arbitrage* architectural component is coded “cA” under the “Broker” section of the table.

5.5 CARRIER – ARCHITECTURAL COMPONENTS

As noted in Section 2.2.4, and depicted in the Figure 29 below, the cloud Carrier is the cloud Actor that provides connectivity and transport of cloud services.

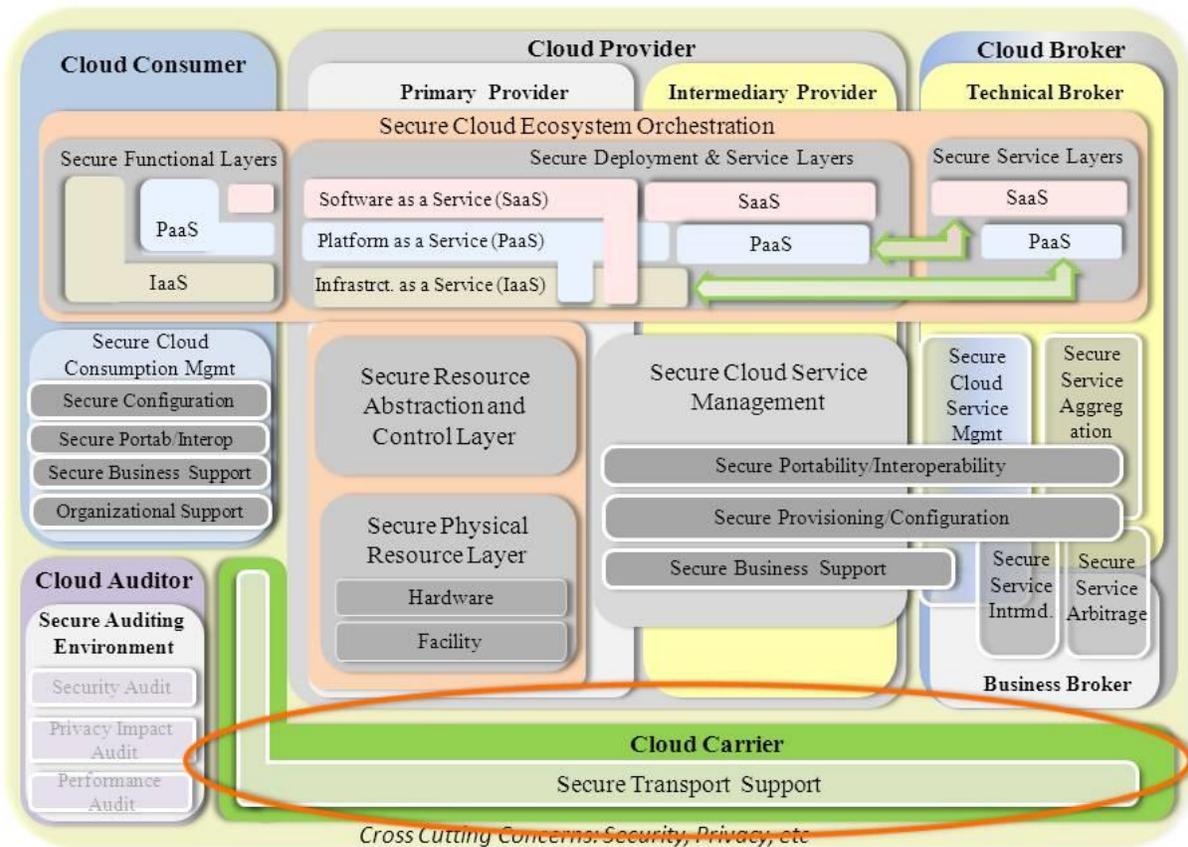


Figure 29: SRA – Cloud Carrier

From the Consumer’s standpoint, the cloud Carrier role is somewhat obscured due to the more direct relationship that Consumer may have with Provider and/or Broker - unless one of these parties is also performing 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.

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.

In Annex E that provides the high-level *security components* mapped to the *architectural component* of a cloud Carrier, the *Secure Transport Support* architectural component is coded “T” under the “Carrier” section of the table.

5.6 AUDITOR – ARCHITECTURAL COMPONENTS

As noted in Section 2.2.5, and depicted in the Figure 30 below, the cloud Auditor is the cloud Actor that conducts independent assessments of cloud services, information systems operations, performance, privacy impact and security of cloud implementations.

The cloud Auditor performs a large variety of audits such as security, privacy and performance audits, for any of the 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 audited of cloud Actor audited.

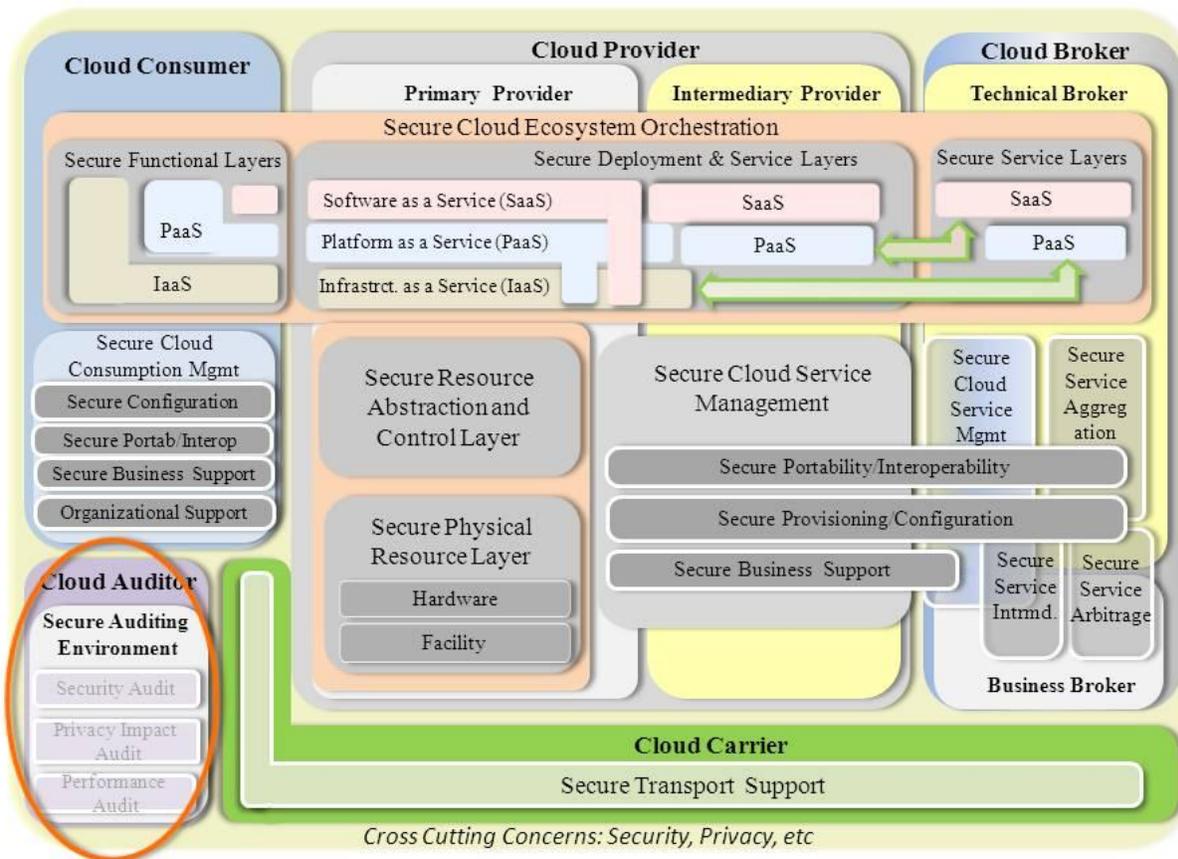


Figure 30: SRA – Cloud Auditor

The *Secure Auditing Environment* architectural component that supports cloud audit processes requires, but is not limited to, the following mechanisms to be in place:

- *Security Components and related security controls* – Information about the security components and the relevant security controls in place 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* – Collection of 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 process, Auditors may be required to ensure and 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.
- *SLA's* – 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 SLA's in a secure manner.
- *Privacy* – Privacy Impact assessments requires the availability of system security and configuration information as well as data protections implemented to protect data in the cloud.

In Annex E that provides the high-level *security components* mapped to the *architectural component* of a cloud Auditor, the *Secure Environment* architectural component is coded “E” under the “Auditor” section of the table.

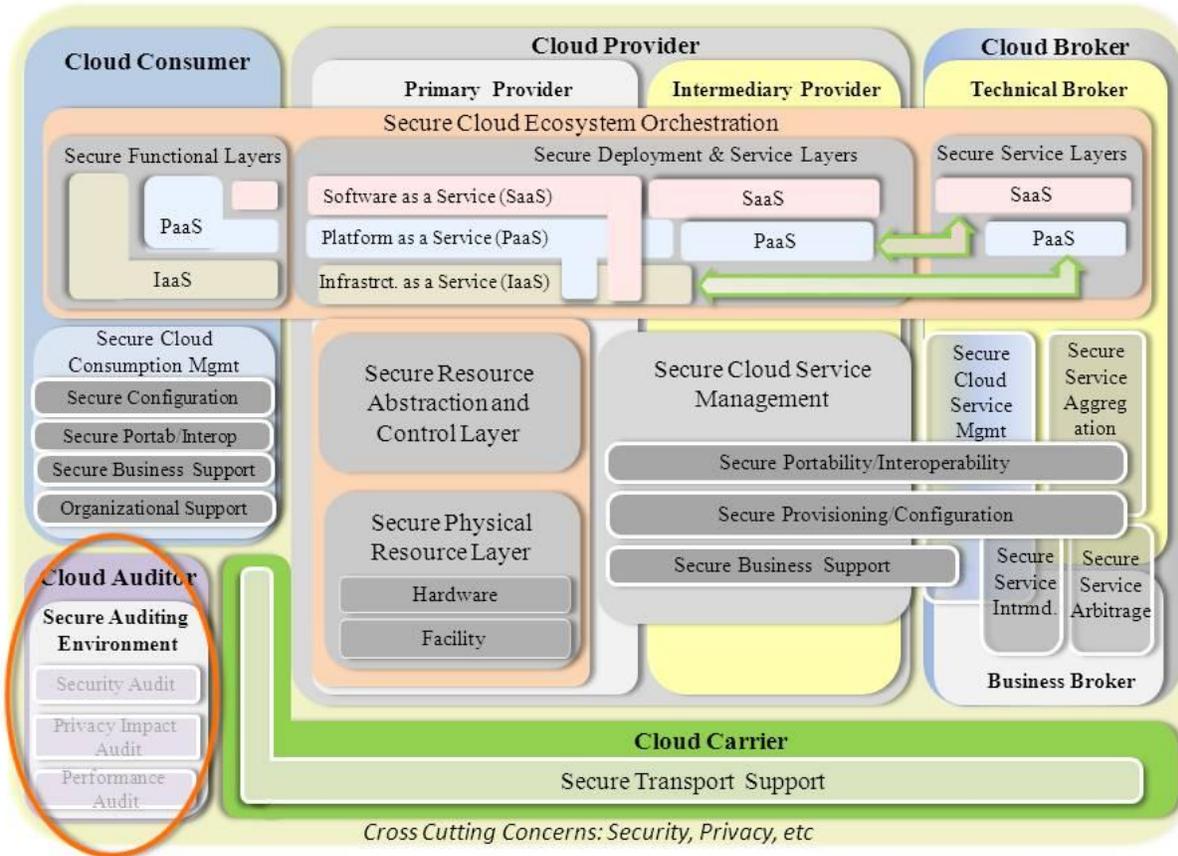


Figure 31: SRA – Cloud Auditor

DRAFT

6 SECURITY REFERENCE ARCHITECTURE: A METHODOLOGY OF ORCHESTRATING A CLOUD ECOSYSTEM

6.1 ORCHESTRATION METHODOLOGY OVERVIEW

The cloud *Actors* involved with the service models by either providing (cloud Providers), consuming (Cloud Consumers) or brokering (Cloud Broker) cloud offerings are dependent 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 collaboratively these responsibilities.

For those service models (IaaS, PaaS or SaaS) where the responsibilities of implementing the *security components* and to protect the data migrated to the Cloud are split among the Consumer, the Broker, and the Provider, regulatory and/or other security requirements need to be articulated among the cloud *Actors* involved in architecting and building the cloud Ecosystem. For example, in the case of implementing Intellectual Property (IP) protections, the cloud Consumer will need to clearly mark their IP information in transit and at rest while stored in the Cloud and that it is not to be shared with others. In turn, the cloud Provider will assert that the IP is indeed protected and secure and maintains it this way.

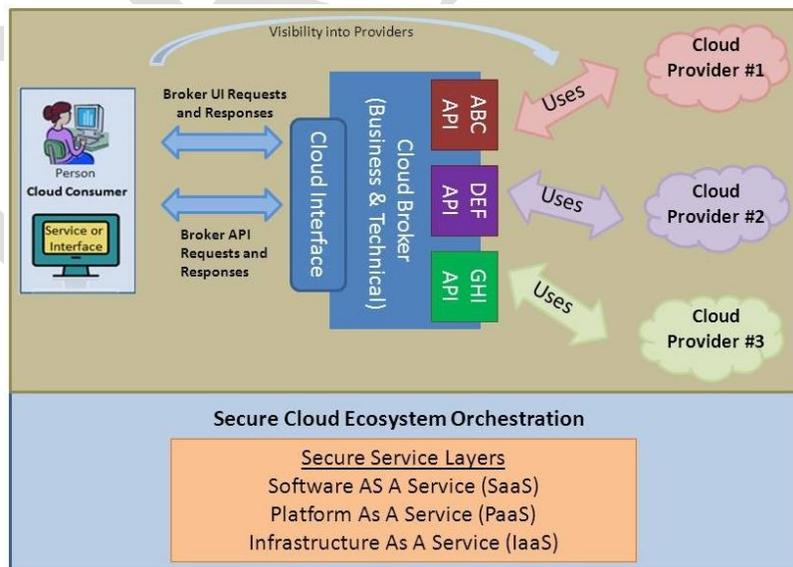


Figure 32: Secure Cloud Ecosystem Orchestration – Actors Interactions

Figure 31 depicts the interactions among the Consumer, the Provider, and the Broker while orchestrating a secure Cloud Ecosystem, for each of the Secure Service Layers defined in the SP 500-292, NIST Cloud Computing Reference Architecture such as: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

To better illustrate the interactions among cloud *Actors* and their roles and responsibilities in orchestrating a Secure Cloud Ecosystem, we will identify a use case of an USG agency service selected to be migrated to the cloud and follow all necessary steps to orchestrate a Secure Cloud Ecosystem, and identify 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 SRA.

6.2 CLOUD ECOSYSTEM ORCHESTRATION USE CASE

6.2.1 USE CASE DESCRIPTION

The use case illustrates the secure interactions between the Cloud Consumer, Cloud Broker and Cloud Provider while orchestrating a Secure Cloud Ecosystem for the migration and hosting of the Consumer's Unified Messaging Service (UMS) to the Cloud.

The cloud services are aggregated by the Technical Broker that enables additional functionality by providing a single User Interface (UI) and Application Programming Interface (API) for all cloud Providers whose services are aggregated. The cloud services are provided by multiple cloud Providers, all known to the cloud Consumer, including but not limited to cross-border entities, 3rd party contractors and subcontractors. 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 Section 4.4 for more details).

Consumer's Service Description

The cloud Consumer aims to reduce IT services support cost by implementing a cloud-based Unified Messaging Service. This service includes email, calendar, and synchronization with wireless mobile devices, and collaboration services. The current email system is classified as a Moderate Impact system based on NIST FIPS 199.

Current Messaging Service Capabilities:

The current email system supports a single sign-on (SSO) capability and supports multiple platforms for integrated messaging, calendar, and collaboration. Multiple clients are supported, such as email clients (Outlook, Thunderbird, MacMail, Entourage), calendar software (Outlook 2007,

Outlook 2010, and iCalendar), and common browsers (Internet Explorer 7.0, 8.0 & 9.0, Chrome, Firefox 3.x, and Safari) on operating systems such as Windows, Linux, and Mac OS. The current system also implements tools for spam filtering, anti-virus, anti-malware protection, anti-phishing protection, screening of outbound messages, and auto-forwarding restrictions.

Cloud Unified Messaging Service Requirements:

The new cloud-based UMS implementation is required to seamlessly support all capabilities of the current system. Additionally, the Consumer expects to improve the management of the service and to expand collaboration capabilities through increased use of integrated messaging and collaboration tools, and, optionally, to obtain archival and e-discovery capabilities. The 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 cloud-based UMS solution must provide users with the ability to share and collaborate on documents with both internal users and authenticated external users through a document repository. The document repository needs to provide version control, capturing information such as what has changed, who made the change, and when the change was made. A single Unified Interface (UI) portal would be used to access all aspects of the UMS. The UMS must include instant messaging and web conferencing as part of the solution, which must be also integrated in the interface as well.

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. Continuity and/or Transportability of services should be supported in order for the cloud Consumer to promptly resume services in the event of failures or catastrophes.

6.2.2 CLOUD SOLUTION ANALYSIS AND HIGH-LEVEL DESIGN

In the process of performing a risk analysis and researching the Cloud options (e.g. optimal deployment model, most suitable service type, necessary security components and associated security controls deemed necessary) for insuring the Moderate Impact level per FIPS 199 and FISMA compliance for the cloud-based UMS, the Consumer may use the information provided in this document. See Section 2.1 which outlines how cloud Consumers incorporate the Risk Management Framework into the selection of the appropriate security controls (NIST Special Publication 800-37 Rev 1).

After performing the risk assessment and identifying all security requirements for the system, the Consumer may leverage on the Security Reference Architecture (SRA) and the associated set of security components to identify the components important to be implemented for securing the UMS, prioritize these components, select the service type and the deployment model that best suits their needs, and identify the best composite architecture for the cloud Ecosystem of the UMS.

To build more flexibility into the framework provided by the SRA, in this section, in Table 5, we define a Security Index System (SIS) that provides five indexes perceived as *priority weights* a cloud Consumer may use while assessing the UMS’ security requirements to prioritize the implementation of *security components*.

We show how the cloud Consumer can assign Security Indexes to each *security component* (Annex E) considering the UMS service’s need for Confidentiality (C), Integrity (I) and Availability (A). Additionally, an Aggregated Security Index System (ASIS) can be obtained for each *security component* by summing the individual Security Indexes of the CIA security triad. The ASIS can be used to prioritize the implementation of the *security components*. A prioritization heat map like the one presented herein in Annex F, Section 15.3 for this use case can be created using the ASIS. When necessary, heat maps of the Confidentiality, Integrity, or Availability (CIA) security triad’s posture can be created in the same way we generated here the ASIS heat map.

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 CIA 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 Annex D, Section 11.1 table, for the service model adopted (IaaS, PaaS or SaaS).

Security Index Symbol	Security Index Value	Security Index Applicability
SIO	0	SIO should be applied to the Confidentiality, Integrity or Availability element associated with a <i>security component</i> when there is no priority to implement this component as there are no adverse effects on the cloud Ecosystem’s Confidentiality, Integrity or Availability security posture respectively.
SII	1	SII should be applied to the Confidentiality, Integrity or Availability element associated with a <i>security component</i> when there is a low priority to implement this component as it has limited* adverse effects on the cloud Ecosystem’s Confidentiality, Integrity or Availability security posture respectively.

SI2	2	SI2 should be applied to the Confidentiality, Integrity or Availability element associated with a <i>security component</i> when there is a moderate priority to implement the security component as it has a serious* effect on the cloud Ecosystem’s Confidentiality, Integrity or Availability security posture respectively.
SI3	3	SI3 should be applied to the Confidentiality, Integrity or Availability element associated with a <i>security component</i> when there is a high priority to implement the security component based upon severe**** effects on the cloud Ecosystem’s Confidentiality, Integrity or Availability security posture respectively.
SI4	4	SI4 should be applied to the Confidentiality, Integrity or Availability element associated with a <i>security component</i> when there is a critical priority to implement the security component based upon its critical**** effects the cloud Ecosystem’s Confidentiality, Integrity or Availability security posture respectively.

Table 5: Security Indexes System

In defining the Security Index System in Table 1, we leveraged the definitions provided by the Committee on National Security Systems in the “Security Categorization and Control Selection for National Security Systems” available at http://www.cnss.gov/Assets/pdf/Final_CNSSI_1253.pdf for different levels of adverse effects caused by the loss of Confidentiality, Integrity or Availability (CIA security triad).

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 confidentiality, integrity, or availability 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 confidentiality, integrity, or availability 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, for example, the loss of confidentiality, integrity, or availability 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 confidentiality, integrity, or availability might: (i) generate the 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; (ii) cause a catastrophic loss of mission capability to an extreme and long 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; or (iv) result in total financial loss; (v) result in catastrophic harm to individuals exceeding mission expectations.

In Annex F, Section 15.2 we present, the SIS for the CIA security triad and the ASIS used to prioritize the *security components* for the Unified Messaging System use case. The SIS example given in this document is not provided as guidance for any UMS migration to the cloud.

Coupling the prioritized set of *security components* with the data aggregated in the SRA that indicates cloud Actors' responsibilities of implementing and integrating the components for different service types (IaaS, PaaS, SaaS), the Consumer can make a more educated decision regarding the Cloud deployment model and service type that best suits the needs of their UMS.

The same aggregated information aids the cloud Consumer in selecting the cloud Ecosystem composition that best matches their internal expertise and required assurance levels. In our example, the Consumer selects for the implementation of the cloud-based UMS a "Software as a Service" (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. The cloud Consumer delegates the cloud Provider and cloud Technical Broker to install, patch, upgrade or backup applications and the associated data, but needs to be presented with verifiable proof that these operations are performed correctly and securely. The cloud Consumer is not concerned with the underlying cloud infrastructure or individual application capabilities beyond selecting an application that meets the Consumers' mission critical requirements.

To achieve all the above listed capabilities and requirements, the cloud Consumer seeks service from a cloud Broker requesting help with selecting an optimal mix of cloud Providers for their secure business support and required assurance levels. The cloud Consumer also seeks a full range of technical broker-based intermediation and service aggregation capabilities for aggregating services of multiple cloud Providers to meet its minimum design and requirements for service availability, single sign-on (SSO) for authenticating and authorizing end users. The Broker will provide the UI portal and Application Programming Interface (API) 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, secure cloud infrastructure service orchestration within and across cloud service Providers and 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 produces and delivers either rating and/or ranking assessments of the proposed cloud Provider or their marketplace based on the broker's cloud Provider arbitrage model. The cloud Consumer business and technical staff form business relationships with the cloud Providers selected from arbitrage, securely configure the Broker's technical interfaces with cloud Providers' credentials, and securely access the Broker's technical capabilities to carry out a range of intermediation and/or aggregation operations on the selected cloud Providers. The cloud Consumer selects the cloud Provider(s) after carefully evaluating the arbitrage results provided by the Broker.

An overall list of all categorizations and aspects of the secure Cloud Ecosystem Orchestration use case are summarized in Annex F, Section 13.1.

6.2.3 RISK ASSESSMENT 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 insure that, post migration to the cloud, the Unified Messaging System remains compliant with the Federal Information Security Management Act (FISMA).

The cloud Consumer will perform a risk assessment and identify all security controls necessary to be implemented for each *security component* identified as needed, for each cloud Actor involved in the Cloud Orchestration for the UMS. The SIS for the CIA security triad and the ASIS are transitively applied to the selected security controls. ARIS may provide a prioritization of the security controls. The cloud Consumer retains the security controls identified as its responsibility for in-house implementation and highlights the security controls the other cloud Actors need to have implemented to secure the UMS and to maintain the system's compliance with FISMA. The latest sets of security controls are translated into service requirements as part of SLA negotiation process as described later in this section.

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 the Step 2 of the [NIST SP 800-37 Risk Management Framework \(RMF\)](#) (see Section 2.1 of this document and the [NIST SP 00-37](#) document). For this purpose, as

guided by the NIST SP 800-37 document, cloud Consumer performs three tasks to accomplish the proper selection of security controls appropriate for their business and mission critical processes and services:

- TASK 2-1: Identify the security controls that are provided by the organization as common controls for organizational information systems and document the controls in a security plan (or equivalent document).
- TASK 2-2: Select the security controls for the information system and document the controls in the security plan.
- TASK 2-3: Develop a strategy for the continuous monitoring of security control effectiveness and any proposed or actual changes to the information system and its operational environment.

With the sets of security controls identified for each of the *security component* 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 Service Agreement and Service Level Agreement negotiation processes.

Section 2.1 of this document references the Risk Management Framework and the associated NIST security standards and guidelines that cloud Actors supporting the cloud Ecosystem Orchestration should follow to implement all steps described in the NIST SP 800-37, Risk Management Framework. Figure 32 below depicts the risk analysis and assessment steps described above.

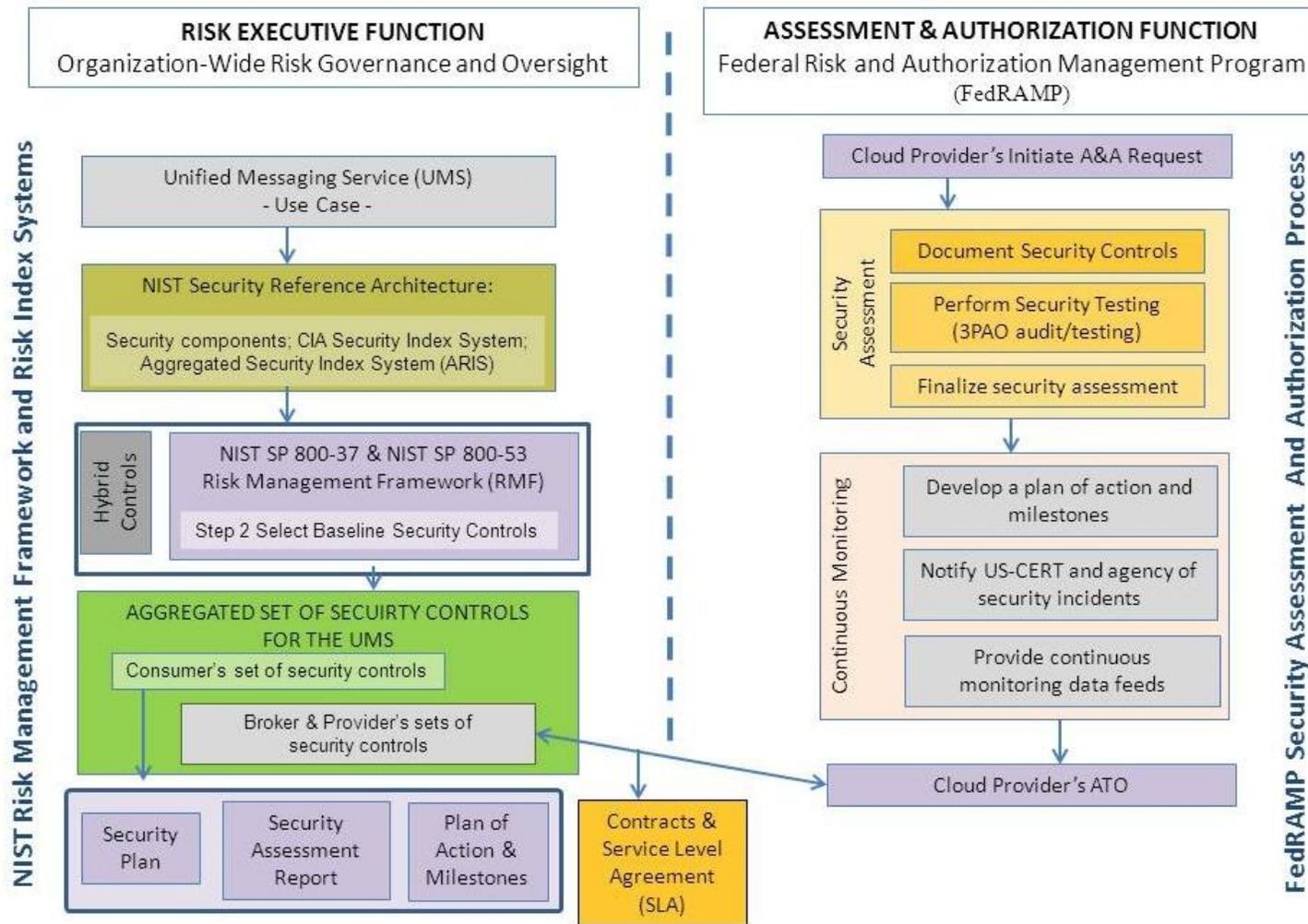


Figure 33: NIST Risk Management Framework and the FedRAMP A&A Process

6.2.4 CLOUD ECOSYSTEM HIGH-LEVEL ARCHITECTURE

In selecting the cloud Brokers and cloud Providers a US Government cloud Consumer needs to ensure that the selected parties have been Assessed and Authorized (A&A) by Federal Risk and Authorization Management Program (FedRAMP) and have been issued an Authorization to Operate (ATO). FedRAMP assesses systems that are categorized per [FIPS 199, Standards for Security Categorization of Federal Information and Information Systems](#), as *low* and *moderate impact* systems offered by cloud Providers. The assessment is done by third party assessors authorized by FedRAMP, while FedRAMP retains the authorization process. The assessment is done against specifically-defined security controls and baseline security controls for information systems defined in [NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations](#). The FedRAMP's set of security controls are also well aligned with [NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach](#). Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Cloud Consumer may leverage the ATO as a proof of proper implementation of the security controls assessed by FedRAMP and negotiate only the implementation of the security components that are necessary for the UMS but not included in the set of security controls assessed under FedRAMP.

6.2.5 SERVICE AGREEMENT OVERVIEW

An important step in the process of selecting the cloud Providers that meet the cloud Consumer's security requirements is the negotiation of the contractual terms and agreements; in completing the Service Level Agreements (SLA) and signing the service contract referred to as Service Agreement (SA). The Consumer needs to pay special attention to the SLAs and involve the agency's procurement, technical and policy experts to fulfill the agency's mission and fulfill the agency's performance requirements.

Cloud Service Agreements play an important role in the procurement of cloud computing services by specifying, in measurable terms, what cloud Provider will render to the cloud Consumer.

A part or sub-set of a cloud Service Agreement is the Service Level Agreement 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.

Since the basis of the provided services are specified within the contract and SLA, to accurately compare different offerings of cloud services it is necessary to be able to easily and accurately compare the underlying provisions of contracts and SLAs of all potential cloud Providers.

Figure 33 depicts a *mind map* of the basic components of a Service Agreement, including the cloud the corresponding Service Level Agreement (highlighted in blue).

At the time this document is written, there are no standards or specifications providing information or guidance on cloud computing contracts and Service Level Agreements. Therefore, cloud Providers are using self-defined contractual terms in their contracts and SLAs and cover self-identified resources, different time periods, covering, and offer different guarantees, making the Consumer’s evaluation and differential-analysis of the details received from different cloud Providers very difficult.

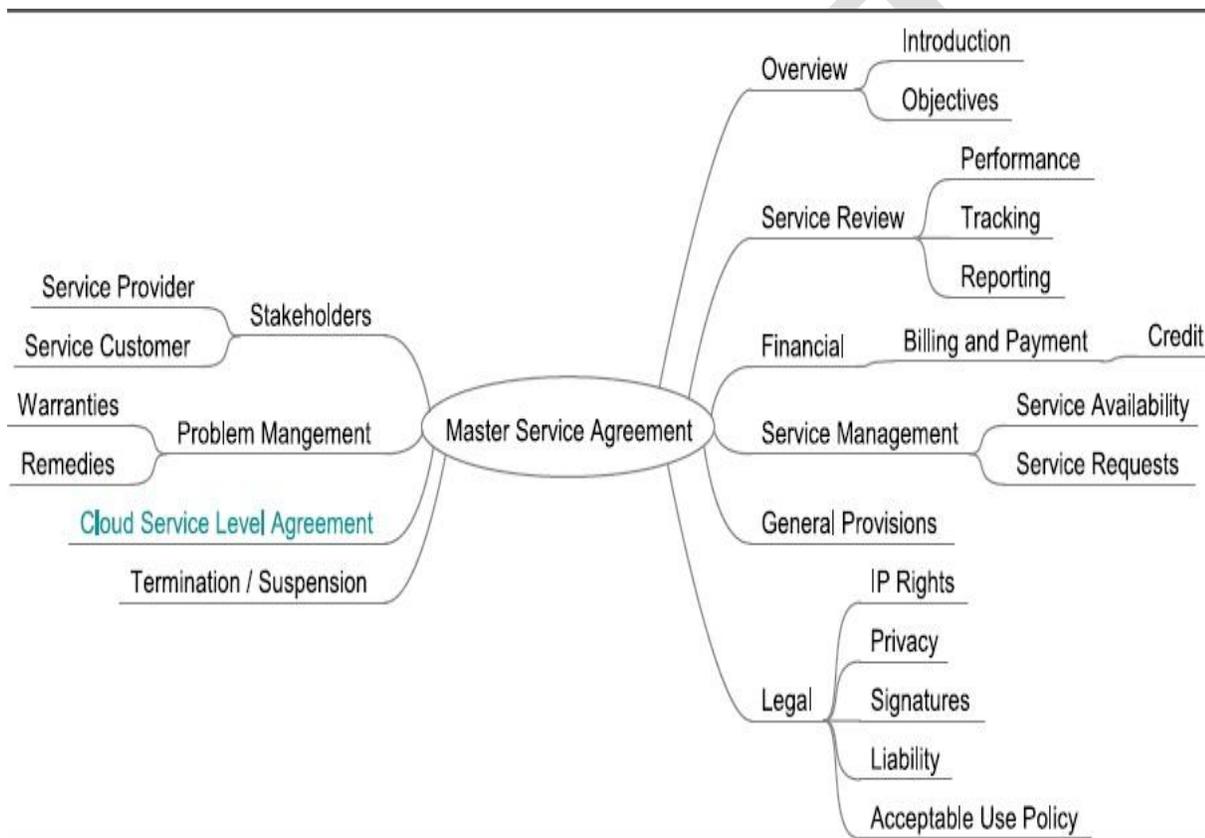


Figure 34: Service Agreement Mind Map

Another concern is that many cloud Providers offer a default contract that is often written to protect the Provider’s interests and can severely constrain the visibility of the cloud Consumer into the delivery mechanisms of the service. Therefore, without a thorough risk analysis coupled with a secure cloud Ecosystem orchestration like the one introduced in this document, and adequate guidance on negotiating SLAs, all of the ambiguities listed above leave the cloud Customer at risk in adopting cloud services.

In order to assess whether the levels of expectations defined in the customer-based SLA have been met, metrics are needed. These metrics define the measures to be used (i.e. availability) and the range of acceptable results of a particular measurement (i.e. 99.5%).

These metrics are a critical piece of the SLA section of an SA 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.

NIST, in collaboration with other government agencies, is continuously striving to provide useful information on this topic. NIST 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

Until formal guidance on SLA and cloud service metrics are available, the set of prioritized *security components* and associated security controls identified to be implemented by each cloud Actor in the secure cloud Ecosystem orchestration process as derived by the methodology described in this SRA 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 continuously or periodically monitored to ensure compliance with all functional and security requirements set forth in the SLAs and SAs.

7 SECURITY REFERENCE ARCHITECTURE: CLOUD DEPLOYMENT MODES

[THIS IS A PLACE HOLDER FOR THE FINAL DISCUSSION OF THE CLOUD DEPLOYMENT MODES]

As identified in the [NIST SP 800-145, “A NIST definition of cloud computing”](#), a cloud infrastructure may be operated in one of the following *deployment models*: Public cloud, Private cloud, Community cloud, or Hybrid cloud. The differences are based on how exclusive the computing resources are made to a cloud Consumer.

A Public cloud is owned by an organization selling cloud services. The Cloud serves multiple public Consumers and has the infrastructure and computing resources made available to the general public over a public network.

The five essential characteristics that all types of cloud services exhibit:

- *on-demand self-service,*
- *broad network access,*
- *resource pooling,*
- *rapid elasticity,* and
- *measured service.*

Annex D provides a complete set of collected, validated, and aggregated data for a Public cloud, Data is aggregated by cloud *Actor* in section 13.1 and by cloud Ecosystem with emphasis on the service types in Section 15.2. In these tables, each row represents a *security component*. In section 13.1, where data is aggregated per cloud *Actor*, each column under the *Actor* representing a service type: IaaS, PaaS and SaaS. In section 13.2, where data is aggregated per cloud Ecosystem based on the service type, column under a service type represents an Actors.

8 GLOSSARY AND ACRONYMS

A&A:	Assessment and Authorization
Assessment:	in this contest, 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 http://www.gsa.gov/portal/category/102371
CA:	Certificate Authority
C&A:	Certification and Accreditation – terminology replaced by “Assessment and Authorization”.
Chain of custody:	the seizure, custody, control, transfer, analysis, and disposition of physical or electronic evidence.
CPE:	Customer Premises Equipment
Cloud Auditor:	see NIST SP-500-292 Reference Architecture
Cloud Broker:	see NIST SP-500-292 Reference Architecture
Cloud Consumer:	see NIST SP-500-292 Reference Architecture
Cloud Carrier:	see NIST SP-500-292 Reference Architecture
Cloud Provider:	see NIST SP-500-292 Reference Architecture
FedRAMP:	the Federal Risk and Authorization Management Program – see http://www.gsa.gov/portal/category/102371 for more information.
FISMA:	Federal Information Security Management Act – see http://www.nist.gov/itl/csd/sma/fisma.cfm
FIPS:	Federal Information Processing Standard- see http://www.nist.gov/itl/fips.cfm for more information

- GSA: General Service Administration- see <http://www.gsa.gov> for additional information
- Hypervisor: one of many hardware virtualization techniques allowing multiple operating systems to run concurrently on a host computer (also called Virtual Machine Manager (VMM))
- IaaS: Infrastructure as a Service – see NIST SP 500-292 for additional information
- 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.
- PaaS: Platform as a Service – see NIST SP 500-292 for additional information
- SaaS: Software as a Service – see NIST SP 500-292 for additional information

DRAFT

9 REFERENCES

Vivek Kundra (US CIO), “25 Point Implementation Plan to Reform Federal Information Technology Management”, December 2010, <https://cio.gov/wp-content/uploads/downloads/2012/09/25-Point-Implementation-Plan-to-Reform-Federal-IT.pdf>.

Vivek Kundra (US CIO), “Federal Cloud Computing Strategy”, February 8, 2011, <http://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf>.

Office of Management and Budget, Circular A-130, Section 8b (3), “Securing Agency Information Systems”, <http://csrc.nist.gov/drivers/documents/a130trans4.pdf>.

Federal Information Security Management Act of 2002 (Title III of E-Gov), December 2002, <http://csrc.nist.gov/drivers/documents/FISMA-final.pdf>

Michael Hogan et. al., “NIST Cloud Computing Standards Roadmap”, NIST SP 500-291, July 2011, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909024.

Fang Liu et. al., “NIST Cloud Computing Reference Architecture”, NIST SP 500-292, September 2011, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505.

US Government Cloud Computing Technology Roadmap Volume I, High-Priority requirements to Further USG Agency Cloud Computing Adoption, NIST SP 500-293 (vol. 1), <http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/Documents>.

US Government Cloud Computing Technology Roadmap Volume II, Useful Information for Cloud Adopters, Draft NIST SP 500-293 (vol. 2), <http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/Documents>.

Join Task Force Transformation Initiative, “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach”, NIST SP 800-37, February 2010, <http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>

Join Task Force Transformation Initiative, “Recommended Security Controls for Federal Information Systems and Organizations”, NIST SP 800-53, Rev.3, August 2009, <http://csrc.nist.gov/publications/PubsSPs.html>.

Kelly Dempsey, et. al. “Information Security Continuous Monitoring for Federal Information Systems and Organizations”, NIST SP 800-137, September 2011, <http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf>.

Wayne Jansen and Tim Grance, “*The NIST Definition of Cloud Computing*”, NIST SP 800-144, December 2011, <http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf>.

Peter Mell and Tim Grance, “*The NIST Definition of Cloud Computing*”, NIST SP 800-145, August 2011, <http://csrc.nist.gov/publications/nistpubs/800-145/sp800-145.pdf>.

Lee Badger, et. al., “*Cloud Computing Synopsis and Recommendations*”, May 2012, <http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf>.

Cade Metz, DDoS Attack Rains Down on Amazon Cloud, The Register, October 5, 2009, http://www.theregister.co.uk/2009/10/05/amazon_bitbucket_outage/.

Zhifeng Xiao and Yang Xiao, Security and Privacy in Cloud Computing, IEEE Communication Surveys & Tutorials, Accepted for Publication, 2012, http://zxiao.students.cs.ua.edu/pub/Xiao_CloudSecurity.pdf

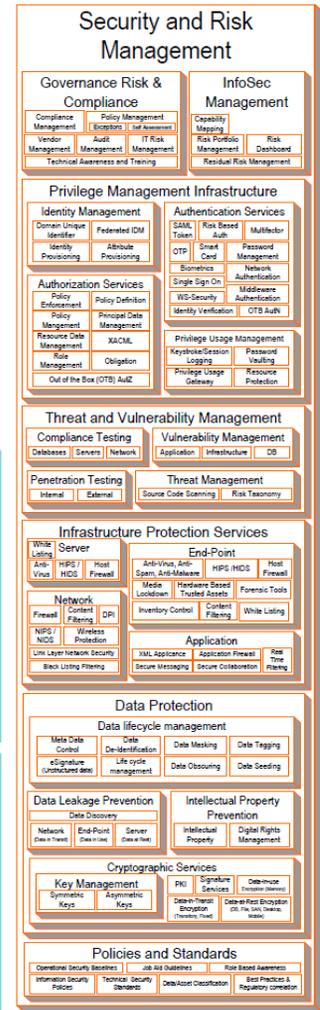
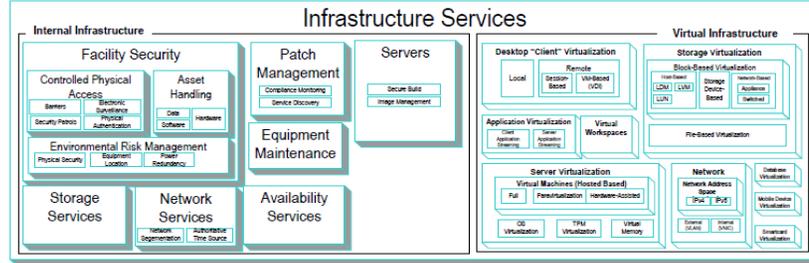
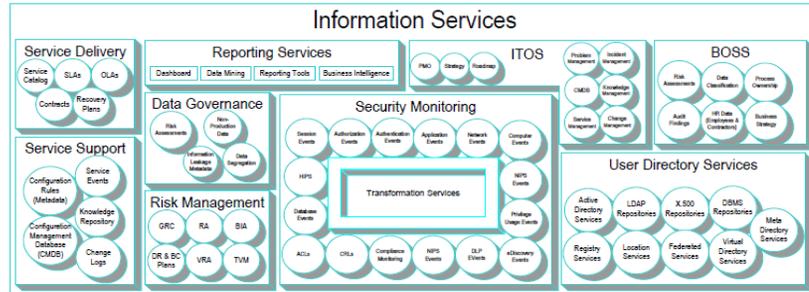
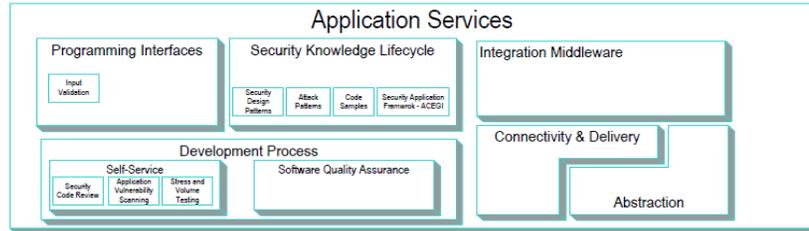
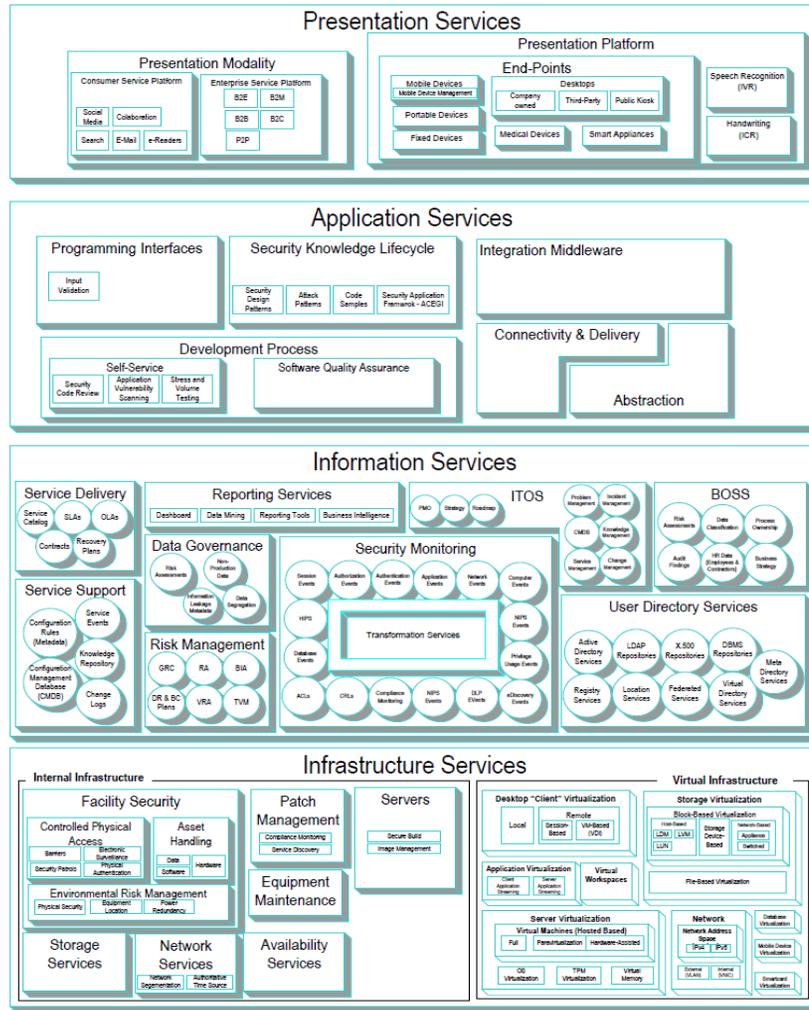
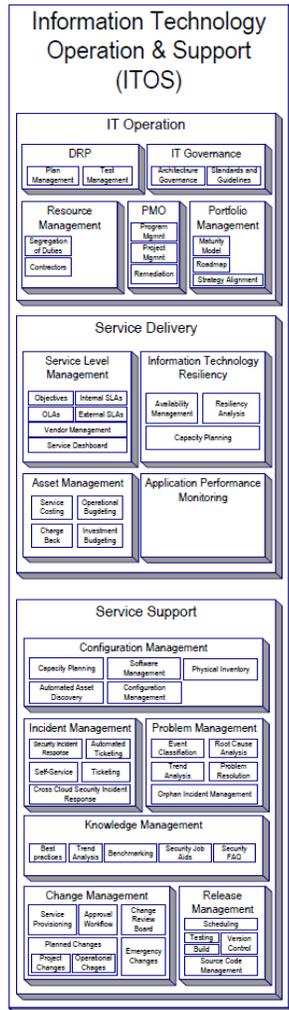
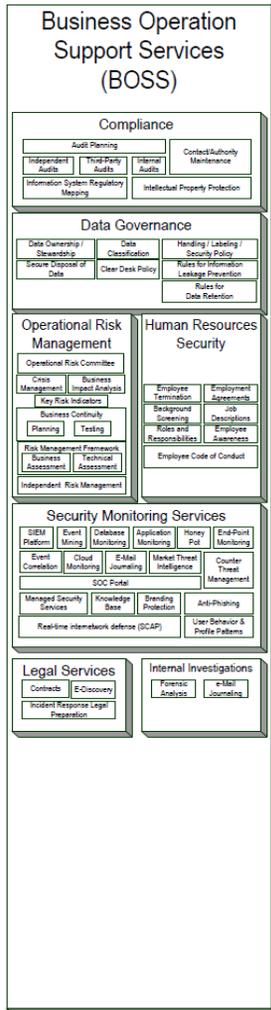
DRAFT

APPENDIX A: ACTIVE MEMBERS

Richard J Blake, General Services Administration
Ron Martin, Open Security Exchange
Sundararajan Ramanathan, Capgemini

DRAFT

10 ANNEX A: TRUSTED COMPUTING INITIATIVE REFERENCE ARCHITECTURE



13 ANNEX D: AGGREGATED DATA

13.1 ACTORS-BASED DATA AGGREGATION

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	A	L
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	
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	
BOSS	Data Governance	Secure Disposal of Data		M P	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		P M	X	X	A	A	A	X	B	B	B	A	A
BOSS	Operational Risk Management	Operational Risk Committee		P M	X	A	A	X	X	X	A	A	A	A	A
BOSS	Operational Risk Management	Key Risk Indicators		P M	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	AC	X	X	X	X	X	X	B	B	B	A	A
ITOS	IT Operations	Resource Management	Contractors	AC	A	A	A	A	A	A	A	A	A	A	A
ITOS	Service Delivery	Information Technology Resiliency	Resiliency Analysis	AU	X	A	A	X	X	X	B	B	B	A	
ITOS	Service Delivery	Information Technology Resiliency	Capacity Planning	AU	X	A	A	X	X	X	B	B	B	A	
ITOS	Service Support	Configuration Management	Automated Asset Discovery	AU	A	A	A	A	A	A	B	B	B	A	
ITOS	Service Support	Problem Management	Event Classification	AU	X	X	X	A	X	X	B	B	B	A	A
ITOS	Service Support	Problem Management	Root Cause Analysis	AU	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	CM	A	A	A	A	A	A	A	A	A		
ITOS	Service Support	Configuration Management	Software Management	CM	X	X	A	X	X	X	B	B	B	A	
ITOS	Service Support	Configuration Management	Configuration Management	CM	X	X	A	X	X	X	B	B	B	A	
ITOS	Service Support	Configuration Management	Physical Inventory	CM	A	A	A	A	A	A	B	B	B	A	
ITOS	Service Support	Knowledge Management	Benchmarking	CM	A	A	A	A	A	A	A	A	A	X	A
ITOS	Service Support	Knowledge Management	Security Job Aids	CM	A	A	A	A	A	A	A	A	A	X	A
ITOS	Service Support	Knowledge Management	Security FAQ	CM	A	A	A	A	A	A	A	A	A	A	A
ITOS	Service Support	Change Management	Service Provisioning	CM	A	A	A	X	X	X	A	A	A	X	A
ITOS	Service Support	Change Management	Approval Workflow	CM	A	A	A	X	X	X	A	A	A	A	
ITOS	Service Support	Change Management	Change Review Board	CM	A	A	A	X	X	X	A	A	A	A	
ITOS	Service Support	Change Management	Planned Changes	CM	A	A	A	X	X	X	A	A	A	A	
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	M A	A	A	A	X	X	X	A	A	A	A	
ITOS	Service Support	Release Management	Scheduling	M A	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	P M	X	A	A	X	X	X	B	B	B	X	A
ITOS	IT Operations	IT Governance	Architecture Governance	P M	A	A	A	A	A	A	A	A	A	X	-
ITOS	IT Operations	IT Governance	Standards and Guidelines	P M	X	X	X	A	X	X	A	A	A	A	
ITOS	IT Operations	PMO	Program Mngmt	P M	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	
ITOS	IT Operations	Portfolio Management	Roadmap	P M	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		
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	AC	X	X				X	B	B	B		
Presentation Services	Presentation Modality	Consumer Service Platform	Collaboration	AC	X	X				X	B	B	B		
Presentation Services	Presentation Modality	Consumer Service Platform	E-Mail	AC	X	X				X	B	B	B		

Presentation Services	Presentation Modality	Enterprise Service Platform	B2M	AC	X	X	X	A	A	X	B	B	B		
Presentation Services	Presentation Modality	Enterprise Service Platform	B2B	AC	X	X	X	A	A	X	B	B	B		
Presentation Services	Presentation Modality	Enterprise Service Platform	B2C	AC	X	X	X	A	A	X	B	B	B		
Presentation Services	Presentation Modality	Enterprise Service Platform	P2P	AC	X	X	X	A	A	X	B	B	B		
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
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	
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		C M	A	A	A	A	A	A	A	A	A	x
Information Services	Service Delivery	SLA's		C M	A	A	A	X	X	X	B	B	B	A
Information Services	ITOS	CMDB		C M	A	A	A	X	X	X	B	B	B	A
Information Services	ITOS	Change Management		C M	A	A	A	X	X	X	B	B	B	A
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		CP	A	A	A	X	X	X	A	A	A	A
Information Services	BOSS	GR Data (Employee & contractors)		IA	A	A	A	A	A	A	A	A	A	X

Information Services	Security Monitoring	Authorization Events		IA	X	X	X	A	X	X	B	B	B	X	
Information Services	Security Monitoring	Authentication Events		IA	X	X	X	X	X	X	B	B	B	A	
Information Services	Security Monitoring	ACL's		IA	A	A	A	X	X	X	B	B	B	A	
Information Services	Security Monitoring	CRL's		IA	A	A	A	X	X	X	B	B	B	A	
Information Services	User Directory Services	Active Directory Services		IA	A	A	A	X	X	X	B	B	B	A	
Information Services	User Directory Services	LDAP Repositories		IA	A	A	A	X	X	X	B	B	B	A	
Information Services	User Directory Services	X.500 Repositories		IA	A	A	A	X	X	X	B	B	B	A	
Information Services	User Directory Services	DBMS Repositories		IA	X	A	A	A	X	X	B	B	B	A	
Information Services	User Directory Services	Registry Services		IA	A	A	A	X	X	X	B	B	B	A	
Information Services	User Directory Services	Location Services		IA	A	A	A				B	B	B	x	
Information Services	User Directory Services	Federated Services		IA	X	X	A	A	A	X	B	B	B	X	
Information Services	User Directory Services	Virtual Directory Services		IA	X	A	A	A	X	X	B	B	B	X	
Information Services	User Directory Services	Meta Directory Services		IA	X	A	A	A	X	X	B	B	B	A	
Information Services	ITOS	Incident Management		IR	X	X	X	X	X	X	B	B	B	A	
Information Services	Service Support	Service Events		IR	X	X	A	X	X	X	B	B	B	A	

Information Services	BOSS	Data Classification		RA	X	X	X	X	X	X	A	A	A	A	
Information Services	Data Governance	Risk Assessments		RA	X	X	X	A	A	A	B	B	B	X	
Information Services	Risk Management	Risk Assessments		RA	X	X	X	A	A	A	B	B	B	A	
Information Services	Risk Management	Business Impact Assessment.		RA	X	X	X	X	X	X	B	B	B	X	
Information Services	Risk Management	VRA		RA	X	X	X	A	A	X	B	B	B	x	A
Information Services	Risk Management	TVM		RA	X	X	X	A	A	X	B	B	B	x	
Information Services	Service Delivery	OLA's		SA	A	A	A	A	A	A	A	A	A	A	
Information Services	Data Governance	Non-Production Data		SA	X	X	X	A	X	X	B	B	B	A	
Information Services	Security Monitoring	NIPS Events		SC	X	A	A	X	X	X	B	B	B	A	
Information Services	Security Monitoring	DLP Events		SC	X	A	A	X	X	X	B	B	B	A	
Information Services	Data Governance	Information Leakage Metadata		SI	X	X	A	A	A	X	B	B	B	A	
Information Services	Data Governance	Data Segregation		SI	X	A		X	X	X	B	B	B	X	
Information Services	Security Monitoring	Transformation Services		SI	X	X	A	X	X	X	B	B	B	A	
Information Services	Security Monitoring	Session Events		SI	X	X	A	X	X	X	B	B	B	A	
Information Services	Security Monitoring	Application Events		SI	X	X	A	A	A	X	B	B	B	A	

Information Services	Security Monitoring	Network Events		SI	X	X	A	A	X	X	B	B	B	X	
Information Services	Security Monitoring	Computer Events		SI	X	X	A	A	X	X	B	B	B	x	
Information Services	Security Monitoring	Host Intrusion Protection Systems (HIPS)		SI	X	X	A	A	A	X	B	B	B	A	
Information Services	Security Monitoring	Database Events		SI	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	
Information Services	Risk Management	GRC		P M	X	X	X	A	X	X	A	A	A	A	A

Information Services	Risk Management	DR & BC Plans		P M	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		M A				A	A	A	B	B	B	A	
Infrastructure Services	Internal Infrastructure: Equipment Maintenance			M A				A	A	A	B	B	B	A	
Infrastructure Services	Internal Infrastructure: Storage Services			M P				A	A	A	B	B	B	A	A
Infrastructure Services	Virtual Infrastructure: Storage Virtualization	Block-Based Virtualization	Storage Device-Based	M P	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	

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	
		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		SC	X	A	A	X	X	X	B	B	B	A	
		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		P M				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	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	Privilege Management Infrastructure	Identity Management	Domain Unique Identifier	IA	A	A	A	A	A	A	B	B	B	A	
S & RM	Privilege Management Infrastructure	Identity Management	Federated IDM	IA	X	X	A	A	A	X	B	B	B	A	
S & RM	Privilege Management Infrastructure	Identity Management	Identity Provisioning	IA	X	X	X	A	A	X	B	B	B	A	
S & RM	Privilege Management Infrastructure	Identity Management	Attribute Provisioning	IA	X	X	X	A	A	X	B	B	B	A	
S & RM	Privilege Management Infrastructure	Authorization Services	Policy Enforcement	IA	X	X	X	A	A	X	B	B	B	X	
S & RM	Privilege Management Infrastructure	Authorization Services	Policy definition	IA	X	X	X	A	A	X	B	B	B	A	
S & RM	Privilege Management Infrastructure	Authorization Services	Principal Data Management	IA	X	X	X	A	A	X	B	B	B	A	
S & RM	Privilege Management Infrastructure	Authorization Services	XACML	IA	A	A	A	X	X	X	B	B	B	A	
S & RM	Privilege Management Infrastructure	Authorization Services	Role Management	IA	X	X	X	X	X	X	B	B	B	A	

S & RM	Privilege Management Infrastructure	Authorization Services	Obligation	IA	A	A	A	X	X	X	B	B	B	A	
S & RM	Privilege Management Infrastructure	Authorization Services	Out of the Box (OTB) autZ	IA	X	A	A	X	X	X	B	B	B	A	
S & RM	Privilege Management Infrastructure	Authentication Services	SAML Token	IA	A	A	A	X	X	X	B	B	B	X	
S & RM	Privilege Management Infrastructure	Authentication Services	Risk Based Authentication	IA	X	X	X	X	X	X	B	B	B	X	
S & RM	Privilege Management Infrastructure	Authentication Services	Multifactor	IA	X	X	A	X	X	X	B	B	B	X	
S & RM	Privilege Management Infrastructure	Authentication Services	OTP	IA	A	A	A	X	X	X	B	B	B	A	
S & RM	Privilege Management Infrastructure	Authentication Services	Smart Card	IA	X	X	A	A	A	X	B	B	B	A	
S & RM	Privilege Management Infrastructure	Authentication Services	Password Management	IA	X	X	X	X	X	X	B	B	B	X	
S & RM	Privilege Management Infrastructure	Authentication Services	Biometrics	IA	X	X	X	A	A	X	B	B	B	A	
S & RM	Privilege Management Infrastructure	Authentication Services	Network Authentication	IA	X	A	A	X	X	X	B	B	B	A	
S & RM	Privilege Management Infrastructure	Authentication Services	Single Sign On	IA	A	A	A	X	X	X	B	B	B	A	
S & RM	Privilege Management Infrastructure	Authentication Services	WS-Security	IA	X	X	A	X	X	X	B	B	B	A	
S & RM	Privilege Management Infrastructure	Authentication Services	Middleware Authentication	IA	X	X	A	X	X	X	B	B	B	A	
S & RM	Privilege Management Infrastructure	Authentication Services	Identity Verification	IA	X	X	X	X	X	X	B	B	B	A	
S & RM	Privilege Management Infrastructure	Authentication Services	Out-of-The-Box (OTB) Authentication	IA	X	X	A	X	X	X	B	B	B	A	

S & RM	Privilege Management Infrastructure	Privilege Usage Management	Keystroke/Session Logging	IA	X	X	X	X	X	X	B	B	B	A	
S & RM	Privilege Management Infrastructure	Privilege Usage Management	Password Vaulting	IA	X	X	A	X	X	X	B	B	B	A	
S & RM	Threat and Vulnerability Management	Compliance Testing	Network Authentication	IA	X	X	A	X	X	X	B	B	B	A	A
S & RM	Infrastructure Protection Services	End-Point	Forensic Tools	IR	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		PL	X	X	A	A	X	X	B	B	B	A	
S & RM	Governance Risk & Compliance	Policy Management	Exceptions	RA	X	X	X	X	X	X	B	B	B	X	A
S & RM	Governance Risk & Compliance	Policy Management	Self-Assessment	RA	X	X	X	A	A	A	B	B	B	A	A
S & RM	InfoSec Management	Risk Dashboard		RA	X	X	X	X	X	X	B	B	B	A	
S & RM	Threat and Vulnerability Management	Vulnerability Management	application	RA	X	X	A	X	X	X	B	B	B	A	A
			Infrastructure	RA	X	A	A	X	X	X	B	B	B	A	A
			DB	RA	X	X	A	X	X	X	B	B	B	X	A
		Penetration Testing	Internal	RA	X	X	A	A	X	X	B	B	B	X	A
			External	RA	X	X	A	X	X	X	B	B	B	X	A
		Threat Management	Source Code Scanning	RA	X	X	X	X	X	X	B	B	B	X	A
			Risk Taxonomy	RA	X	X	X	A	X	X	B	B	B	X	
S & RM	Policies and Standards	Data/ Asset Classification		RA	X	X	X	X	X	X	A	A	A	X	A

S & RM	Governance Risk & Compliance	Vendor Management		SA	X	X	X	X	X	X	B	B	B	X	A
S & RM	Data Protection	Data Lifecycle Management	Life cycle management	SA	X	X	X	X	X	X	B	B	B	X	A
S & RM	Policies and Standards	Technical Security Standards		SA	X	X	X	X	X	X	A	A	A	X	A
S & RM	Privilege Management Infrastructure	Privilege Usage Management	Resource Protection	SC	A	A	A	X	X	X	B	B	B	A	
S & RM	Infrastructure Protection Services	Network	Deep Packet Inspection (DPI)	SC	X	A	A	X	X	X	B	B	B	A	A
S & RM	Infrastructure Protection Services	Network	Wireless Protection	SC	A	A	A	X	X	X	B	B	B	A	A
S & RM	Infrastructure Protection Services	Network	Link Layer Network security	SC	A	A	A	X	X	X	B	B	B	A	A
S & RM	Infrastructure Protection Services	Application	XML Appliance	SC	X	X	A	A	X	X	B	B	B	A	A
S & RM	Infrastructure Protection Services	Application	Secure Messaging	SC	X	X	A	A	A	X	B	B	B	A	A
S & RM	Data Protection	Data Lifecycle Management	Data De-Identification	SC	X	X	X	A	X	X	B	B	B	A	A
S & RM	Data Protection	Data Lifecycle Management	Data Masking	SC	X	X	X	A	X	X	B	B	B	A	A
S & RM	Data Protection	Data Lifecycle Management	Data Tagging	SC	X	X	A	A	X	X	B	B	B	A	A
S & RM	Data Protection	Data Lifecycle Management	Data Obscuring	SC	X	X	X	A	X	X	B	B	B	A	A
S & RM	Data Protection	Data Leakage Prevention	Data Discovery	SC	X	X	X	A	X	X	B	B	B	A	A
S & RM	Data Protection	Data Leakage Prevention	Network (Data in Transit)	SC	X	X	A	X	X	X	B	B	B	A	A

S & RM	Data Protection	Data Leakage Prevention	End-Point (data in Use)	SC	X	X	X	X	X	X	B	B	B	A	A
S & RM	Data Protection	Data Leakage Prevention	Server (data at Rest)	SC	X	X	A	X	X	X	B	B	B	A	A
S & RM	Cryptographic Services	Key Management	Symmetric Keys	SC	X	X	X	X	X	X	B	B	B	A	A
S & RM	Cryptographic Services	Key Management	Asymmetric Keys	SC	X	X	X	X	X	X	B	B	B	A	A
S & RM	Cryptographic Services	PKI		SC	X	X	X	X	X	X	B	B	B	A	A
S & RM	Cryptographic Services	Data in use (memory) Encryption		SC	X	X	A	X	X	X	B	B	B	A	A
S & RM	Cryptographic Services	Data in Transit Encryption (Transitory, Fixed)		SC	X	X	X	X	X	X	B	B	B	A	A
S & RM	Cryptographic Services	Data as Rest Encryption (DB, File, SAN, Desktop, Mobile)		SC	X	X	X	X	X	X	B	B	B	X	A
S & RM	Infrastructure Protection Services	Server	Anti-virus	SI	X	X	A	X	X	X	B	B	B	X	
S & RM	Infrastructure Protection Services	Server	HIPS/HIDS (Intrusion Protection /Detection)	SI	X	A	A	X	X	X	B	B	B	X	
S & RM	Infrastructure Protection Services	End-Point	Anti-Virus, Anti-Spam, Anti-Malware	SI	X	X	A	A	A	X	B	B	B	X	
S & RM	Infrastructure Protection Services	End-Point	HIPS/HIDS (Intrusion Protection /Detection)	SI	X	X	A	A	X	X	B	B	B	X	A
S & RM	Infrastructure Protection Services	End-Point	Hardware Based trusted Assets	SI	A	A	A	X	X	X	B	B	B	X	A
S & RM	Infrastructure Protection Services	Network	NIPS/NIDS	SI	X	A	A	X	X	X	B	B	B	X	A
S & RM	Data Protection	Data Lifecycle Management	eSignature	SI	X	X	X	A	X	X	B	B	B	A	A

S & RM	Cryptographic Services	Signature Services		SI	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

13.2 SERVICE-BASED ECOSYSTEM-LEVEL DATA AGGREGATION

Security component definitions can be found on the [CSA's interactive site: https://research.cloudsecurityalliance.org/tci/](https://research.cloudsecurityalliance.org/tci/)

Domain	High-level Security Component	Mid-level Security Component	Low-level Security Component	800-53 Family	IaaS				PaaS				SaaS				Carrier	Auditor
					Consumer	Provider	Broker	U	Consumer	Provider	Broker	U	Consumer	Provider	Broker	U	A	L
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
BOSS	Security Monitoring Services	Event Correlation		AU
BOSS	Security Monitoring Services	Email Journaling		AU
BOSS	Security Monitoring Services	User Behaviors and Profile Patterns		AU
BOSS	Legal Services	E-Discovery		AU
BOSS	Legal Services	Incident Response Legal Preparation		AU
BOSS	Internal Investigations	Forensic Analysis		AU
BOSS	Internal Investigations	e-Mail Journaling		AU
BOSS	Compliance	Independent Audits		CA
BOSS	Compliance	Third Party Audits		CA
BOSS	Operational Risk Management	Business Impact Analysis		CP
BOSS	Operational Risk Management	Business Continuity		CP
BOSS	Operational Risk Management	Crisis Management		IR
BOSS	Operational Risk	Risk Management		IR

X	A	B	X
X	A	B	X
X	A	B	X
X	A	B	X
X	X	A	X
X	X	A	X
X	X	A	X
X	X	A	X
A	A	A	A
A	A	B	Ab
A	A	B	Ab
A	X	A	X
X	X	B	X
A	X	B	X
A	A	A	A

X	X	B	X
X	X	B	X
X	X	B	X
X	X	B	X
X	X	A	X
X	X	A	X
X	X	A	X
X	X	A	X
A	A	A	A
A	A	B	Ab
A	A	B	Ab
A	X	A	X
A	X	B	X
A	X	B	X
A	A	A	A

A	X	B	X
A	X	B	X
A	X	B	X
A	X	B	X
X	X	A	X
X	X	A	X
X	X	A	X
X	X	A	X
A	A	A	A
A	A	B	Ab
A	A	B	Ab
A	X	A	X
A	X	B	X
A	X	B	X
A	A	A	A

A	
X	
A	
A	A
A	A
A	A
X	A
X	A
X	A
A	A
A	A
X	
X	A
A	A

	Management	Framework		
BOSS	Operational Risk Management	Independent Risk Management		IR
BOSS	Security Monitoring Services	Database Monitoring		IR
BOSS	Security Monitoring Services	Application Monitoring		IR
BOSS	Security Monitoring Services	End-Point Monitoring		IR
BOSS	Security Monitoring Services	Cloud Monitoring		IR
BOSS	Data Governance	Secure Disposal of Data		MP
BOSS	Human Resource Security	Employee Termination		PS
BOSS	Human Resource Security	Employment Agreements		PS
BOSS	Human Resource Security	Background Screening		PS
BOSS	Human Resource Security	Job Descriptions		PS
BOSS	Human Resource Security	Roles and Responsibilities		PS
BOSS	Human Resource Security	Employee Code of Conduct		PS

A	X	B	X	
X	A	B	X	
X	A	B	X	
X	A	B	X	
X	X	B	X	
X	X	A	X	
X	X	B	X	
X	X	B	X	
X	X	B	X	
X	X	B	X	
X	X	B	X	
X	X	B	X	

A	X	B	X	
A	X	B	X	
X	X	B	X	
X	A	B	X	
X	X	B	X	
A	X	A	X	
X	X	B	X	
X	X	B	X	
X	X	B	X	
X	X	B	X	
X	X	B	X	
X	X	B	X	

A	X	B	X	
	X	B	X	
X	X	B	X	
X	A	B	X	
X	X	B	X	
A	X	A	X	
X	X	B	X	
X	X	B	X	
X	X	B	X	
X	X	B	X	
X	X	B	X	
X	X	B	X	

X				A
A				
A				
A				
A				
A				A
A				A
A				A
A				A
A				A
A				A

BOSS	Compliance	Information Systems Regulatory Mapping		RA
BOSS	Data Governance	Data Ownership - Personnel Responsibilities / Stewardship		RA
BOSS	Data Governance	Data Classification		RA
BOSS	Security Monitoring Services	Managed (Outsourced) Security Services		SA
BOSS	Legal Services	Contracts		SA
BOSS	Security Monitoring Services	Honey Pot		SC
BOSS	Security Monitoring Services	Real Time Internetwork Defense (SCAP)		SC
BOSS	Data Governance	Rules for Data Retention		SI
BOSS	Security Monitoring Services	SIEM Platform		SI
BOSS	Security Monitoring Services	Anti Phishing		SI
BOSS	Compliance	Contract/ Authority Maintenance		PM
BOSS	Operational Risk Management	Operational Risk Committee		PM

A	X	B	X
X	A	A	X
X	X	A	X
X	A	B	X
X	X	A	X
A			Ab
A	X	B	X
A	X	B	X
X	A	B	X
A	A	B	Ab
X	A	B	X
X	X	A	X

A	X	B	X
X	X	A	X
X	X	A	X
X	X	B	X
X	X	A	X
A	A		Ab
A	X	B	X
A	X	B	X
X	X	B	X
A	A	B	Ab
X	A	B	X
A	X	A	X

A	X	B	X
X	X	A	X
X	X	A	X
X	X	B	X
X	X	A	X
	A		Ab
A	X	B	X
A	X	B	X
A	X	B	X
A	A	B	Ab
A	X	B	X
A	X	A	X

X
A
A
A
A
X
A
X
A
X
A

A
A
A
A
A
A
A

ITOS	Service Support	Configuration Management	Physical Inventory	CM
ITOS	Service Support	Knowledge Management	Benchmarking	CM
ITOS	Service Support	Knowledge Management	Security Job Aids	CM
ITOS	Service Support	Knowledge Management	Security FAQ	CM
ITOS	Service Support	Change Management	Service Provisioning	CM
ITOS	Service Support	Change Management	Approval Workflow	CM
ITOS	Service Support	Change Management	Change Review Board	CM
ITOS	Service Support	Change Management	Planned Changes	CM
ITOS	Service Support	Release Management	Version Control	CM
ITOS	Service Support	Release Management	Source Code Management	CM
ITOS	IT Operations	DRP	Plan Management	CP
ITOS	Service Support	Configuration Management	Capacity Planning	CP
ITOS	Service Support	Incident Management	Security Incident Response	IR
ITOS	Service Support	Incident Management	Automated Ticketing	IR
ITOS	Service Support	Incident Management	Ticketing	IR
ITOS	Service Support	Incident Management	Cross Cloud Security Incident Response	IR
ITOS	Service Support	Problem Management	Trend Analysis	IR
ITOS	Service Support	Problem Management	Orphan Incident Management	IR

A	A	B	Ab
A	A	A	A
A	A	A	A
A	A	A	A
A	X	A	X
A	X	A	X
A	X	A	X
A	X	A	X
A	X	A	X
X	X	A	X
X	X	A	X
X	X	B	X
X	X	B	X
X	X	B	X
X	X	B	X
X	X	B	X
A	X	B	X
A	X	B	X

A	A	B	Ab
A	A	A	A
A	A	A	A
A	A	A	A
A	X	A	X
A	X	A	X
A	X	A	X
A	X	A	X
A	X	A	X
X	X	A	X
X	X	A	X
A	X	B	X
A	X	B	X
X	X	B	X
X	X	B	X
X	X	B	X
A	X	B	X
A	X	B	X

A	A	B	Ab
A	A	A	A
A	A	A	A
A	A	A	A
A	X	A	X
A	X	A	X
A	X	A	X
A	X	A	X
A	X	A	X
X	X	A	X
X	X	A	X
A	X	B	X
A	X	B	X
X	X	B	X
X	X	B	X
X	X	B	X
A	X	B	X
A	X	B	X

A	
A	A
A	A
A	A
A	A
A	A
A	
A	
A	
A	
A	
A	
A	
X	
X	A
X	A
X	
X	
X	
X	
X	
X	
A	

ITOS	Service Support	Knowledge Management	Trend Analysis	IR
ITOS	Service Support	Change Management	Emergency Changes	MA
ITOS	Service Support	Release Management	Scheduling	MA
ITOS	Service Delivery	Asset Management	Service Costing (Internal)	SA
ITOS	Service Support	Incident Management	Self-Service	SA
ITOS	Service Delivery	Information Technology Resiliency	Availability Management	SC
ITOS	Service Delivery	Application Performance Monitoring		SI
ITOS	Service Support	Release Management	Testing	SI
ITOS	Service Support	Release Management	Build	SI
ITOS	IT Operations	DRP	Test Management	PM
ITOS	IT Operations	IT Governance	Architecture Governance	PM
ITOS	IT Operations	IT Governance	Standards and Guidelines	PM
ITOS	IT Operations	PMO	Program Mngmt	PM
ITOS	IT Operations	PMO	Project Mgnmt	PM
ITOS	IT Operations	PMO	Remediation	PM
ITOS	IT Operations	Portfolio Management	Roadmap	PM
ITOS	IT Operations	Portfolio Management	Strategy Alignment	PM
ITOS	Service Delivery	Service Level Management	Objectives	PM

A	X	A	X	A	X	A	X	A	X	A	A		
A	X	A	X	A	X	A	X	A	X	A			
A	X	A	X	A	X	A	X	A	X	A			
A	A	B	Ab	A	A	B	Ab	A	A	B	Ab	X	
A	X	B	X	A	X	B	X	A	X	B	X	A	
X	X	B	X	A	X	B	X	A	X	B	X	X	
X	A	A	X	X	X	A	X	A	X	A	X	A	
A	X	A	X	A	X	A	X	A	X	A	X	A	
A	X	A	X	A	X	A	X		X	A	X	A	
X	X	B	X	A	X	B	X	A	X	B	X	A	A
A	A	A	A	A	A	A	A	A	A	A	A	A	-
X	A	A	X	X	X	A	X	X	X	A	X	A	
A	A	A	A	A	A	A	A	A	A	A	A	A	A
A	A	A	A	A	A	A	A	A	A	A	A	A	A
A	A	A	A	A	A	A	A	A	A	A	A	A	A
A	A	A	A	A	A	A	A	A	A	A	A	A	
A	A	A	A	A	A	A	A	A	A	A	A	A	
X	X	B	X	X	X	B	X	X	X	B	X	X	

ITOS	Service Delivery	Service Level Management	OLAs	PM
ITOS	Service Delivery	Service Level Management	Internal SLAs	PM
ITOS	Service Delivery	Service Level Management	External SLAs	PM
ITOS	Service Delivery	Service Level Management	Vendor Management	PM
ITOS	Service Delivery	Service Level Management	Service Dashboard	PM
ITOS	Service Delivery	Asset Management	Operational Budgeting	PM
ITOS	Service Delivery	Asset Management	Investment Budgeting	PM
ITOS	Service Support	Problem Management	Problem Resolutions	PM
ITOS	Service Support	Knowledge Management	Best Practices	PM
Presentation Services	Presentation Modality	Consumer Service Platform	Social Media	AC
Presentation Services	Presentation Modality	Consumer Service Platform	Collaboration	AC
Presentation Services	Presentation Modality	Consumer Service Platform	E-Mail	AC
Presentation Services	Presentation Modality	Enterprise Service Platform	B2M	AC
Presentation Services	Presentation Modality	Enterprise Service Platform	B2B	AC
Presentation Services	Presentation Modality	Enterprise Service Platform	B2C	AC

X	A	B	X		X	X	B	X		X	X	B	X		X		A
X	A	A	X		X	A	A	X		X	A	A	X		A		A
X	X	B	X		X	X	B	X		X	X	B	X		X		A
A	A	A	A		A	A	A	A		A	A	A	A		A		A
X	X	B	X		A	X	B	X		A	X	B	X		A		A
A	A	A	A		A	A	A	A		A	A	A	A		A		
A	A	A	A		A	A	A	A		A	A	A	A		A		
A	X	B	X		A	X	B	X		A	X	B	X		X		
X	X	A	X		X	X	A	X		A	X	A	X		A		
X		B	X		X		B	X			X	B	X				
X		B	X		X		B	X			X	B	X				
X	A	B	X		X	A	B	X		X	X	B	X				
X	A	B	X		X	A	B	X		X	X	B	X				
X	A	B	X		X	A	B	X		X	X	B	X				

Presentation Services	Presentation Modality	Enterprise Service Platform	P2P	AC
Presentation Services	Presentation Platform	End-Points	Mobile Devices	AC
Presentation Services	Presentation Platform	End-Points	Fixed Devices	AC
Presentation Services	Presentation Platform	End-Points	Desktops	AC
Presentation Services	Presentation Platform	End-Points	Portable Devices	AC
Presentation Services	Presentation Platform	End-Points	Medical Devices	AC
Presentation Services	Presentation Platform	End-Points	Smart Appliances	AC
Presentation Services	Presentation Modality	Consumer Service Platform	Search	SC
Presentation Services	Presentation Modality	Consumer Service Platform	e-Readers	SC
Presentation Services	Presentation Modality	Enterprise Service Platform	B2E	SC
Presentation Services	Presentation Platform	Speech Recognition (IVR)		SC
Presentation Services	Presentation Platform	Handwriting (ICR)		SC

X	A	B	X
X	A	B	X
X	A	B	X
X	A	B	X
X	A	B	X
X	A	B	X
X	A	B	X
X	A	B	X
X		B	X
X		B	X
X	A	B	X
X		B	X
X		B	X

X	A	B	X
X	A	B	X
X	A	B	X
X	A	B	X
X	A	B	X
X	A	B	X
X	A	B	X
X	A	B	X
X		B	X
X		B	X
X	A	B	X
X		B	X
X		B	X

X	X	B	X
X	A	B	X
X	A	B	X
X	A	B	X
X	A	B	X
X	A	B	X
X	A	B	X
X	A	B	X
	X	B	X
	X	B	X
X	X	B	X
X		B	X
X		B	X

Applicati on Services	Security Knowledge Lifecycle	Attack Patterns		CM
Applicati on Services	Security Knowledge Lifecycle	Security Design Patterns		SA
Applicati on Services	Security Knowledge Lifecycle	Security Application Framework - ACEGI		SA
Applicati on Services	Development Processes	Self Service	Security Code Review	SA
Applicati on Services	Development Processes	Self Service	Application Vulnerability Scanning	SA
Applicati on Services	Development Processes	Self Service	Stress Volume Testing	SA
Applicati on Services	Development Processes	Software Quality Assurance		SA
Applicati on Services	Integration Middleware			SA
Applicati on Services	Connectivity & Delivery			CM
Applicati on Services	Programming Interfaces	Input Validation		SI
Applicati on Services	Security Knowledge Lifecycle	Code Samples		SI
Applicati on Services	Abstraction			SC

X	X	B	X
X	X	B	X
X	A	B	X
X	X	B	X
X	X	B	X
A	X	B	X
X	X	B	X
X	A	B	X
X	X	B	X
X	X	B	X
A	X	B	X
A	X	B	X
A	X	B	X
X	A	A	X

A	X	B	X
A	X	B	X
A	X	B	X
X	X	B	X
X	X	B	X
A	X	B	X
X	X	B	X
X	X	B	X
A	X	B	X
A	X	B	X
A	X	B	X
	X	B	X
X	X	A	X

A	X	B	X
A	X	B	X
A	X	B	X
X	X	B	X
A	X	B	X
A	X	B	X
X	X	B	X
A	X	B	X
A	X	B	X
A	X	B	X
	X	B	X
A	X	A	X

A	A
A	
A	A
A	A
A	A
X	A
A	A
A	
A	
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	B	X	X	X	B	X	X	X	B	X
Information Services	Reporting Services	Dashboard		CA	A	X	A	X	A	X	A	X	A	X	A	X
Information Services	Reporting Services	Data Mining		CA	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
Information Services	Reporting Services	Business Intelligence		CA	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
Information Services	Service Delivery	Service Catalog		CM	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
Information Services	ITOS	CMDB		CM	A	X	B	X	A	X	B	X	A	X	B	X
Information Services	ITOS	Change Management		CM	A	X	B	X	A	X	B	X	A	X	B	X
Information Services	Service Support	Configuration Rules (Metadata)		CM	A	A	B	Ab	A	A	B	Ab	A	A	B	Ab

Information Services	Service Support	Configuration Management Database (CMDB)		CM
Information Services	Service Support	Change Logs		CM
Information Services	Security Monitoring	Compliance Monitoring		CM
Information Services	Security Monitoring	Privilege Usage Events		CM
Information Services	Service Delivery	Recovery Plans		CP
Information Services	BOSS	GR Data (Employee & contractors)		IA
Information Services	Security Monitoring	Authorization Events		IA
Information Services	Security Monitoring	Authentication Events		IA
Information Services	Security Monitoring	ACL's		IA
Information Services	Security Monitoring	CRL's		IA
Information Services	User Directory Services	Active Directory Services		IA
Information Services	User Directory Services	LDAP Repositories		IA

A	A	B	Ab
A	A	B	Ab
A	X	B	X
X	X	B	X
A	X	A	X
A	A	A	A
X	A	B	X
X	X	B	X
A	X	B	X
A	X	B	X
A	X	B	X
A	X	B	X
A	X	B	X
A	X	B	X

A	A	B	Ab
A	A	B	Ab
A	X	B	X
X	X	B	X
A	X	A	X
A	A	A	A
X	X	B	X
X	X	B	X
A	X	B	X
A	X	B	X
A	X	B	X
A	X	B	X
A	X	B	X
A	X	B	X

A	A	B	Ab
A	A	B	Ab
A	X	B	X
X	X	B	X
A	X	A	X
A	A	A	A
X	X	B	X
X	X	B	X
A	X	B	X
A	X	B	X
A	X	B	X
A	X	B	X
A	X	B	X
A	X	B	X

A	
X	
A	
A	
A	
A	
A	
A	
X	
X	
A	
A	

Information Services	User Directory Services	X.500 Repositories		IA
Information Services	User Directory Services	DBMS Repositories		IA
Information Services	User Directory Services	Registry Services		IA
Information Services	User Directory Services	Location Services		IA
Information Services	User Directory Services	Federated Services		IA
Information Services	User Directory Services	Virtual Directory Services		IA
Information Services	User Directory Services	Meta Directory Services		IA
Information Services	ITOS	Incident Management		IR
Information Services	Service Support	Service Events		IR
Information Services	BOSS	Data Classification		RA
Information Services	Data Governance	Risk Assessments		RA
Information Services	Risk Management	Risk Assessments		RA
Information Services	Risk	Business		RA

A	X	B	X
X	A	B	X
A	X	B	X
A		B	Ab
X	A	B	X
X	A	B	X
X	A	B	X
X	X	B	X
X	X	B	X
X	X	A	X
X	A	B	X
X	A	B	X
X	X	B	X

A	X	B	X
A	X	B	X
A	X	B	X
A		B	Ab
X	A	B	X
A	X	B	X
A	X	B	X
X	X	B	X
X	X	B	X
X	X	A	X
X	A	B	X
X	A	B	X
X	X	B	X

A	X	B	X
A	X	B	X
A	X	B	X
A		B	Ab
A	X	B	X
A	X	B	X
A	X	B	X
X	X	B	X
A	X	B	X
X	X	A	X
X	A	B	X
X	A	B	X
X	X	B	X

A	
A	
A	
A	
A	
A	
A	
X	
X	
A	
X	
X	
A	

on Services	Management	Impact Assessment.		
Information Services	Risk Management	VRA		RA
Information Services	Risk Management	TVM		RA
Information Services	Service Delivery	OLA's		SA
Information Services	Data Governance	Non-Production Data		SA
Information Services	Security Monitoring	NIPS Events		SC
Information Services	Security Monitoring	DLP Events		SC
Information Services	Data Governance	Information Leakage Metadata		SI
Information Services	Data Governance	Data Segregation		SI
Information Services	Security Monitoring	Transformation Services		SI
Information Services	Security Monitoring	Session Events		SI
Information Services	Security Monitoring	Application Events		SI
Information	Security Monitoring	Network Events		SI

X	A	B	X
X	A	B	X
A	A	A	A
X	A	B	X
X	X	B	X
X	X	B	X
X	A	B	X
X	X	B	X
X	X	B	X
X	X	B	X
X	A	B	X
X	A	B	X
X	A	B	X
X	A	B	X

X	A	B	X
X	A	B	X
A	A	A	A
X	X	B	X
A	X	B	X
A	X	B	X
X	A	B	X
A	X	B	X
X	X	B	X
X	X	B	X
X	A	B	X
X	A	B	X
X	X	B	X
X	X	B	X

X	X	B	X
X	X	B	X
A	A	A	A
X	X	B	X
A	X	B	X
A	X	B	X
A	X	B	X
	X	B	X
A	X	B	X
A	X	B	X
A	X	B	X
A	X	B	X
A	X	B	X
A	X	B	X

A			
X			
A			
A			
X			
A			
A			
A			
A			
A			
A			
A			
X			

Services				
Information Services	Security Monitoring	Computer Events		SI
Information Services	Security Monitoring	Host Intrusion Protection Systems (HIPS)		SI
Information Services	Security Monitoring	Database Events		SI
Information Services	Service Delivery	Contracts		PM
Information Services	ITOS	PMO		PM
Information Services	ITOS	Strategy		PM
Information Services	ITOS	Roadmap		PM
Information Services	ITOS	Knowledge Management		PM
Information Services	ITOS	Service Management		PM
Information Services	BOSS	Risk Assessments		PM
Information Services	BOSS	Process Ownership		PM
Information Services	BOSS	Business Strategy		PM

X	A	B	X	X	X	B	X	A	X	B	X	A							
X	A	B	X	X	A	B	X	A	X	B	X	A							
X	A	B	X	X	A	B	X	A	X	B	X	A							
A	A	A	A	A	A	A	A	A	A	A	A	A							
A		A	A	A		A	A			A	A	A							
A	A	A	A	A	A	A	A	A	A	A	A	A							
A	A	B	Ab	A	A	B	Ab	A	A	B	Ab	A							
X	A	B	X	X	X	B	X	A	X	B	X	A							
X	A	A	X	X	A	A	X	X	A	A	X	X							
X	A	A	X	X	A	A	X	X	A	A	X	A							
A	A	A	A	A	A	A	A	A	A	A	A	A							

Information Services	Service Support	Knowledge Repository		PM
Information Services	Risk Management	GRC		PM
Information Services	Risk Management	DR & BC Plans		PM
Infrastructure Services	Virtual Infrastructure: Storage Virtualization	Block-Based Virtualization	Network-Based	AC
Infrastructure Services	Internal Infrastructure: Network Services	Authoritative Time Source		AU
Infrastructure Services	Internal Infrastructure: Patch Management	Service Discovery		MA
Infrastructure Services	Internal Infrastructure: Equipment Maintenance			MA
Infrastructure Services	Internal Infrastructure: Storage Services			MP
Infrastructure Services	Virtual Infrastructure: Storage Virtualization	Block-Based Virtualization	Storage Device-Based	MP
Infrastructure Services	Internal Infrastructure: Facility Security	Controlled Physical Access	Barriers	PE
Infrastructure	Internal	Controlled	Security Patrols	PE

A	A	B	Ab
X	A	A	X
X	X	B	X
X	X	B	X
	X	B	X
	A	B	Ab
	A	B	Ab
	A	B	Ab
X	X	B	X
	A	B	Ab
	A	B	Ab
	A	B	Ab

A	A	B	Ab
X	X	A	X
X	X	B	X
A	X	B	X
	X	B	X
	A	B	Ab
	A	B	Ab
	A	B	Ab
A	X	B	X
	A	B	Ab
	A	B	Ab

A	A	B	Ab
X	X	A	X
X	X	B	X
A	X	B	X
	X	B	X
	A	B	Ab
	A	B	Ab
	A	B	Ab
A	X	B	X
	A	B	Ab
	A	B	Ab

A	
A	A
X	
A	
X	
X	
A	A
A	
A	
A	

Infrastructure Services	Virtual Infrastructure: Desktop "Client" Virtualization	Local		SC
Infrastructure Services	Virtual Infrastructure: Desktop "Client" Virtualization	Remote	Session-Based	SC
Infrastructure Services	Virtual Infrastructure: Desktop "Client" Virtualization	Remote	VM-Based (VDI)	SC
Infrastructure Services	Virtual Infrastructure: Storage Virtualization	Block-Based Virtualization	Host-Based	SC
Infrastructure Services	Virtual Infrastructure: Storage Virtualization	File-Based virtualization		SC
Infrastructure Services	Virtual Infrastructure: Application Virtualization	Client Application Streaming		SC
		Server Application Streaming		SC
Infrastructure Services	Virtual Infrastructure: Virtual Workspaces			SC
Infrastructure Services	Virtual Infrastructure: Server	Virtual Machines (host based)	Full	SC
			Paravirtualization	SC

X	A	B	X	A	X	B	X	A	X	B	X	A			
X	X	B	X	A	X	B	X	A	X	B	X	A			
X	X	B	X	A	X	B	X	A	X	B	X	A			
X	X	B	X	A	X	B	X	A	X	B	X	A			
X	X	B	X	A	X	B	X	A	X	B	X	A			
X	X	B	X	A	X	B	X	A	X	B	X	A			
X	X	B	X	A	X	B	X		X	B	X	A			
X	X	B	X	A	X	B	X	A	X	B	X	A			
X	X	B	X	A	X	B	X	A	X	B	X	A			
X	X	B	X	A	X	B	X	A	X	B	X	A			

	Services			
S & RM	Infrastructure Protection Services	End-Point	Host Firewall	AC
S & RM	Infrastructure Protection Services	End-Point	Content Filtering	AC
S & RM	Infrastructure Protection Services	End-Point	White Listing	AC
S & RM	Infrastructure Protection Services	Network	Content Filtering	AC
S & RM	Infrastructure Protection Services	Network	Firewall	AC
S & RM	Infrastructure Protection Services	Network	Black Listing Filtering	AC
S & RM	Infrastructure Protection Services	Application	Application Firewall	AC
S & RM	Infrastructure Protection Services	Application	Secure Collaboration	AC
S & RM	Infrastructure Protection Services	Application	Real Time Filtering	AC
S & RM	Data Protection	Data Lifecycle Management	Meta data Control	AC
S & RM	Data Protection	Data Lifecycle Management	Data Seeding	AC
S & RM	Data Protection	Intellectual Property Prevention	Digital Rights Management	AC
S & RM	Policies and	Role Based		AC

X	A	B	X	
X	A	B	X	
X	A	B	X	
X	A	B	X	
X	X	B	X	
X	X	B	X	
X	X	B	X	
X	A	B	X	
X	A	B	X	
X	A	B	X	
A	X	B	X	
X	A	A	X	

X	X	B		
X	A	B		
A	X	B		
X	X	B		
X	X	B		
A	X	B		
X	X	B		
X	A	B		
X	X	B		
X	A	B		
A	X	B		
X	A	A		

A	X	B		
A	X	B		
A	X	B		
A	X	B		
A	X	B		
A	X	B		
A	X	B		
A	X	B		
A	X	B		
A	X	B		
A	X	B		
X	A	A		

X				A
X				A
X				A
X				A
X				A
X				A
X				A
X				A
X				A
X				A
X				A
X				A

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

X	X	B	X	
X	X	B	X	
X	X	B	X	
X	X	B	X	
X	X	B	X	
A	X	A	X	
X	X	B	X	
X	A	B	X	
X	A	B	X	
A	A	A	A	
A	A	A	A	
A	A	A	A	
A	A	B	Ab	
X	A	B	X	
X	A	B	X	

X	X	B		
X	X	B		
X	X	B		
X	X	B		
A	X	B		
A	X	A		
X	X	B		
A	X	B		
X	X	B		
A	A	A	A	
A	A	A	A	
A	A	B	Ab	
X	A	B		
X	A	B		

X	X	B		
X	X	B		
X	X	B		
A	X	B		
A	X	B		
A	X	A		
X	X	B		
A	X	B		
A	X	B		
A	A	A	A	
A	A	A	A	
A	A	B	Ab	
A	X	B		
X	X	B		

A				
X				
X				
A				
A				
X				
X				
A				
A				
A				
A				
A				
A				
A				
A				

	Management Infrastructure	Management	Provisioning	
S & RM	Privilege Management Infrastructure	Identity Management	Attribute Provisioning	IA
S & RM	Privilege Management Infrastructure	Authorization Services	Policy Enforcement	IA
S & RM	Privilege Management Infrastructure	Authorization Services	Policy definition	IA
S & RM	Privilege Management Infrastructure	Authorization Services	Principal Data Mngmnt	IA
S & RM	Privilege Management Infrastructure	Authorization Services	XACML	IA
S & RM	Privilege Management Infrastructure	Authorization Services	Role Management	IA
S & RM	Privilege Management Infrastructure	Authorization Services	Oligation	IA
S & RM	Privilege Management Infrastructure	Authorization Services	Out of the Box (OTB) autZ	IA
S & RM	Privilege Management Infrastructure	Authentication Services	SAML Token	IA
S & RM	Privilege Management Infrastructure	Authentication Services	Risk Based Auth	IA
S & RM	Privilege Management Infrastructure	Authentication Services	Multifactor	IA
S & RM	Privilege Management	Authentication Services	OTP	IA

X	A	B	X	
X	A	B	X	
X	A	B	X	
X	A	B	X	
A	X	B	X	
X	X	B	X	
A	X	B	X	
X	X	B	X	
X	X	B	X	
X	X	B	X	
A	X	B	X	

X	A	B		
X	A	B		
X	A	B		
X	A	B		
A	X	B		
X	X	B		
A	X	B		
A	X	B		
X	X	B		
X	X	B		
A	X	B		
A	X	B		

X	X	B		
X	X	B		
X	X	B		
X	X	B		
A	X	B		
X	X	B		
A	X	B		
A	X	B		
X	X	B		
A	X	B		
A	X	B		

A				
A				
A				
A				
A				
A				
A				
A				
A				
A				
A				

	Infrastructure			
S & RM	Privilege Management Infrastructure	Authentication Services	Smart Card	IA
S & RM	Privilege Management Infrastructure	Authentication Services	Password Management	IA
S & RM	Privilege Management Infrastructure	Authentication Services	Biometrics	IA
S & RM	Privilege Management Infrastructure	Authentication Services	Network Authentication	IA
S & RM	Privilege Management Infrastructure	Authentication Services	Single Sign On	IA
S & RM	Privilege Management Infrastructure	Authentication Services	WS-Security	IA
S & RM	Privilege Management Infrastructure	Authentication Services	Middleware Auth	IA
S & RM	Privilege Management Infrastructure	Authentication Services	Identity Verification	IA
S & RM	Privilege Management Infrastructure	Authentication Services	Out-of-The-Box (OTB) Auth	IA
S & RM	Privilege Management Infrastructure	Privilege Usage Management	Keystroke/Sessi on Logging	IA
S & RM	Privilege Management Infrastructure	Privilege Usage Management	Password Vaulting	IA
S & RM	Threat and Vulnerability Management	Compliance Testing	Network Autehntication	IA

X	A	B	X	
X	X	B	X	
X	A	B	X	
X	X	B	X	
A	X	B	X	
X	X	B	X	
X	X	B	X	
X	X	B	X	
X	X	B	X	
X	X	B	X	
X	X	B	X	
X	X	B	X	
X	X	B	X	

X	A	B		
X	X	B		
X	A	B		
A	X	B		
A	X	B		
X	X	B		
X	X	B		
X	X	B		
X	X	B		
X	X	B		
X	X	B		
X	X	B		
X	X	B		

A	X	B		
X	X	B		
X	X	B		
A	X	B		
A	X	B		
A	X	B		
A	X	B		
X	X	B		
A	X	B		
X	X	B		
A	X	B		
A	X	B		

A				
A				
A				
X				
A				
A				
A				
A				
A				
A				
A				
X				
X				A

S & RM	Infrastructure Protection Services	End-Point	Forensic Tools	IR
S & RM	Infrastructure Protection Services	End-Point	Media Lockdown	MP
S & RM	InfoSec Management	Residual Risk Management		PL
S & RM	Governance Risk & Compliance	Policy Management	Exceptions	RA
S & RM	Governance Risk & Compliance	Policy Management	Self Assessment	RA
S & RM	InfoSec Management	Risk Dashboard		RA
S & RM	Threat and Vulnerability Management	Vulnerability Management	application	RA
			Infrastructure	RA
			DB	RA
		Penetration Testing	Internal	RA
			External	RA
		Threat Management	Source Code Scanning	RA
			Risk Taxonomy	RA
		S & RM	Policies and Standards	Data/ Asset Classification
S & RM	Governance Risk & Compliance	Vendor Management		SA
S & RM	Data Protection	Data Lifecycle Management	Life cycle management	SA
S & RM	Policies and	Technical		SA

X	A	B	X
A	X	B	X
X	A	B	X
X	X	B	X
X	A	B	X
X	X	B	X
X	X	B	X
X	A	B	X
X	X	B	X
X	X	B	X
X	A	B	X
X	X	A	X
X	X	B	X
X	X	B	X
X	X	A	X

X	A	B	
A	X	B	
X	X	B	
X	X	B	
X	A	B	
X	X	B	
X	X	B	
X	X	B	
X	X	B	
X	X	B	
X	X	B	
X	X	A	
X	X	B	
X	X	B	
X	X	A	

X	X	B	
A	X	B	
A	X	B	
X	X	B	
X	A	B	
X	X	B	
A	X	B	
A	X	B	
A	X	B	
A	X	B	
X	X	B	
X	X	B	
X	X	A	
X	X	B	
X	X	A	

A	A
X	A
A	
X	A
A	A
A	A
A	A
A	A
A	A
A	
A	A
A	A
X	A

	Services	Management		
S & RM	Cryptographic Services	Key Management	Asymmetric Keys	SC
S & RM	Cryptographic Services	PKI		SC
S & RM	Cryptographic Services	Data in use (memory) Encryption		SC
S & RM	Cryptographic Services	Data in Transit Encryption (Transitory, Fixed)		SC
S & RM	Cryptographic Services	Data as Rest Encryption (DB, File, SAN, Desktop, Mobile)		SC
S & RM	Infrastructure Protection Services	Server	Anti-virus	SI
S & RM	Infrastructure Protection Services	Server	HIPS/HIDS (Intrusion Protection /Detection)	SI
S & RM	Infrastructure Protection Services	End-Point	Anti-Virus, Anti-Spam, Anti-Malware	SI
S & RM	Infrastructure Protection Services	End-Point	HIPS/HIDS (Intrusion Protection /Detection)	SI
S & RM	Infrastructure Protection Services	End-Point	Hardware Based trusted Assets	SI
S & RM	Infrastructure Protection Services	Network	NIPS/NIDS	SI

X	X	B	X
X	X	B	X
X	X	B	X
X	X	B	X
X	X	B	X
X	X	B	X
X	X	B	X
X	A	B	X
X	A	B	X
A	X	B	X
X	X	B	X

X	X	B	
X	X	B	
X	X	B	
X	X	B	
X	X	B	
X	X	B	
X	X	B	
X	A	B	
X	X	B	
A	X	B	
A	X	B	

X	X	B	
X	X	B	
A	X	B	
X	X	B	
X	X	B	
A	X	B	
A	X	B	
A	X	B	
A	X	B	
A	X	B	
A	X	B	

X	
X	
X	
X	
A	
A	
A	
A	
A	
A	
X	
X	

A
A
A
A
A

S & RM	Data Protection	Data Lifecycle Management	eSignature	SI
S & RM	Cryptographic Services	Signature Services		SI
S & RM	Governance Risk & Compliance	IT Risk Management		PM
S & RM	InfoSec Management	Risk Portfolio Management		PM
S & RM	Privilege Management Infrastructure	Authorization Services	Policy Management	PM
S & RM	Privilege Management Infrastructure	Authorization Services	Resource Data management	PM
S & RM	Policies and Standards	Information Security Polices		PM

X	A	B	X
X	X	B	X
X	X	B	X
A	A	B	Ab
X	A	B	X
X	A	B	X
A	A	A	A

X	X	B	
X	X	B	
X	X	B	
A	A	B	Ab
X	A	B	
X	A	B	
A	A	A	A

X	X	B	
X	X	B	
X	X	B	
A	A	B	Ab
X	X	B	
X	X	B	
A	A	A	A

A
X
X
A
A
A
A

A
A
A
A

DRAFT

14 ANNEX E: MAPPING OF THE ARCHITECTURAL COMPONENTS

CONSUMER	PROVIDER	BROKER	CARRIER	AUDITOR
<ul style="list-style-type: none"> • Secure Cloud Consumption / Service Management [=B+C+I+O] 	<ul style="list-style-type: none"> • Secure Cloud Provisioning / Service Management [=B+C+I] 	<ul style="list-style-type: none"> • Secure Cloud Service Management [=B+C+I] 	<ul style="list-style-type: none"> • Secure Transport Support [T] 	<ul style="list-style-type: none"> • Secure Auditing Environment [E]
<ul style="list-style-type: none"> o Secure Business / Payments Support [B] 	<ul style="list-style-type: none"> o Secure Business Support [B] 	<ul style="list-style-type: none"> o Secure Business Support [B] 		
<ul style="list-style-type: none"> o Secure Consumption / Configuration [C] 	<ul style="list-style-type: none"> o Secure Provisioning / Configuration [C] 	<ul style="list-style-type: none"> o Secure Provisioning / Configuration [C] 		
<ul style="list-style-type: none"> o Secure Portability/ Interoperability [I] 	<ul style="list-style-type: none"> o Secure Portability / Interoperability [I] 	<ul style="list-style-type: none"> o Secure Portability / Interoperability [I] 		
<ul style="list-style-type: none"> o Secure Organizational Support [O] 	<ul style="list-style-type: none"> • Secure Cloud Ecosystem Orchestration [=L] 	<ul style="list-style-type: none"> • Secure Cloud Ecosystem Orchestration [=L] 		
<ul style="list-style-type: none"> • Secure Cloud Ecosystem Orchestration [=L] 	<ul style="list-style-type: none"> o Secure Service Layers [L] 	<ul style="list-style-type: none"> o Secure Service Layers [L] 		
<ul style="list-style-type: none"> o Secure Functional Layers [L] 	<ul style="list-style-type: none"> o Secure Resource Abstraction & Control Layer [R] 	<ul style="list-style-type: none"> • Secure Cloud Aggregation [=C2+I2] 		
	<ul style="list-style-type: none"> o Secure Physical Resource Layers [P] 	<ul style="list-style-type: none"> o Secure Provisioning / Configuration [aC] 		
		<ul style="list-style-type: none"> o Secure Portability/Interoperability [aI] 		
		<ul style="list-style-type: none"> • Secure Cloud Arbitrage [cA] 		
		<ul style="list-style-type: none"> • Secure Cloud Intermediation [cl] 		

Table 6: Cloud Actors' Architectural Components

BOSS	Compliance	Intellectual Property Protection	AC
BOSS	Data Governance	Handling/ Labeling/ Security Policy	AC
BOSS	Data Governance	Clear Desk Policy	AC
BOSS	Data Governance	Rules for Information Leakage Prevention	AC
ITOS	IT Operations	Resource Management	AC AC
Presentation Services	Presentation Modality	Consumer Service Platform	AC AC AC
Presentation Services	Presentation Modality	Enterprise Service Platform	AC
Presentation Services			AC
Presentation Services			AC
Presentation Services			AC
Presentation Services	Presentation Platform	End-Points	AC
Presentation Services			AC

CONSUMER				
B	C	I	O	L
B				
	C	I		L
B				
B				
B			O	
				L
	C			L

PROVIDER					
B	C	I	L	R	P
B			L		
B			L		
B	C		L		
B	C	I	L		
		I	L		
		I			

BROKER							
B	C	I	L	aC	al	cA	cl
B							
B							cl
B							
		I	L	aC	al	cA	cl
B	C		L	aC		cA	cl

CARRIER
T

AUDITOR
E
E
E
E

BOSS	Security Monitoring Services	User Behaviors and Profile Patterns	AU
BOSS	Legal Services	E-Discovery	AU
BOSS	Legal Services	Incident Response Legal Preparation	AU
BOSS	Internal Investigations	Forensic Analysis	AU
BOSS	Internal Investigations	e-Mail Journaling	AU
ITOS	Service Delivery	Information Technology Resiliency	AU
ITOS			AU
ITOS	Service Support	Configuration Management	AU
ITOS	Service Support	Problem Management	AU
ITOS			AU
Information Services	BOSS	Audit Findings	AU
Information Services	Security Monitoring	eDiscovery Events	AU
Infrastructure Services	Internal Infrastructure: Network Services	Authoritative Time Source	AU
S & RM	Governance Risk & Compliance	Compliance Management	AU

CONSUMER				
B	C	I	O	L
	C	I		
	C	I		
	C			L
				L
B	C	I		
	C	I		
B	C	I		
			O	
B		I		L
				L
			O	

PROVIDER					
B	C	I	L	R	P
	C		L		
B	C	I	L		P
B	C	I	L		
B	C	I	L		
B				R	
	C	I	L		P
	C	I			P
	C	I	L		P
B					
B	C	I	L		P
	C	I	L	R	P
B	C	I	L		P

BROKER							
B	C	I	L	aC	al	cA	cl
			L			cA	cl
B							
B							
		I	L		al	cA	cl
		I	L		al	cA	cl
			L			cA	cl
		I	L		al	cA	cl
			L			cA	cl
B							
		I	L		al	cA	cl
			L			cA	cl

CARRIER
T
T
T

AUDITOR
E
E
E

Information Services	Security Monitoring	Compliance Monitoring	CM
Information Services	Security Monitoring	Privilege Usage Events	CM
Infrastructure Services	Internal Infrastructure: Servers		CM
S & RM	InfoSec Management	Capability Mapping	CM
S & RM	Infrastructure Protection Services	End-Point	CM
S & RM	Data Protection	Intellectual Property Prevention (Protection?)	CM
S & RM	Policies and Standards	Operational Security Baselines & Job Aid Guidance	CM
BOSS	Operational Risk Management	Business Impact Analysis & Business Continuity	CP
BOSS			
ITOS	IT Operations	DRP	CP
ITOS	Service Support	Configuration Management	CP
Information Services	Service Delivery	Recovery Plans	CP

CONSUMER				
B	C	I	O	L
	C		O	
	C		O	
				L
B			O	
	C		O	
B			O	
B				
B	C			
B	C			
			O	L

PROVIDER					
B	C	I	L	R	P
	C	I	L		P
	C		L		P
					P
B		I	L		P
B			L		P
B	C		L		P
					P
		I	L		
	C	I	L		P
	C	I	L		
B	C	I	L		P

BROKER							
B	C	I	L	aC	al	cA	cl
			L			cA	cl
			L			cA	cl
B	C						
B	C						
B							

CARRIER
T
T
T

AUDITOR
E
E
E
E
E

S & RM	Threat and Vulnerability Management	Compliance Testing	IA
BOSS	Operational Risk Management	Crisis Management	IR
BOSS	Operational Risk Management	Risk Management Framework	IR
BOSS	Operational Risk Management	Independent Risk Management	IR
BOSS	Security Monitoring Services	Database Monitoring	IR
BOSS	Security Monitoring Services	Application Monitoring	IR
BOSS	Security Monitoring Services	End-Point Monitoring	IR
BOSS	Security Monitoring Services	Cloud Monitoring	IR
ITOS	Service Support	Incident Management	IR
ITOS			IR
ITOS			IR
ITOS			IR
ITOS	Service Support	Problem Management	IR
ITOS			IR

CONSUMER				
B	C	I	O	L
				L
B				
B				
B				
		I		L
		I		L
		I		L
		I		L
B				L

PROVIDER					
B	C	I	L	R	P
	C		L		P
B	C	I	L		
	C	I			
B	C	I	L		
	C	I	L		P
	C	I	L		P
	C	I			P
B	C		L		P
B	C		L		P

BROKER							
B	C	I	L	aC	al	cA	cl
B			L				
B							
B							

CARRIER
T
T
T

AUDITOR
E
E
E
E
E

ITOS	Service Support	Knowledge Management	IR
Information Services	ITOS	Incident Management	IR
Information Services	Service Support	Service Events	IR
S & RM	Infrastructure Protection Services	End-Point	IR
ITOS	Service Support	Change Management & Release Management	MA
ITOS			MA
Infrastructure Services	Internal Infrastructure: Patch Management	Service Discovery	MA
Infrastructure Services	Internal Infrastructure: Equipment Maintenance		MA
BOSS	Data Governance	Secure Disposal of Data	MP
Infrastructure Services	Internal Infrastructure: Storage Services		MP

CONSUMER				
B	C	I	O	L
	C			L
		I		L
				L
	C		O	
	C	I		
	C			
	C			
	C	I		L
	C			L

PROVIDER					
B	C	I	L	R	P
B	C		L		P
B			L		
B	C		L		P
	C		L		P
	C	I	L		P
				R	P
					P
	C		L		
					P

BROKER							
B	C	I	L	aC	al	cA	cl
B							
B							

CARRIER
T
T
T
T

AUDITOR
E
E
E
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					
Infrastructure Services	Virtual Infrastructure: Storage Virtualization	Block-Based Virtualization	MP					L				L	R	P													
S & RM	Infrastructure Protection Services	End-Point	MP	B	C		O					L		P									T		E		
Infrastructure Services	Internal Infrastructure: Facility Security	Controlled Physical Access	PE					L						P												E	
Infrastructure Services			PE																								E
Infrastructure Services			PE																								E
Infrastructure Services			PE																								E
Infrastructure Services	Internal Infrastructure: Facility Security	Asset Handling	PE		C					C				P												E	
Infrastructure Services			PE																							E	
Infrastructure Services			PE																							E	
Infrastructure Services	Internal Infrastructure: Facility Security	Environmental Risk Management	PE		C			L						P												E	
Infrastructure Services			PE																							E	
Infrastructure Services			PE																							E	
S & RM	InfoSec Management	Residual Risk Management	PL		C	I				C		L		P													

BOSS	Human Resource Security	Employment Agreement, Background Screening & Employee Termination	PS
BOSS			PS
BOSS			PS
BOSS	Human Resource Security	Job Descriptions, Roles and Responsibilities & Employee Code of Conduct	PS
BOSS			PS
BOSS			PS
BOSS	Compliance	Information Systems Regulatory Mapping	RA
BOSS	Data Governance	Data Ownership - Personnel Responsibilities/ Stewardship	RA
BOSS	Data Governance	Data Classification	RA
Information Services	BOSS	Data Classification	RA
Information Services	Data Governance	Risk Assessments	RA
Information Services	Risk Management	Risk Assessments	RA
Information Services	Risk Management	Business Impact Assessment.	RA

CONSUMER				
B	C	I	O	L
B				L
B				
B				
B	C	I		
B	C	I		L
B	C	I		L
	C			L
	C			L
B			O	L

PROVIDER					
B	C	I	L	R	P
			L		P
			L		P
	C	I	L		P
B		I	L		
B		I	L		
B		I	L		
B		I			
B					
B			L		

BROKER							
B	C	I	L	aC	al	cA	cl
B							
B							
			L				
			L				

CARRIER
T
T
T

AUDITOR
E
E
E
E

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

S & RM	Cryptographic Services	Key Management Lower comp: Synchronous keys, Asynchronous keys	SC
S & RM			SC
S & RM	Cryptographic Services	PKI	SC
S & RM	Cryptographic Services	Data in use (memory) Encryption	SC
S & RM	Cryptographic Services	Data in Transit Encryption (Transitory, Fixed)	SC
S & RM	Cryptographic Services	Data as Rest Encryption (DB, File, SAN, Desktop, Mobile)	SC
BOSS	Data Governance	Rules for Data Retention	SI
BOSS	Security Monitoring Services	SIEM Platform	SI
BOSS	Security Monitoring Services	Anti-Phishing	SI
ITOS	Service Delivery	Application Performance Monitoring	SI
ITOS	Service Support	Release Management	SI
ITOS			SI

CONSUMER				
B	C	I	O	L
	C			L
	C		O	L
				L
				L
				L
B	C	I		L
	C	I		L
				L
B				L
B	C	I		

PROVIDER					
B	C	I	L	R	P
	C	I	L		
	C	I	L		
	C	I	L		
	C	I	L		
B	C	I	L		
	C	I	L		
B	C	I			
B	C	I	L		
	C		L		P

BROKER							
B	C	I	L	aC	al	cA	cl
B							
B							
B							
				aC			

CARRIER
T
T
T
T
T

AUDITOR
E
E
E
E
E
E
E

Information Services	BOSS	Process Ownership	PM
Information Services	BOSS	Business Strategy	PM
Information Services	Service Support	Knowledge Repository	PM
Information Services	Risk Management	Governance, Risk management, Compliance (GRC)	PM
Information Services	Risk Management	Disaster Recovery (DR) & Business Continuity (BC) Plans	PM
Infrastructure Services	Internal Infrastructure: Patch Management	Compliance Monitoring	PM
S & RM	Governance Risk & Compliance	IT Risk Management	PM
S & RM	InfoSec Management	Risk Portfolio Management	PM
S & RM	Privilege Management Infrastructure	Authorization Services	PM
S & RM			PM
S & RM	Policies and Standards	Information Security Polices	PM

CONSUMER				
B	C	I	O	L
B			O	
B			O	
	C		O	L
B			O	L
B			O	L
B	C			L
	C		O	
			O	

PROVIDER					
B	C	I	L	R	P
B					
B					
					P
B			L		
B			L		
	C			R	P
			L		P
					P
	C	I	L		
	C				P

BROKER							
B	C	I	L	aC	al	cA	cl
B							
B							
B							
B							
B							
	C	I					

CARRIER
T
T
T

AUDITOR
E
E

15.1 USE CASE SUMMARY

<p>Services Covered</p> <ul style="list-style-type: none">• Broker cloud secure service provisioning• Broker cloud secure service status and metrics• Broker cloud secure service control and management• Identity management between cloud broker and cloud service provider• Continuous monitoring status between cloud broker and cloud service provider• Broker based identity and credential management integration• Broker based secure service orchestration• Broker based integrated secure service status and metrics• Broker cloud secure service control and management• Broker cloud secure service arbitrage• Broker-based technical integration with CSPs returned in aggregation (minimum requirement)• Broker-based business integration with CSP's for secure account creation and credential acquisition (advanced capability)• Broker based arbitrage models capable of approximating cloud consumer requirements to a degree that automated secure provisioning is acceptable (advanced capability)• Broker based ability to perform full or human-assisted workload transition from CSP to CSP (advanced capability)	<p>Featured Deployment and Service Models:</p> <ul style="list-style-type: none">• All Deployment Models• All Service Models
---	--

<p>Actors:</p> <ul style="list-style-type: none"> • Cloud Consumer • A marketplace or ecosystem of at least two and typically many cloud service providers • Cloud Broker 	<p>Systems</p> <ul style="list-style-type: none"> • Cloud broker secure provisioning system • Cloud broker continuous monitoring system • Cloud broker identity management • Cloud broker APIs to each cloud service provider • Cloud service provider identity management, provisioning and monitoring systems, secure accessed by broker • Cloud broker identity management system with cloud consumer-facing integration capabilities • Cloud broker secure orchestration system with Cross-CSP secure orchestration capabilities • Cloud broker based continuous monitoring offering an integrated view across multiple CSP's • Cloud broker based secure reporting offering an integrated view across multiple CSP's • Cloud broker model for gathering cloud consumer business, technical and policy/security parameters • Cloud broker model for rating and ranking CSP capabilities in a consistent and meaningful manner • Cloud broker system to deliver rankings to cloud consumers • Business transaction systems between broker and CSPs • Automated service selection systems between broker and cloud consumers
<p>Notable Services:</p> <p>Broker to CSP secure business interfaces</p> <p>Combined cloud secure service business and technical brokerage</p> <p>Advanced arbitrage and decision support systems</p> <p>Cross-CSP services for automated or semi-automated workload migration</p>	

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

15.2 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	Security 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

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

Infrastructure Services	Virtual Infrastructure: Storage Virtualization	File-Based virtualization		SC	0.00	1.00	3.00	4.00
Infrastructure Services	Virtual Infrastructure: Application Virtualization	Client Application Streaming		SC	1.00	1.00	3.00	5.00
Infrastructure Services	Virtual Infrastructure: Application Virtualization	Server Application Streaming		SC	1.00	1.00	3.00	5.00
Infrastructure Services	Virtual Infrastructure: Virtual Workspaces			SC	0.00	0.00	0.00	0.00
Infrastructure Services	Virtual Infrastructure: Server Virtualization	Virtual Machines (host based)	Full	SC	0.00	0.00	2.00	2.00
Infrastructure Services	Virtual Infrastructure: Server Virtualization	Virtual Machines (host based)	Paravirtualization	SC	0.00	0.00	2.00	2.00
Infrastructure Services	Virtual Infrastructure: Server Virtualization	Virtual Machines (host based)	Hardware-Assisted	SC	0.00	0.00	2.00	2.00
Infrastructure Services	Virtual Infrastructure: Server Virtualization	OS Virtualization		SC	0.00	0.00	2.00	2.00
Infrastructure Services	Virtual Infrastructure: Server Virtualization	TPM Virtualization		SC	0.00	0.00	2.00	2.00
Infrastructure Services	Virtual Infrastructure: Server Virtualization	Virtual Memory		SC	0.00	0.00	2.00	2.00
Infrastructure Services	Virtual Infrastructure: Network	Network Address Space	IPv4	SC	0.00	0.00	2.00	2.00
Infrastructure Services	Virtual Infrastructure: Network	Network Address Space	IPv6	SC	0.00	0.00	2.00	2.00
Infrastructure Services	Virtual Infrastructure: Network	VLAN		SC	0.00	1.00	3.00	4.00
Infrastructure Services	Virtual Infrastructure: Network	VNIC		SC	0.00	1.00	3.00	4.00
Infrastructure Services	Virtual Infrastructure: Database Virtualization			SC	0.00	0.00	2.00	2.00
Infrastructure Services	Virtual Infrastructure: Mobile Device Virtualization			SC	0.00	0.00	2.00	2.00
Infrastructure Services	Virtual Infrastructure: Smartcard Virtualization			SC	0.00	0.00	2.00	2.00
Infrastructure 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 S & RM	Infrastructure Protection Services Infrastructure Protection Services	Server Server	White Listing Host Firewall	AC AC	3.00	1.00	2.00	6.00
S & RM	Infrastructure Protection Services	End-Point	Host Firewall	AC	3.00	2.00	3.00	8.00
S & RM S & RM S & RM S & RM S & RM	Infrastructure Protection Services Infrastructure Protection Services Infrastructure Protection Services Infrastructure Protection Services Infrastructure Protection Services Infrastructure Protection Services Infrastructure Protection Services	End-Point End-Point Network Network Application	Content Filtering White Listing Content Filtering Firewall Black Listing Filtering Application Firewall	AC AC AC AC AC AC	3.00 3.00 3.00 3.00 3.00 3.00	1.00 2.00 1.00 3.00 1.00	2.00 3.00 2.00 4.00 2.00	6.00 8.00 6.00 10.00 6.00
S & RM S & RM S & RM S & RM	Infrastructure Protection Services Infrastructure Protection Services Data Protection Data Protection	Application Application Data Lifecycle Management Data Lifecycle Management	Secure Collaboration Real Time Filtering Meta data Control Data Seeding	AC AC AC AC	3.00 3.00 3.00	2.00 2.00 1.00	3.00 3.00 1.00	8.00 8.00 5.00
S & RM	Data Protection	Intellectual Property Prevention	Digital Rights Management	AC	2.00	0.00	1.00	3.00
S & RM	Policies and Standards	Role Based Awareness		AC	3.00	1.00	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

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

DRAFT

15.3 ASIS HEAT MAP

