NIST Special Publication 800-200

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

NIST Cloud Computing Security Reference Architecture

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

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

This page left intentionally blank

Reports on Computer Systems Technology

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

Acknowledgements

NIST gratefully acknowledges the broad contributions of the NIST Cloud Computing Security Working Group (NCC SWG), chaired by Dr. Michaela Iorga. Dr. Iorga was principal editor for this document with assistance in editing and formatting from Hannah Wald, Technical Writer, Booz Allen Hamilton, Inc, and Karen Scarfone of Scarfone Cybersecurity.

The following list (in alphabetical order by last name) includes contributors[1] and internal reviewers who previously agreed to be acknowledged in this document. The list will be updated when we receive more confirmations from our members.

Contributors list and their affiliation at the time the work was developed:

Wayne W. **Armour**, Independent Consultant
Nadeem **Bukhari**, Kinamik Data Integrity
William **Butler**, PhD., Capitol College – Graduate School of Information Assurance
Alvaro A. **Cardenas**, Fujitsu Laboratories of America
Pw **Carey**, Compliance Partners, LLC
Aradhna **Chetal**, Boeing
Kyle **Coble**, Department of Homeland Security
Vince **Grimaldi**, Independent Consultant
Muhammad F. **Islam**, PhD candidate, George Washington Univ. & Booz Allen Hamilton, Inc.
Jerry **Kickenson**, SWIFT
Juanita **Koilpillai**, Electrosoft Services, Inc.
Prabha **Kumar**, PhD., Department of Defense – Chief Information Office
Nancy M. **Landreville**, PhD., EmeSec (under contract, Dept. of Veterans Affairs) & UMD
Anne L. **Lee**, PhD., U.S. Air Force - Space and Missile Systems Center
Cheng-Yin **Lee**, Independent Consultant
Chan **Lim**, IBM
Ketan **Mehta**, Booz Allen Hamilton, Inc.
Mark **Potter**, Danya International
Keyun **Ruan**, PhD., University College Dublin & EADS N.V., XENSIX Inc.
Arnab **Roy**, PhD., Fujitsu Laboratories of America
Michael A. **Salim**, American Data Technology, Inc.
Ken E. **Stavinoha**, PhD., Cisco Systems

INTERNAL REVIEWERS:

Wayne W. **Armour**, Independent Consultant
Jerry **Kickenson**, SWIFT

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

Juanita **Koilpillai,** Electrosoft Services, Inc.
Michael A. **Salim**, American Data Technology, Inc.
Ken E. **Stavinoha**, PhD., Cisco Systems
Steven **Woodward**, Cloud Perspectives

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

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

Table of Contents

List of Figures

List of Tables

EXECUTIVE SUMMARY

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

- NIST SP 500-291, *Cloud Computing Standards Roadmap*
- NIST SP 500-292, *NIST Cloud Computing Reference Architecture*
- NIST SP 500-293 Volume I, *US Government Cloud Computing Technology Roadmap Volume I, High-Priority requirements to Further USG Agency Cloud Computing Adoption*
- NIST SP 500-293 Volume II, *US Government Cloud Computing Technology Roadmap Volume II, Useful Information for Cloud Adopters* (Draft)
- NIST SP 500-293 Volume III, *US Government Cloud Computing Technology Roadmap Volume III, Technical Considerations for USG Cloud Computing Deployment Decisions (Draft)*
- NIST SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing*
- NIST SP 800-145, *The NIST Definition of Cloud Computing*
- NIST SP 800-146, *Cloud Computing Synopsis and Recommendations* (Draft)

This document was developed as part of a collective effort by the NIST Cloud Computing Security Working Group (NCC SWG) in response to the priority action plans for the early USG cloud computing adoption identified in NIST SP 500-293 Volume I. NIST SP 500-293 highlights concerns around the protection and control of cloud Consumer data.

This document introduces the NIST Cloud Computing Security Reference Architecture (NCC-SRA or, for the sake of brevity, SRA), providing a comprehensive formal model to serve as a security overlay to the architecture described in NIST SP 500-292. This document also describes a methodology for using the formal model and an associated set of Security Components (derived from the capabilities identified in the Cloud Security Alliance's Trusted Cloud Initiative – Reference Architecture [TCI-RA]) to orchestrate a secure cloud Ecosystem. The orchestration requires a risk based approach that follows the Risk Management Framework (RMF) described in NIST SP 800-37 (Rev. 1): *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* to cloud-based Federal information systems. Often, the set of tasks necessary to complete in order to follow the risk management best-practice steps, are known as the RMF for Cloud Ecosystems (RMF4CE) when applied to cloud-based information system.

Commented [IM1]: This document might be first to go out, ahead of the 800-173, so this is the initial source for introducing the term. Should we indicate that "it is known" or should we introduce the name here. Something like.. " For the sake of brevity, we will refer to this methodology as …"

The study upon which the SRA is based collected, aggregated, and validated data for a Public cloud, considering all three cloud service models – Software as a Service (SaaS), Platform as a Service

(PaaS), and Infrastructure as a Service (IaaS) – and all cloud Actors (i.e., cloud Consumer, Provider, Broker, Carrier, and Auditor). While this document focuses on a Public cloud deployment model because it best supports illustrative examples of all of the SRA Security Components and security considerations, the SRA (the formal model, the set of Security Components, and the methodology for applying the RMF4CE) is agnostic with respect to cloud deployment model, and its methodology can easily be applied to Private, Community, or Hybrid clouds.

The SRA introduces a risk-based approach to determine each cloud Actor's responsibility for implementing specific controls throughout the lifecycle of the cloud Ecosystem. Specifically, for each instance of the cloud Ecosystem, the Security Components are analyzed to identify the level of involvement of each cloud Actor in implementing those components. The ultimate objective of this document is to demystify the process of describing, identifying, categorizing, analyzing, and selecting cloud-based services for cloud Consumers 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.

Commented [KS2]: Not sure about this wording. There are other considerations to take into account. The most secure and efficient solution may not be the best overall.

1 INTRODUCTION

Cloud computing changes the emphasis from procuring, maintaining, and operating the necessary IT hardware and related infrastructure to meeting the agency's mission and taking advantage of higher-quality, added-value capabilities and faster services at lower cost to users. However, a cloud computing environment does not inherently provide the same level of security and compliance with US government (USG) mandates as was achieved in the traditional IT model. The ability of an agency acting as a cloud Consumer to comply with business, regulatory, operational, or security requirements in a cloud environment is a direct result of the cloud service and deployment models adopted by the agency, the cloud architecture, and the deployment and management of the resources in the cloud environment.

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

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

The NIST Cloud Computing Security Working Group (NCC SWG) was created to achieve broad collaboration between Federal and other stakeholders in an effort to address the security-related concerns expressed by Federal managers. One of the tasks of the NCC SWG is to design a Cloud Computing Security Reference Architecture that supplements SP 500-292: *NIST Cloud Computing Reference Architecture (RA)* with a formal model and identifies the core set of Security Components recommended for building a successful and secure cloud Ecosystem. This document facilitates USG acquisition of cloud services with the proper security level by explaining the interdependent security requirements between typical cloud service parties (known as cloud Actors), and by providing a methodology for identifying the desired cloud Ecosystem functional and security requirements in a building blocks approach of cloud security components.

Commented [IM3]: Need to make sure we define what is a 'security component' in the context of SRA

1.1 AUDIENCE

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

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

This publication presumes that readers possess a fundamental understanding of the following topics:

- Cloud computing, particularly the cloud definition provided by NIST SP 800-145 and the cloud deployment model discussions in NIST SP 500-292.
- The NIST Risk Management Framework (RMF) described in NIST SP 800-37 Revision 1
- Risk-based assessment for IT systems as described in NIST SP 800-30, *Guide for Conducting Risk Assessments* and International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC) 27005, *Information technology-Security techniques – Information security risk management systems*

Because of the evolving nature of security considerations in a cloud environment, readers are encouraged to refer to other resources referenced in this publication, most of which are available online.

1.2 OBJECTIVES

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

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

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

The SRA is intended to be an elastic, dynamic framework that is layered over the NIST Cloud Computing RA and takes into account the following:

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

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

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

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

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

1.3 SCOPE

This publication describes the components of the SRA, specifically:

- A formal model
- A set of Security Components that leverages the CSA TCI-RA
- A methodology for using the formal model and the set of Security Components to apply the NIST RMF to cloud-based Federal information systems. This methodology is known as the RMF for Cloud Ecosystems (RMF4CE).

This publication collects, aggregates, and validates data for a Public cloud deployment model, with all three service models (SaaS, PaaS, and IaaS) and all cloud Actors. This focus on a Public cloud deployment model is for purposes of example only, as it best supports illustrative examples of all of the SRA Security Components and security considerations. The SRA (the formal model, the set of Security Components, and the RMF4CE methodology) is agnostic with respect to cloud deployment

---

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

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

models, and its methodology can easily be applied to data and operations hosted in Public, Private, Community, or Hybrid clouds.

1.4 STRUCTURE OF THE PUBLICATION

The rest of this publication is organized into six sections supported by six annexes.

Section 2 presents a comprehensive overview of the SRA. This includes clarification of the roles and responsibilities of all cloud Actors described in NIST SP 500-292.

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

Section 4 introduces the SRA formal model and discusses the Architectural Components of the model for each cloud Actor.

Section 5 describes the orchestration of a secure cloud Ecosystem as defined by interactions between the cloud Actors for implementing and integrating the Security Components. To better illustrate the interactions among cloud Actors and their roles and responsibilities in orchestrating a cloud Ecosystem, the section provides a use case example – a generic USG agency service migrated to the cloud – and highlights the necessary steps to secure the cloud Ecosystem and to determine the high-level cloud architecture that meets the cloud Consumer's security requirements. This section concludes with the negotiation of the contractual terms and agreements in Service Level Agreements (SLAs).

Section 6 defines selected terms and acronyms used within the publication.

Section 7 lists the references for the publication.

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

Commented [KS4]: Annex A is the TCI-RA. Is that another way of stating what this Annex A description currently says?

Annex B depicts how the Security Components are mapped or paired to the NIST SP 800-53 security control families using the color code presented in **Table 3**.

Annex C is the generic heat map of cloud Actor responsibilities for implementing Security Components and associated security controls in a cloud Ecosystem.

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

Annex E presents a matrix that maps the high-level security components, and with them the NIST SP 800-53 security control families, to the Architectural Components and Sub-Components defined for each cloud Actor.

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

1.5 USING THE PUBLICATION

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

- **Describe** the service that should be migrated to the cloud
- **Identify** the necessary capabilities of the service
- **Categorize** the Information System to determine the impact levels and the Security Components and associated security control baselines (three sets of baseline controls corresponding to low-impact, moderate-impact, and high-impact information systems). Baseline controls are chosen based on the security category and associated impact level of information systems determined in accordance with Federal Information Processing Standard (FIPS) 199: *Standards for Security Categorization of Federal Information and Information Systems* and FIPS 200: *Minimum Security Requirements for Federal Information and Information Systems*, respectively [16][17].
- **Analyze and select** the most appropriate instance of a cloud Ecosystem by identifying the cloud composite architecture, such as the cloud deployment and service models:
    - 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 (i.e., 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 SIS as described in **Sec. 5.2.2**;
    - Identifying the NIST SP 800-53 (Rev. 4): *Security and Privacy Controls for Federal Information Systems and Organizations* security controls necessary for each Security Component;
    - 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.

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

Commented [KS5]: I am not sure if this is still needed. It follows a series of steps that I don't remember seeing elsewhere in the cloud WG publications. I have not edited this text.

2 BACKGROUND

This document presents the NIST Cloud Computing Security Reference Architecture (SRA) formal model derived from NIST SP 500-292, *NIST Cloud Computing Reference Architecture*; an associated set of Security Components derived from the CSA TCI-RA; and the RMF4CE methodology for using the formal model and the Security Components to orchestrate a secure cloud Ecosystem by applying the NIST RMF from NIST SP 800-37 Revision 1 to cloud-based Federal information systems. This section provides background on the SRA and clarifies roles and responsibilities for all cloud Actors described in NIST SP 500-292.

2.1 REVIEW OF THE FEDERAL CLOUD COMPUTING STRATEGY

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

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

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

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

2.2 APPROACH

Figure 1 below depicts the SRA approach described in detail in this publication.

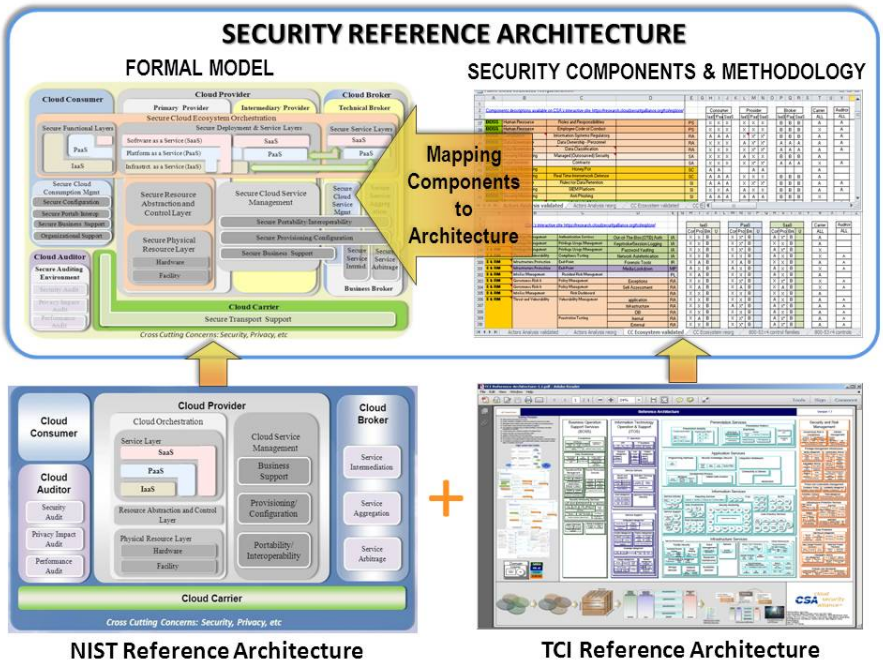


Figure 1: NIST Cloud Computing Security Reference Architecture Approach

The SRA is based on a three-dimensional approach using the following constructs defined in the NIST RA:

- The three types of service models: IaaS, PaaS, and SaaS
- The four types of deployment models: Public, Private, Hybrid, and Community
- The five types of Actors: cloud Provider, Consumer, Broker, Carrier, and Auditor

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

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

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

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

- Public IaaS, Public PaaS, Public SaaS
- Private IaaS, Private PaaS, Private SaaS
- Hybrid IaaS, Hybrid PaaS, Hybrid SaaS
- Community IaaS, Community PaaS, Community SaaS

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

However, **Figure 2** provides a graphical representation of the SRA three-dimensional approach that would lead to twelve cloud instances for which data can be collected, aggregated, and analyzed by applying the same concepts described in this document for a Public cloud Ecosystem.

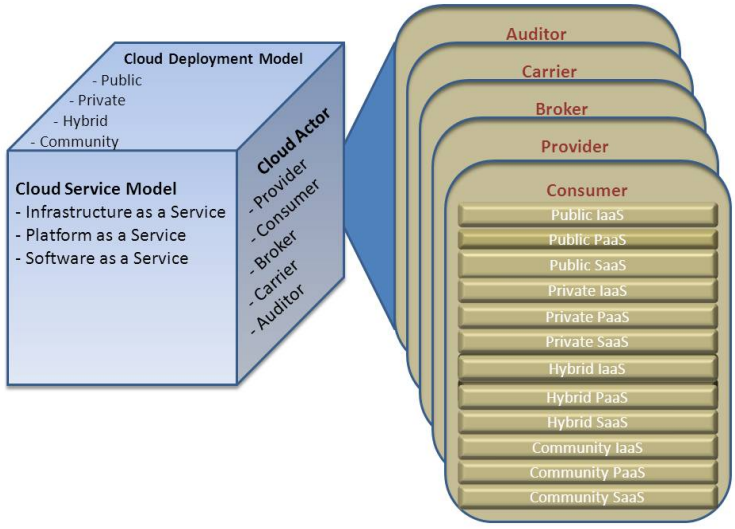


Figure 2: Security Reference Architecture Constructs and Instances

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

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

2.3 RISK MANAGEMENT

FISMA [6] requires that Federal agencies implement security and privacy controls commensurate with risk for all Federal information systems. FISMA and Office of Management and Budget (OMB) Circular A-130, Section 8b (3), *Securing Agency Information Systems* [18] also require any entities operating systems on behalf of the Federal government – including cloud Providers – to meet the same security and privacy requirements as Federal agencies. Security and privacy requirements for cloud Providers, including the security and privacy controls for information systems processing, storing, or transmitting Federal information, are expressed in appropriate contracts or other formal agreements using the RMF and associated NIST security standards, Special Publications, and guidelines.

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

The assurance or confidence that the risk presented by using cloud services is at an acceptable level depends on the trust that the organization places in the external cloud Provider and Broker, when involved in the orchestration of the cloud Ecosystem and on the ability to assess the Provider's and Broker's compliance with requirements for all security controls deemed necessary.

This risk management process ensures that issues are identified and mitigated early in the investment cycle with routine and periodic reviews. In addition, the CIO Council maintains a library[4] of helpful

[4] https://cio.gov/resources/document-library/

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

2.3.1 THE RISK MANAGEMENT FRAMEWORK

The Risk Management Framework (RMF), defined in NIST SP 800-37 Revision 1 and illustrated in **Fig. 3** below, provides a disciplined and structured process that integrates information security and risk management activities into the system development lifecycle. For each identified step, there is at least one standard or guideline; these are also identified in the graphic.

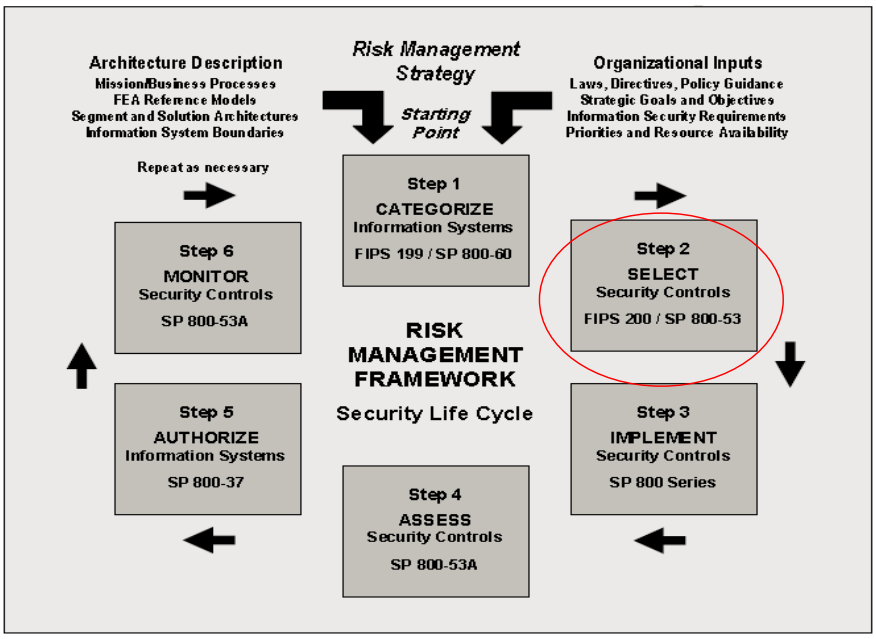


Figure 3: Risk Management Framework (NIST SP 800-37 Rev 1.)

Commented [KS6]: From Kelley D: Step 6 should also reference 800-137. I did find a different version of this graphic that includes 800-137, but it has a lot of other differences. Not sure how you want to proceed.

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

The following is a high-level overview of the six steps in the RMF.

Step 1: Categorize the information system and the information processed, stored, and transmitted by that system based on an impact analysis. This step, including consideration of legislation, policies, directives, regulations, standards, and organizational mission/business/operational requirements, facilitates the identification of security requirements. FIPS 199 provides security categorization guidance for non-national security systems. NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories* provides implementation guidance on the assignment of security categories to information and information systems. CNSSI 1253, *Security Categorization and Control Selection for National Security Systems* provides similar guidance for national security systems, and Department of Defense Instruction (DoDI) 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*, does so for Department of Defense 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. Document the security controls in the security plan. FIPS 200 provides the minimum required (i.e., baseline) security controls for low-, moderate-, and high-security systems. NIST SP 800-53 provides security control selection guidance for non-national security systems. CNSSI 1253 provides similar guidance for national security systems.

Step 3: Implement the security controls specified in the security plan and describe how the controls are employed within the information system and its operating environment. NIST provides a comprehensive resource of standards and specifications that provide secure implementation guidance for much management, operational and technical security controls. FIPS 200; NIST SP 800-30 Revision 1; NIST SP 800-53 Revision 4; NIST SP 800-53A Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*; and CNSSI 1253 are a few of the standards and specifications that provide guidance for the users and developers of security configuration checklists.

Step 4: Assess the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. NIST SP 800-53A Revision 1 provides security control assessment procedures for security controls defined in NIST SP 800-53 Revision 4.

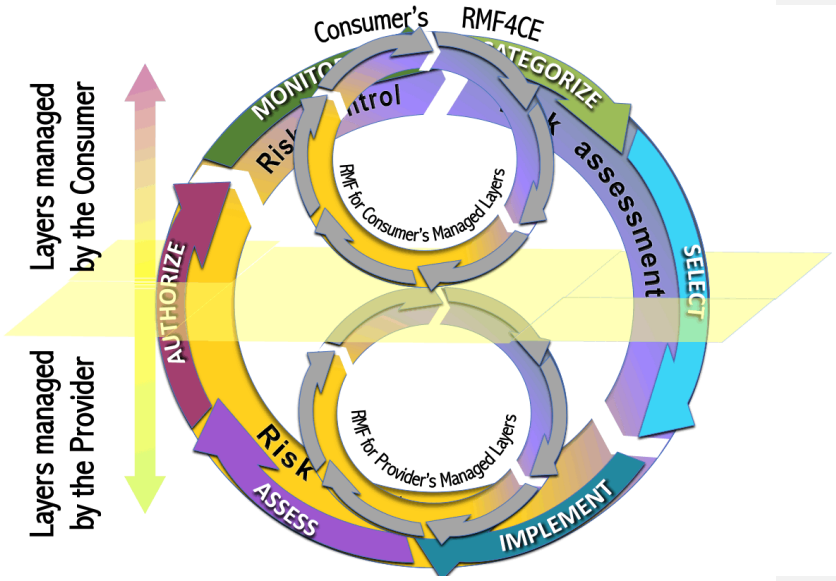
Step 5: Authorize information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable. NIST SP 800-37 Revision 1 provides guidance on authorizing an information system to operate.

Step 6: Monitor the security controls in the information system on an ongoing basis, including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials. NIST SP 800-37 Revision 1 and NIST SP 800-137, *Information Security Continuous Monitoring for Federal Systems and Organizations* provide guidance on monitoring the security controls in the environment of operation, the ongoing risk

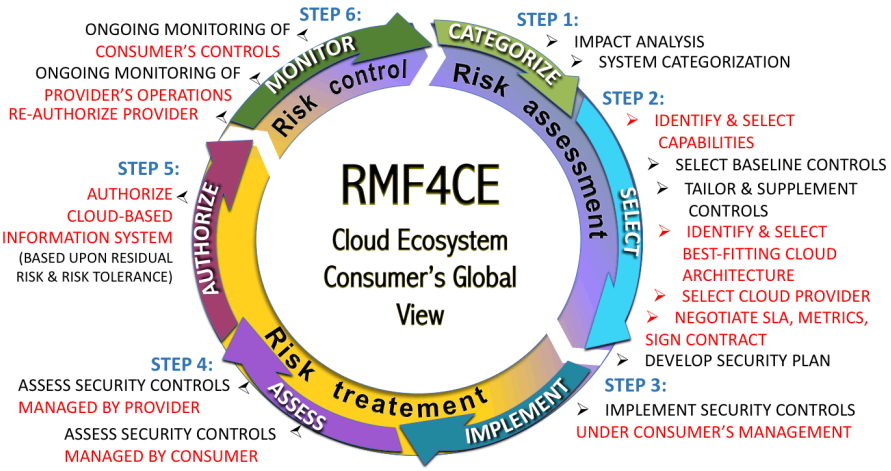
determination and acceptance, and the approved information system authorization to operate status. NIST SP 800-53A Revision 1 provides assessment guidance for monitoring the security controls defined in NIST SP 800-53 Revision 4.

Federal agencies researching cloud-based solutions for their information systems should adapt the six steps of the RMF for use during their evaluation. While the RMF is flexible and easily adaptable in most cases, it assumes a traditional IT environment, so it requires some customization to address the unique characteristics of cloud-based services. For example, since cloud Consumers and other Actors involved in securely orchestrating a cloud Ecosystem have differing degrees of control over cloud-based IT resources, they need to share the responsibility of implementing the security requirements. The RMF can be adapted to take into account the shared responsibilities. Another example is that because the agency has no direct access, management, or control over the functional layers acquired from the Provider, the agency needs to find ways to obtain enough transparency into the Provider's architecture to be able to perform an accurate risk assessment.

The RMF adapted for cloud-based Federal information systems is known as the *Risk Management Framework for Cloud Ecosystems (RMF4CE)*. The RMF4CE uses the same six steps as the RMF, but it supplements them by adding tasks that are specific to cloud-based systems. The following graphic representation capture the RMF applied to the layers managed by Provider, by Consumer and the overall Consumer's view of RMF applied to the entire cloud Ecosystem.



The additional task a cloud Consumer should consider when applying the RMF to the entire cloud Ecosystem are listed below with red.



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

For example, a cloud Consumer planning the migration of its agency's data to a Public IaaS cloud may, upon completion of the risk assessment analysis, follow the steps presented in **Sec. 5** to identify the Security Components that must be implemented to secure the data. This is accomplished by leveraging the Security Components identified in this document for a Public IaaS cloud. The set of Security Components would be a union of the sets assigned in this document to each cloud Actor for

the cloud instance of interest (see **Annex A**), augmented as needed with additional Security Components and controls for the particular data and/or application(s) migrated to the cloud.

2.3.2 MANAGING THE RISK INHERENT IN CLOUD SERVICES

Starting on June 6, 2014, USG agencies are required to accept only cloud Providers that have been assessed and authorized through the Federal Risk and Authorization Management Program (FedRAMP) and have received a FedRAMP Provisional ATO (P-ATO) issued by the Joint Authorization Board (JAB)[5]. FedRAMP is a government-wide program that provides a standard framework for assessing and authorizing cloud service vendors using a standardized approach to security assessment, authorization, and continuous monitoring, similar to the A&A process used to assess Federal agencies for compliance with applicable mandates. The purpose of this process is to assess whether a cloud service vendor adheres to the minimum mandated security requirements for Federal agencies and implements the identified security controls for low- and moderate-impact systems as described in FIPS 199: *Standards for Security Categorization of Federal Information and Information Systems* and FIPS 200: *Minimum Security Requirements for Federal Information and Information Systems* [16][17].

Commented [KS7]: The URL in the footnote is invalid.

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

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

Federal agencies are responsible and accountable for the information security risk incurred by the use of information system services offered by external suppliers, including cloud Providers and Brokers. The RMF4CE provides a structured, yet flexible approach for managing the portion of risk resulting from the incorporation of cloud-based information systems into the mission and business processes of the organization. Cloud Consumers can require cloud Providers to implement all steps in the

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

RMF4CE process, with the exception of the security authorization step. That remains an inherent Federal responsibility directly linked to the management of risk related to the use of cloud services.

The RMF4CE can be used to address the security risks associated with cloud systems by incorporating it into the terms and conditions of the contracts with external cloud Providers and Brokers. Performance aspects of these terms and conditions are also incorporated into the SLA, which is an intrinsic part of the SA between the cloud Consumer and the Provider and/or Broker. Contractual terms should include, for example, guarantees of the cloud Consumer's timely access to or the Provider's timely delivery of cloud audit logs, continuous monitoring logs, and any user access logs. More information is provided in **Sec.** Error! Reference source not found. of this document.

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

USG cloud Consumers should also require cloud Providers and Brokers to present appropriate evidence that demonstrates their compliance with the RMF in protecting Federal information. It is important to emphasize that, while the six steps of the RMF4CE cover the entire lifecycle of cloud-based information systems, this publication is primarily focused on Step 2 and only provides pointers for the other steps.

2.4 ASSUMPTIONS, CLARIFICATIONS, AND DEFINITIONS

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

2.4.1 CLOUD COMPUTING SERVICE AND DEPLOYMENT MODELS

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

2.4.1.1 SERVICE MODELS

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

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

In an IaaS deployment, the capability provided to the cloud Consumer is to provision processing, storage, networks, and other fundamental computing resources where the cloud Consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The cloud

Consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

In a PaaS deployment, the capability provided to the cloud Consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming, libraries, services, and tools supported by the Provider. The cloud Consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

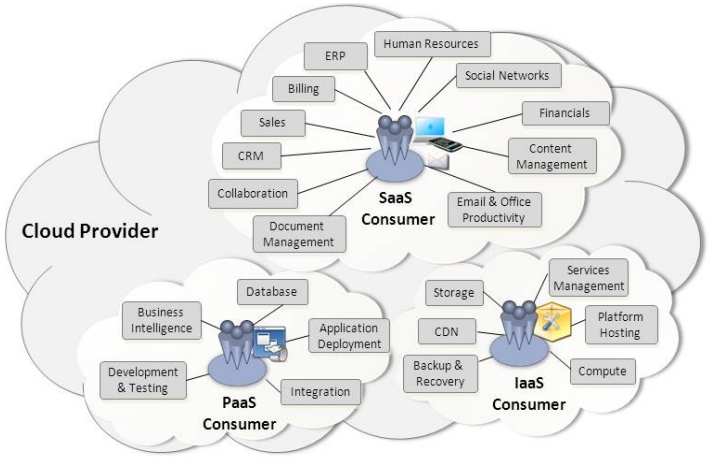


Figure 4: Example of Services Available to a Cloud Consumer (NIST SP 500-292)

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

2.4.1.2 DEPLOYMENT MODELS

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

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

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

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

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

2.4.2 CLOUD ECOSYSTEM

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

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

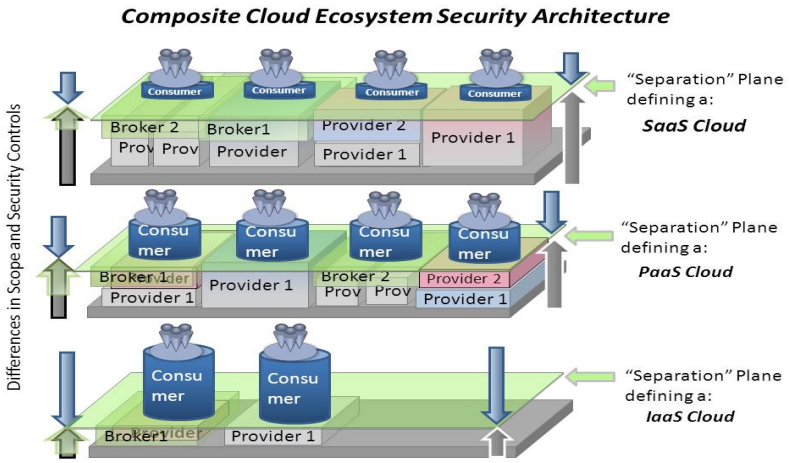


Figure 5: Composite Cloud Ecosystem Security Architecture

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

It is important to note that the cloud Carrier involved in the cloud Ecosystem is not represented in the diagram because the service provided by the Carrier (i.e., data transport) can be accomplished using different vehicles, from dedicated communication channels to the open Internet, that involve multiple Internet Service Providers and backbone network operators. This complexity makes it difficult to illustrate the 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 Carrier's role. However, it is important to highlight that the Carrier role is critical to the functioning of the cloud Ecosystem. In a cloud Ecosystem that serves the needs of USG organizations, it is the Consumer's (i.e., agency's) responsibility to identify, based upon the risk analysis performed, the full set of security controls that must be mandated and implemented to secure the operations and data migrated to the cloud, and implement those security controls that fall directly under its area of responsibility. It is also the Consumer's responsibility to determine/identify the subset of security controls that fall under Broker, Carrier, and Provider responsibilities, based on the type of cloud Ecosystem used. The union of all subsets of security controls must result in a combined set that can fully secure the cloud Ecosystem.

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

- Risk Management
  - Risk Analysis
  - Risk Assessments
  - Vulnerability Assessments
  - Incident Reporting and Response
- Business Continuity
  - Disaster Recovery Plans
  - Restoration plan Incorporating and Quantifying the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for Services
- Physical Security
  - Physical and Environmental Security Policy
  - Contingency Plan
  - Emergency Response Plan
  - Facility Layout
  - Security Infrastructure
  - Human Resources
  - Environmental Security
  - Visual Inspection of the Facility
- User Account Termination Procedures
- Compliance with National and International/Industry Standards on Security
- Transparent View of the Security Posture of the Cloud Providers, Brokers, and Carriers

2.4.3 CLOUD CONSUMER

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

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

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

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

external subsystems storing, processing, or transmitting Federal information and any services provided by, or associated with, the subsystem.

2.4.4 CLOUD PROVIDER

A *cloud Provider* is the entity responsible for making a service available to cloud Consumers (either directly or indirectly via a Broker). A Provider acquires and manages the computing infrastructure required for providing the services, runs the cloud software that provides the services (at least for SaaS and PaaS service deployments), and makes arrangements to deliver the cloud services to the Consumers through network access.

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

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

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

- Primary Provider (labeled "Provider 1" in the Cloud Composite Architecture)
- Intermediary Provider (labeled "Provider 2" in the Cloud Composite Architecture)

2.4.4.1 PRIMARY CLOUD PROVIDER EXAMPLE

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

2.4.4.2 INTERMEDIARY CLOUD PROVIDER EXAMPLE

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

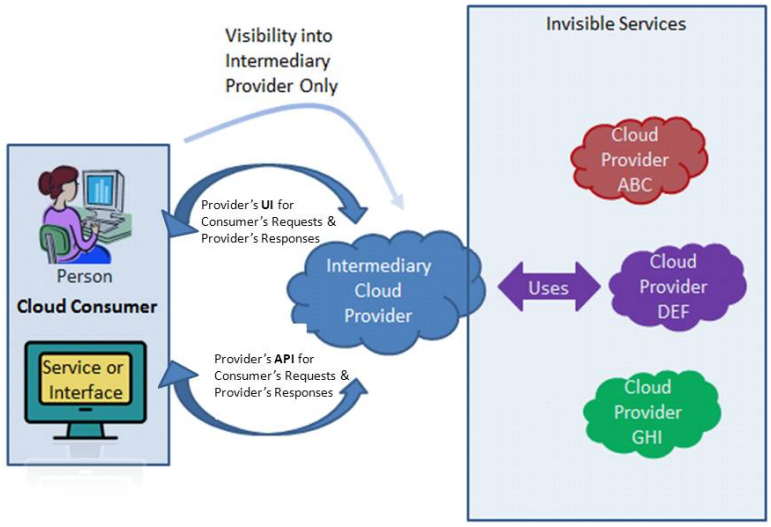


Figure 6: Intermediary Cloud Provider Example

2.4.5 CLOUD BROKER

NIST SP 500-292, *NIST Cloud Computing Reference Architecture* defines a *cloud Broker* as an entity that manages the use, performance, and delivery of cloud services, and negotiates relationships between cloud Providers and Consumers [13]. The purpose of this section is to elaborate on the description of the cloud Broker provided in NIST SP 500-292, to provide a better description of the roles and types of services that a Broker may offer to Consumers, and to emphasize the differences between a Broker and a Provider.

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

It is important to note that in the majority of the graphical representations of a Broker, the transparency shown in the images does not imply a Broker is modifying the functional layers provided by a Provider. Rather, such transparency indicates that the Broker, in addition to providing extra functionality, allows the Consumer to have a particular level of visibility into and information about the Provider services. Also, when necessary, the Broker facilitates direct communication with the

Commented [KS8]: Michaela and Anil:

From public comments: Agreed to add the following to 2.4.5:

"*The opacity to cloud Consumers and often cloud Brokers of supply chains between primary, secondary (and sometimes tertiary) cloud Providers is a significant issue in cloud arbitrage; where a cloud Consumer or cloud Broker can only see the interface presented by the primary Provider, and it makes it impossible to determine whether apparently-independent cloud Providers truly operate as primary or intermediary cloud Providers sharing any common elements in their own dependencies. Highlighting the "transparency" factor as core architectural difference between a technical Broker and intermediary Provider is key in understanding the liabilities assumed by intermediary cloud Providers on behalf of all their partners in the business negotiation process.*"

Provider in the orchestration of the cloud Ecosystem and during operational processes. Herein, this is referred to as the "*transparent visibility* into the primary service Providers," as noted above.

Commented [KS9]: Is this OK? Should it be "Primary Providers" instead of "primary service Providers"? Can we remove the quotes? Can we remove the "as noted above"?

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

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

2.4.5.1 DIFFERENTIATING BUSINESS AND TECHNICAL BROKER SERVICES

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

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

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

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

2.4.5.2 A CLOUD BROKERAGE EXAMPLE

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

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

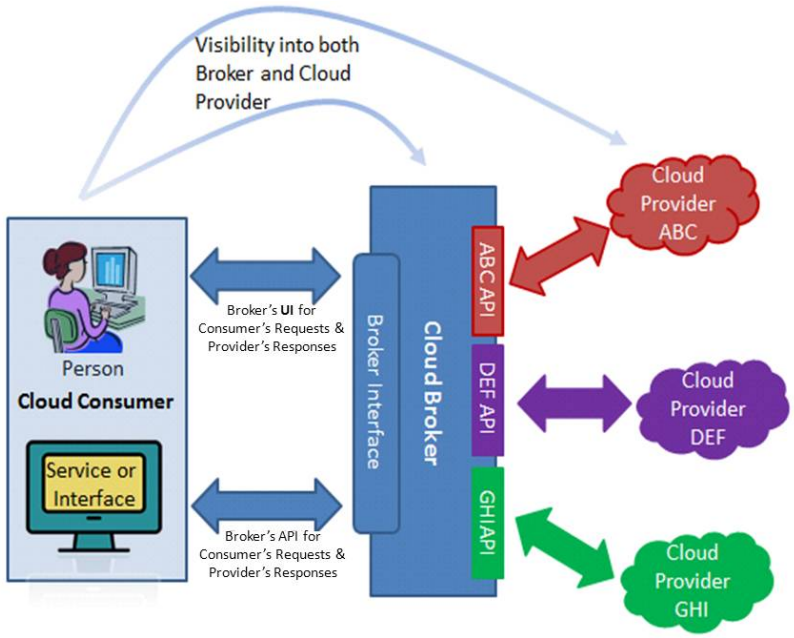


Figure 7: Cloud Broker Example

A 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, and cost and usage reporting.

2.4.6 CLOUD CARRIER

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

Commented [KS10]: I have never heard of this before. I Googled for it and it seems to be another term for smartphones, tablets, etc. Suggest adjusting this sentence to say "smartphones, and tablets" instead of "mobile phones, and mobile Internet devices (MIDs)"

The security concerns of the Carrier role include consideration for the exposures and threats that would be present in the transmission of data to and from a cloud structure. Due to the evolutionary nature of the Internet and the development over time of new methods for signal transmission, there

are inherent vulnerabilities in the channels that transmit data to and from cloud structures. Security breaches at juncture and insertion points present a challenging security problem for Carriers in both cloud and non-cloud transmissions. For these reasons, the Carrier is responsible for maintaining security control points that span the systems it manages, as well as security testing, risk management, and preventative tasks that would be expected to reduce vulnerabilities in transmission channels. Carriers can offer dedicated lines of communication between endpoints, including interstate and international dedicated lines.

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

2.4.7 CLOUD AUDITOR

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

An Auditor can make an assessment of the security controls in the information system, in accordance with generally accepted auditing standards, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to the security requirements for the system. The security auditing should also include the verification of compliance with regulation and security policy. For example, an Auditor can be tasked with ensuring that the correct policies are applied to data retention according to relevant rules for the applicable jurisdictions providing legislative and regulatory data compliance oversight. The Auditor may ensure that fixed content has not been modified and that the legal and business data archival requirements have been satisfied.

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

The underlying service model used by the systems being audited plays a secondary role from the viewpoint of the Auditor. The relevant Security Components in support of the cloud service should be audited against the tailored security controls (e.g., NIST SP 800-53). The cloud Auditor should be provided reasonable access to the Security Components in order to perform the assessment. It is assumed that an Auditor would also have some persistent and sensitive information regarding its client files as well. Therefore, the Auditor will need to be cognizant of the Security Components available to support this function by using widely accepted industry best practices, such as those addressed in GAO-12-331G Government Auditing Standards.

2.4.8 BUSINESS MODELS AND NIST REFERENCE ARCHITECTURE

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

Consider the relationships of the entities in **Figure 8** – three agencies and two cloud service vendors. Agency 1 uses the PaaS services from Vendor A, while implementing in house its end users' business management. In this business relationship, Agency 1 is a Consumer of the PaaS services offered by Vendor A as a Primary Provider. Agency 2 also uses the PaaS services offered by Vendor A. In this case, Vendor A also implements the business management functions (authorization contract management) of Agency 2's end users. Agency 2 is a Consumer of the cloud services offered by Vendor A as a Primary Provider. It is important to note that Vendor A, in its role of Provider, offers different cloud service packages to different Consumers. In the last scenario depicted in **Figure 8**, Agency 3 consumes Vendor B's SaaS services while it contracts with Vendor A the business management functions of its end users. In this business scenario, a particular level of trust must exist or be established between Vendor B and Vendor A. In this case, Agency 3 is a Consumer of SaaS services offered by Vendor B as a Provider, while Vendor A is a Broker for Agency 3, since it is providing value-added business management functionality.

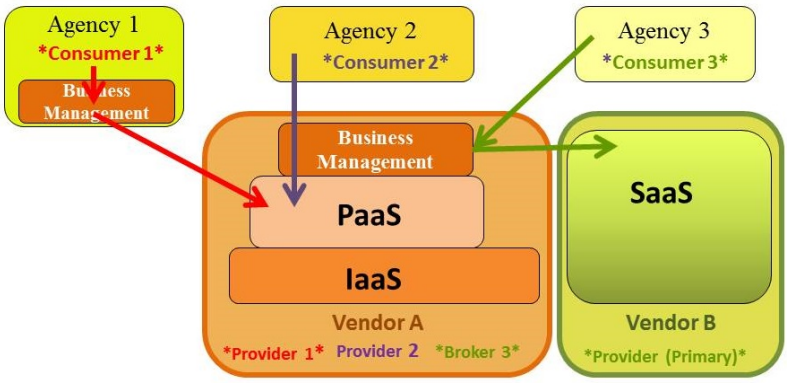


Figure 8: Business Models Versus NIST Reference Architecture

In summary, it is important to keep in mind that the NIST RA and SRA do not constitute a comprehensive, one-to-one translation of all organizations' business models, but rather allow for

Commented [KS11]: Wording, not sure what is missing

Commented [KS12]: Of or for?

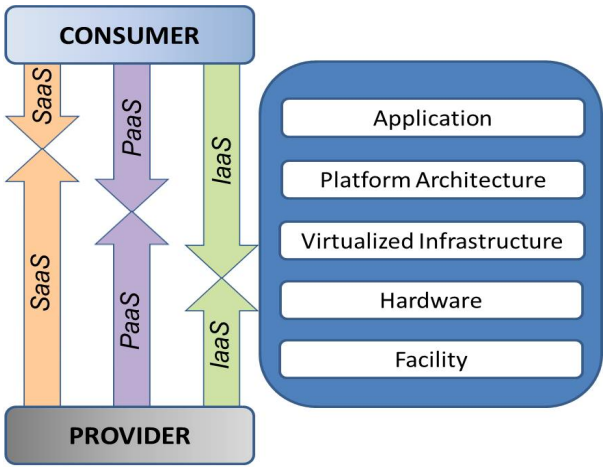
Commented [KS13]: Of or for?

flexible mapping of the business models employed by all cloud service vendors. The architecture described in these two publications defines cloud Actors based upon the roles they play in relation to their business partners and customers in the context of cloud services.

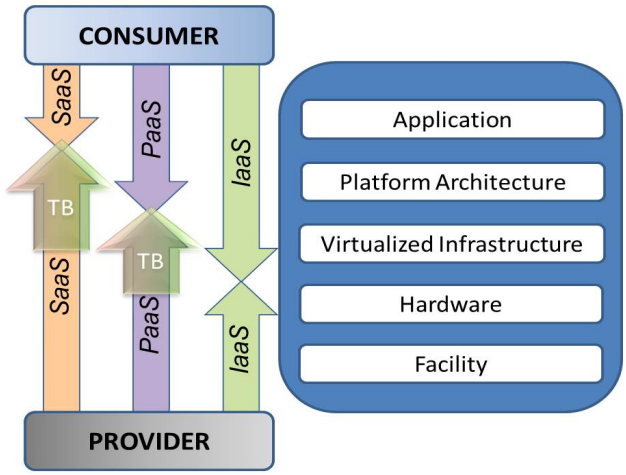
2.4.9 SECURITY CONSERVATION PRINCIPLE

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

Commented [KS14]: Service and deployment models?



a)



Legend: TB = cloud Technical Broker

b)

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

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

Commented [KS15]: Service and deployment models?

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

3 SECURITY REFERENCE ARCHITECTURE: DATA ANALYSIS METHODOLOGY

The SRA leverages the CSA TCI-RA shown in **Annex A**. To accomplish this, the team that authored this publication extracted all of the capabilities described in the TCI-RA while preserving the path to the three root-domains (Business Operation Support Service [BOSS], Information Technology Operation and Support [ITOS], and Security and Risk Management [S&RM]) and generated a total set of 346 Security Components. An example of the resulting data collection form is shown in **Table 1**.

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

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

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

3.1 DATA COLLECTION

The data collection effort was focused on populating the SRA formal model by assessing the applicability of each Security Component for a given cloud instance. Accordingly, each blank cell

under each Actor heading (note the cloud Consumer, cloud Provider, etc. columns in **Table 1**) was marked with one of the following:

- "X" to indicate that the Security Component should be implemented by the Actor to secure the Consumer's applications and data in the Cloud.
- "A" to indicate that the Security Component should be implemented internally, independent of the Consumer's data, for administrative or best practice reasons.
- "B," specific to Business Brokers only, to indicate a Security Component that is implemented to secure the cloud computing business-oriented service. The marking also emphasizes that the Business Broker only provides business and relationship services, and does not have any contact with the Consumer's data migrated to the cloud.
- A blank cell indicates that the Security Component cannot be implemented by the particular Actor or is not necessary in securing the cloud Ecosystem.

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

The purpose of the markings is to provide Consumers with a reference they can use to identify the Security Components that are applicable for a particular cloud service model. The markings also indicate which Actor(s) in the cloud Ecosystem – Consumer, Provider, or Broker, in most cases – is responsible for a particular Security Component based on the use case or type of cloud service offered.[6] As indicated by the data sets, there are areas in which the responsibility for a particular Security Component may reside with multiple Actors depending on the specifics of the Component and the particular use case.

It is important to distinguish between responsibility for identifying and setting Security Components requirements and for implementing them. The Consumer is always accountable for ensuring that all appropriate provisions for an effective security control environment are identified and implementation requirements are in place. This accountability cannot be relinquished.

For some Security Components in certain cloud service models, the Consumer is both accountable and responsible for implementation. For example, "Security Monitoring Services - Endpoint Monitoring" is a Security Component that, regardless of the service model, can only be implemented by the Consumer.

Even when responsibility for implementation is outsourced to another Actor, if a Security Component is applicable, the Consumer remains accountable for identifying that Security Component and for requiring implementation through contractual means. For example, "Data Governance – Secure Disposal of Data" is a Security Component that the Consumer may be able to implement for a IaaS

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

service model but needs to be implemented by Provider(s) for all other service models. The Consumer needs to ensure through contractual means that the Component is properly implemented by the Provider(s) of the cloud services.

3.2 DATA AGGREGATION AND VALIDATION

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

Figure 10 captures graphically the derivation of the Security Components, the data collection process, and the two types of data aggregation used to analyze the set of Security Components for each cloud service model.

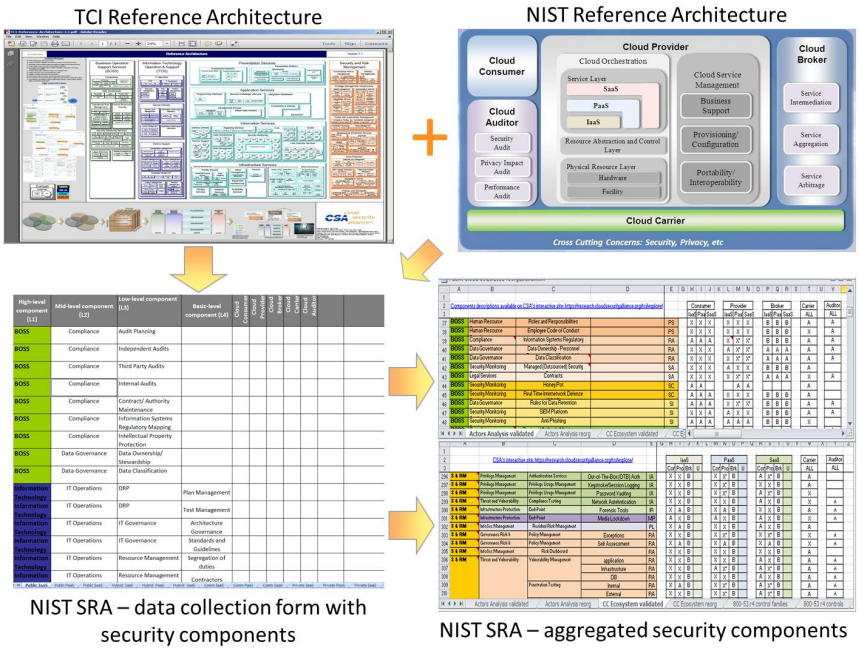


Figure 10: Security Components Overview

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

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

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

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

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

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

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

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

1. Identify the "floor" or lowest service layer of the Technical Broker or Intermediary Provider (e.g., "Infrastructure" layer if the Broker builds its services supplementing an IaaS Provider).
2. Identify the "ceiling" or highest service layer of the Technical Broker or Intermediary Provider (e.g., "Platform" layer if the Broker offers PaaS services).

3. Extract from the data sets provided in **Annex D** the Primary Provider set of Security Components corresponding to the [floor]aaS and the one corresponding to the [ceiling]aaS.
4. Perform a logical subtraction of the [floor]aaS from the [ceiling]aaS.

Figure 11 illustrates this approach.

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

Example:

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

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

Legend:

SC – set of Security Components
PP – Primary Provider
IP – Intermediary Provider
TB – Technical Broker

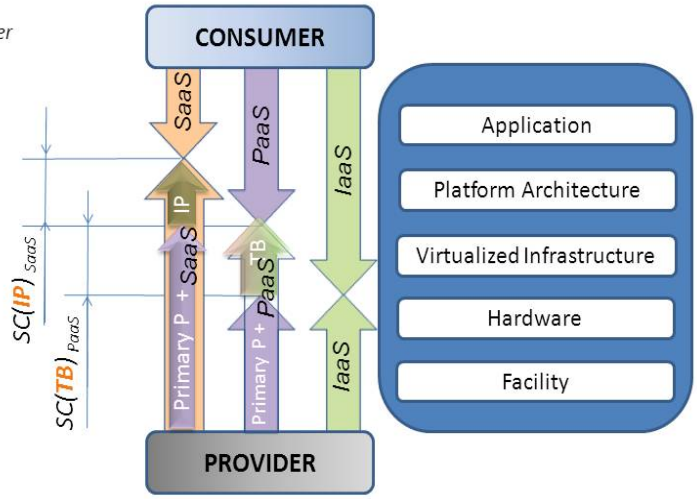


Figure 11: Security Components for Technical Broker & Intermediary Provider

3.4 MAPPING SECURITY COMPONENTS TO SECURITY CONTROL FAMILIES

NIST SP 500-293 Volume II (Draft), *US Government Cloud Computing Technology Roadmap Volume II: Useful Information for Cloud Adopters* identifies the need for clarification of security control roles and responsibilities as a challenging security requirement. To address this issue, this publication maps the Security Components identified in the SRA to the NIST SP 800-53 security control families. This mapping is necessary to set a common ground for agency Consumers and for Providers and Brokers in the private sector.

This section outlines the process used to map the Security Components to the security control families of NIST SP 800-53. The mapping or assignment of the Security Components to one of the eighteen families of security controls identified in NIST SP 800-53 was accomplished by sorting each Component into the "best fit" security control family. It is important to note that this mapping is not based upon particular security controls defined in NIST SP 800-53, since each Security Component may be associated with multiple NIST SP 800-53 security controls that often belong to different control families.

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

Table 2: TCI Reference Architecture - Domains and Service Layer

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

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

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

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

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

Commented [KS16]: I could not find this in the appendices. Wasn't sure what you would want it changed to.

3.5 EMPIRICAL DATA ANALYSIS AND THE GENERIC HEAT MAP

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

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

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

[AX AX AX] => 3.0	The vector is: AX AX AX -> 3
[XX AX AX] => 2.5	The vector has (2) AX + (1) XX -> 2.5
[XA AX AX] => 2.0 [XX XX AX] => 2.0	The vector has (2) AX or (1) AX+(2) XX -> 2
[XA XX AX] => 1.5 [XX XX XX] => 1.5	The vector has (1) AX + (1) XX or (3) XX ->1.5
[XA XA AX] => 1.0 [XA XX XX] => 1.0	The vector has (1) AX or (2) XX -> 1
[XA XA XX] => 0.5	The vector has (1) XX -> 0.5
[XA XA XA] => 0.0	The vector is: XA XA XA -> 0
AA AA AA => admin only	The vector is: AA AA AA
Null cells	The vector has empty cells

Figure 12: Legend of the Generic Heat Map

Commented [KS17]: Some of the cells says "The vector has" and some say "The vector is". Is that correct or should those all be the same?

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

Table 4: Security Component - Vector Generation

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

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

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

In the example in **Table 4**, the vector (**X**A, **X**A, **A**X) shown means that for this Security Component, the Consumer has "X" for IaaS, "X" for PaaS, and "A" for SaaS, meaning that it is the Consumer's responsibility to implement that Component in an IaaS or PaaS cloud and that the Security Component can only be implemented by the Provider for SaaS. When using SaaS, the Consumer can at most implement this Security Component for internal administrative functions. The same vector (X**A,** X**A,** A**X)**, indicates that the Provider has "A" for IaaS, "A" for PaaS, and "X" for SaaS, meaning that, for IaaS or PaaS, the Security Component can only be implemented internally by the Provider for its own administrative reasons and not to secure a Consumer's data or services, while the Provider is solely responsible for that same Security Component in SaaS.

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

Commented [KS18]: Should this be explained?

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

4 SECURITY REFERENCE ARCHITECTURE: FORMAL MODEL

4.1 OVERVIEW OF THE FORMAL MODEL

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

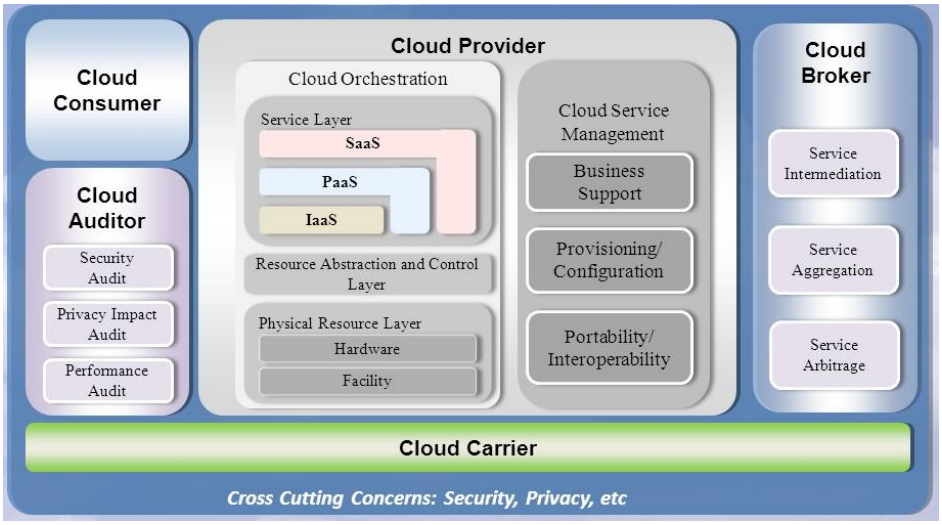


Figure 13: NIST Cloud Computing Reference Architecture (updated)

The SRA formal model presented in **Figure 14** below depicts, in a layered representation, the cloud Actors in the background and the Architectural Components defined for each Actor in the foreground. The Architectural Components and Sub-Components are stretched across multiple Actors when different Actors could perform similar or identical functions. For example, "Secure Provisioning and Configuration" is an Architectural Sub-Component indicating a service both Providers and Technical Brokers could implement as part of "Secure Cloud Service Management." Additionally, the Technical Broker could offer "Secure Service Aggregation" to its customers. The technical configuration and provisioning aspects associated with the aggregation are represented in the diagram by stretching the "Secure Provisioning and Configuration" Architectural Sub-Component across the graphical

representation of the "Secure Service Aggregation" Architectural Component. It is also important to note that the Consumer could implement "Secure Configuration" as part of "Secure Cloud Consumption Management" when needed to complement the services offered by the Provider and/or Technical Broker.

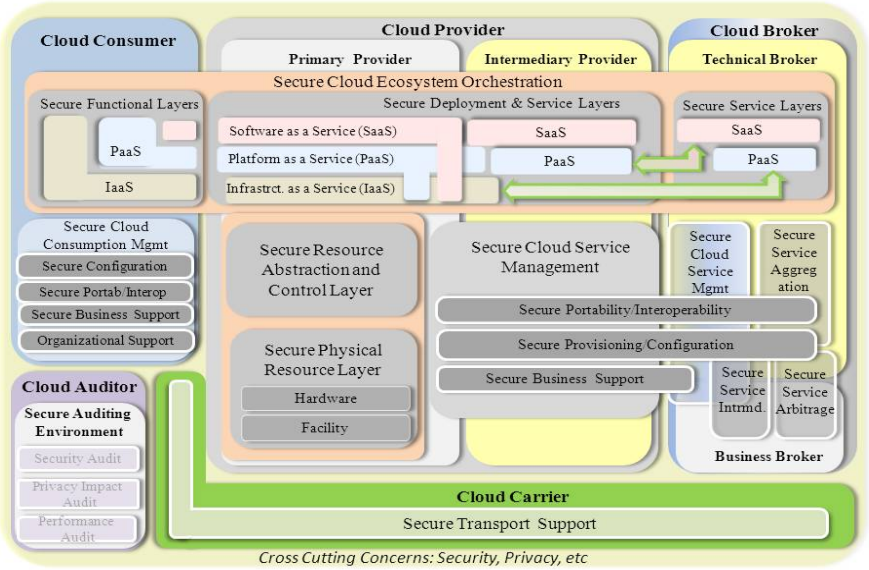


Figure 14: Formal Model - Security Reference Architecture

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

Cloud Consumer

- Secure Cloud Consumption Management
  - Secure Configuration
  - Secure Portability and Interoperability
  - Secure Business Support
  - Secure Organizational Support
- Secure Cloud Ecosystem Orchestration
- Secure Functional Layers

Cloud Provider

- Secure Cloud Service Management
  - Secure Provisioning and Configuration
  - Secure Portability and Interoperability

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

Cloud Carrier

- Secure Transport Support

Cloud Auditor

- Secure Auditing Environment

Cloud Broker

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

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

Annex B of this document presents a matrix that maps the high-level Security Components, and with them the NIST SP 800-53 security control families, to the Architectural Components and Sub-Components defined for each Actor. For instance, the "Policy and Standards – Role-based Awareness" Security Component is mapped to the Consumer's "Secure Cloud Consumption Management" Architectural Component, in particular the "Secure Consumption/Configuration" Architectural Sub-Components, indicating that the Consumer is required to address the secure processes and policies.

4.2 CONSUMER - ARCHITECTURAL COMPONENTS

NIST SP 500-292, *NIST Cloud Computing Reference Architecture* identifies the Provider's and Broker's services based on the areas in which the Actors conduct their activities. Our publication

leverages the services described for each Actor in NIST SP 500-292 to define the Architectural Components of the SRA. Since the NIST RA lacks an introduction to and analysis of the Consumer's responsibilities and functions, our publication contains the first introduction and description of the Consumer's Architectural Components. These Components are derived from the Consumer's responsibilities and functions in orchestrating a cloud Ecosystem and have no equivalent components in the NIST RA. The Consumer's Architectural Components complement the Provider's and Broker's Architectural Components as derived from the NIST RA.

Figure 15 highlights the Consumer on the SRA formal model diagram.

The cloud 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

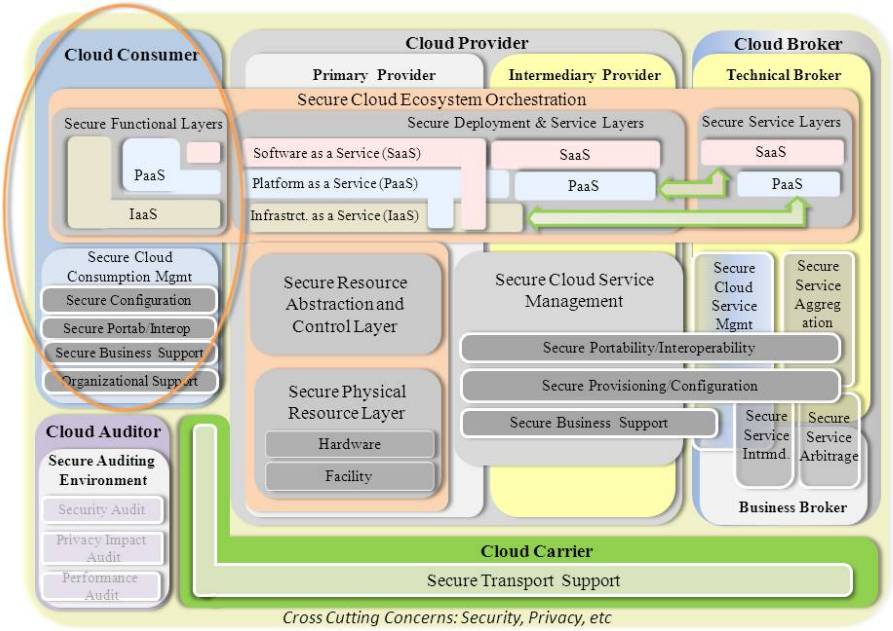


Figure 15: SRA – Cloud Consumer

Commented [IM19]: Deployment boundary is outside of orchestration boundary

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

4.2.1 SECURE CLOUD CONSUMPTION MANAGEMENT

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

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

These lead to the following main Architectural Sub-Components:

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

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

One of the challenges Consumers face when moving applications and data to the cloud is ensuring that the RMF4CE is applied properly and the near-real-time management and ongoing information system authorization meets the agency's needs through a robust continuous monitoring process (see NIST SP 800-37 for more details). The responsibility for performing continuous monitoring activities is shared among Actors involved in the cloud Ecosystem. Without shared agreements and a well-structured, cost-effective automation process that ensures that the effectiveness of the security controls can be measured in near-real-time, continuous monitoring of security controls is difficult to implement.

One possible solution that can support the continuous monitoring process and ensure that the proper mechanisms are in place is the adoption of standards such as the Security Content Automation Protocol (SCAP).[7] For example, operating system (OS) images used by a Provider can introduce risks to Consumers and their organizations when using pre-owned virtual machines where the OS images were uploaded with built-in Trojans. Malicious conversion of the cloud services into "bot-net-in-a-box" or spam servers can wreak havoc on operations. By using standards such as SCAP, Actors can collaborate on checking security policy compliance, identifying vulnerabilities in OS images, and measuring deviations from required configuration settings. Additionally, Consumers can gain

Commented [KS20]: Public comments: change "such as " to "similar to".

Also, add: (or find elsewhere already in the pub?)
Real time monitoring with intelligent filtering of reported data is ideal. Security automation is an essential part of an information security program. NIST SP 800-137: "*Information Security Continuous Monitoring for Federal Information Systems and Organizations"* recommends the use of open interoperable data specifications such as Security Content Automation Protocol (SCAP) - NIST SP 800-126;

Commented [KS21]: Not sure what this means

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

measurable data to map to high-level NIST SP 800-53 requirements and to gain the necessary information to make cost-effective, risk-based decisions with regards to the organizational information systems operating in a cloud Ecosystem.

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

4.2.1.1 SECURE BUSINESS SUPPORT

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

- Managing business relationships with the other 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 Actors in accordance with security best practices involving secure business processes and continuity of operations
- Managing service contracts, including setting up, negotiating, and closing/terminating contracts to ensure security concerns are addressed
- Procuring services only after security concerns have been addressed
- Managing payment and invoice 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 for the organization's employees and contractors through access control policies, business continuity plans, and various productivity tracking mechanisms for use by the Consumer. These are the services that enable the secure daily operations of a business in a cloud environment.

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

4.2.1.2 SECURE CONFIGURATION

The Consumer's *Secure Configuration* Architectural Component includes any capabilities, tools, or policies that ensure the secure configuration of cloud resources and compliance with the applicable security standards, specifications, and mandates (e.g., NIST SP 800-53, NIST SP 800-37, FIPS 199) as well as requirements set forth in the SLA. Criteria for securely configuring cloud resources may also include proprietary measures that have been set forth between the Consumer and Provider.

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

- *Rapid provisioning:* automatically deploying cloud systems based on the requested service/resources/capabilities. Securely managing rapid provisioning means, for example, ensuring that the requests are from an authenticated and authorized source.
- *Resource changing:* adjusting configuration/resource assignment for repairs, upgrades, and joining new nodes into the cloud. Securely managing resource changing means, for example, that requests for changes in resources and in any configuration of resources are received from an authenticated and authorized source.
- *Monitoring and reporting:* discovering and monitoring virtual resources, monitoring cloud operations and events, and generating security reports. Performance reports in the context of security such as excessive use of resources compared to normal use.
- *Metering:* providing a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, active user accounts). Securely managing metering means that Providers implement specific internal controls to ensure that storage can be encrypted, processing can be sandboxed, abnormal bandwidth usage can be reported, and user account management is in compliance with Consumer security policies.
- *SLA management:* encompassing the SLA contract definitions (basic schema with the Quality of Service parameters), SLA monitoring, and SLA enforcement according to defined policies. In the context of secure configuration, the SLAs will need to provide ample visibility in order to ensure compliance with secure configuration management mandates as defined in NIST SP 800-53.

Commented [KS22]: Not a sentence, not sure what this means.

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

4.2.1.3 SECURE PORTABILITY AND INTEROPERABILITY

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

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

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

4.2.1.4 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 Consumer, the Security Components mapped to the Secure Organizational Support Architectural Sub-Component include (but are not limited to): Compliance Management; Audit Management under Governance Risk & Compliance; Technical Security Standards; Best Practice & Regulatory Correlation; and Information Security Policies under Policies and Standards.

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

4.2.2 SECURE CLOUD ECOSYSTEM ORCHESTRATION

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

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

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

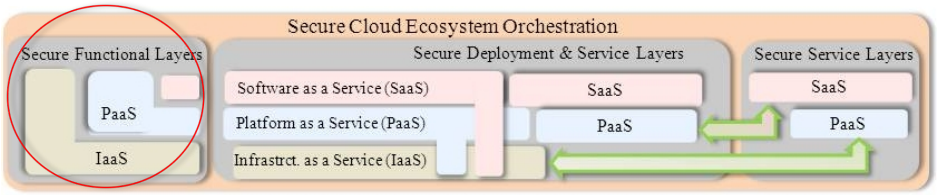


Figure 16: Secure Cloud Ecosystem Orchestration

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

4.2.2.1 SECURE FUNCTIONAL LAYER

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

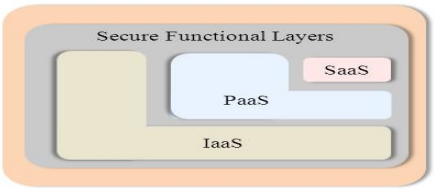


Figure 17: Secure Functional Layers

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

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

Commented [KS23]: Wording. Maybe it should be "limited or no access"?

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

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

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

4.3 PROVIDER – ARCHITECTURAL COMPONENTS

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

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

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

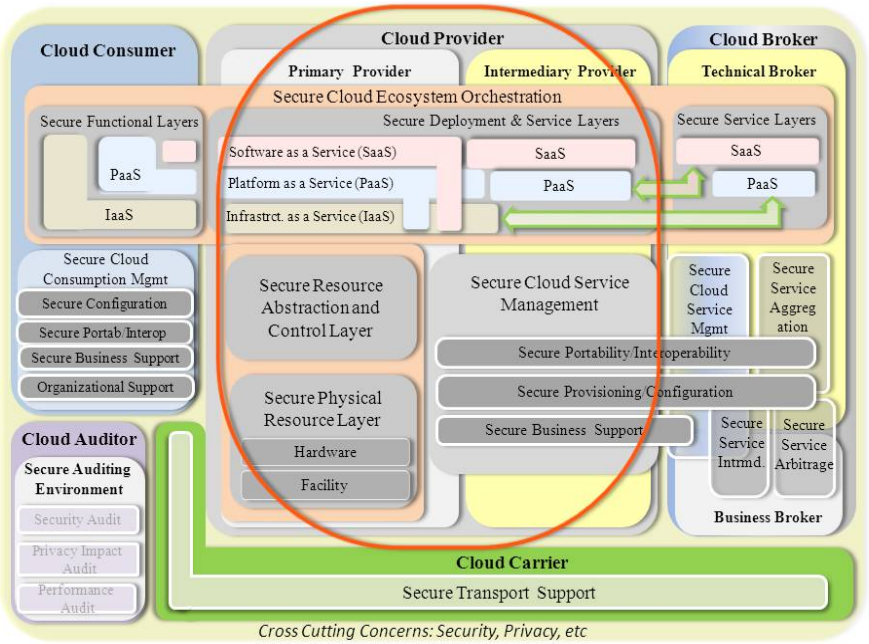


Figure 18: SRA – Cloud Provider

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

4.3.1 SECURE CLOUD ECOSYSTEM ORCHESTRATION

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

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

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

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

Commented [KS24]: There is a wording issue here (too many instances of "Provider"). Not sure what the desired wording is.

Commented [KS25]: The figure uses a different name than the one in italics here. It sounds like they should be the same.

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

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

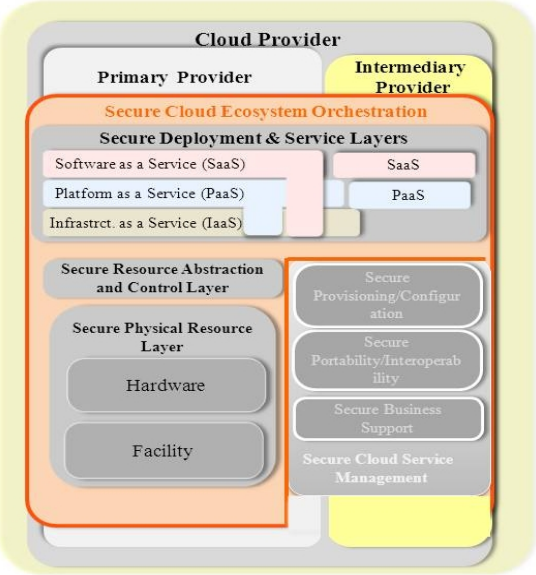


Figure 19: Secure Service Orchestration – Stack Diagram

4.3.1.1 SECURE DEPLOYMENT AND SERVICE LAYER

Figure 20 depicts the Secure Deployment and Service Layers. The set of Security Components a Provider can implement to secure the Service Layer depends upon the particular type of cloud service offered (i.e., SaaS, PaaS, or IaaS) and the cloud deployment model (e.g., Public, Private). For each of the twelve instances of cloud Ecosystems, the set of Security Components a Provider is responsible for implementing is intrinsically correlated with the sets of Security Components implemented by the other Actors involved in the cloud Ecosystem.

Figure 20: Secure Deployment and Service Layers

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

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

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

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

Commented [KS26]: I was expecting this to be called the Secure Deployment and Service Layer Architectural Component.

4.3.1.2 SECURE RESOURCE ABSTRACTION AND CONTROL LAYER

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

Commented [KS27]: wording

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

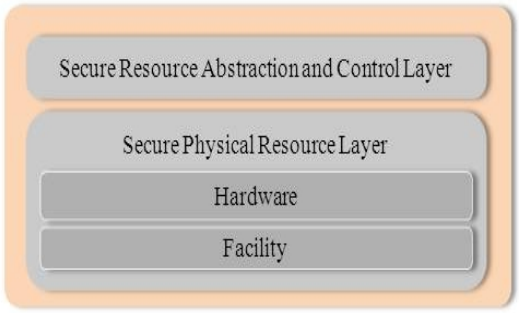


Figure 21: Secure Resource Abstraction and Control Layer and Secure Physical Resource Layer

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

Applying the RMF4CE on behalf of a USG Consumer and providing continuous monitoring is a responsibility shared among all Actors involved in the cloud Ecosystem. Providers should implement well-structured, cost-effective automation processes for continuous monitoring of security controls to ensure their effectiveness and to provide near-real-time measurements of security parameters in

support of a risk-based decision process with regards to the organizational information systems operating in a cloud Ecosystem. As discussed earlier in **Sec. 4.2.1**, one possible solution that can support the continuous monitoring process and that would ensure proper security mechanisms are in place is the adoption of standards such as SCAP.

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

4.3.1.3 SECURE PHYSICAL RESOURCE LAYER

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

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

4.3.2 SECURE CLOUD SERVICE MANAGEMENT

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

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

Figure 22 below expands upon the NIST RA diagram shown in **Fig. 13**. It identifies the *Secure Cloud Service 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 Providers, secure cloud service management is offered by both Primary and Intermediary Providers.

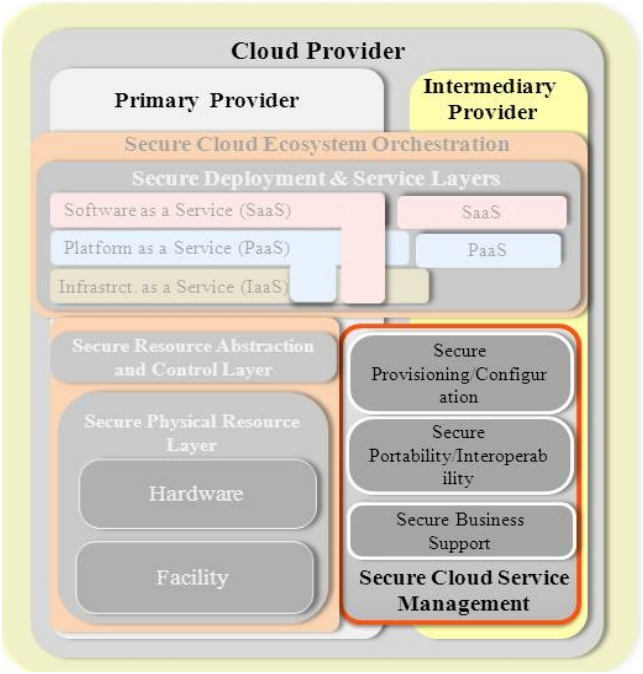


Figure 22: Secure Cloud Service Management – Stack Diagram

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

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

4.3.2.1 SECURE PROVISIONING AND CONFIGURATION

The *Secure Provisioning and Configuration* Architectural Sub-Component includes all Security Components (such as capabilities, tools, and 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 Consumer and Provider in SLAs.

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

- *Rapid provisioning:* Automatically deploying, in a secure manner, cloud systems based on the requested service, resources, or capabilities. Since availability of services is intrinsically correlated with the secure, rapid provisioning of cloud capability based on varying needs and demand levels, measures need to be taken to ensure that the deployment mechanisms and availability of new resources and capability are not subject to denial of service (DoS) attacks.[8]
- *Resource changing:* Adjusting configuration/resource assignment for repairs, upgrades, and joining new nodes into the cloud based on new and updated security configuration policies and requirements.
- *Monitoring and Reporting:* Discovering and monitoring virtual resources, monitoring cloud operations and events, and generating security reports that include abnormal performance measures. Reporting should provide enough visibility – preferably in an automated way – to support the Consumer's continuous monitoring requirements.
- *Metering:* Providing a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, active user accounts). The metering capability needs to be protected from tampering. Sufficient evidence of these protections will support Consumers in their efforts to meet monitoring requirements and mandates.
- *SLA management:* Encompassing the SLA contract definition (basic schema with the Quality of Service parameters), SLA monitoring, and SLA enforcement according to defined security policies.

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

4.3.2.2 SECURE PORTABILITY AND INTEROPERABILITY

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

- Direct DOS – the attacking target is determined, and the availability of the targeted cloud service is fully lost due to the attack.
- Indirect DOS – the attack is twofold: 1) all services hosted in the same physical machine with the target victim will be affected; and 2) the attack is initiated without a specific target.

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

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

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

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

4.3.2.3 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 client-facing business operations that support the Provider's role of enabling business support to Consumers, Brokers, and other Providers involved in the orchestration of the cloud Ecosystem in a secure manner.

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

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

- *Customer management*: Manage customer accounts, open/close/terminate accounts, manage user profiles, and manage customer relationships by providing points-of-contact and resolving customer issues based upon security policies of the Consumer.
- *Contract Management:* Manage service contracts, including setup, negotiation, and close/termination, to include supplying information that supports the Consumer's security auditing and reporting requirements.

- *Inventory Management:* Set up and manage service catalogs, etc. in a secure manner.
- *Accounting and Billing:* Manage customer billing information, send billing statements, process received payments, and track invoices to ensure that any fraudulent activities are identified, tracked, and corrected efficiently.
- *Reporting and Auditing:* Monitor end users' operations, and generate reports to support the Consumer's security auditing and monitoring requirements.
- *Pricing and Rating:* Evaluate cloud services and determine prices, handle promotions and pricing rules based on an end user's profile without violating Consumer protections as afforded to them by the law.

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

4.4 BROKER – ARCHITECTURAL COMPONENTS

Section 2.4.5 clarifies the role of the Broker defined in NIST SP 500-292: *NIST Cloud Computing Reference Architecture*. The Broker is defined as an entity that manages the use, performance, and delivery of cloud services, and negotiates relationships between Providers and Consumers.

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

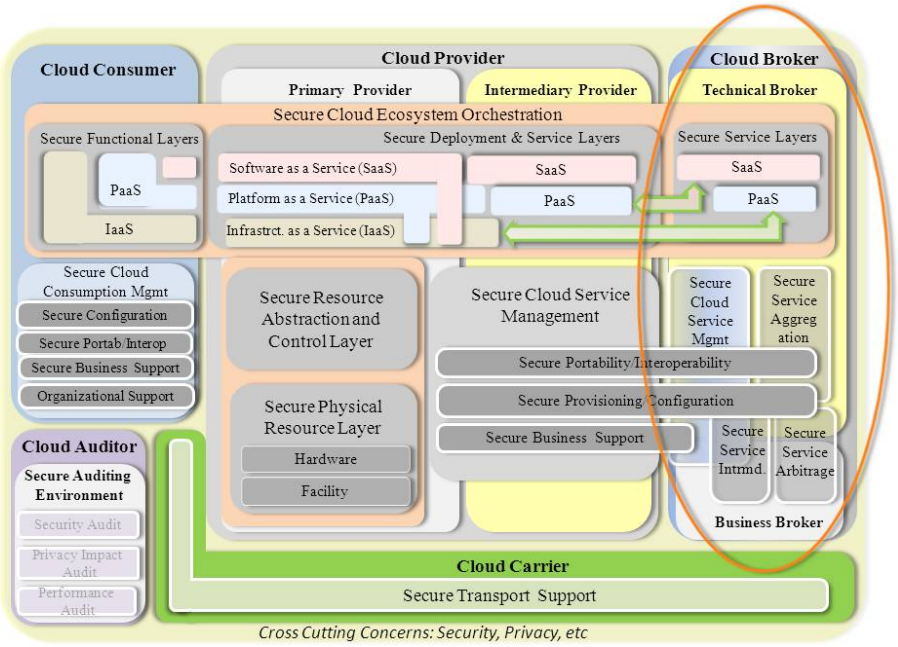


Figure 23: SRA – Cloud Broker

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

- *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 Broker provides data integration and ensures the secure movement of data between the Consumer and multiple Providers based upon the security policies of the Consumer. Secure Service Aggregation can be described from the perspective of the:
  - portability and interoperability technical requirements
  - 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 Broker has the flexibility to choose services from multiple Providers. The

Broker can, for example, use a credit-scoring service to measure and select a 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 Broker to improve some specific capability and offer value-added services to Consumers, while ensuring the security policies of the Consumer are maintained. The improvement can be managing access to cloud services, identity management, performance reporting, enhanced security, etc.
- *Secure Cloud Service Management:* This Architectural Component includes all Security Components that support the management of all service-related functions (technical and business) that are necessary for the operations of the services offered by the Broker. Secure Cloud Service Management can be described from the perspective of the:
  - business support requirements
  - provisioning and configuration business requirements
  - portability and interoperability business requirements
- *Secure Cloud Ecosystem Orchestration*: This Architectural Component includes all Security Components that a Technical Broker needs to implement to secure the functionality implemented and the additional services offered based upon the cloud deployment model (e.g., Private, Public) and service model (SaaS, PaaS, or IaaS).

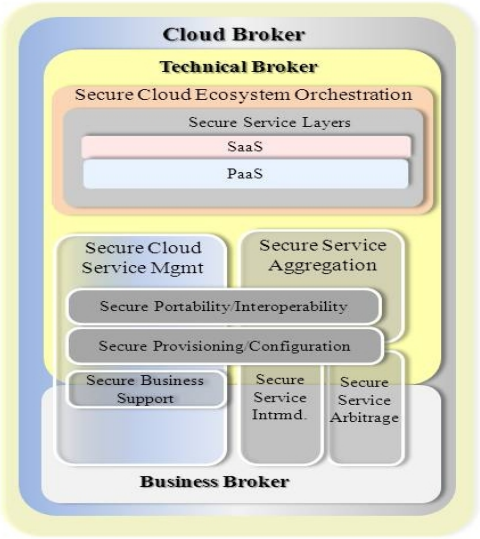


Figure 24: Cloud Broker – Architectural Components

Commented [KS28]: This graphic is not referenced until a few pages later. It is nearly identical to Figure 25 (just color/emphasis differ) so I don't think moving it makes sense. So I'd recommend either adding a reference here or deleting the figure.

The set of Security Components a Technical Broker could implement to protect the Consumer's data migrated to the cloud is, in practice, identical to the set of Security Components an Intermediary

Provider that offers homologous services should implement. Additional information on how to extract the Technical Broker's set of Security Components is detailed in **Sec. 4.4.1**.

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

4.4.1 TECHNICAL BROKER

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

As emphasized earlier in **Sec. 2.4.5.1**, a Technical Broker interacts with the Consumer's operational processes, cloud artifacts, and/or cloud data by aggregating services from multiple Providers and adding a layer of technical functionality by addressing single-point-of-entry and interoperability issues. In the SRA formal model, the Architectural Components for the Broker in general and for the Technical Broker in particular are designed in such a way as to emphasize all major roles the Actor has. For example, the Secure Portability/Interoperability Architectural Sub-Component extends over Secure Service Management and Secure Service Aggregation (see **Fig. 24**) to indicate that for a Broker there are two aspects of this activity: a business/management aspect under Secure Service Management and a technical aspect under Secure Service Aggregation. Since an Intermediary Provider does not aggregate services, but rather embeds services offered by a Primary Provider, the business and technical aspects of the activity cannot be separately identified. However, the overall set of Security Components that secure homologous services provided by a Technical Broker or an Intermediary Provider are the same.

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

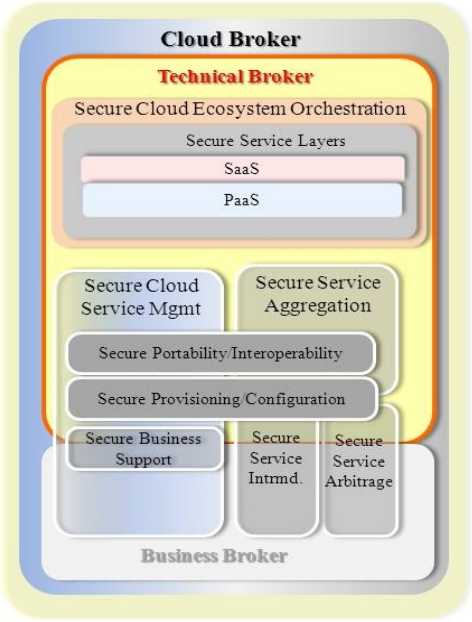


Figure 25: Technical Broker – Architectural Components

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

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

4.4.2 BUSINESS BROKER

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

Figure 26 depicts the Business Broker role in providing security services within the SRA.

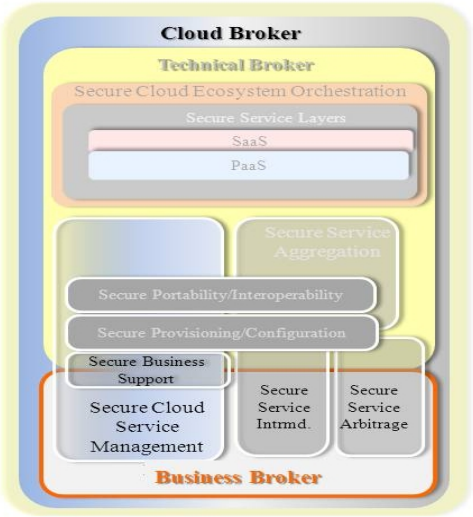


Figure 26: Business Broker – Architectural Components

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

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

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

4.4.3 SECURE CLOUD ECOSYSTEM ORCHESTRATION

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

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

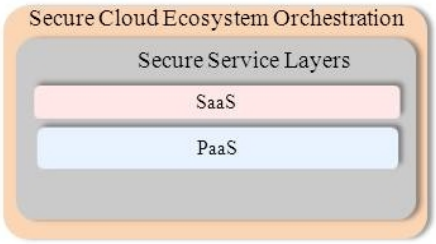


Figure 27: Secure Cloud Ecosystem Orchestration – Broker Stack Diagram

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

4.4.3.1 SECURE SERVICE LAYERS

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

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

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

software, SDKs, or deployment and management tools. The Broker could also offer tools and processes that secure such aggregation.

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

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

4.4.4 SECURE SERVICE AGGREGATION

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

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

Commented [KS29]: Should "to" be "from"?

The set of Security Components covered by the Broker's Secure Service Aggregation Architectural Component is similar to the set of components an Intermediary Provider offering similar services would need to implement (see **Sec. 4.3**). The technical differences consist of the transparency offered by the 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 Consumers and multiple aggregated Providers, should offer security services in both directions of the functional stack – upwards towards Consumers and downwards towards the underlying Providers. Correspondingly, all reports and plans should consider the Broker to Consumer interface and the Broker to Provider(s) interface.

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

- Secure Provisioning and Configuration
- Secure Portability and Interoperability

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

Annex E provides the high-level SRA Security Components mapped to the Architectural Components of a Provider. The Secure Service Aggregation Architectural Component is basically

comprised of the sum of the Secure Provisioning and Configuration ("aC") mapping and Secure Portability and Interoperability ("aI") under the "Broker" section of the table.

4.4.5 SECURE CLOUD SERVICE MANAGEMENT

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

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

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

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

Figure 28: Secure Cloud Service Management – Broker Stack Diagram

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

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

4.4.5.1 SECURE PORTABILITY AND INTEROPERABILITY

The *Secure Portability and Interoperability* Architectural Sub-Component for Brokers ensures that data and applications can be moved securely between multiple cloud Ecosystems as required by the Consumer. Brokers should keep system maintenance time and disruptions (i.e., downtime) at an acceptable minimum level defined in the SLAs. They should also offer Consumers a mechanism to interoperate their data and applications among multiple cloud Ecosystems through a secure and unified management interface. Requirements for secure portability and interoperability vary based on the cloud service model adopted.

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

4.4.5.2 SECURE PROVISIONING AND CONFIGURATION

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

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

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

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

4.4.5.3 SECURE BUSINESS SUPPORT

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

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

Some of the Brokers' business support responsibilities are:

- *Customer Management*: Manage customer accounts, open/close/terminate accounts, manage user profiles, and manage customer relationships by providing points-of-contact and resolving customer issues and problems, etc. in accordance with the Consumer's security requirements.
- *Contract Management:* Manage service contracts, and setup/negotiate/close/terminate contracts, 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 are authorized with the appropriate tools and processes to protect from fraudulent activities.
- *Reporting and Auditing:* Monitor users' operations; generate reports, etc. in accordance with security audit and reporting requirements of the Consumer.
- *Pricing and Rating:* Evaluate cloud services and determine prices, handle promotions and pricing rules based on a user's profile, etc. while protecting Consumer privacy.

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

4.4.6 SECURE SERVICE INTERMEDIATION

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

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

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

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

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

4.4.7 SECURE SERVICE ARBITRAGE

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

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

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

4.5 CARRIER – ARCHITECTURAL COMPONENTS

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

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

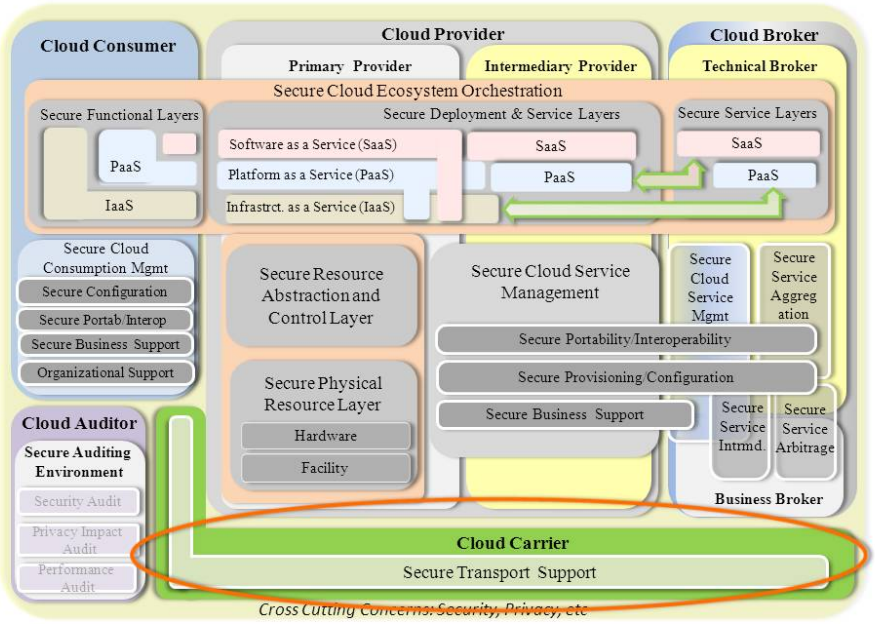


Figure 29: SRA – Cloud Carrier

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

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

4.6 AUDITOR – ARCHITECTURAL COMPONENTS

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

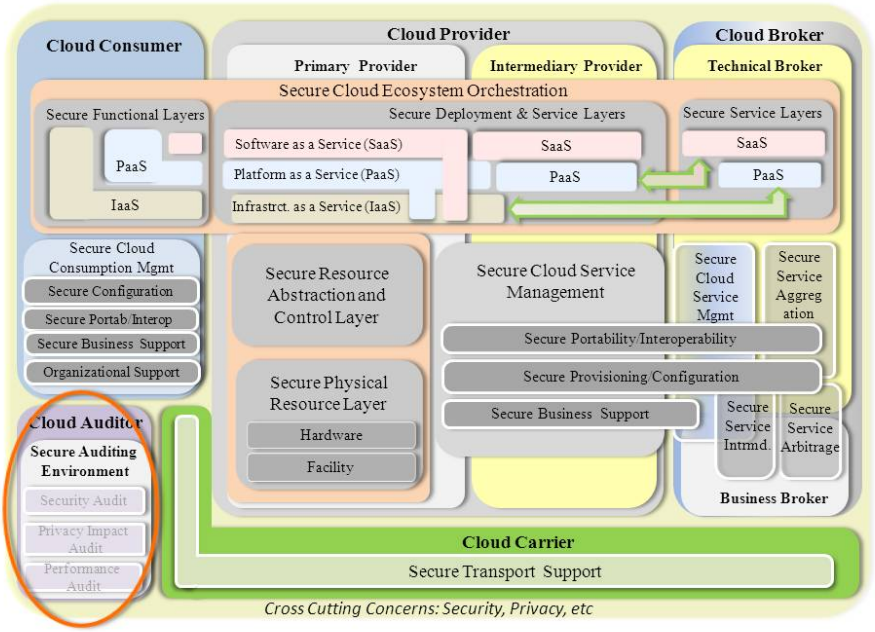


Figure 30: SRA – Cloud Auditor

Auditors can perform a large variety of audits for any of the other Actors. The 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 Auditor are typically independent of the type of cloud service model and/or Actor audited.

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

- *Security Components and related security controls*: Information about the Security Components and the relevant security controls in place must be available to the Auditors.
- *Secure Archival*: In support of audit findings for legal and business processes, such as eDiscovery, archival requirements and implementations are available to the Auditors.
- *Secure Storage*: Objective evidence from responsible parties can be collected and stored in the cloud in a secure fashion for future reference, and thus encryption and obfuscation storage information can be made available to the Auditors.
- *Data Location*: During the assessment process, Auditors may be required to ensure that the relevant jurisdictional rules can be applied to the data and as such, data location information should be made available.
- *Metering*: Performance audits will require information from the metering systems in place, and secure access to this information must be made available to the Auditors.

- *SLAs*: Service audits will require access to all agreements in place between the parties requiring the audit and the parties being audited, as well as any mechanisms that support the implementations of the SLAs in a secure manner.
- *Privacy*: Privacy Impact Assessments require the availability of system security and configuration information as well as any mechanisms implemented to protect data in the cloud Ecosystem.

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

5 SRA: A METHODOLOGY FOR ORCHESTRATING A SECURE CLOUD ECOSYSTEM

5.1 ORCHESTRATION METHODOLOGY OVERVIEW

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

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

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

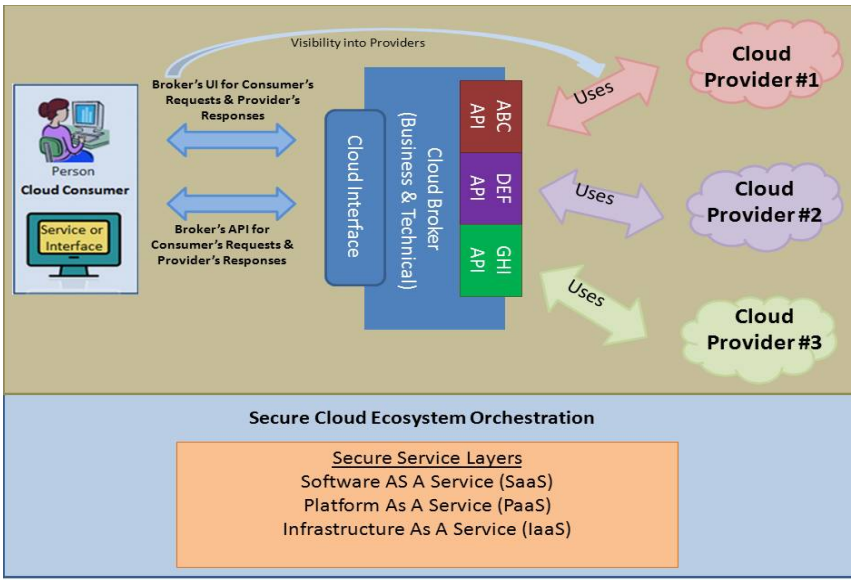


Figure 31: Secure Cloud Ecosystem Orchestration – Actors Interactions

5.2 CLOUD ECOSYSTEM ORCHESTRATION USE CASE

To better illustrate the interactions among Actors and their roles and responsibilities in orchestrating a secure cloud Ecosystem, this publication includes a use case of a USG agency service selected for migration to the cloud. The details in this use case are provided for purposes of illustration only; those in actual implementations will vary. The use case follows all the necessary steps to orchestrate a secure cloud Ecosystem, and it identifies the security requirements and the Security Components that need to be implemented to secure the Ecosystem prior to adding important data and functionality. The approach presented in this section leverages the data aggregated for the SRA. This example follows the RMF4CE steps introduced in **Sec. 2.3.1**.

The use case illustrates, from the Consumer's perspective, the approach of applying the RMF4CE steps when tasked with migrating a service or an in-house application to the cloud Ecosystem. The scope of this exercise is to exemplify the process of securely orchestrating, in collaboration with the other Actors, a cloud Ecosystem for the migration of the Consumer's Unified Messaging Service (UMS) to the cloud. This section provides more details for Step 1, 2 and 3, highlighting how to leverage the information provided in this document to complete Step 2. The rest of the steps are reviewed at a high level, with pointers to additional NIST work, when available. The RMF4CE steps are summarized below:

- **Step 1: Categorize** the information system and the information it processes, stores, and transmits. Identify operational, performance, security, and privacy requirements.
- **Step 2: Select** and tailor the security and privacy controls, select the cloud architecture, evaluate cloud Providers, select one or more Providers, and negotiate agreements with the Providers.
- **Step 3: Implement** the security and privacy controls for which the Consumer is responsible.
- **Step 4: Assess** the Provider's implementation of the tailored security and privacy controls.
- **Step 5: Authorize** the cloud-based information system to operate.
- **Step 6: Monitor** the system's operations for both Provider and Consumer security and privacy controls. Assess the system's security posture. Reassess and reauthorize each Provider's service.

5.2.1 STEP 1 – CATEGORIZE – CLOUD CONSUMER'S SERVICE DESCRIPTION

Step 1, Categorize, has two components: categorize the system and its information, and identify operational, performance, security, and privacy requirements.

5.2.1.1 CATEGORIZE THE SYSTEM AND ITS INFORMATION

The Consumer aims to reduce the cost of IT services support by implementing a cloud-based UMS. This service includes e-mail, calendar, synchronization with wireless mobile devices, and collaboration services. The current e-mail system is classified as a Moderate impact system based on FIPS 199 [16].

In-House Messaging Service Capabilities

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

Commented [KS30]: The versions specified are quite old. Not sure that the version numbers even need to be supplied. Recommend dropping them (saying Outlook instead of Outlook 2007, for instance).

Cloud-Based UMS Functional Requirements:

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

The UMS solution must include instant messaging and web conferencing. It must also provide users with the ability to share and collaborate on documents with both internal users and authenticated

external users through a document repository. All aspects of the UMS must be accessible through a single unified User Interface (UI) portal.

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

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

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

5.2.1.2 IDENTIFY REQUIREMENTS

After identifying all functional requirements for the system migrated to the cloud, the Consumer may leverage the SRA to perform a risk assessment and identify the Security Components that should be implemented to secure the UMS; prioritize them by performing a C/I/A analysis; and select the necessary security controls that best suits its needs for the UMS.

5.2.2 STEP 2 – SELECT – CLOUD CONSUMER'S SERVICE DESCRIPTION

Step 2, Select, has several components, including selecting and tailoring the security and privacy controls, selecting the cloud architecture, evaluating cloud Providers, selecting one or more Providers, and negotiating agreements with the Providers. The subsections below highlight key aspects of these components.

5.2.2.1 THE SECURITY INDEX SYSTEM

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

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

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

Table 5: Security Indexes System

Security Index Symbol	Security Index Value	Security Index Applicability
SI0	0	SI0 should be applied to a Security Component if the loss of a Confidentiality, Integrity, or Availability property associated with the Component is expected to have **no** adverse effects on the cloud Ecosystem's security posture.
SI1	1	SI1 should be applied to a Security Component if the loss of a Confidentiality, Integrity, or Availability property associated with the Component is expected to have **limited*** adverse effects on the cloud Ecosystem's security posture.
SI2	2	SI2 should be applied to a Security Component if the loss of a Confidentiality, Integrity, or Availability property associated with the Component is expected to have **serious**** adverse effects on the cloud Ecosystem's security posture.
SI3	3	SI3 should be applied to a Security Component if the loss of a Confidentiality, Integrity, or Availability property associated with the Component is expected to have **severe***** adverse effects on the cloud Ecosystem's security posture.
SI4	4	SI4 should be applied to a Security Component if the loss of a Confidentiality, Integrity, or Availability property associated with the Component is expected to have **critical****** adverse effects on the cloud Ecosystem's security posture.

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

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

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

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

**** A **critical** adverse effect means that the loss of a C/I/A property might: (i) generate vulnerabilities in system architecture/design or sabotage or subversion of a system's security functions or critical Security Components, as defined in NIST SP 800-53; (ii) cause a catastrophic loss of mission capability to such an extent and duration that the organization is not able to recover one or more of its system security functions; (iii) result in irrecoverable failure to organizational, critical infrastructure, or jeopardized national security assets; (iv) result in total financial loss; or (v) result in catastrophic harm to individuals exceeding mission expectations.

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

5.2.2.2 SECURITY CONTROLS OVERVIEW

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

Commented [KS31]: Comma?

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

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

5.2.2.3 SELECT THE CLOUD ECOSYSTEM ARCHITECTURE

The information aggregated so far aids the Consumer in selecting the cloud Ecosystem composition that best matches its internal expertise and required assurance levels. In this use case example, the Consumer selects for the implementation of the cloud-based UMS a Public SaaS cloud. Such a model will allow the Consumer to create, destroy, archive, and terminate individual user accounts automatically for its employees, without consuming resources for the underlying cloud infrastructure or individual application capabilities beyond selecting the application that meets its mission-critical

requirements, and negotiating, when necessary, the additional security controls that need to be implemented by the Broker or Provider to support the necessary security posture for the UMS.

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

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

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

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

Commented [KS32]: wording

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

An overall list of all categorizations and aspects of the secure cloud Ecosystem Orchestration use case is provided in **Annex F**.

5.2.2.4 SLA NEGOTIATION

The sets of security controls are translated into service requirements as part of the SLA negotiation process. With the sets of security controls identified for each of the Security Components for each Actor, and with the ASIS transitively inherited by the security controls from the Security Components, the Consumer may proceed with the SA and SLA negotiation processes.

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

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

- the steps followed above for applying the RMF4CE (left side of the diagram)
- the FedRAMP A&A process (right side of the diagram)

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

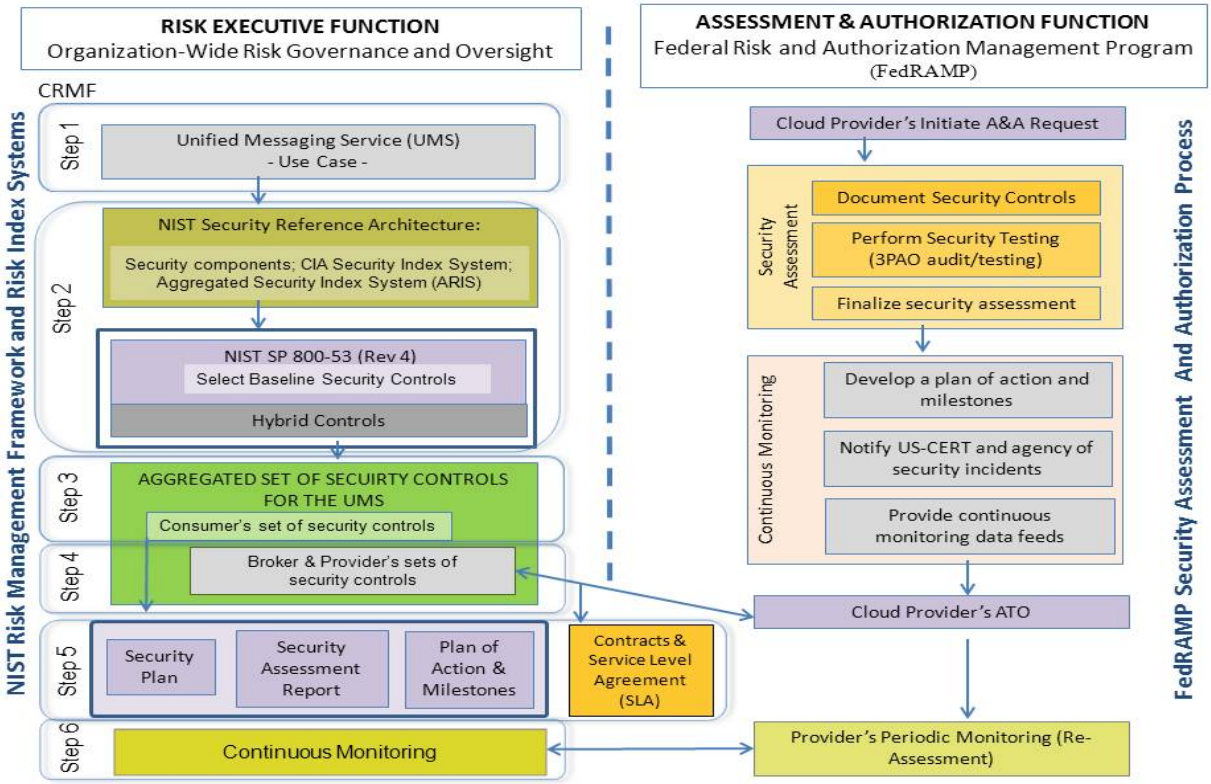


Figure 32 a): NIST Risk Management Framework and the FedRAMP A&A Process

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

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

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

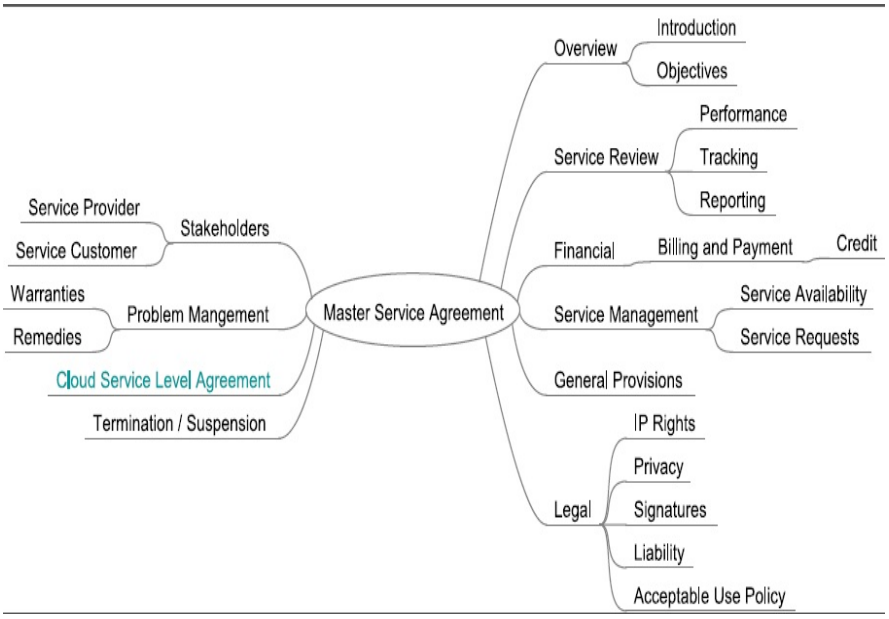


Figure 33: Service Agreement Mind Map

A further challenge in comparing and selecting service offerings is that Providers may offer a default contract written from the Provider's perspective. Such default contracts may not adequately meet the

Consumer's needs and may constrain the visibility of the Consumer into the delivery mechanisms of the service. The thorough risk analysis coupled with secure cloud Ecosystem orchestration introduced in this document, along with adequate guidance on negotiating SLAs, are intended to assist the Consumer in managing risk and making informed decisions for adopting cloud services.

5.2.3 STEP 3 – IMPLEMENT CONTROLS

*** TBD ***

5.2.4 STEP 4 – ASSESS CONTROLS

*** TBD ***

5.2.5 STEP 5 – AUTHORIZE CLOUD SERVICES

*** TBD ***

Metrics are needed to assess whether the expectations defined in the customer-based SLA have been met. These metrics define the measures to be used (e.g., availability) and the range of acceptable results for a particular measurement (e.g., 99.5%). These metrics are a critical piece of the SLA since they are one of the artifacts the Consumer can use to monitor the cloud service and to ensure the Provider can be held accountable to the contractual terms. A set of well-defined and organized metrics for SLAs can also help Consumers have a more consistent way to compare, manage, and negotiate cloud services with multiple Providers.[9]

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

5.2.6 STEP 6 – MONITOR CLOUD SERVICES

NIST SP 800-37 describes an effective operational continuous monitoring program as one that includes:

---

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

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

The continuous monitoring required by NIST SP 800-37 for all information systems refers to the auditing and continuous monitoring requirements from the operational perspective, and not to FedRAMP's ongoing A&A, which is also referred to as continuous monitoring in FedRAMP's *Concept of Operations* (CONOPS)[10] document. However, FedRAMP does work in coordination with the Department of Homeland Security (DHS) to establish a framework for continuous monitoring, FISMA reporting, incident response, and remediation.

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

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

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

6 GLOSSARY AND ACRONYMS

3PAO:	**6.1.1.1** Third-Party Independent Assessor
A&A:	Assessment and Authorization
6.1.1.2 API:	**6.1.1.3** Application Programming Interface
ASIS:	Aggregated Security Index System
Assessment:	In this context, the process by which a third party assessment organization generates a security assessment package for review.
6.1.1.4 ATO:	**6.1.1.5** Authorization-To-Operate
Authorization:	In this context, the process by which the FedRAMP Joint Authorization Board (JAB) reviews the security assessment package based on a prioritized approach and decides on a grant of provisional authorization. See http://www.gsa.gov/portal/category/102371 for more information.
6.1.1.6 BC:	**6.1.1.7** Business Continuity
BOSS:	Business Operation Support Service
Business Broker:	A Broker that only provides business and relationship services, and does not have any contact with the Consumer's data, operations, or artifacts (e.g., images, volumes, firewalls) in the cloud.
C&A:	Certification and Accreditation – terminology replaced by "Assessment and Authorization" (A&A).
C/I/A:	Confidentiality, Integrity, Availability
CA:	Certificate Authority

Commented [KS34]: This URL told me to visit fedramp.gov instead.

Chain of Custody:	The seizure, custody, control, transfer, analysis, and disposition of physical or electronic evidence.
6.1.1.8 CIO:	**6.1.1.9** Chief Information Officer
Cloud Auditor:	A party that can conduct an independent assessment of cloud services, with the intent to express an opinion thereon. An Auditor can evaluate the services provided by a Provider in terms of security controls, privacy impact, performance, etc. Audits can be used to verify conformance to standards (set forth in mandates, the service contract, industry best practices, or other sources) through review of objective evidence.
Cloud Broker:	**6.1.1.10** An entity that manages the use, performance, and delivery of cloud services, and negotiates relationships between Providers and Consumers. *See also* Business Broker *and* Technical Broker.
Cloud Carrier:	**6.1.1.11** An entity that acts as an intermediary providing connectivity and transport of cloud services between Consumers and Providers through network, telecommunications, and other access devices.
Cloud Consumer:	An organization that uses, or consumes, cloud services. Consumers are ultimately responsible for ensuring the security and compliance of the cloud services they use.
Cloud Provider:	An entity that provides cloud computing services. Providers may offer their services directly to Consumers or do so through a third party, such as an Intermediary Provider or Broker. *See also* Broker, Intermediary Provider, *and* Primary Provider.
6.1.1.12 CMDB:	**6.1.1.13** Configuration Management Database
6.1.1.14 CNSSI:	**6.1.1.15** Committee for National Security Systems Instruction

Community Cloud:		**6.1.1.16**	A cloud infrastructure that is provisioned for exclusive use by a specific community of Consumers that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
6.1.1.17	CONOPS:	**6.1.1.18**	Concept of Operations
CPE:		Customer Premises Equipment	
6.1.1.19	CPU:	**6.1.1.20**	Central Processing Unit
CSA:		**6.1.1.21**	Cloud Security Alliance
6.1.1.22	DBMS:	**6.1.1.23**	Database Management System
6.1.1.24	DHS:	**6.1.1.25**	Department of Homeland Security
6.1.1.26	DLP:	**6.1.1.27**	Data Loss Prevention
DoS *or* DDoS:		Denial of Service or Distributed Denial of Service attack. This type of attack can jeopardize the cloud service by saturating the limited network bandwidth and interrupting the configuration/routing information. It can also cause the computing platform to slow down responses to legitimate requests because it is overloaded with non-legitimate traffic.	
6.1.1.28	DPI:	**6.1.1.29**	Deep Packet Inspection
6.1.1.30	DR:	**6.1.1.31**	Disaster Recovery
6.1.1.32	DRP:	**6.1.1.33**	Disaster Recovery Plan

6.1.1.34	FAQ:	Frequently Asked Questions	
FedRAMP:		**6.1.1.35**	Federal Risk and Authorization Management Program – see http://www.gsa.gov/portal/category/102371 for more information.
FIPS:		Federal Information Processing Standard – see http://www.nist.gov/itl/fips.cfm for more information.	
FISMA:		Federal Information Security Modernization Act – see http://www.nist.gov/itl/csd/sma/fisma.cfm for more information.	
6.1.1.36	GAO:	**6.1.1.37**	Government Accounting Office
6.1.1.38	GRC:	**6.1.1.39**	Governance, Risk Management, and Compliance
GSA:		General Services Administration – see http://www.gsa.gov for more information.	
HIDS:		**6.1.1.40**	Host Intrusion Detection System
6.1.1.41	HIPS:	**6.1.1.42**	Host Intrusion Prevention System
6.1.1.43	HVAC:	**6.1.1.44**	Heating, Ventilation, and Air Conditioning
Hypervisor:		One of many hardware virtualization techniques allowing multiple operating systems to run concurrently on a host computer. *See also* Virtual Machine Manager (VMM).	

Commented [KS35]: This URL needs to be updated.

Commented [KS36]: Looks like this URL is no longer valid. I found http://csrc.nist.gov/groups/SMA/fisma/ but it references the original FISMA act, and not the 2014 version. Should we just point to the new act? Maybe http://www.dhs.gov/fisma?

IaaS:		Infrastructure as a Service. In an IaaS deployment, the capability provided to the Consumer is to provision processing, storage, networks, and other fundamental computing resources where the Consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The Consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications, and possibly limited control of select networking components (e.g., host firewalls).	
6.1.1.45	ICAM:	**6.1.1.46**	Identity and Credentials Management
6.1.1.47	ICR:	**6.1.1.48**	Intelligent Character Recognition
6.1.1.49	IDE:	**6.1.1.50**	Integrated Development Environment
6.1.1.51	IDM:	**6.1.1.52**	Identity Management
Intermediary Cloud Provider:		**6.1.1.53**	The entity or service vendor that has the capability to interact with other Providers without offering visibility or transparency into the Primary Provider(s). An Intermediary Provider uses services offered by a Primary Provider as invisible components of its own service, which it presents to the Customer as an integrated offering.
6.1.1.54	IP:	**6.1.1.55**	Intermediary Provider
6.1.1.56	IP:	Intellectual Property	
6.1.1.57	IT:	**6.1.1.58**	Information Technology
6.1.1.59	ITL:	**6.1.1.60**	Information Technology Laboratory
ITOS:		Information Technology Operation and Support	
6.1.1.61	IVR:	Interactive Voice Response	

6.1.1.62	JAB:	**6.1.1.63**	Joint Authorization Board
6.1.1.64	LDAP:	**6.1.1.65**	Lightweight Directory Access Protocol
6.1.1.66	MID:	**6.1.1.67**	Mobile Internet Device
Multi-Tenancy:		The concept of Consumers sharing both virtualized infrastructure and application servers. In multi-tenant cloud architectures, database and application servers are typically shared to reduce the cost to Consumers, but with sharing resources and co-location of data come risks to data that must be mitigated.	
NCC-SRA:		NIST Cloud Computing Security Reference Architecture	
6.1.1.68	NCC SWG:	**6.1.1.69**	NIST Cloud Computing Security Working Group
NIDS:		**6.1.1.70**	Network Intrusion Detection System
6.1.1.71	NIPS:	**6.1.1.72**	Network Intrusion Prevention System
6.1.1.73	NIST:	**6.1.1.74**	National Institute of Standards and Technology
6.1.1.75	NSTIC:	**6.1.1.76**	National Strategy for Trusted Identities in Cyberspace
OLA:		**6.1.1.77**	Operational Level Agreement
6.1.1.78	OMB:	**6.1.1.79**	Office of Management and Budget
6.1.1.80	OTB:	**6.1.1.81**	Out of the Box
6.1.1.82	OS:	**6.1.1.83**	Operating System
6.1.1.84	OTP:	**6.1.1.85**	One-Time Password

PaaS:			Platform as a Service. In a PaaS deployment, the capability provided to the Consumer is to deploy onto the cloud infrastructure consumer-created or applications created using programming capabilities, libraries, services, and tools supported by the Provider. The Consumer does not manage or control the underlying cloud infrastructure, including networks, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
6.1.1.86	PKI:	**6.1.1.87**	Public Key Infrastructure
6.1.1.88	PMO:	**6.1.1.89**	Program Management Office
PP:		**6.1.1.90**	Primary Provider
Primary Cloud Provider:		**6.1.1.91**	An entity that offers cloud services hosted on infrastructure that it owns. It may make these services available to Consumers through a third party (such as a Broker or Intermediary Provider), but the defining characteristic of a Primary Provider is that it does not source its service offerings from other Providers.
Private Cloud:		**6.1.1.92**	A cloud infrastructure that is provisioned for exclusive use by a single organization comprising multiple Consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
Public Cloud:		**6.1.1.93**	A cloud infrastructure that is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the Provider.
RA:		**6.1.1.94**	NIST Cloud Computing Reference Architecture, described in the document of the same name (NIST SP 500-292). The SRA builds upon the RA.

RMF:		**6.1.1.95**	NIST Risk Management Framework
6.1.1.96	RMF4CE:	**6.1.1.97**	Risk Management Framework for Cloud Ecosystems. This is defined in NIST SP 800-173.
6.1.1.98	RPO:	Recovery Point Objective	
6.1.1.99	RTO:	**6.1.1.100**	Recovery Time Objective
S&RM:		Security and Risk Management	
SA:		Service Agreement	
SaaS:		Software as a Service. In a SaaS deployment, the capability provided to the Consumer is to use the Provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The Consumer does not manage or control the underlying cloud infrastructure, including networks, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.	
6.1.1.101	SAML:	**6.1.1.102**	Security Assertion Markup Language
6.1.1.103	SAN:	**6.1.1.104**	Storage Area Network
6.1.1.105	SC:	**6.1.1.106**	Security Components
6.1.1.107	SCAP:	**6.1.1.108**	Security Content Automation Protocol
6.1.1.109	SDK:	**6.1.1.110**	Software Development Kit
6.1.1.111	SIEM:	**6.1.1.112**	Security Information and Event Management

SIS:		Security Index System	
SLA:		Service Level Agreement	
6.1.1.113	SOC:	**6.1.1.114**	Security Operations Center
6.1.1.115	SP:	**6.1.1.116**	Special Publication
6.1.1.117	SRA:	**6.1.1.118**	Security Reference Architecture
6.1.1.119	SSO:	**6.1.1.120**	Single Sign-On
6.1.1.121	TB:	**6.1.1.122**	Technical Broker
TCI-RA:		The Cloud Security Alliance's (CSA) Trusted Cloud Initiative Reference Architecture	
Technical Cloud Broker:		**6.1.1.123**	An entity that interacts with the Consumer's operational processes, cloud artifacts, and/or cloud data by aggregating services from multiple Providers and adding a layer of technical functionality by addressing single-point-of-entry, interoperability issues, or any other king of aggregation of services and cloud functionality.
6.1.1.124	TPM:	**6.1.1.125**	Trusted Platform Module
6.1.1.126	TVM:	**6.1.1.127**	Threat and Vulnerability Management
6.1.1.128	UI:	**6.1.1.129**	User Interface
6.1.1.130	UMS:	**6.1.1.131**	Unified Messaging System
6.1.1.132	USG:	United States Government	

Commented [KS37]: wording

6.1.1.133	VDI:	**6.1.1.134**	Virtual Desktop Infrastructure
6.1.1.135	VLAN:	**6.1.1.136**	Virtual Local Area Network
6.1.1.137	VM:	**6.1.1.138**	Virtual Machine
VMM:		Virtual Machine Manager. One of many hardware virtualization techniques allowing multiple operating systems to run concurrently on a host computer. *See also* Hypervisor.	
6.1.1.139	VNIC:	**6.1.1.140**	Virtual Network Interface Card
6.1.1.141	XACML:	**6.1.1.142**	Extensible Access Control Markup Language
6.1.1.143	XML:	**6.1.1.144**	Extensible Markup Language

7 REFERENCES

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

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

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

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

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

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

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

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

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

Commented [KS38]: I still need to do the following:
Reformat as a table.
Update the entries marked with comments once Michaela or Anil provides feedback.
Ensure every entry uses the same format.
Add entries for other documents referencesd in the publication.
Renumber all the references to be sequential in the document.

Commented [KS39]: This was revised in March 27, 2014. This old URL no longer works. New URL is long and messy, so I suggest changing it to https://www.cnss.gov/CNSS/issuances/Instructions.cfm I don't see a version number for 1253.

Does updating this necessitate any changes within the main body of the document?

Commented [KS40]: Update to FISMA of 2014? See earlier comment on FISMA and changing the URL being used.

Does updating this necessitate any changes within the main body of the document?

Commented [KS41]: http://www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf Version 2, released in July 2013. Author list is gone.

Does updating this necessitate any changes within the main body of the document?

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

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

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

[12] V. Kundra, *Federal cloud computing strategy*, The White House, U.S. Chief Information Officer, (2011). http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf

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

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

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

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

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

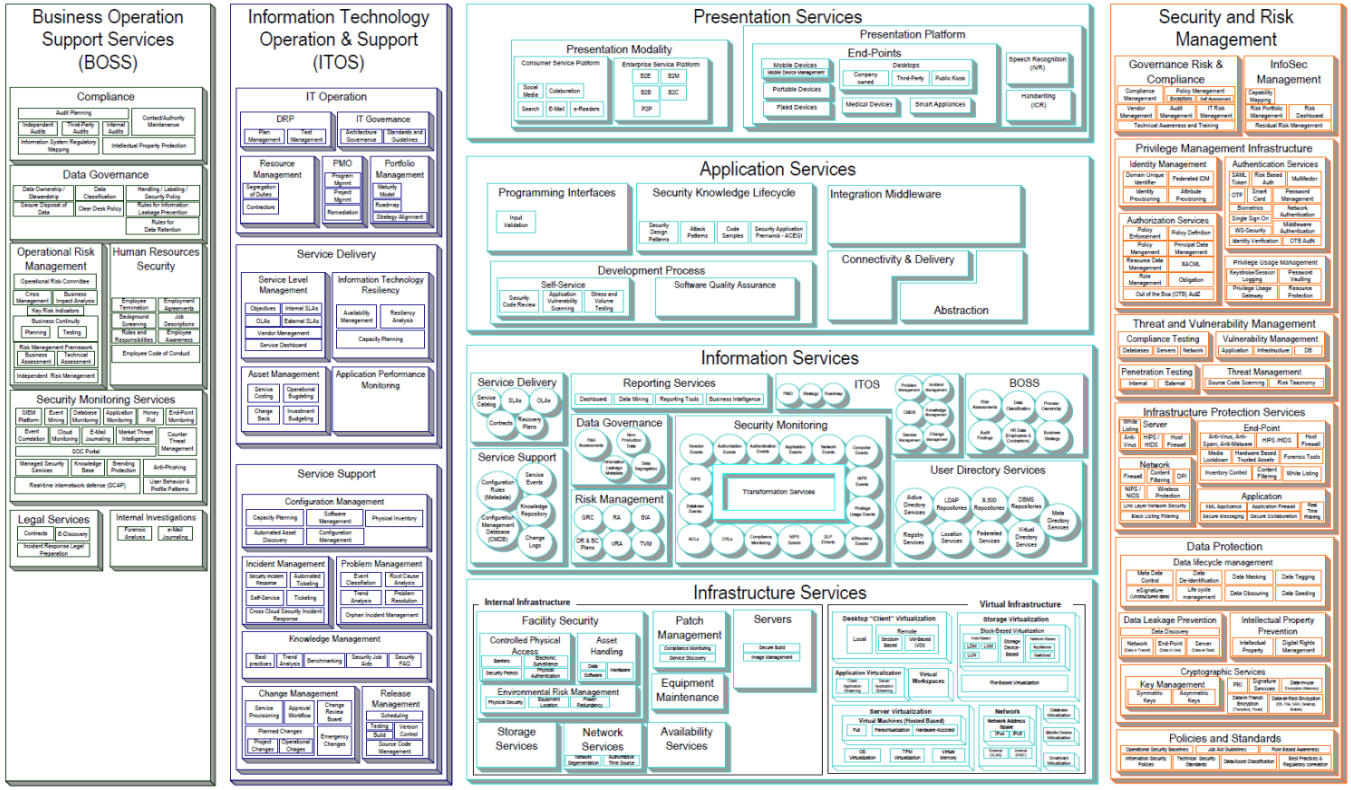
[18] U.S. Office of Management and Budget, *Securing agency information systems* (Circular A-130, Section 8b (3)) (2000). http://csrc.nist.gov/drivers/documents/a130trans4.pdf

[19] Z. Xiao and Y. Xiao, "Security and Privacy in Cloud Computing", *IEEE Communications Surveys & Tutorials*, (2013). http://yangxiao.cs.ua.edu/IEEE_COMST_2013_Cloud_Computing.pdf

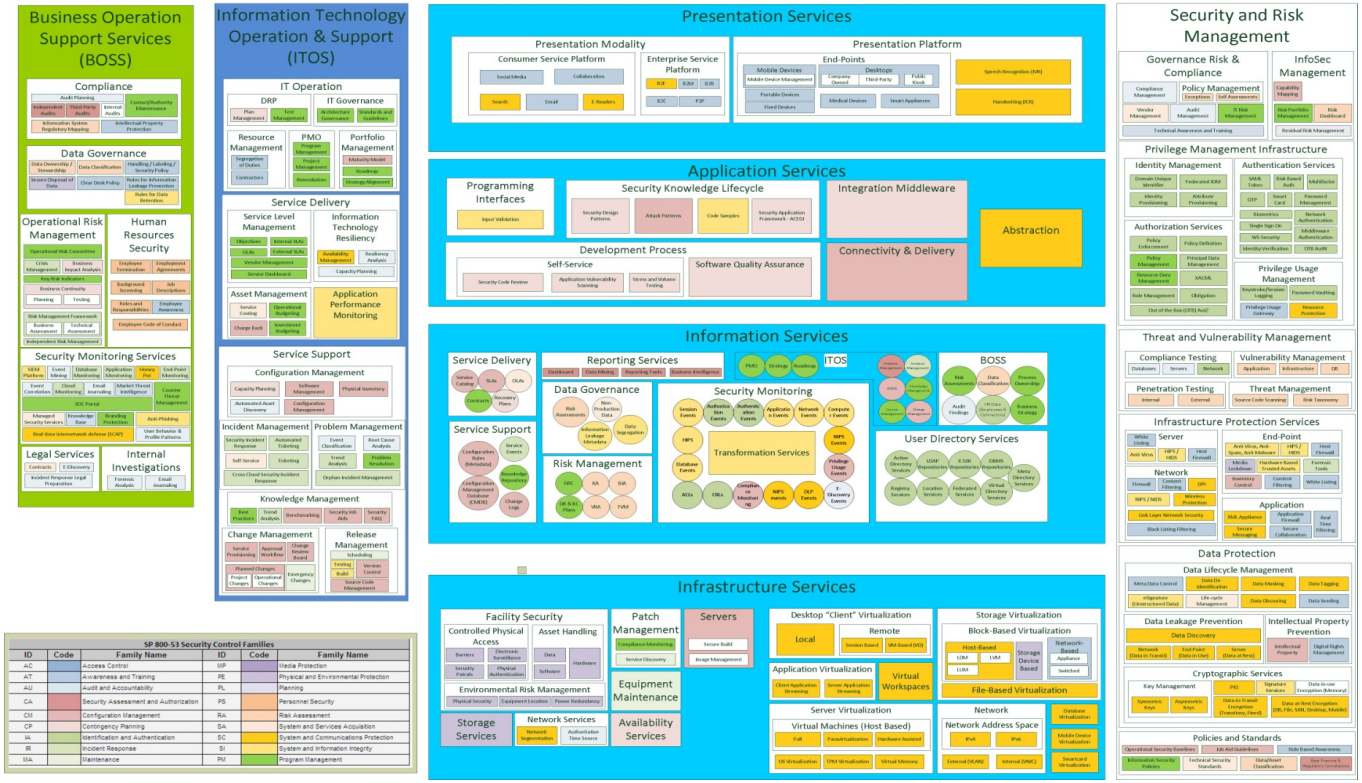
Commented [KS42]: This should be updated to Revision 4. Name has changed. http://dx.doi.org/10.6028/NIST.SP.800-53r4

Does updating this necessitate any changes within the main body of the document?

8 ANNEX A: TRUSTED COMPUTING INITIATIVE REFERENCE ARCHITECTURE

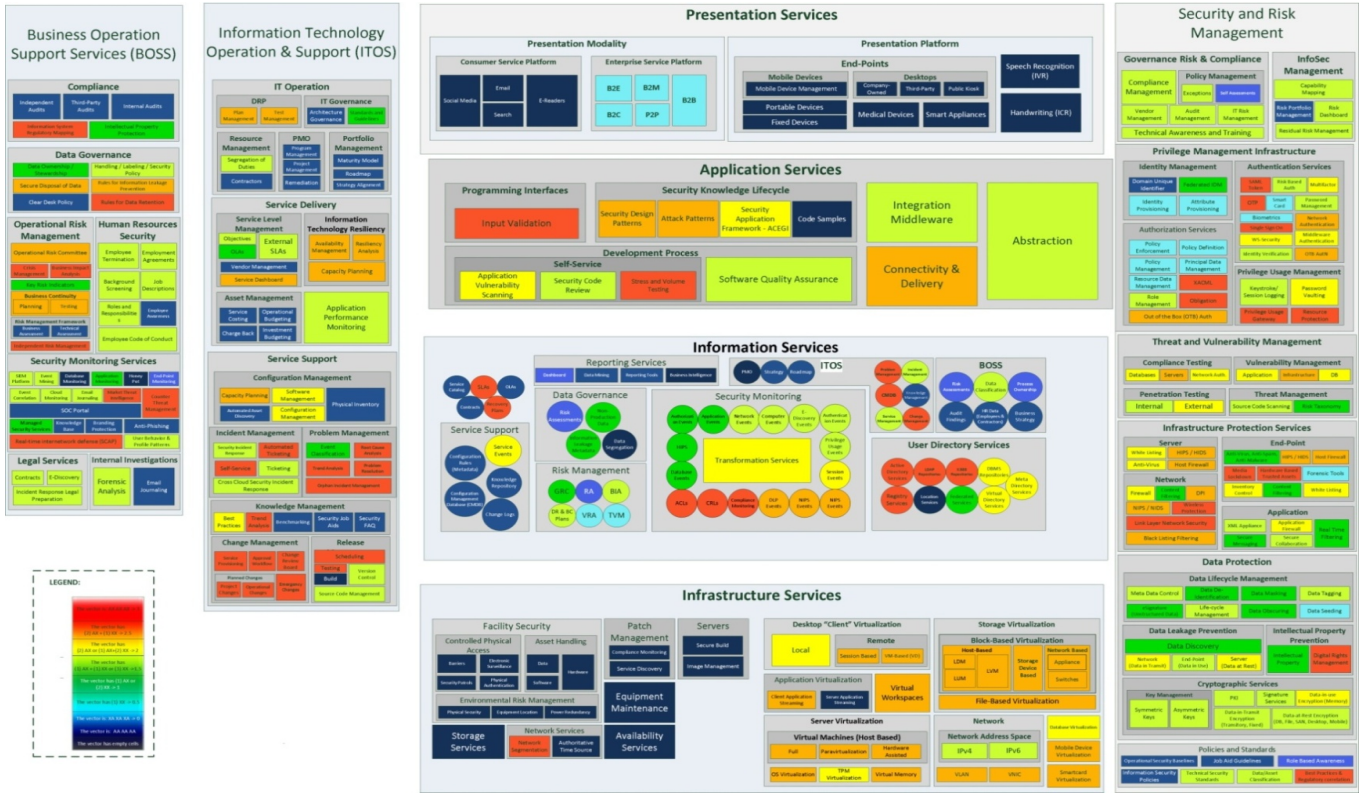


9 ANNEX B: MAPPING TO NIST SP 800-53 SECURITY CONTROL FAMILIES



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

10 ANNEX C: GENERIC HEAT MAP



11 ANNEX D: AGGREGATED DATA

11.1 ACTORS-BASED DATA AGGREGATION

LEGEND:

In the table below

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

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

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

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

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

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

BOSS	Security Monitoring Services	Knowledge Base		AT	A	A	A	A	A	A	B	B	B	A	
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	Endpoint 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		MP	X	A	A	X	X	X	A	A	A	X	A
BOSS	Human Resource Security	Employee Termination		PS	X	X	X	X	X	X	B	B	B	A	A
BOSS	Human Resource Security	Employment Agreements		PS	X	X	X	X	X	X	B	B	B	A	A
BOSS	Human Resource Security	Background Screening		PS	X	X	X	X	X	X	B	B	B	A	A
BOSS	Human Resource Security	Job Descriptions		PS	X	X	X	X	X	X	B	B	B		A
BOSS	Human Resource Security	Roles and Responsibilities		PS	X	X	X	X	X	X	B	B	B	A	A
BOSS	Human Resource Security	Employee Code of Conduct		PS	X	X	X	X	X	X	B	B	B	X	A
BOSS	Compliance	Information Systems Regulatory Mapping		RA	A	A	A	X	X	X	B	B	B	A	A
BOSS	Data Governance	Data Ownership - Personnel Responsibilities/ Stewardship		RA	X	X	X	A	X	X	A	A	A	A	A
BOSS	Data Governance	Data Classification		RA	X	X	X	X	X	X	A	A	A	A	A
BOSS	Security Monitoring Services	Managed (Outsourced) Security Services		SA	X	X	X	A	X	X	B	B	B	A	
BOSS	Legal Services	Contracts		SA	X	X	X	X	X	X	A	A	A	X	A
BOSS	Security Monitoring Services	Honeypot		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	Security Information and Event Management (SIEM) Platform		SI	X	X	A	A	X	X	B	B	B	A	A
BOSS	Security Monitoring Services	Anti-Phishing		SI	A	A	A	A	A	A	B	B	B	X	
BOSS	Compliance	Contract/ Authority Maintenance		PM	X	X	A	A	A	X	B	B	B	A	A

BOSS	Operational Risk Management	Operational Risk Committee		PM	X	A	A	X	X	X	A	A	A	A	A				
BOSS	Operational Risk Management	Key Risk Indicators		PM	X	X	A	A	A	X	A	A	A	A					
BOSS	Security Monitoring Services	Counter Threat Management		PM	A	A	A	X	X	X	B	B	B	A					
BOSS	Security Monitoring Services	Security Operations Center (SOC) Portal		PM	A	A	A	A	A	A	B	B	B	A					
BOSS	Security Monitoring Services	Branding Protection		PM	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	CM	A	A	A	A	A	A	A	A	A	A					
ITOS	Service Delivery	Asset Management	Change Back	CM	A	A	A	A	A	A	A	A	A	A					
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				

Commented [KS43]: Change to "Counterthreat"?

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	Disaster Recovery Plan (DRP)	Plan Management	CP	X	A	A		X	X	X		B	B	B		A					
ITOS	Service Support	Configuration Management	Capacity Planning	CP	X	A	A		X	X	X		B	B	B		A					
ITOS	Service Support	Incident Management	Security Incident Response	IR	X	X	X		X	X	X		B	B	B		A					
ITOS	Service Support	Incident Management	Automated Ticketing	IR	A	A	A		X	X	X		B	B	B		A		A			
ITOS	Service Support	Incident Management	Ticketing	IR	X	X	X		X	X	X		B	B	B		A		A			
ITOS	Service Support	Incident Management	Cross-Cloud Security Incident Response	IR	X	X	X		X	X	X		B	B	B		A					
ITOS	Service Support	Problem Management	Trend Analysis	IR	A	A	A		X	X	X		B	B	B		A					
ITOS	Service Support	Problem Management	Orphan Incident Management	IR	A	A	A		X	X	X		B	B	B		A					
ITOS	Service Support	Knowledge Management	Trend Analysis	IR	A	A	A		X	X	X		A	A	A		A		A			
ITOS	Service Support	Change Management	Emergency Changes	MA	A	A	A		X	X	X		A	A	A		A					
ITOS	Service Support	Release Management	Scheduling	MA	A	A	A		X	X	X		A	A	A		X					
ITOS	Service Delivery	Asset Management	Service Costing (Internal)	SA	A	A	A		A	A	A		B	B	B		x					
ITOS	Service Support	Incident Management	Self-Service	SA	A	A	A		X	X	X		B	B	B		x					
ITOS	Service Delivery	Information Technology Resiliency	Availability Management	SC	X	A	A		X	X	X		B	B	B		A					
ITOS	Service Delivery	Application Performance Monitoring		SI	X	X	A		A	X	X		A	A	A		x					
ITOS	Service Support	Release Management	Testing	SI	A	A	A		X	X	X		A	A	A		X					
ITOS	Service Support	Release Management	Build	SI	A	A			X	X	X		A	A	A		X					
ITOS	IT Operations	DRP	Test Management	PM	X	A	A		X	X	X		B	B	B		X		A			

ITOS	IT Operations	IT Governance	Architecture Governance	PM	A	A	A		A	A	A		A	A	A		X		-
ITOS	IT Operations	IT Governance	Standards and Guidelines	PM	X	X	X		A	X	X		A	A	A		A		
ITOS	IT Operations	Program Management Office (PMO)	Program Mgmt	PM	A	A	A		A	A	A		A	A	A		A		A
ITOS	IT Operations	PMO	Project Mgmt	PM	A	A	A		A	A	A		A	A	A		A		A
ITOS	IT Operations	PMO	Remediation	PM	A	A	A		A	A	A		A	A	A		A		A
ITOS	IT Operations	Portfolio Management	Roadmap	PM	A	A	A		A	A	A		A	A	A		A		
ITOS	IT Operations	Portfolio Management	Strategy Alignment	PM	A	A	A		A	A	A		A	A	A		A		
ITOS	Service Delivery	Service Level Management	Objectives	PM	X	X	X		X	X	X		B	B	B		A		
ITOS	Service Delivery	Service Level Management	Operational Level Agreements (OLAs)	PM	X	X	X		A	X	X		B	B	B		A		A
ITOS	Service Delivery	Service Level Management	Internal SLAs	PM	X	X	X		A	A	A		A	A	A		A		A
ITOS	Service Delivery	Service Level Management	External SLAs	PM	X	X	X		X	X	X		B	B	B		A		A
ITOS	Service Delivery	Service Level Management	Vendor Management	PM	A	A	A		A	A	A		A	A	A		A		A
ITOS	Service Delivery	Service Level Management	Service Dashboard	PM	X	A	A		X	X	X		B	B	B		A		A
ITOS	Service Delivery	Asset Management	Operational Budgeting	PM	A	A	A		A	A	A		A	A	A		A		
ITOS	Service Delivery	Asset Management	Investment Budgeting	PM	A	A	A		A	A	A		A	A	A		A		
ITOS	Service Support	Problem Management	Problem Resolutions	PM	A	A	A		X	X	X		B	B	B		A		
ITOS	Service Support	Knowledge Management	Best Practices	PM	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	Endpoints	Mobile Devices	AC	X	X	X	A	A	A	B	B	B			
Presentation Services	Presentation Platform	Endpoints	Fixed Devices	AC	X	X	X	A	A	A	B	B	B			
Presentation Services	Presentation Platform	Endpoints	Desktops	AC	X	X	X	A	A	A	B	B	B			
Presentation Services	Presentation Platform	Endpoints	Portable Devices	AC	X	X	X	A	A	A	B	B	B			
Presentation Services	Presentation Platform	Endpoints	Medical Devices	AC	X	X	X	A	A	A	B	B	B			
Presentation Services	Presentation Platform	Endpoints	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			

Commented [KS44]: Spell out abbreviations here and in the following rows. Some such as B2M have many meanings and I don't know which is the intended one.

Presentation Services	Presentation Platform	Speech Recognition (Interactive Voice Response, IVR)		SC	X	X	X				B	B	B		
Presentation Services	Presentation Platform	Handwriting (Intelligent Character Recognition, 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	A								
Information Services	Reporting Services	Reporting Tools		CA	A	A	A	A	A	A	B	B	B	A								
Information Services	Reporting Services	Business Intelligence		CA	A	A	A				A	A	A	A								
Information Services	ITOS	Problem Management		CA	A	A	A	X	X	X	B	B	B	A								
Information Services	Service Delivery	Service Catalog		CM	A	A	A	A	A	A	A	A	A	x								
Information Services	Service Delivery	SLAs		CM	A	A	A	X	X	X	B	B	B	A								
Information Services	ITOS	Configuration Management Database (CMDB)		CM	A	A	A	X	X	X	B	B	B	A								
Information Services	ITOS	Change Management		CM	A	A	A	X	X	X	B	B	B	A								
Information Services	Service Support	Configuration Rules (Metadata)		CM	A	A	A	A	A	A	B	B	B	A								

Information Services	Service Support	CMDB		CM	A	A	A	A	A	A	B	B	B	X		
Information Services	Service Support	Change Logs		CM	A	A	A	A	A	A	B	B	B	X		
Information Services	Security Monitoring	Compliance Monitoring		CM	A	A	A	X	X	X	B	B	B	A		
Information Services	Security Monitoring	Privilege Usage Events		CM	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	ACLs		IA	A	A	A	X	X	X	B	B	B	A		
Information Services	Security Monitoring	CRLs		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		

Commented [KS45]: What does this stand for?

Commented [KS46]: Is this Certificate Revocation Lists?

Information Services	User Directory Services	Database Management System (DBMS) Repositories		I A	X	A	A	A	X	X	B	B	B	A		
Information Services	User Directory Services	Registry Services		I A	A	A	A	X	X	X	B	B	B	A		
Information Services	User Directory Services	Location Services		I A	A	A	A				B	B	B	x		
Information Services	User Directory Services	Federated Services		I A	X	X	A	A	A	X	B	B	B	X		
Information Services	User Directory Services	Virtual Directory Services		I A	X	A	A	A	X	X	B	B	B	X		
Information Services	User Directory Services	Meta Directory Services		I A	X	A	A	A	X	X	B	B	B	A		
Information Services	ITOS	Incident Management		I R	X	X	X	X	X	X	B	B	B	A		
Information Services	Service Support	Service Events		I R	X	X	A	X	X	X	B	B	B	A		
Information Services	BOSS	Data Classification		R A	X	X	X	X	X	X	A	A	A	A		
Information Services	Data Governance	Risk Assessments		R A	X	X	X	A	A	A	B	B	B	X		
Information Services	Risk Management	Risk Assessments		R A	X	X	X	A	A	A	B	B	B	A		
Information Services	Risk Management	Business Impact Assessment.		R A	X	X	X	X	X	X	B	B	B	X		
Information Services	Risk Management	VRA		R A	X	X	X	A	A	X	B	B	B	x		A

Commented [KS47]: What does this stand for?

Information Services	Risk Management	Threat and Vulnerability Management (TVM)		RA	X	X	X	A	A	X	B	B	B	x					
Information Services	Service Delivery	OLAs		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	Network Intrusion Prevention System (NIPS) Events		SC	X	A	A	X	X	X	B	B	B	A					
Information Services	Security Monitoring	Data Loss Prevention (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 Prevention 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		PM	A	A	A	A	A	A	A	A	A	A	
Information Services	ITOS	PMO		PM	A	A	A				A	A	A	A	
Information Services	ITOS	Strategy		PM	A	A	A	A	A	A	A	A	A	A	
Information Services	ITOS	Roadmap		PM	A	A	A	A	A	A	A	A	A	A	
Information Services	ITOS	Knowledge Management		PM	A	A	A	A	A	A	B	B	B	A	
Information Services	ITOS	Service Management		PM	X	X	A	A	X	X	B	B	B	A	
Information Services	BOSS	Risk Assessments		PM	X	X	X	A	A	A	A	A	A	A	
Information Services	BOSS	Process Ownership		PM	X	X	X	A	A	A	A	A	A	A	
Information Services	BOSS	Business Strategy		PM	A	A	A	A	A	A	A	A	A	A	
Information Services	Service Support	Knowledge Repository		PM	A	A	A	A	A	A	B	B	B	A	
Information Services	Risk Management	Governance, Risk Management, and Compliance (GRC)		PM	X	X	X	A	X	X	A	A	A	A	A
Information Services	Risk Management	Disaster Recovery (DR) & Business Continuity (BC) Plans		PM	X	X	X	X	X	X	B	B	B	A	

Infrastructure Services	Virtual Infrastructure: Storage Virtualization	Block-Based Virtualization	Network-Based	AC	X	A	A	X	X	X	B	B	B	A	
Infrastructure Services	Internal Infrastructure: Network Services	Authoritative Time Source		AU				X	X	X	B	B	B	A	
Infrastructure Services	Internal Infrastructure: Patch Management	Service Discovery		MA				A	A	A	B	B	B	A	
Infrastructure Services	Internal Infrastructure: Equipment Maintenance			MA				A	A	A	B	B	B	A	
Infrastructure Services	Internal Infrastructure: Storage Services			MP				A	A	A	B	B	B	A	A
Infrastructure Services	Virtual Infrastructure: Storage Virtualization	Block-Based Virtualization	Storage Device-Based	MP	X	A	A	X	X	X	B	B	B	A	
Infrastructure Services	Internal Infrastructure: Facility Security	Controlled Physical Access	Barriers	PE				A	A	A	B	B	B	A	
Infrastructure Services	Internal Infrastructure: Facility Security	Controlled Physical Access	Security Patrols	PE				A	A	A	B	B	B	A	
Infrastructure Services	Internal Infrastructure: Facility Security	Controlled Physical Access	Electronic Surveillance	PE				A	A	A	B	B	B	A	A
Infrastructure Services	Internal Infrastructure: Facility Security	Controlled Physical Access	Physical Authentication	PE				A	A	A	B	B	B	A	A
Infrastructure Services	Internal Infrastructure: Facility Security	Asset Handling	Data	PE				A	A	A	B	B	B	A	A
Infrastructure Services	Internal Infrastructure: Facility Security	Asset Handling	Storage	PE				A	A	A	B	B	B	X	
Infrastructure Services	Internal Infrastructure: Facility Security	Asset Handling	Hardware	PE				A	A	A	B	B	B	X	A

Infrastructure Services	Internal Infrastructure: Facility Security	Environmental Risk Management	Physical Security	PE				A	A	A	B	B	B	X		
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	Virtual Machine (VM) Based (Virtual Desktop Infrastructure, 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	Virtual Infrastructure:			SC	X	A	A	X	X	X	B	B	B	A		

Services	Virtual Workspaces															
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	
		Trusted Platform Module (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	
		Virtual Local Area Network (VLAN)		SC	X	A	A	X	X	X	B	B	B	X	
		Virtual Network Interface Card (VNIC)		SC	X	A	A	X	X	X	B	B	B	X	
Infrastructure Services	Virtual Infrastructure: Database Virtualization			SC	X	X	A	X	X	X	B	B	B		
Infrastructure Services	Virtual Infrastructure: Mobile Device Virtualization			SC	X	A	A	X	X	X	B	B	B		
Infrastructure Services	Virtual Infrastructure: Smartcard Virtualization			SC	X	A	A	X	X	X	B	B	B		
Infrastructure Services	Internal Infrastructure: Patch Management	Compliance Monitoring		PM				A	A	A	B	B	B		
S & RM	Privilege Management Infrastructure	Privilege Usage Management	Privilege Usage Gateway	AC	A	A	A	X	X	X	B	B	B	X	
S & RM	Infrastructure Protection Services	Server	Whitelisting	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	

Commented [KS48]: Why is part of this row and the next two blank?

S & RM	Infrastructure Protection Services	Endpoint	Host Firewall	AC	X	X	A	A	X	X	B	B	B	A	A
S & RM	Infrastructure Protection Services	Endpoint	Content Filtering	AC	X	X	A	A	A	X	B	B	B	A	A
S & RM	Infrastructure Protection Services	Endpoint	Whitelisting	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	Blacklisting 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	Metadata 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	Endpoint	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 Identity Management (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	Extensible Access Control Markup Language (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) Auth	IA	X	A	A	X	X	X	B	B	B	A	
S & RM	Privilege Management Infrastructure	Authentication Services	Security Assertion Markup	IA	A	A	A	X	X	X	B	B	B	X	

Commented [KS49]: Should this say S&RM?

			Language (SAML) Token													
S & RM	Privilege Management Infrastructure	Authentication Services	Risk-Based Authentication	I A	X	X	X	X	X	X	B	B	B	X	
S & RM	Privilege Management Infrastructure	Authentication Services	Multifactor	I A	X	X	A	X	X	X	B	B	B	X	
S & RM	Privilege Management Infrastructure	Authentication Services	One-Time Password (OTP)	I A	A	A	A	X	X	X	B	B	B	A	
S & RM	Privilege Management Infrastructure	Authentication Services	Smart Card	I A	X	X	A	A	A	X	B	B	B	A	
S & RM	Privilege Management Infrastructure	Authentication Services	Password Management	I A	X	X	X	X	X	X	B	B	B	X	
S & RM	Privilege Management Infrastructure	Authentication Services	Biometrics	I A	X	X	X	A	A	X	B	B	B	A	
S & RM	Privilege Management Infrastructure	Authentication Services	Network Authentication	I A	X	A	A	X	X	X	B	B	B	A	
S & RM	Privilege Management Infrastructure	Authentication Services	Single Sign On	I A	A	A	A	X	X	X	B	B	B	A	
S & RM	Privilege Management Infrastructure	Authentication Services	WS-Security	I A	X	X	A	X	X	X	B	B	B	A	
S & RM	Privilege Management Infrastructure	Authentication Services	Middleware Authentication	I A	X	X	A	X	X	X	B	B	B	A	
S & RM	Privilege Management Infrastructure	Authentication Services	Identity Verification	I A	X	X	X	X	X	X	B	B	B	A	
S & RM	Privilege Management Infrastructure	Authentication Services	Out-of-The-Box (OTB) Authentication	I A	X	X	A	X	X	X	B	B	B	A	
S & RM	Privilege Management Infrastructure	Privilege Usage Management	Keystroke/Session Logging	I A	X	X	X	X	X	X	B	B	B	A	
S & RM	Privilege Management Infrastructure	Privilege Usage Management	Password Vaulting	I A	X	X	A	X	X	X	B	B	B	A	
S & RM	Threat and Vulnerability Management	Compliance Testing	Network Authentication	I A	X	X	A	X	X	X	B	B	B	A	A
S & RM	Infrastructure Protection Services	Endpoint	Forensic Tools	I R	X	X	X	A	A	X	B	B	B	A	A

S & RM	Infrastructure Protection Services	Endpoint	Media Lockdown	MP	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
			Database	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	Lifecycle 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

Commented [KS50]: Next several rows look mis-formatted

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	Endpoint (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	Public Key Infrastructure (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 at Rest Encryption (Database, 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 Prevention /Detection)	SI	X	A	A	X	X	X	B	B	B	X	
S & RM	Infrastructure Protection Services	Endpoint	Anti-Virus, Anti-Spam, Anti-Malware	SI	X	X	A	A	A	X	B	B	B	X	

S & RM	Infrastructure Protection Services	Endpoint	HIPS/HIDS (Intrusion Protection /Detection)	S I	X	X	A	A	X	X	B	B	B	X		A
S & RM	Infrastructure Protection Services	Endpoint	Hardware-Based Trusted Assets	S I	A	A	A	X	X	X	B	B	B	X		A
S & RM	Infrastructure Protection Services	Network	NIPS/NIDS	S I	X	A	A	X	X	X	B	B	B	X		A
S & RM	Data Protection	Data Lifecycle Management	eSignature	S I	X	X	X	A	X	X	B	B	B	A		A
S & RM	Cryptographic Services	Signature Services		S I	X	X	X	X	X	X	B	B	B	A		A
S & RM	Governance Risk & Compliance	IT Risk Management		P M	X	X	X	X	X	X	B	B	B	A		A
S & RM	InfoSec Management	Risk Portfolio Management		P M	A	A	A	A	A	A	B	B	B	A		
S & RM	Privilege Management Infrastructure	Authorization Services	Policy Management	P M	X	X	X	A	A	X	B	B	B	X		
S & RM	Privilege Management Infrastructure	Authorization Services	Resource Data Management	P M	X	X	X	A	A	X	B	B	B	A		
S & RM	Policies and Standards	Information Security Polices		P M	A	A	A	A	A	A	A	A	A	X		A

11.2 SERVICE-BASED ECOSYSTEM-LEVEL DATA AGGREGATION

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

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

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

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

		Defense (SCAP)																					
BOSS	Data Governance	Rules for Data Retention		SI	A	X	B	X	A	X	B	X	A	X	B	X	A		A
BOSS	Security Monitoring Services	SIEM Platform		SI	X	A	B	X	X	X	B	X	A	X	B	X	X		A
BOSS	Security Monitoring Services	Anti-Phishing		SI	A	A	B	Ab	A	A	B	Ab	A	A	B	Ab	A		
BOSS	Compliance	Contract/ Authority Maintenance		PM	X	A	B	X	X	A	B	X	A	X	B	X	X		A
BOSS	Operational Risk Management	Operational Risk Committee		PM	X	X	A	X	A	X	A	X	A	X	A	X	A		A
BOSS	Operational Risk Management	Key Risk Indicators		PM	X	A	A	X	X	A	A	X	A	X	A	X	A		
BOSS	Security Monitoring Services	Counter Threat Management		PM	A	X	B	X	A	X	B	X	A	X	B	X	A		
BOSS	Security Monitoring Services	SOC Portal		PM	A	A	B	Ab	A	A	B	Ab	A	A	B	Ab	X		
BOSS	Security Monitoring Services	Branding Protection		PM	A	A	B	Ab	A	A	B	Ab	A	A	B	Ab	A		A
ITOS	IT Operations	Resource Management	Segregation of Duties	AC	X	X	B	X	X	X	B	X	X	X	B	X	A		A
ITOS	IT Operations	Resource Management	Contractors	AC	A	A	A	A	A	A	A	A	A	A	A	A	A		A
ITOS	Service Delivery	Information Technology Resiliency	Resiliency Analysis	AU	X	X	B	X	A	X	B	X	A	X	B	X	X		
ITOS	Service Delivery	Information Technology Resiliency	Capacity Planning	AU	X	X	B	X	A	X	B	X	A	X	B	X	X		
ITOS	Service Support	Configuration Management	Automated Asset Discovery	AU	A	A	B	Ab	A	A	B	Ab	A	A	B	Ab	A		

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

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

ITOS	Service Delivery	Application Performance Monitoring		SI		X	A	A	X		X	X	A	X		A	X	A	X		A			
ITOS	Service Support	Release Management	Testing	SI		A	X	A	X		A	X	A	X		A	X	A	X		A			
ITOS	Service Support	Release Management	Build	SI		A	X	A	X		A	X	A	X			X	A	X		A			
ITOS	IT Operations	DRP	Test Management	PM		X	X	B	X		A	X	B	X		A	X	B	X		A			A
ITOS	IT Operations	IT Governance	Architecture Governance	PM		A	A	A	A		A	A	A	A		A	A	A	A		A			-
ITOS	IT Operations	IT Governance	Standards and Guidelines	PM		X	A	A	X		X	X	A	X		X	X	A	X		A			
ITOS	IT Operations	PMO	Program Mgmt	PM		A	A	A	A		A	A	A	A		A	A	A	A		A			A
ITOS	IT Operations	PMO	Project Mgmt	PM		A	A	A	A		A	A	A	A		A	A	A	A		A			A
ITOS	IT Operations	PMO	Remediation	PM		A	A	A	A		A	A	A	A		A	A	A	A		A			A
ITOS	IT Operations	Portfolio Management	Roadmap	PM		A	A	A	A		A	A	A	A		A	A	A	A		A			
ITOS	IT Operations	Portfolio Management	Strategy Alignment	PM		A	A	A	A		A	A	A	A		A	A	A	A		A			
ITOS	Service Delivery	Service Level Management	Objectives	PM		X	X	B	X		X	X	B	X		X	X	B	X		X			
ITOS	Service Delivery	Service Level Management	OLAs	PM		X	A	B	X		X	X	B	X		X	X	B	X		X			A
ITOS	Service Delivery	Service Level Management	Internal SLAs	PM		X	A	A	X		X	A	A	X		X	A	A	X		A			A
ITOS	Service Delivery	Service Level Management	External SLAs	PM		X	X	B	X		X	X	B	X		X	X	B	X		X			A

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

Presentation Services	Presentation Modality	Enterprise Service Platform	P2P	A C	X	A	B	X	X	A	B	X	X	X	B	X							
Presentation Services	Presentation Platform	Endpoints	Mobile Devices	A C	X	A	B	X	X	A	B	X	X	A	B	X							
Presentation Services	Presentation Platform	Endpoints	Fixed Devices	A C	X	A	B	X	X	A	B	X	X	A	B	X							
Presentation Services	Presentation Platform	Endpoints	Desktops	A C	X	A	B	X	X	A	B	X	X	A	B	X							
Presentation Services	Presentation Platform	Endpoints	Portable Devices	A C	X	A	B	X	X	A	B	X	X	A	B	X							
Presentation Services	Presentation Platform	Endpoints	Medical Devices	A C	X	A	B	X	X	A	B	X	X	A	B	X							
Presentation Services	Presentation Platform	Endpoints	Smart Appliances	A C	X	A	B	X	X	A	B	X	X	A	B	X							
Presentation Services	Presentation Modality	Consumer Service Platform	Search	S C	X		B	X	X		B	X		X	B	X							
Presentation Services	Presentation Modality	Consumer Service Platform	e-Readers	S C	X		B	X	X		B	X		X	B	X							
Presentation Services	Presentation Modality	Enterprise Service Platform	B2E	S C	X	A	B	X	X	A	B	X	X	X	B	X							
Presentation	Presentation Platform	Speech Recognition (IVR)		S C	X		B	X	X		B	X	X		B	X							

Services																							
Presentation Services	Presentation Platform	Handwriting (ICR)		SC	X		B	X	X		B	X	X		B	X				
Application Services	Security Knowledge Lifecycle	Attack Patterns		CM	X	X	B	X	A	X	B	X	A	X	B	X	A		A	
Application Services	Security Knowledge Lifecycle	Security Design Patterns		SA	X	X	B	X	A	X	B	X	A	X	B	X	A			
Application Services	Security Knowledge Lifecycle	Security Application Framework - ACEGI		SA	X	A	B	X	A	X	B	X	A	X	B	X	A		A	
Application Services	Development Processes	Self Service	Security Code Review	SA	X	X	B	X	X	X	B	X	X	X	B	X	A		A	
Application Services	Development Processes	Self Service	Application Vulnerability Scanning	SA	X	X	B	X	X	X	B	X	A	X	B	X	A		A	
Application Services	Development Processes	Self Service	Stress Volume Testing	SA	A	X	B	X	A	X	B	X	A	X	B	X	X		A	
Application Services	Development Processes	Software Quality Assurance		SA	X	X	B	X	X	X	B	X	X	X	B	X	A		A	
Application Services	Integration Middleware			SA	X	A	B	X	X	X	B	X	A	X	B	X	A			
Application Services	Connectivity & Delivery			CM	X	X	B	X	A	X	B	X	A	X	B	X	A			

Application Services	Programming Interfaces	Input Validation		SI	A	X	B	X	A	X	B	X	A	X	B	X	A		
Application Services	Security Knowledge Lifecycle	Code Samples		SI	A	X	B	X	A	X	B	X		X	B	X	A		A
Application Services	Abstraction			SC	X	A	A	X	X	X	A	X	A	X	A	X	A		
Information Services	BOSS	Audit Findings		AU	A	A	A	A	A	A	A	A	A	A	A	A	A		
Information Services	Security Monitoring	eDiscovery Events		AU	X	X	B	X	X	X	B	X	X	X	B	X	A		
Information Services	Reporting Services	Dashboard		CA	A	X	A	X	A	X	A	X	A	X	A	X	A		
Information Services	Reporting Services	Data Mining		CA	A	A	A	A	A	A	A	A	A	A	A	A	A		
Information Services	Reporting Services	Reporting Tools		CA	A	A	B	Ab	A	A	B	Ab	A	A	B	Ab	X		
Information Services	Reporting Services	Business Intelligence		CA	A		A	A	A		A	A	A		A	A	A		
Information Services	ITOS	Problem Management		CA	A	X	B	X	A	X	B	X	A	X	B	X	X		
Information	Service Delivery	Service Catalog		CM	A	A	A	A	A	A	A	A	A	A	A	A	A		

Services																							
Information Services	Service Delivery	SLA´s		C M	A	X	B	X	A	X	B	X	A	X	B	X	X						
Information Services	ITOS	CMDB		C M	A	X	B	X	A	X	B	X	A	X	B	X	A						
Information Services	ITOS	Change Management		C M	A	X	B	X	A	X	B	X	A	X	B	X	X						
Information Services	Service Support	Configuration Rules (Metadata)		C M	A	A	B	Ab	A	A	B	Ab	A	A	B	Ab	A						
Information Services	Service Support	Configuration Management Database (CMDB)		C M	A	A	B	Ab	A	A	B	Ab	A	A	B	Ab	A						
Information Services	Service Support	Change Logs		C M	A	A	B	Ab	A	A	B	Ab	A	A	B	Ab	X						
Information Services	Security Monitoring	Compliance Monitoring		C M	A	X	B	X	A	X	B	X	A	X	B	X	A						
Information Services	Security Monitoring	Privilege Usage Events		C M	X	X	B	X	X	X	B	X	X	X	B	X	A						
Information Services	Service Delivery	Recovery Plans		C P	A	X	A	X	A	X	A	X	A	X	A	X	A						
Information Services	BOSS	GR Data (Employee & contractors)		IA	A	A	A	A	A	A	A	A	A	A	A	A	A						

Information Services	Security Monitoring	Authorization Events		IA		X	A	B	X		X	X	B	X		X	X	B	X		A		
Information Services	Security Monitoring	Authentication Events		IA		X	X	B	X		X	X	B	X		X	X	B	X		A		
Information Services	Security Monitoring	ACLs		IA		A	X	B	X		A	X	B	X		A	X	B	X		X		
Information Services	Security Monitoring	CRLs		IA		A	X	B	X		A	X	B	X		A	X	B	X		X		
Information Services	User Directory Services	Active Directory Services		IA		A	X	B	X		A	X	B	X		A	X	B	X		A		
Information Services	User Directory Services	LDAP Repositories		IA		A	X	B	X		A	X	B	X		A	X	B	X		A		
Information Services	User Directory Services	X.500 Repositories		IA		A	X	B	X		A	X	B	X		A	X	B	X		A		
Information Services	User Directory Services	DBMS Repositories		IA		X	A	B	X		A	X	B	X		A	X	B	X		A		
Information Services	User Directory Services	Registry Services		IA		A	X	B	X		A	X	B	X		A	X	B	X		A		
Information Services	User Directory Services	Location Services		IA		A		B	Ab		A		B	Ab		A		B	Ab		A		
Information	User Directory Services	Federated Services		IA		X	A	B	X		X	A	B	X		A	X	B	X		A		

Services																							
Information Services	User Directory Services	Virtual Directory Services		IA	X	A	B	X	A	X	B	X	A	X	B	X	A		
Information Services	User Directory Services	Meta Directory Services		IA	X	A	B	X	A	X	B	X	A	X	B	X	A		
Information Services	ITOS	Incident Management		IR	X	X	B	X	X	X	B	X	X	X	B	X	X		
Information Services	Service Support	Service Events		IR	X	X	B	X	X	X	B	X	A	X	B	X	X		
Information Services	BOSS	Data Classification		RA	X	X	A	X	X	X	A	X	X	X	A	X	A		
Information Services	Data Governance	Risk Assessments		RA	X	A	B	X	X	A	B	X	X	A	B	X	X		
Information Services	Risk Management	Risk Assessments		RA	X	A	B	X	X	A	B	X	X	A	B	X	X		
Information Services	Risk Management	Business Impact Assessment.		RA	X	X	B	X	X	X	B	X	X	X	B	X	A		
Information Services	Risk Management	VRA		RA	X	A	B	X	X	A	B	X	X	X	B	X	A		A
Information Services	Risk Management	TVM		RA	X	A	B	X	X	A	B	X	X	X	B	X	X		

Information Services	Service Delivery	OLAs		SA		A	A	A	A		A	A	A	A		A	A	A	A		A		
Information Services	Data Governance	Non-Production Data		SA		X	A	B	X		X	X	B	X		X	X	B	X		A		
Information Services	Security Monitoring	NIPS Events		SC		X	X	B	X		A	X	B	X		A	X	B	X		X		
Information Services	Security Monitoring	DLP Events		SC		X	X	B	X		A	X	B	X		A	X	B	X		A		
Information Services	Data Governance	Information Leakage Metadata		SI		X	A	B	X		X	A	B	X		A	X	B	X		A		
Information Services	Data Governance	Data Segregation		SI		X	X	B	X		A	X	B	X			X	B	X		A		
Information Services	Security Monitoring	Transformation Services		SI		X	X	B	X		X	X	B	X		A	X	B	X		A		
Information Services	Security Monitoring	Session Events		SI		X	X	B	X		X	X	B	X		A	X	B	X		A		
Information Services	Security Monitoring	Application Events		SI		X	A	B	X		X	A	B	X		A	X	B	X		A		
Information Services	Security Monitoring	Network Events		SI		X	A	B	X		X	X	B	X		A	X	B	X		X		
Information	Security Monitoring	Computer Events		SI		X	A	B	X		X	X	B	X		A	X	B	X		A		

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

Information Services	BOSS	Business Strategy		PM	A	A	A	A	A	A	A	A	A	A	A	A	A			
Information Services	Service Support	Knowledge Repository		PM	A	A	B	Ab	A	A	B	Ab	A	A	B	Ab	A			
Information Services	Risk Management	GRC		PM	X	A	A	X	X	X	A	X	X	X	A	X	A		A	
Information Services	Risk Management	DR & BC Plans		PM	X	X	B	X	X	X	B	X	X	X	B	X	X			
Infrastructure Services	**Virtual Infrastructure:** Storage Virtualization	Block-Based Virtualization	Network-Based	AC	X	X	B	X	A	X	B	X	A	X	B	X	A			
Infrastructure Services	**Internal Infrastructure:** Network Services	Authoritative Time Source		AU		X	B	X		X	B	X		X	B	X	X			
Infrastructure Services	**Internal Infrastructure**: Patch Management	Service Discovery		MA		A	B	Ab		A	B	Ab		A	B	Ab	X			
Infrastructure Services	**Internal Infrastructure:** Equipment Maintenance			MA		A	B	Ab		A	B	Ab		A	B	Ab	X			
Infrastructure Services	**Internal Infrastructure:** Storage Services			MP		A	B	Ab		A	B	Ab		A	B	Ab	A		A	
Infrastructure	**Virtual Infrastructure:** Storage	Block-Based Virtualization	Storage Device-Based	MP	X	X	B	X	A	X	B	X	A	X	B	X	A			

Services	Virtualization																						
Infrastructure Services	**Internal Infrastructure:** Facility Security	Controlled Physical Access	Barriers	PE		A	B	Ab		A	B	Ab		A	B	Ab	A						
Infrastructure Services	**Internal Infrastructure:** Facility Security	Controlled Physical Access	Security Patrols	PE		A	B	Ab		A	B	Ab		A	B	Ab	A						
Infrastructure Services	**Internal Infrastructure:** Facility Security	Controlled Physical Access	Electronic Surveillance	PE		A	B	Ab		A	B	Ab		A	B	Ab	A	A					
Infrastructure Services	**Internal Infrastructure:** Facility Security	Controlled Physical Access	Physical Authentication	PE		A	B	Ab		A	B	Ab		A	B	Ab	A	A					
Infrastructure Services	**Internal Infrastructure:** Facility Security	Asset Handling	Data	PE		A	B	Ab		A	B	Ab		A	B	Ab	A	A					
Infrastructure Services	**Internal Infrastructure:** Facility Security	Asset Handling	Storage	PE		A	B	Ab		A	B	Ab		A	B	Ab	A						
Infrastructure Services	**Internal Infrastructure:** Facility Security	Asset Handling	Hardware	PE		A	B	Ab		A	B	Ab		A	B	Ab	A	A					
Infrastructure Services	**Internal Infrastructure:** Facility Security	Environmental Risk Management	Physical Security	PE		A	B	Ab		A	B	Ab		A	B	Ab	A						
Infrastructure Services	**Internal Infrastructure:** Facility Security	Environmental Risk Management	Equipment Location	PE		A	B	Ab		A	B	Ab		A	B	Ab	A	A					
Infrastructure Services	**Internal Infrastructure:** Facility Security	Environmental Risk Management	Power Redundancy	PE		A	B	Ab		A	B	Ab		A	B	Ab	A	A					

Infrastructure Services	**Internal Infrastructure:** Servers			C M		A	B	A b		A	B	A b		A	B	A b		A						
Infrastructure Services	**Internal Infrastructure:** Availability Services			C P		A	B	A b		A	B	A b		A	B	A b		X						
Infrastructure Services	**Internal Infrastructure:** Network Services	Network Segmentation		S C	A	X	B	X		A	X	B	X		A	X	B	X		X					
Infrastructure Services	**Virtual Infrastructure**: Desktop "Client" Virtualization	Local		S C	X	A	B	X		A	X	B	X		A	X	B	X		A					
Infrastructure Services	**Virtual Infrastructure**: Desktop "Client" Virtualization	Remote	Session-Based	S C	X	X	B	X		A	X	B	X		A	X	B	X		A					
Infrastructure Services	**Virtual Infrastructure**: Desktop "Client" Virtualization	Remote	VM-Based (VDI)	S C	X	X	B	X		A	X	B	X		A	X	B	X		A					
Infrastructure Services	**Virtual Infrastructure:** Storage Virtualization	Block-Based Virtualization	Host-Based	S C	X	X	B	X		A	X	B	X		A	X	B	X		A					
Infrastructure Services	**Virtual Infrastructure:** Storage Virtualization	File-Based Virtualization		S C	X	X	B	X		A	X	B	X		A	X	B	X		A					
Infrastructure	**Virtual Infrastructure:** Applicatio	Client Application Streaming		S C	X	X	B	X		A	X	B	X		A	X	B	X		A					

Services	n Virtualization	Server Application Streaming		SC	X	X	B	X	X	X	B	X		X	B	X	A				
Infrastructure Services	**Virtual Infrastructure**: Virtual Workspaces			SC	X	X	B	X	A	X	B	X	A	X	B	X	A				
Infrastructure Services	**Virtual Infrastructure:** Server Virtualization	Virtual Machines (host based)	Full	SC	X	X	B	X	A	X	B	X	A	X	B	X	A				
			Paravirtualization	SC	X	X	B	X	A	X	B	X	A	X	B	X	A				
			Hardware-Assisted	SC	X	X	B	X	A	X	B	X	A	X	B	X	A				
		OS Virtualization		SC	X	X	B	X	A	X	B	X	A	X	B	X	A				
		TPM Virtualization		SC	X	X	B	X	X	X	B	X	A	X	B	X	A				
		Virtual Memory		SC	X	X	B	X	A	X	B	X	A	X	B	X					
Infrastructure Services	**Virtual Infrastructure:** Network	Network Address Space	IPv4	SC	X	X	B	X	X	X	B	X	X	X	B	X	X				
			IPv6	SC	X	X	B	X	X	X	B	X	X	X	B	X	X				
		VLAN		SC	X	X	B	X	A	X	B	X	A	X	B	X	X				
		VNIC		SC	X	X	B	X	A	X	B	X	A	X	B	X					
Infrastructure Services	**Virtual Infrastructure:** Database Virtualization			SC	X	X	B	X	X	X	B	X	A	X	B	X					
Infrastructure Services	**Virtual Infrastructure**: Mobile Device Virtualization			SC	X	X	B	X	A	X	B	X	A	X	B	X					
Infrastructure Services	**Virtual Infrastructure:** Smartcard Virtualization			SC	X	X	B	X	A	X	B		A	X	B						

Infrastructure Services	**Internal Infrastructure**: Patch Management	Compliance Monitoring		PM		A	B	Ab		A	B	Ab		A	B	Ab	X		
S & RM	Privilege Management Infrastructure	Privilege Usage Management	Privilege Usage Gateway	AC	A	X	B	X	A	X	B		A	X	B		X		
S & RM	Infrastructure Protection Services	Server	Whitelisting	AC	X	A	B	X	A	X	B		A	X	B		A		A
S & RM	Infrastructure Protection Services	Server	Host Firewall	AC	X	X	B	X	A	X	B		A	X	B		A		
S & RM	Infrastructure Protection Services	Endpoint	Host Firewall	AC	X	A	B	X	X	X	B		A	X	B		X		A
S & RM	Infrastructure Protection Services	Endpoint	Content Filtering	AC	X	A	B	X	X	A	B		A	X	B		X		A
S & RM	Infrastructure Protection Services	Endpoint	Whitelisting	AC	X	A	B	X	A	X	B		A	X	B		X		A
S & RM	Infrastructure Protection Services	Network	Content Filtering	AC	X	A	B	X	X	X	B		A	X	B		X		A
S & RM	Infrastructure Protection Services	Network	Firewall	AC	X	X	B	X	X	X	B		A	X	B		X		A
S & RM	Infrastructure Protection Services	Network	Blacklisting Filtering	AC	X	X	B	X	A	X	B		A	X	B		X		A
S & RM	Infrastructure Protection Services	Application	Application Firewall	AC	X	X	B	X	X	X	B		A	X	B		A		A
S & RM	Infrastructure Protection Services	Application	Secure Collaboration	AC	X	A	B	X	X	X	B		A	X	B		A		A
S & RM	Infrastructure	Application	Real Time Filtering	AC	X	A	B	X	X	A	B		A	X	B		A		A

	Protection Services																						
S & RM	Data Protection	Data Lifecycle Management	Metadata Control	AC	X	A	B	X	X	X	B		A	X	B		A		A	
S & RM	Data Protection	Data Lifecycle Management	Data Seeding	AC	X	A	B	X	X	A	B		X	X	B		A		A	
S & RM	Data Protection	Intellectual Property Prevention	Digital Rights Management	AC	A	X	B	X	A	X	B		A	X	B		A		A	
S & RM	Policies and Standards	Role Based Awareness		AC	X	A	A	X	X	A	A		X	A	A		A		A	
S & RM	Governance Risk & Compliance	Technical Awareness and Training		AT	X	X	B	X	X	X	B		X	X	B		A			
S & RM	Governance Risk & Compliance	Compliance Management		AU	X	X	B	X	X	X	B		X	X	B		X			
S & RM	Governance Risk & Compliance	Audit Management		AU	X	X	B	X	X	X	B		X	X	B		X			
S & RM	Threat and Vulnerability Management	Compliance Testing	Databases	AU	X	X	B	X	X	X	B		A	X	B		A			
			Servers	AU	X	X	B	X	A	X	B		A	X	B		A		A	
S & RM	Policies and Standards	Best Practices & Regulatory Correlation		CA	A	X	A	X	A	X	A		A	X	A		X		A	
S & RM	InfoSec Management	Capability Mapping		CM	X	X	B	X	X	X	B		X	X	B		X		A	
S & RM	Infrastructure Protection Services	Endpoint	Inventory Control	CM	X	A	B	X	A	X	B		A	X	B		A		A	
S & RM	Data Protection	Intellectual Property Prevention	Intellectual Property	CM	X	A	B	X	X	X	B		A	X	B		A		A	

S & RM	Policies and Standards	Operational Security Baselines		CM	A	A	A	A	A	A	A	A	A	A	A	A	A		A
	Policies and Standards	Job Aid Guidelines		CM	A	A	A	A	A	A	A	A	A	A	A	A	A		A
S & RM	Privilege Management Infrastructure	Identity Management	Domain Unique Identifier	IA	A	A	B	Ab	A	A	B	Ab	A	A	B	Ab	A		
S & RM	Privilege Management Infrastructure	Identity Management	Federated IDM	IA	X	A	B	X	X	A	B		A	X	B		A		
S & RM	Privilege Management Infrastructure	Identity Management	Identity Provisioning	IA	X	A	B	X	X	A	B		X	X	B		A		
S & RM	Privilege Management Infrastructure	Identity Management	Attribute Provisioning	IA	X	A	B	X	X	A	B		X	X	B		A		
S & RM	Privilege Management Infrastructure	Authorization Services	Policy Enforcement	IA	X	A	B	X	X	A	B		X	X	B		A		
S & RM	Privilege Management Infrastructure	Authorization Services	Policy Definition	IA	X	A	B	X	X	A	B		X	X	B		A		
S & RM	Privilege Management Infrastructure	Authorization Services	Principal Data Mgmt	IA	X	A	B	X	X	A	B		X	X	B		A		
S & RM	Privilege Management Infrastructure	Authorization Services	XACML	IA	A	X	B	X	A	X	B		A	X	B		A		
S & RM	Privilege Management Infrastructure	Authorization Services	Role Management	IA	X	X	B	X	X	X	B		X	X	B		A		

S & RM	Privilege Management Infrastructure	Authorization Services	Oligation	IA		A	X	B	X		A	X	B			A	X	B			A		
S & RM	Privilege Management Infrastructure	Authorization Services	Out of the Box (OTB) Auth	IA		X	X	B	X		A	X	B			A	X	B			A		
S & RM	Privilege Management Infrastructure	Authentication Services	SAML Token	IA		A	X	B	X		A	X	B			A	X	B			A		
S & RM	Privilege Management Infrastructure	Authentication Services	Risk-Based Auth	IA		X	X	B	X		X	X	B			X	X	B			A		
S & RM	Privilege Management Infrastructure	Authentication Services	Multifactor	IA		X	X	B	X		X	X	B			A	X	B			A		
S & RM	Privilege Management Infrastructure	Authentication Services	OTP	IA		A	X	B	X		A	X	B			A	X	B			A		
S & RM	Privilege Management Infrastructure	Authentication Services	Smart Card	IA		X	A	B	X		X	A	B			A	X	B			A		
S & RM	Privilege Management Infrastructure	Authentication Services	Password Management	IA		X	X	B	X		X	X	B			X	X	B			A		
S & RM	Privilege Management Infrastructure	Authentication Services	Biometrics	IA		X	A	B	X		X	A	B			X	X	B			A		
S & RM	Privilege Management Infrastructure	Authentication Services	Network Authentication	IA		X	X	B	X		A	X	B			A	X	B			X		
S & RM	Privilege Management	Authentication Services	Single Sign On	IA		A	X	B	X		A	X	B			A	X	B			A		

Commented [KS51]: Should this be "Obligation"?

	Infrastructure																						
S & RM	Privilege Management Infrastructure	Authentication Services	WS-Security	IA	X	X	B	X	X	X	B		A	X	B		A						
S & RM	Privilege Management Infrastructure	Authentication Services	Middleware Auth	IA	X	X	B	X	X	X	B		A	X	B		A						
S & RM	Privilege Management Infrastructure	Authentication Services	Identity Verification	IA	X	X	B	X	X	X	B		X	X	B		A						
S & RM	Privilege Management Infrastructure	Authentication Services	Out-of-The-Box (OTB) Auth	IA	X	X	B	X	X	X	B		A	X	B		A						
S & RM	Privilege Management Infrastructure	Privilege Usage Management	Keystroke/ Session Logging	IA	X	X	B	X	X	X	B		X	X	B		A						
S & RM	Privilege Management Infrastructure	Privilege Usage Management	Password Vaulting	IA	X	X	B	X	X	X	B		A	X	B		X						
S & RM	Threat and Vulnerability Management	Compliance Testing	Network Authentication	IA	X	X	B	X	X	X	B		A	X	B		X		A				
S & RM	Infrastructure Protection Services	Endpoint	Forensic Tools	IR	X	A	B	X	X	A	B		X	X	B		A		A				
S & RM	Infrastructure Protection Services	Endpoint	Media Lockdown	MP	A	X	B	X	A	X	B		A	X	B		X		A				
S & RM	InfoSec Management	Residual Risk Management		PL	X	A	B	X	X	X	B		A	X	B		A						
S & RM	Governance Risk & Compliance	Policy Management	Exceptions	RA	X	X	B	X	X	X	B		X	X	B		X		A				

S & RM	Governance Risk & Compliance	Policy Management	Self Assessment	RA	X	A	B	X		X	A	B			X	A	B			X		A
S & RM	InfoSec Management	Risk Dashboard		RA	X	X	B	X		X	X	B			X	X	B			A		
S & RM	Threat and Vulnerability Management	Vulnerability Management	Application	RA	X	X	B	X		X	X	B			A	X	B			A		A
			Infrastructure	RA	X	X	B	X		A	X	B			A	X	B			A		A
			DB	RA	X	X	B	X		X	X	B			A	X	B			A		A
		Penetration Testing	Internal	RA	X	A	B	X		X	X	B			A	X	B			A		A
			External	RA	X	X	B	X		X	X	B			A	X	B			A		A
		Threat Management	Source Code Scanning	RA	X	X	B	X		X	X	B			X	X	B			A		A
			Risk Taxonomy	RA	X	A	B	X		X	X	B			X	X	B			A		
S & RM	Policies and Standards	Data/ Asset Classification		RA	X	X	A	X		X	X	A			X	X	A			A		A
S & RM	Governance Risk & Compliance	Vendor Management		SA	X	X	B	X		X	X	B			X	X	B			A		A
S & RM	Data Protection	Data Lifecycle Management	Lifecycle Management	SA	X	X	B	X		X	X	B			X	X	B			A		A
S & RM	Policies and Standards	Technical Security Standards		SA	X	X	A	X		X	X	A			X	X	A			X		A
S & RM	Privilege Management Infrastructure	Privilege Usage Management	Resource Protection	SC	A	X	B	X		A	X	B			A	X	B			X		
S & RM	Infrastructure Protection Services	Network	Deep Packet Inspection (DPI)	SC	X	X	B	X		A	X	B			A	X	B			X		A
S & RM	Infrastructure Protection Services	Network	Wireless Protection	SC	A	X	B	X		A	X	B			A	X	B			X		A

S & RM	Infrastructure Protection Services	Network	Link Layer Network Security	SC	A	X	B	X	A	X	B		A	X	B		X		A
S & RM	Infrastructure Protection Services	Application	XML Appliance	SC	X	A	B	X	X	X	B		A	X	B		A		A
S & RM	Infrastructure Protection Services	Application	Secure Messaging	SC	X	A	B	X	X	A	B		A	X	B		A		A
S & RM	Data Protection	Data Lifecycle Management	Data De-Identification	SC	X	A	B	X	X	X	B		X	X	B		A		A
S & RM	Data Protection	Data Lifecycle Management	Data Masking	SC	X	A	B	X	X	X	B		X	X	B		A		A
S & RM	Data Protection	Data Lifecycle Management	Data Tagging	SC	X	A	B	X	X	X	B		A	X	B		A		A
S & RM	Data Protection	Data Lifecycle Management	Data Obscuring	SC	X	A	B	X	X	X	B		X	X	B		A		A
S & RM	Data Protection	Data Leakage Prevention	Data Discovery	SC	X	A	B	X	X	X	B		X	X	B		A		A
S & RM	Data Protection	Data Leakage Prevention	Network (Data in Transit)	SC	X	X	B	X	X	X	B		A	X	B		A		A
S & RM	Data Protection	Data Leakage Prevention	Endpoint (Data in Use)	SC	X	X	B	X	X	X	B		X	X	B		A		A
S & RM	Data Protection	Data Leakage Prevention	Server (Data at Rest)	SC	X	X	B	X	X	X	B		A	X	B		A		A
S & RM	Cryptographic Services	Key Management	Symmetric Keys	SC	X	X	B	X	X	X	B		X	X	B		X		A
S & RM	Cryptographic Services	Key Management	Asymmetric Keys	SC	X	X	B	X	X	X	B		X	X	B		X		A
S & RM	Cryptographic Services	PKI		SC	X	X	B	X	X	X	B		X	X	B		X		A

S & RM	Cryptographic Services	Data in Use (memory) Encryption		SC	X	X	B	X	X	X	B		A	X	B		X		A
S & RM	Cryptographic Services	Data in Transit Encryption (Transitory, Fixed)		SC	X	X	B	X	X	X	B		X	X	B		X		A
S & RM	Cryptographic Services	Data at Rest Encryption (DB, File, SAN, Desktop, Mobile)		SC	X	X	B	X	X	X	B		X	X	B		A		A
S & RM	Infrastructure Protection Services	Server	Anti-virus	SI	X	X	B	X	X	X	B		A	X	B		A		
S & RM	Infrastructure Protection Services	Server	HIPS/HIDS (Intrusion Protection /Detection)	SI	X	X	B	X	A	X	B		A	X	B		A		
S & RM	Infrastructure Protection Services	Endpoint	Anti-Virus, Anti-Spam, Anti-Malware	SI	X	A	B	X	X	A	B		A	X	B		A		
S & RM	Infrastructure Protection Services	Endpoint	HIPS/HIDS (Intrusion Protection /Detection)	SI	X	A	B	X	X	X	B		A	X	B		A		A
S & RM	Infrastructure Protection Services	Endpoint	Hardware-Based Trusted Assets	SI	A	X	B	X	A	X	B		A	X	B		X		A
S & RM	Infrastructure Protection Services	Network	NIPS/NIDS	SI	X	X	B	X	A	X	B		A	X	B		X		A
S & RM	Data Protection	Data Lifecycle Management	eSignature	SI	X	A	B	X	X	X	B		X	X	B		A		A
S & RM	Cryptographic Services	Signature Services		SI	X	X	B	X	X	X	B		X	X	B		X		A
S & RM	Governance Risk & Compliance	IT Risk Management		PM	X	X	B	X	X	X	B		X	X	B		X		A

S & RM	InfoSec Management	Risk Portfolio Management		PM	A	A	B	Ab	A	A	B	Ab	A	A	B	Ab	A		
S & RM	Privilege Management Infrastructure	Authorization Services	Policy Management	PM	X	A	B	X	X	A	B		X	X	B		A		
S & RM	Privilege Management Infrastructure	Authorization Services	Resource Data management	PM	X	A	B	X	X	A	B		X	X	B		A		
S & RM	Policies and Standards	Information Security Polices		PM	A	A	A	A	A	A	A	A	A	A	A	A	A		A

12 ANNEX E: MAPPING OF THE ARCHITECTURAL COMPONENTS

Commented [KS52]: I need to confirm all names. Reformat bullets and indentations?

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

Table 6: Cloud Actors' Architectural Components

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

			CONSUMER					PROVIDER						BROKER								CARRIER	AUDITOR
			B	C	I	O	L	B	C	I	L	R	P	B	C	I	L	aC	aI	cA	cI		
Infrastructure Services	**Virtual Infrastructure:** Database Virtualization			C	I				C	I	L	R											
Infrastructure Services	**Virtual Infrastructure**: Mobile Device Virtualization			C	I				C	I	L	R											
Infrastructure Services	**Virtual Infrastructure:** Smartcard Virtualization			C	I				C	I	L	R											
S & RM	Privilege Management Infrastructure	Privilege Usage Management		C					C	I	L											T	
S & RM	Infrastructure Protection Services	Network					L			I	L				C							T	E
S & RM																							
S & RM																							
S & RM	Infrastructure Protection Services	Application					L		C	I	L												E
S & RM																							
S & RM	Data Protection	Data Lifecycle Management					L	B	C	I	L		P										E
S & RM																							
S & RM																							
S & RM																							
S & RM	Data Protection	Data Leakage Prevention					L		C	I	L		P		C								E
S & RM																							
S & RM																							
S & RM																							

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

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

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

			CONSUMER					PROVIDER						BROKER								CARRIER	AUDITOR
			B	C	I	O	L	B	C	I	L	R	P	B	C	I	L	aC	aI	cA	cI		
ITOS	IT Operations	PMO	B						C	I			P	B									E
ITOS																							
ITOS																							
ITOS	IT Operations	Portfolio Management	B	C	I		L		C				P										
ITOS																							
ITOS	Service Delivery	Service Level Management	B					B	C	I	L											T	E
ITOS																							
ITOS																							
ITOS																							
ITOS																							
ITOS																							
ITOS	Service Delivery	Asset Management	B	C	I			B	C														
ITOS																							
ITOS	Service Support	Problem Management & Knowledge Management	B	C				B	C		L		P									T	
ITOS																							
Information Services	Service Delivery	Contracts	B					B	C					B									
Information Services	ITOS	Program Management (PMO), Strategy & Roadmap				O			C					B									
Information Services																							
Information Services																							
Information Services	ITOS	Knowledge & Service Management				O			C		L			B									
Information Services																							

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

13 ANNEX F: ECOSYSTEM ORCHESTRATION - SECURITY INDEX SYSTEM

13.1 USE CASE SUMMARY

Services Covered:	Featured Deployment and Service Models:
• Broker cloud secure service provisioning • Broker cloud secure service status and metrics • Broker cloud secure service control and management • Identity management between Broker and Provider • Continuous monitoring status between Broker and 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 Providers returned in aggregation (minimum requirement) • Broker-based business integration with Providers for secure account creation and credential acquisition (advanced capability) • Broker-based arbitrage models capable of approximating 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 Provider to Provider (advanced capability)	• All deployment models • All service models

Actors:	**Systems:**
• Consumer • A marketplace or ecosystem of at least two and typically many Providers • Broker	• Broker secure provisioning system • Broker continuous monitoring system • Broker identity management • Broker APIs to each Provider • Provider identity management, provisioning and monitoring systems, secure access by Broker • Broker identity management system with Consumer-facing integration capabilities • Broker secure orchestration system with cross-Provider secure orchestration capabilities • Broker-based continuous monitoring offering an integrated view across multiple Providers • Broker-based secure reporting offering an integrated view across multiple Providers • Broker model for gathering Consumer business, technical, and policy/security parameters • Broker model for rating and ranking Provider capabilities in a consistent and meaningful manner • Broker system to deliver rankings to Consumers • Business transaction systems between Broker and Providers • Automated service selection systems between Broker and Consumers
Notable Services: Broker to Provider secure business interfaces Combined cloud secure service business and technical brokerage Advanced arbitrage and decision support systems Cross-Provider services for automated or semi-automated workload migration	

Dependencies:

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

Assumptions:

- Consumer has a primary financial and secure service relationship with each Provider. Broker role manages but does not own the relationship with the Provider in this use case.
- Consumer has accepted risks of Broker-based secure access to Providers
- Broker may be in cloud, virtual, or traditional environment. 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 Provider secure capabilities, secure policies, and costs
- Broker has no operational relationship with Providers 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 Provider information
- Consumer has a primary financial and secure service relationship with the Broker but does not necessarily have a business relationship with any particular Provider at any point in time. Consumer to Provider business relationships fall outside the scope of this use case.
- Provider and Broker automated secure business interfaces
- Standards sufficient to support workload migration across Providers
- Advanced decision or decision support systems to drive technical brokerage from arbitrage

13.2 SECURITY INDEX SYSTEM

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

BOSS	Operational Risk Management	Crisis Management		IR	1.00	2.00	1.00	4.00
BOSS	Operational Risk Management	Risk Management Framework		IR	1.00	2.00	2.00	5.00
BOSS	Operational Risk Management	Independent Risk Management		IR	1.00	2.00	2.00	5.00
BOSS	Security Monitoring Services	Database Monitoring		IR	2.00	3.00	3.00	8.00
BOSS	Security Monitoring Services	Application Monitoring		IR	2.00	3.00	3.00	8.00
BOSS	Security Monitoring Services	Endpoint 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	IT Resiliency	Resiliency Analysis	AU	1.00	0.00	2.00	3.00
ITOS	Service Delivery	IT 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	CM	1.00	1.00	2.00	4.00
ITOS	Service Delivery	Asset Management	Change Back	CM	1.00	1.00	1.00	3.00
ITOS	Service Support	Configuration Management	Software Management	CM	1.00	1.00	2.00	4.00
ITOS	Service Support	Configuration Management	Configuration Management	CM	2.00	3.00	3.00	8.00
ITOS	Service Support	Configuration Management	Physical Inventory	CM	1.00	1.00	2.00	4.00
ITOS	Service Support	Knowledge Management	Benchmarking	CM	1.00	2.00	1.00	4.00
ITOS	Service Support	Knowledge Management	Security Job Aids	CM	1.00	2.00	1.00	4.00
ITOS	Service Support	Knowledge Management	Security FAQ	CM	1.00	2.00	1.00	4.00
ITOS	Service Support	Change Management	Service Provisioning	CM	1.00	2.00	1.00	4.00

Commented [KS53]: Split these cells?

ITOS	Service Support	Change Management	Approval Workflow	CM	1.00	2.00	1.00	4.00
ITOS	Service Support	Change Management	Change Review Board	CM	1.00	2.00	2.00	5.00
ITOS	Service Support	Change Management	Planned Changes	CM	1.00	1.00	2.00	4.00
ITOS	Service Support	Release Management	Version Control	CM	1.00	3.00	2.00	6.00
ITOS	Service Support	Release Management	Source Code Management	CM	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 Response	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	IT Resiliency	Availability Management	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 Mgmt	PM	1.00	1.00	1.00	3.00
ITOS	IT Operations	PMO	Project Mgmt	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	Strategy 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	Endpoints	Mobile Devices	AC	3.00	1.00	3.00	7.00
Presentation Services	Presentation Platform	Endpoints	Fixed Devices	AC	3.00	1.00	3.00	7.00
Presentation Services	Presentation Platform	Endpoints	Desktops	AC	3.00	1.00	3.00	7.00
Presentation Services	Presentation Platform	Endpoints	Portable Devices	AC	3.00	1.00	3.00	7.00
Presentation Services	Presentation Platform	Endpoints	Medical Devices	AC	3.00	1.00	3.00	7.00
Presentation Services	Presentation Platform	Endpoints	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		CM	2.00	2.00	2.00	6.00
Application Services	Connectivity & Delivery			CM	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		CM	0.00	1.00	0.00	1.00
Information Services	Service Delivery	SLAs		CM	1.00	2.00	1.00	4.00
Information Services	ITOS	CMDB		CM	3.00	4.00	4.00	11.00
Information Services	ITOS	Change Management		CM	2.00	3.00	3.00	8.00
Information Services	Service Support	Configuration Rules (Metadata)		CM	2.00	2.00	2.00	6.00
Information Services	Service Support	Configuration Management Database (CMDB)		CM	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	ACLs		IA	3.00	3.00	3.00	9.00
Information Services	Security Monitoring	CRLs		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	OLAs		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	Infrastructure Protection Services	Server	White Listing	AC	3.00	1.00	2.00	6.00
S & RM	Infrastructure Protection Services	Server	Host Firewall	AC	3.00	2.00	3.00	8.00
S & RM	Infrastructure Protection Services	Endpoint	Host Firewall	AC	3.00	2.00	3.00	8.00
S & RM	Infrastructure Protection Services	Endpoint	Content Filtering	AC	3.00	1.00	2.00	6.00
S & RM	Infrastructure Protection Services	Endpoint	Whitelisting	AC	3.00	2.00	3.00	8.00
S & RM	Infrastructure Protection Services	Network	Content Filtering	AC	3.00	1.00	2.00	6.00
S & RM	Infrastructure Protection Services	Network	Firewall	AC	3.00	3.00	4.00	10.00
S & RM	Infrastructure Protection Services	Network	Blacklisting Filtering	AC	3.00	1.00	2.00	6.00
	Infrastructure Protection Services	Application	Application Firewall	AC	3.00	3.00	4.00	10.00
S & RM	Infrastructure Protection Services	Application	Secure Collaboration	AC	3.00	2.00	3.00	8.00
S & RM	Infrastructure Protection Services	Application	Real-Time Filtering	AC	3.00	2.00	3.00	8.00
S & RM	Infrastructure Protection Services	Data Lifecycle Management	Metadata Control	AC	3.00	1.00	1.00	5.00
S & RM	Data Protection	Data Lifecycle Management	Data Seeding	AC	2.00	0.00	1.00	3.00
S & RM	Data Protection	Intellectual Property Prevention	Digital Rights Management	AC	3.00	1.00	2.00	6.00
S & RM	Policies and Standards	Role Based Awareness		AC	2.00	2.00	2.00	6.00
S & RM	Governance Risk & Compliance	Technical Awareness and Training		AT	2.00	2.00	2.00	6.00
S & RM	Governance Risk & Compliance	Compliance Management		AU	1.00	2.00	1.00	4.00

S & RM	Governance Risk & Compliance	Audit Management		AU	1.00	1.00	1.00	3.00
S & RM	Threat and Vulnerability Management	Compliance Testing	Databases	AU	3.00	3.00	3.00	9.00
S & RM	Threat and Vulnerability Management	Compliance Testing	Servers	AU	3.00	3.00	3.00	9.00
S & RM	Policies and Standards	Best Practices & Regulatory correlation		CA	2.00	2.00	2.00	6.00
S & RM	InfoSec Management	Capability Mapping		CM	0.00	2.00	3.00	5.00
S & RM	Infrastructure Protection Services	Endpoint	Inventory Control	CM	1.00	2.00	1.00	4.00
S & RM	Data Protection	Intellectual Property Prevention	Intellectual Property	CM	1.00	2.00	1.00	4.00
S & RM	Policies and Standards	Operational Security Baselines		CM	1.00	2.00	2.00	5.00
S & RM	Policies and Standards	Job Aid Guidelines		CM	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 Mgmt	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) Auth	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	Endpoint	Forensic Tools	IR	2.00	2.00	2.00	6.00
S & RM	Infrastructure Protection Services	Endpoint	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	Lifecycle 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 Deidentification	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	Endpoint (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 at 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	Endpoint	Anti-Virus, Anti-Spam, Anti-Malware	SI	3.00	3.00	3.00	9.00
S & RM	Infrastructure Protection Services	Endpoint	HIPS/HIDS (Intrusion Protection /Detection)	SI	3.00	3.00	3.00	9.00
S & RM	Infrastructure Protection Services	Endpoint	Hardware Based trusted Assets	SI	2.00	2.00	1.00	5.00

S & RM	Infrastructure Protection Services	Network	NIPS/NIDS	SI		1.00	3.00	1.00	5.00
S & RM	Data Protection	Data Lifecycle Management	eSignature	SI		3.00	3.00	3.00	9.00
S & RM	Cryptographic Services	Signature Services		SI		3.00	4.00	3.00	10.00
S & RM	Governance Risk & Compliance	IT Risk Management		PM		1.00	2.00	1.00	4.00
S & RM	InfoSec Management	Risk Portfolio Management		PM		1.00	2.00	1.00	4.00
S & RM	Privilege Management Infrastructure	Authorization Services	Policy Management	PM		3.00	3.00	3.00	9.00

13.3 ASIS HEAT MAP