

NIST Cloud Computing Security Reference Architecture (SP 500-299 draft)

NIST Cloud Computing Security Working Group

Dr. Michaela Iorga, NIST

Senior Security Technical Lead for Cloud Computing

Chair, NIST Cloud Computing Security Working Group

Co-Chair, NIST Cloud Computing Forensic Science Working Group

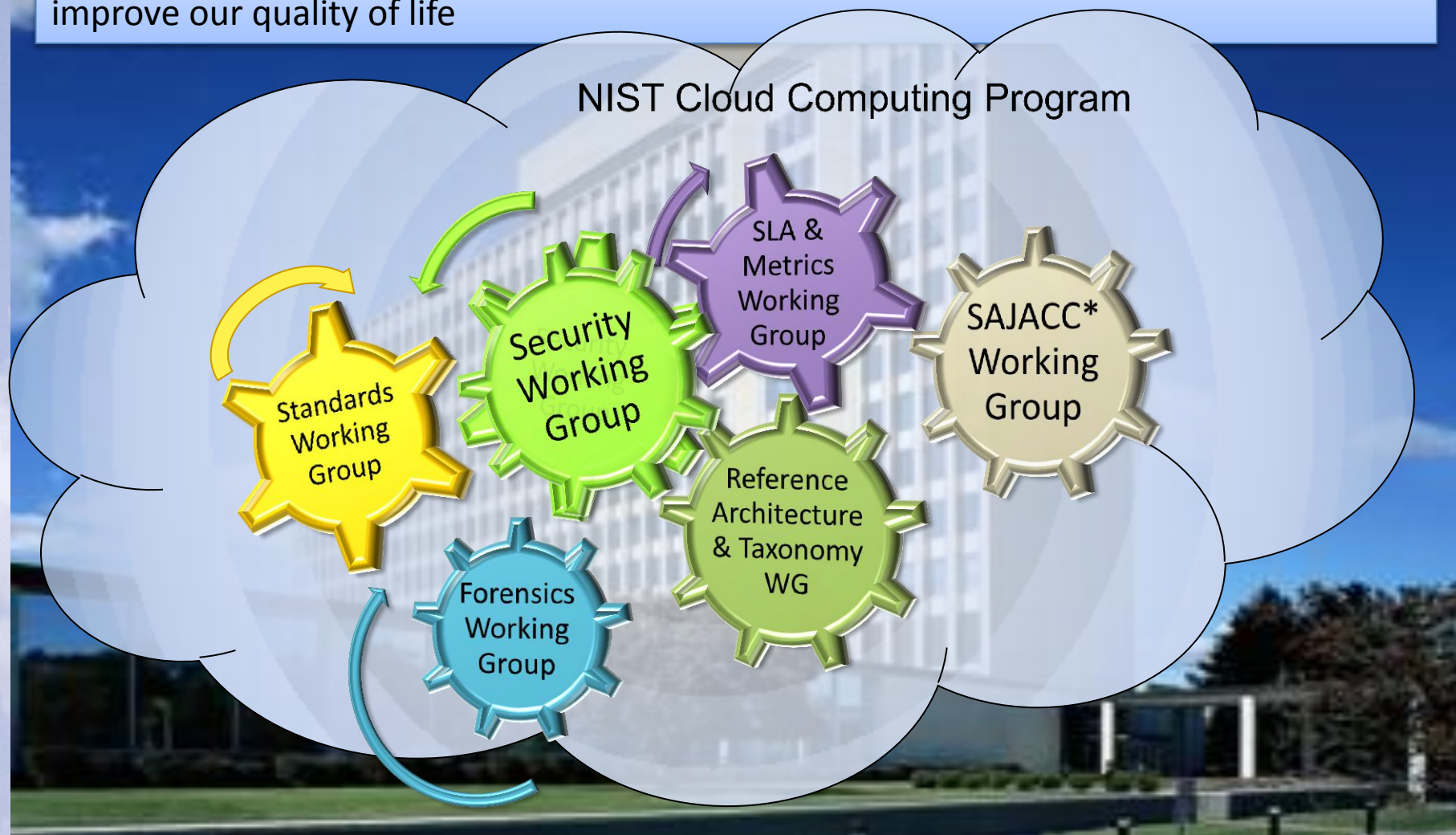
September 2013

NIST Cloud Computing Program Goal

- ***Accelerate the federal government's adoption of cloud computing***
 - ***Build*** a USG Cloud Computing Technology Roadmap which focuses on the highest priority USG cloud computing security, interoperability and portability requirements.
 - ***Lead*** efforts to develop standards and guidelines in close consultation and collaboration with standards bodies, the private sector, and other stakeholders.

NIST MISSION:

To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life



*Standards Acceleration to Jumpstart the Adoption of Cloud Computing (SAJACC) in transition to private sector

NIST - INFORMATION TECHNOLOGY LABORATORY - CLOUD COMPUTING PROGRAM

NIST Cloud Computing Special Publications

- CC Standards Roadmap500-291
- CC Reference Architecture.....500-292
- USG CC Technology Roadmap Draft.....500-293
- **CC Security Reference Architecture.....500-299**
- Guidelines on Security and Privacy800-144
- Definition of Cloud Computing800-145
- CC Synopsis & Recommendations.....800-146

Searchable as “NIST SP xxx-nnn”

NIST Cloud Computing Security Working Group

- *Do we need security (and privacy) in the cloud?*
- *How important is to address security issues?*
- *Is security different in a Cloud environment than a traditional IT system?*

NIST Cloud Computing Security Reference Architecture

Table of Contents

EXECUTIVE SUMMARY	10
1 INTRODUCTION	11
1.1 Background	11
1.2 Objectives	11
1.3 Structure of the Document	13
1.4 Using the Document	13
2 SECURITY REFERENCE ARCHITECTURE: OVERVIEW	15
2.1 Risk Management	15
2.2 Assumptions and Clarifications	16
2.2.1 Cloud Consumer	20
2.2.2 Cloud Provider	20
2.2.2.1 Intermediary Cloud Provider Example	21
2.2.3 Cloud Broker	22
2.2.3.1 Differentiating Business and Technical Broker Services	23
2.2.3.2 A Cloud Brokerage Example	24
2.2.4 Cloud Carrier	25
2.2.5 Cloud Auditor	25
2.2.6 Cloud Services and the Cloud Computing Ecosystem	26
2.2.7 Security Conservation Principle for a Cloud Ecosystem	27
2.3 Our Approach	29
3 SECURITY REFERENCE ARCHITECTURE: DATA	31
3.1 Data Collection	32
3.2 Data Aggregation and Validation	33
3.3 Deriving the Security Responsibilities for Intermediary Provider and Technical Broker	34
3.4 Mapping of Security Components to Security Control Families	35
3.5 Empirical Data Analysis and the Generic Heat Map	36
4 SECURITY REFERENCE ARCHITECTURE: THE FORMAL MODEL	41
4.1 The Formal Model Overview	41
4.2 Consumer - Architectural Components	44
4.2.1 Secure Cloud Consumption Management	45
4.2.1.1 Secure Business Support	45
4.2.1.2 Secure Configuration	45
4.2.1.3 Secure Portability / Interoperability	46
4.2.1.4 Secure Organizational Support	47
4.2.2 Secure Cloud Ecosystem Orchestration	47
4.2.2.1 Secure Functional Layer	48
4.3 Provider - Architectural Components	49
4.3.1 Secure Service Deployment	50
4.3.2 Secure Service Orchestration	50
4.3.2.1 Secure Service Layer	51
4.3.2.2 Secure Resource Allocation and Control Layer	54
4.3.2.3 Secure Physical Resource Layer	55
4.3.3 Secure Cloud Service Management	55
4.3.3.1 Secure Business Support	56
4.3.3.2 Secure Provisioning and Configuration	57
4.3.3.3 Secure Portability and Interoperability	57

NIST Security Reference Architecture

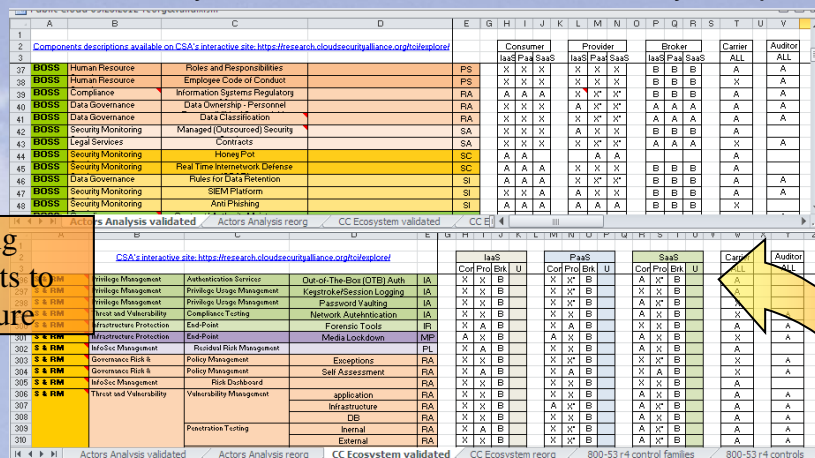
Risk Management Framework (SP 800-37, Rev. 1)

- Step 1: Categorize Information System
- Step 2: Select Security Controls
- Step 3: Implement Security Controls
- Step 4: Assess Security Controls
- Step 5: Authorize Information System
- Step 6: Monitor Security Controls (Repeat process as necessary)

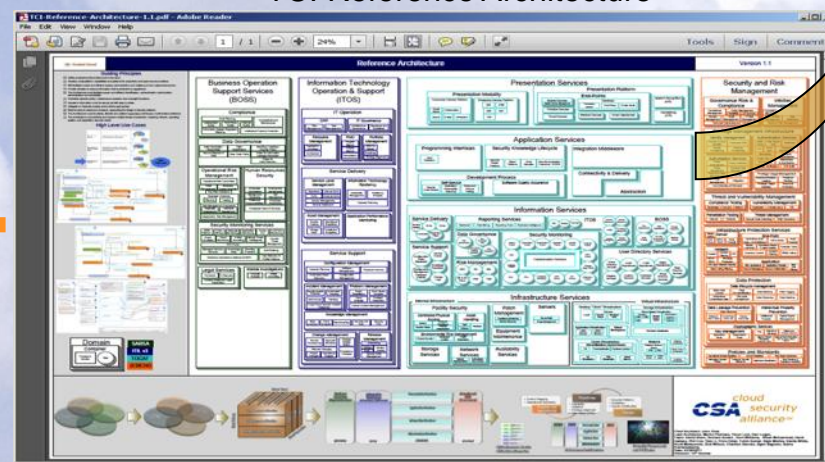
Cloud-adapted Risk Management Framework :

- Step 1: Categorize Application/System to be migrated
- Step 2: Identify Security Requirements, perform a **Risk Assessment** to identify **Security Components (CIA analysis)** & select Security Controls
- Step 3: Select best-fitting Architecture for the System
- Step 4: Assess Service Provider(s)
- Step 5: Approve Use of Service
- Step 6: Monitor Service Provider

NIST Security Reference Architecture – security components



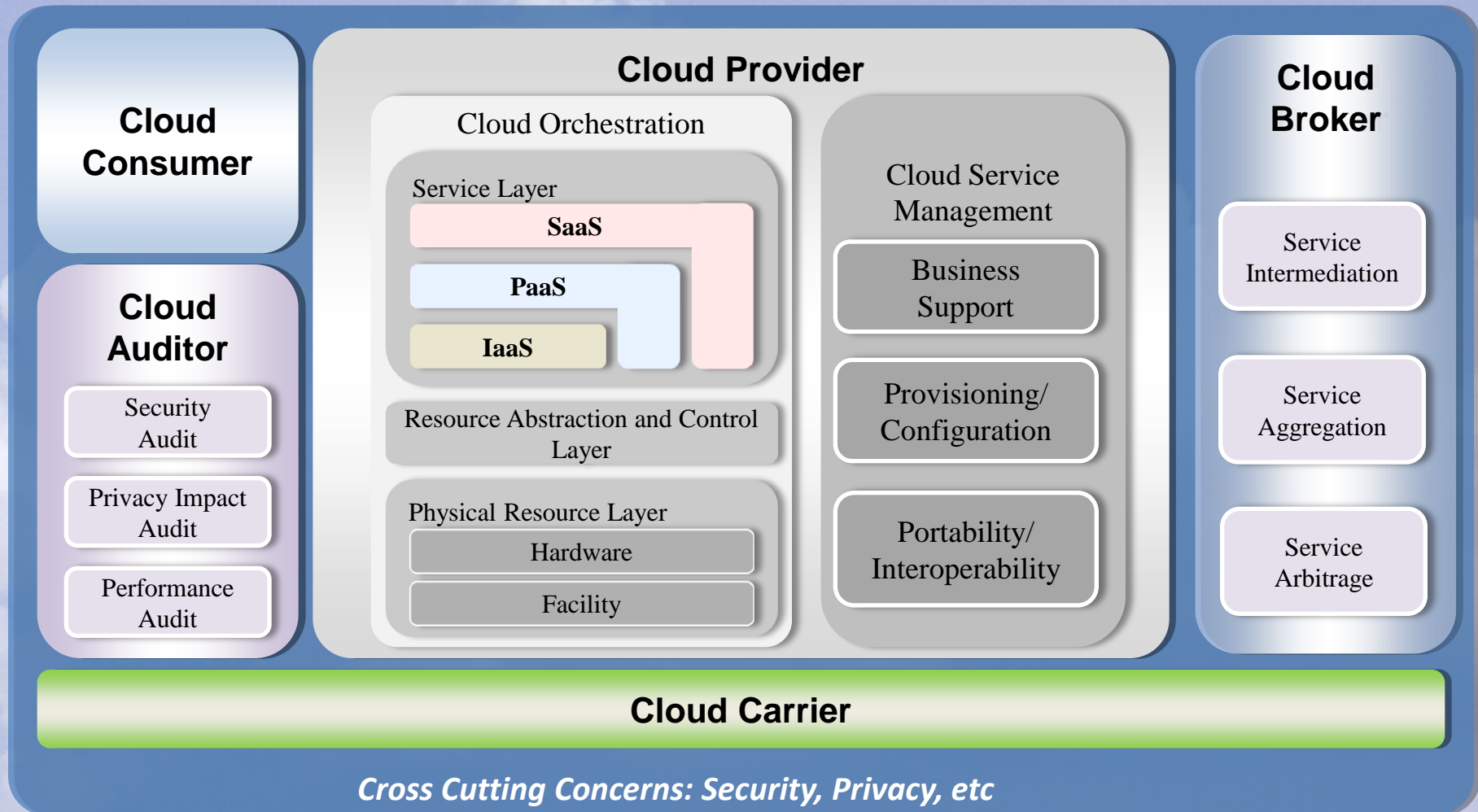
TCI Reference Architecture



NIST CC Reference Architecture (SP 500-292)

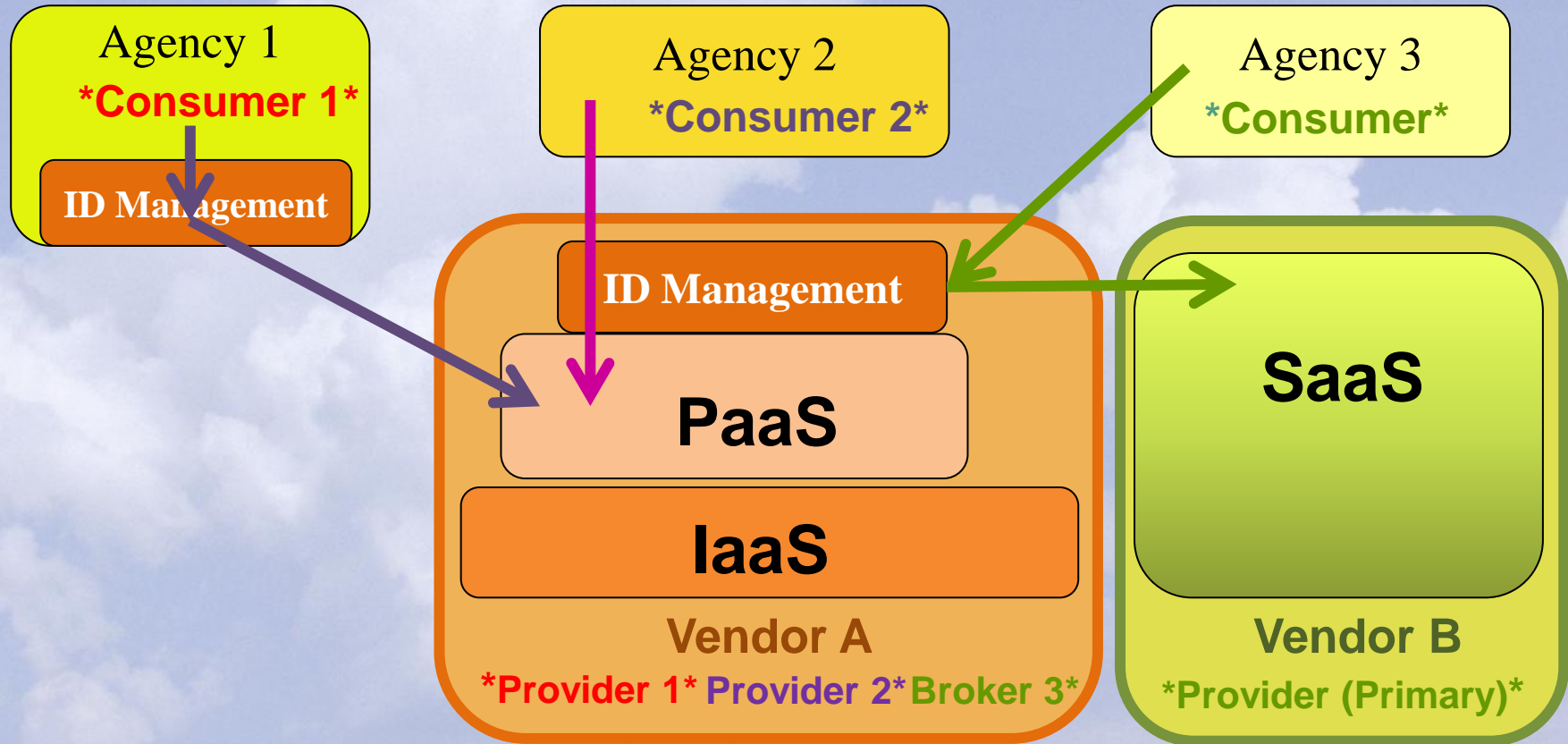
9

with Cross Cutting Concerns shown

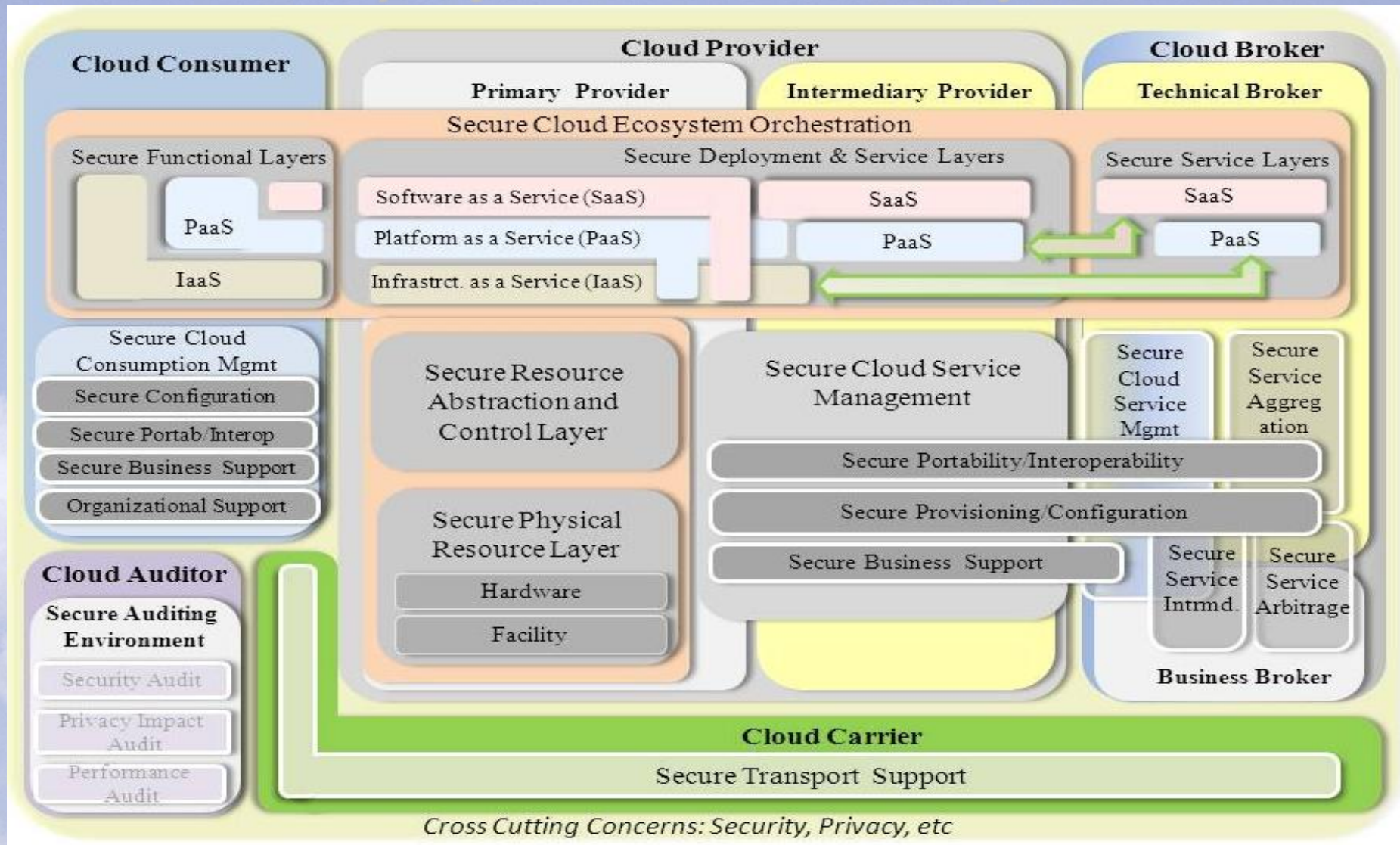


NIST Security Reference Architecture

NIST Reference Architecture <-> Business Models



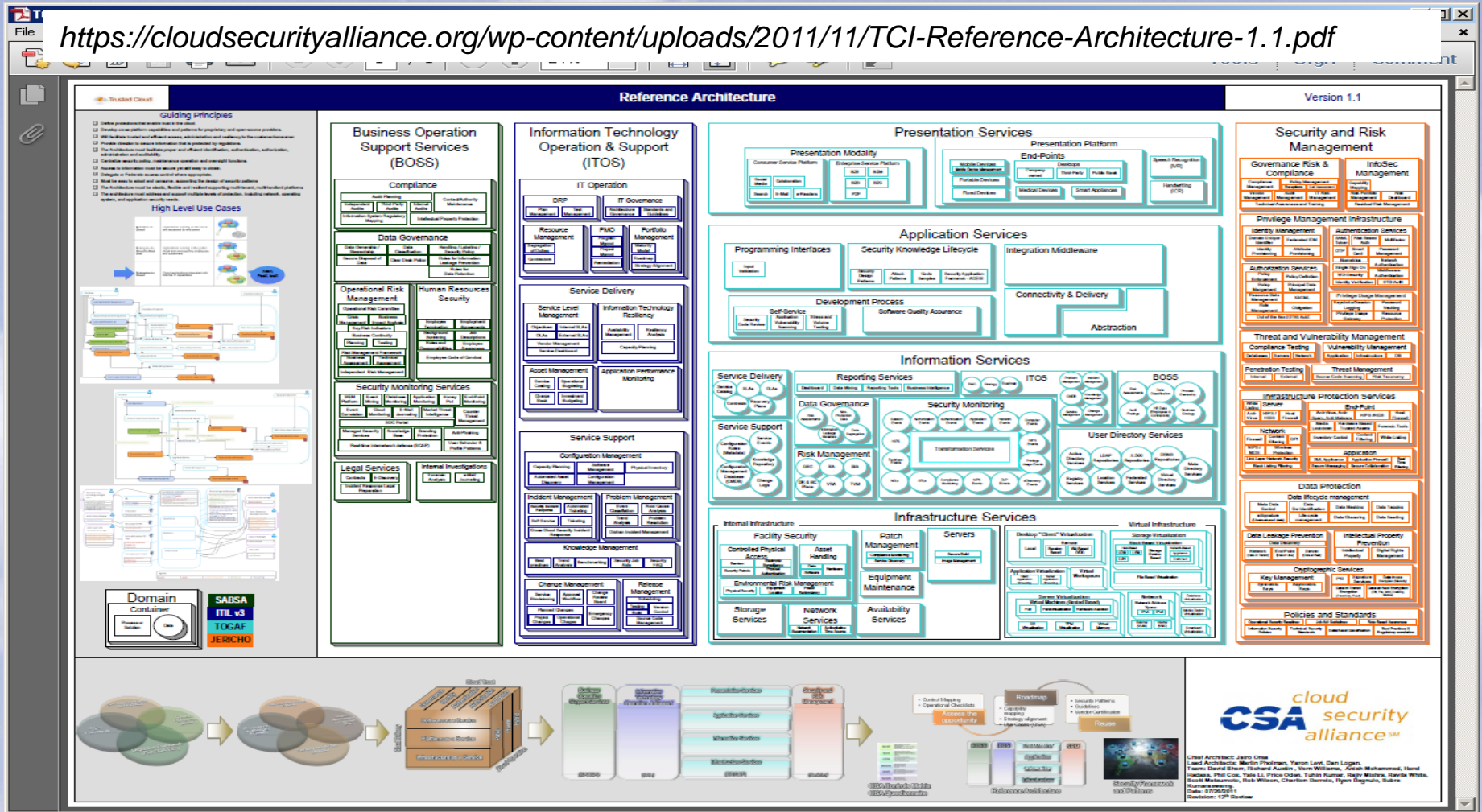
NIST Security Reference Architecture – formal model



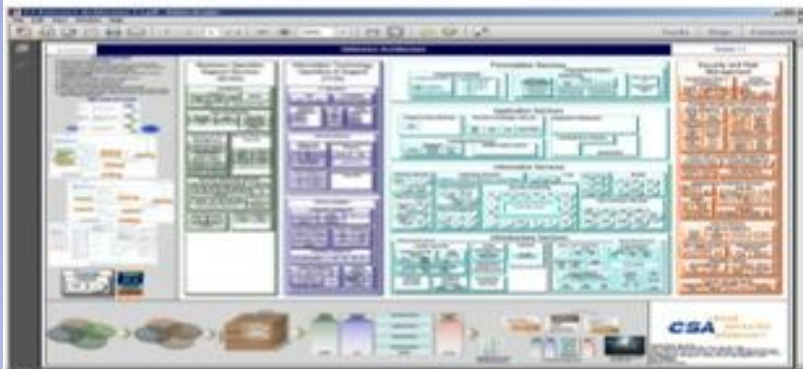
NIST Security Reference Architecture

- NCC SWG leverages on Cloud Security Alliance's **Trusted Cloud Initiative - Reference Architecture**

<https://cloudsecurityalliance.org/wp-content/uploads/2011/11/TCI-Reference-Architecture-1.1.pdf>



TCI Reference Architecture



NIST Reference Architecture



High-level component (1.1)	Mid-level component (2.1)	Low-level component (3.1)	Basic-level component (4.1)	Cloud Extensions	Cloud Provider	Cloud Broker	Cloud Carrier	Cloud Auditor
1.1.1	Compliance	Audit Planning						
1.1.2	Compliance	Independent Audit						
1.1.3	Compliance	Third-Party Audit						
1.1.4	Compliance	Internal Audit						
1.1.5	Compliance	Contract/Auditor						
1.1.6	Compliance	Information Systems						
1.1.7	Compliance	Regulatory Mapping						
1.1.8	Compliance	Intellectual Property Protection						
1.1.9	Data Governance	Data Ownership/Responsibility						
1.1.10	Data Governance	Data Classification						
1.2.1	IT Operations	DRP	Plan Management					
1.2.2	IT Operations	DRP	Plan Management					
1.2.3	IT Operations	IT Governance	Architecture Governance					
1.2.4	IT Operations	IT Governance	Standards and Guidelines					
1.2.5	IT Operations	Resource Management	Segregation of Duties					
1.2.6	IT Operations	Resource Management	Cost Allocation					

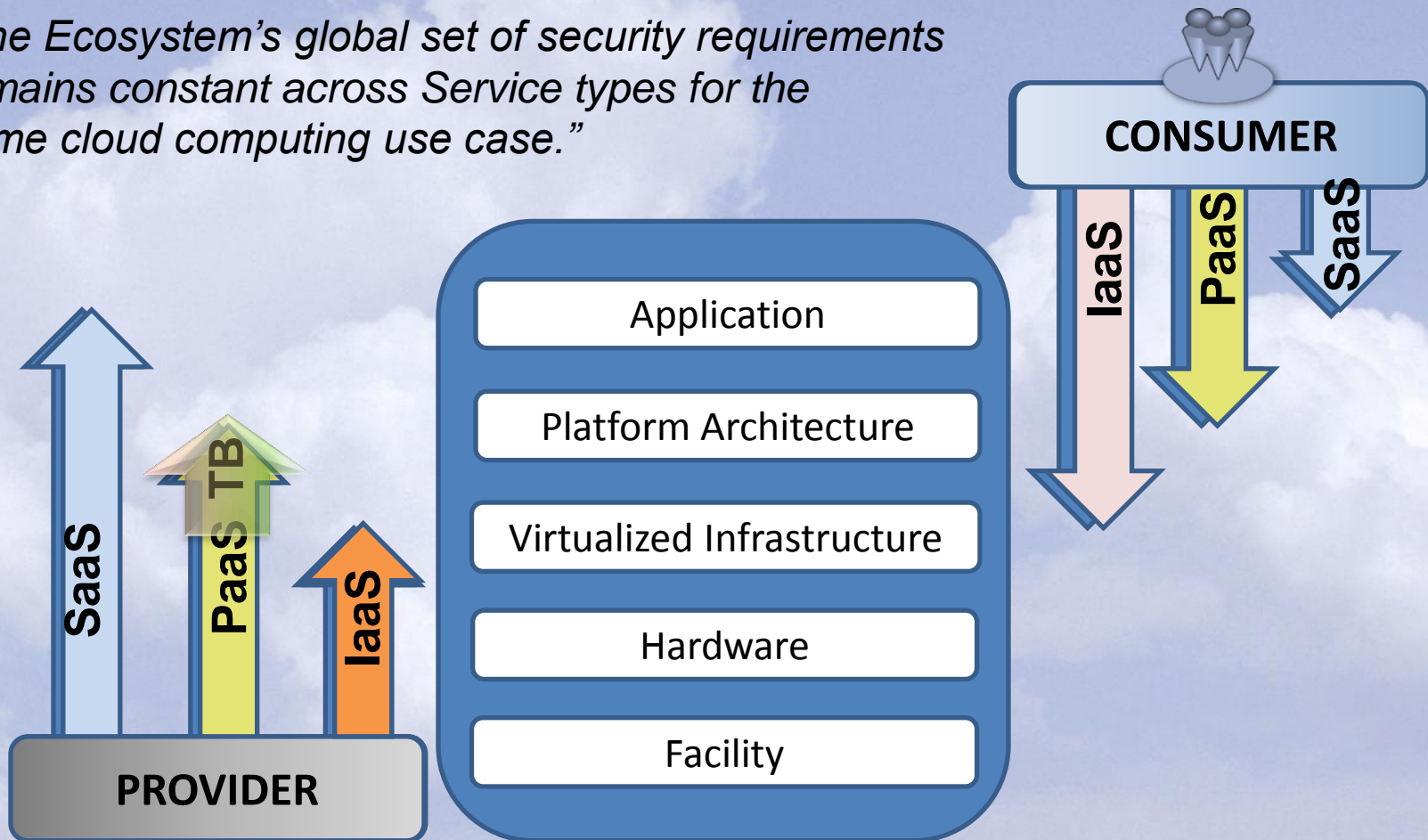
NIST SRA – data collection form with security components

Components identified in the NIST SRA									
Component	Category	Sub-category	Priority	Impact	Frequency	Severity	Complexity	Time	Cost
1.1.1	Compliance	Audit Planning	High	High	High	High	High	High	High
1.1.2	Compliance	Independent Audit	High	High	High	High	High	High	High
1.1.3	Compliance	Third-Party Audit	High	High	High	High	High	High	High
1.1.4	Compliance	Internal Audit	High	High	High	High	High	High	High
1.1.5	Compliance	Contract/Auditor	High	High	High	High	High	High	High
1.1.6	Compliance	Information Systems	High	High	High	High	High	High	High
1.1.7	Compliance	Regulatory Mapping	High	High	High	High	High	High	High
1.1.8	Compliance	Intellectual Property Protection	High	High	High	High	High	High	High
1.1.9	Data Governance	Data Ownership/Responsibility	High	High	High	High	High	High	High
1.1.10	Data Governance	Data Classification	High	High	High	High	High	High	High
1.2.1	IT Operations	DRP	High	High	High	High	High	High	High
1.2.2	IT Operations	DRP	High	High	High	High	High	High	High
1.2.3	IT Operations	IT Governance	High	High	High	High	High	High	High
1.2.4	IT Operations	IT Governance	High	High	High	High	High	High	High
1.2.5	IT Operations	Resource Management	High	High	High	High	High	High	High
1.2.6	IT Operations	Resource Management	High	High	High	High	High	High	High

NIST SRA – aggregated security components

Security Conservation Principle

“The Ecosystem’s global set of security requirements remains constant across Service types for the same cloud computing use case.”



NIST Security Reference Architecture – data analysis

[AX AX AX] => 3.0
 [XX AX AX] => 2.5
 [XA AX AX] => 2.0
 [XX XX AX] => 2.0
 [XA XX AX] => 1.5
 [XX XX XX] => 1.5
 [XA XA AX] => 1.0
 [XA XX XX] => 1.0
 [XA XA XX] => 0.5
 [XA XA XA] => 0.0
 AA AA AA => admin only
 Null cells

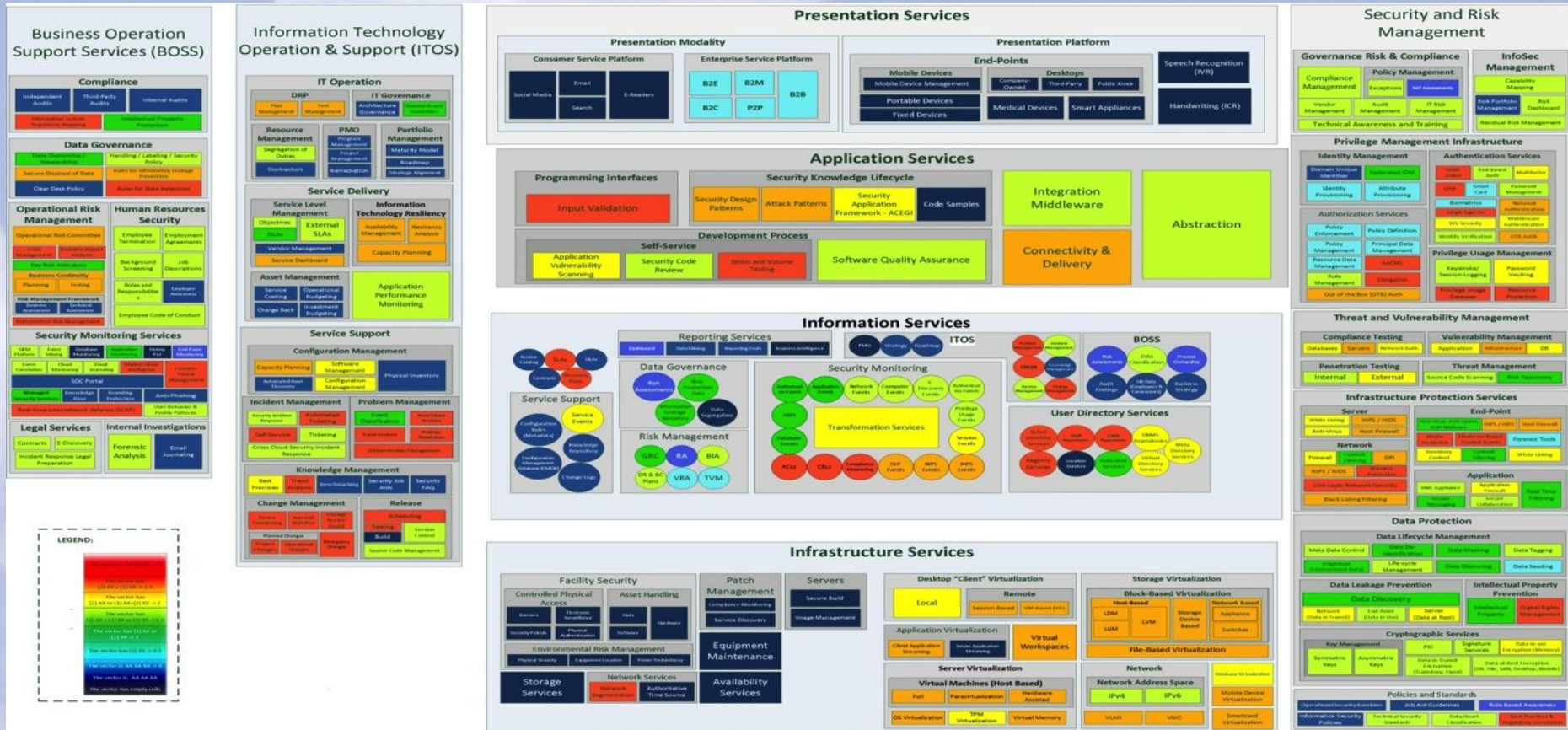
The vector is: AX AX AX -> 3
The vector has (2) AX + (1) XX -> 2.5
The vector has (2) AX or (1) AX+(2) XX -> 2
The vector has (1) AX + (1) XX or (3) XX -> 1.5
The vector has (1) AX or (2) XX -> 1
The vector has (1) XX -> 0.5
The vector is: XA XA XA -> 0
The vector is: AA AA AA
The vector has empty cells

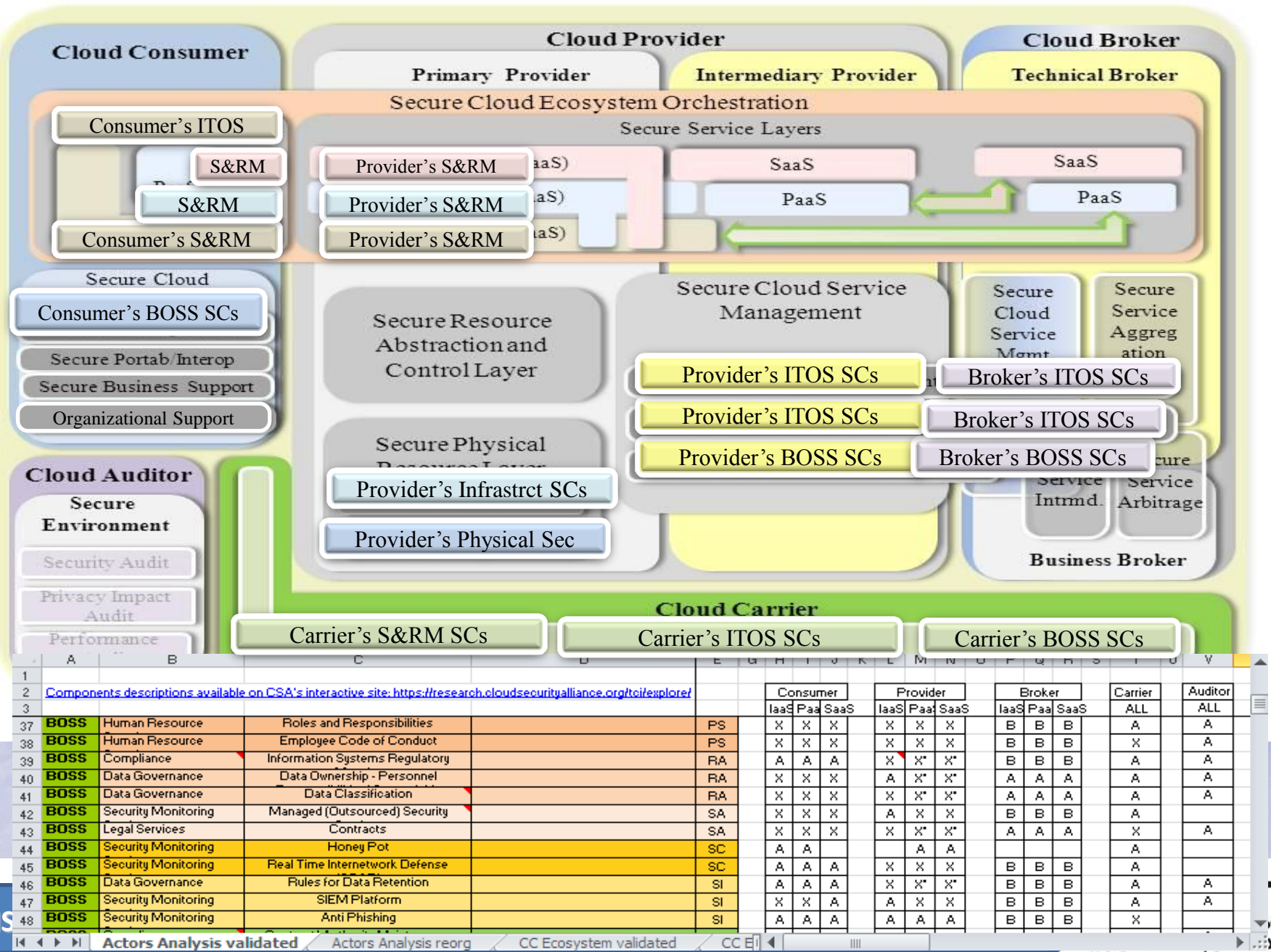
	A	B	C	D	E	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC
1																												
2																												
3																												
13	BOSS	Internal Investigations	Forensic Analysis		AU																							
20	BOSS	Internal Investigations	e-Mail Journaling		AU																							
21	BOSS	Compliance	Independent Audit		CA																							
22	BOSS	Compliance	Third Party Audit		CA																							
23	BOSS	Operational Risk	Business Impact Analysis		CP																							
24	BOSS	Operational Risk	Business Continuity		CP																							
25	BOSS	Operational Risk	Crisis Management		IR																							
26	BOSS	Operational Risk	Risk Management Framework		IR																							
27	BOSS	Operational Risk	Independent Risk		IR																							
28	BOSS	Security Monitoring	Database Monitoring		IR																							
29	BOSS	Security Monitoring	Application Monitoring		IR																							
30	BOSS	Security Monitoring	End-Point Monitoring		IR																							
31	BOSS	Security Monitoring	Cloud Monitoring		IR																							
32	BOSS	Data Governance	Secure Disposal of Data		MP																							
33	BOSS	Human Resource Security	Employee Termination		PS																							
34	BOSS	Human Resource Security	Employment Agreements		PS																							
35	BOSS	Human Resource Security	Background Screening		PS																							
36	BOSS	Human Resource Security	Job Descriptions		PS																							
37	BOSS	Human Resource Security	Roles and Responsibilities		PS																							
38	BOSS	Human Resource Security	Employee Code of Conduct		PS																							
39	BOSS	Compliance	Information Systems		RA																							
40	BOSS	Compliance	Information Systems		RA																							

NIST Security Reference Architecture – data analysis

Heat map that indicates:

- the Consumer's risk associated with the lack of control over the implementation of the identified-as-necessary security components or
- the Provider's responsibility of implementing the identified-as-necessary security components





NIST Security Reference Architecture

– Ecosystem Orchestration (Use Case Example) –

Cloud-adapted Risk Management Framework :

- Step 1: Categorize Information System
- Step 2: Identify Security Req., perform a risk assessment to identify security components (CIA analysis) and select Security Controls
- Step 3: Select best-fitting architecture
- Step 4: Assess Service Provider(s)
- Step 5: Approve Use of Service
- Step 6: Monitor Service Provider

Use Case:

USG Agency plans the migration of their Unified Messaging System (UMS) to the cloud.

Ecosystem Orchestration example presents:

1. UMS description & Categorization (Moderate IL)
2. Cloud solution analysis
 - Identifies the security components
 - Applies a Security Index System to security components for CIA security triad
 - Determines the Aggregated Security Index – a global value used to prioritize the security components' implementation.
3. Defines a high-level architecture
 - Public SaaS – Technical Broker + Provider
4. Research Providers and Brokers with P-ATO | ATO
5. SA and SLA negotiation with Broker and Provider(s) with ATO
6. Monitor Broker & Providers

NIST Security Reference Architecture

– Security Index System –

19

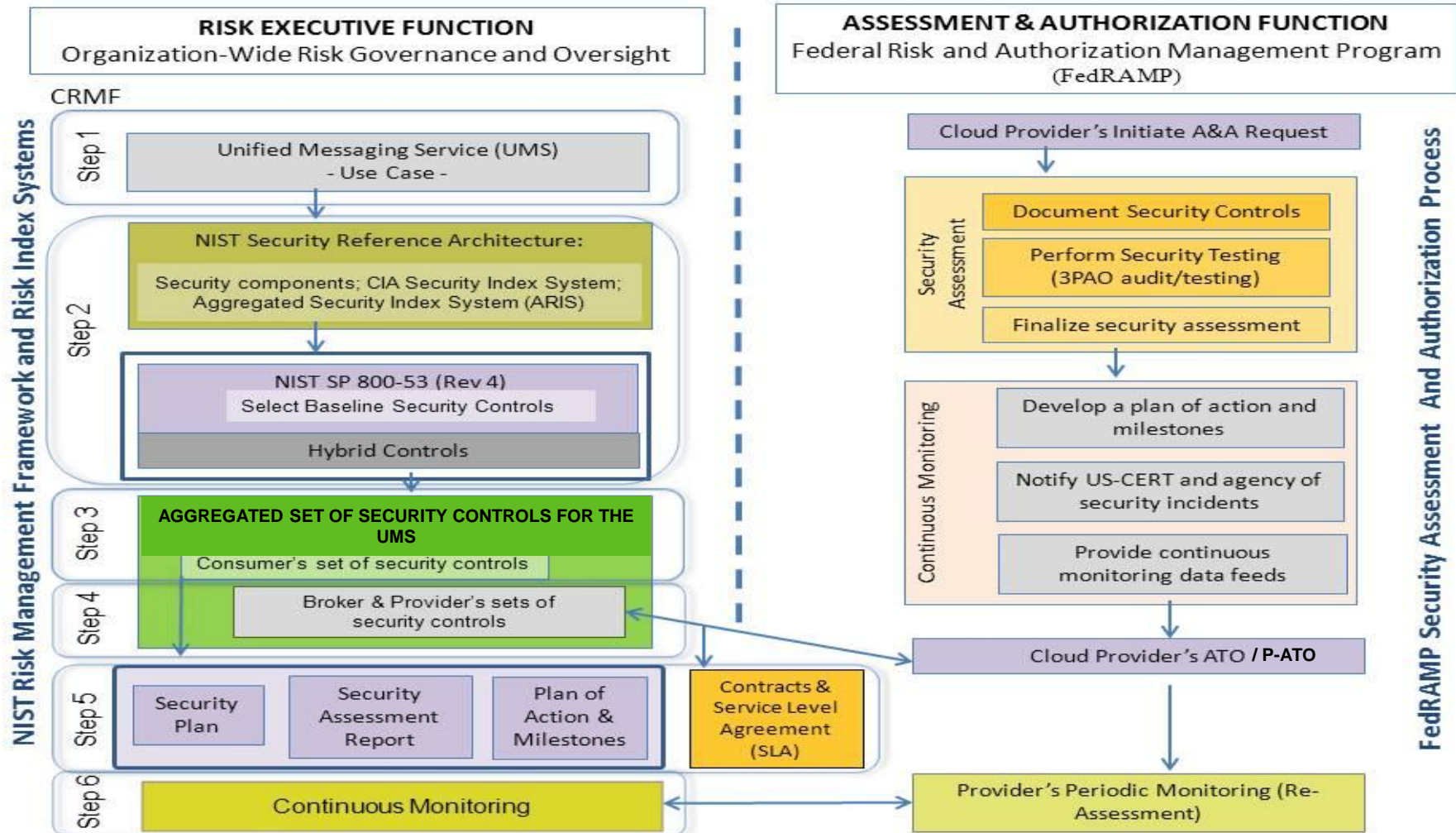
					Security Index System			
					C	I	A	CIA
2								
3								
4	BOSS	Compliance	Intellectual Property		2.00	2.00	2.00	6.00
5	BOSS	Data Governance	Handling/ Labeling/ Security		3.00	2.00	1.00	6.00
6	BOSS	Data Governance	Clear Desk Policy		1.00	0.00	1.00	2.00
7	BOSS	Data Governance	Rules for Information		2.00	3.00	2.00	7.00
8	BOSS	Human Resource Security	Employee Awareness		2.00	3.00	2.00	7.00
9	BOSS	Security Monitoring Services	Market Threat Intelligence		1.00	1.00	1.00	3.00
10	BOSS	Security Monitoring Services	Knowledge Base		1.00	2.00	2.00	5.00
11	BOSS	Compliance	Audit Planning		2.00	2.00	2.00	6.00
12	BOSS	Compliance	Internal Audits		2.00	2.00	2.00	6.00
13	BOSS	Security Monitoring Services	Event Mining		2.00	2.00	2.00	6.00
14	BOSS	Security Monitoring Services	Event Correlation		2.00	3.00	2.00	7.00
15	BOSS	Security Monitoring Services	Email Journaling		2.00	3.00	2.00	7.00
16	BOSS	Security Monitoring Services	User Behaviors and Profile		3.00	2.00	2.00	7.00
17	BOSS	Legal Services	E-Discovery		1.00	2.00	2.00	5.00
18	BOSS	Legal Services	Incident Response Legal		1.00	3.00	1.00	5.00
19	BOSS	Internal Investigations	Forensic Analysis		1.00	1.00	1.00	3.00
20	BOSS	Internal Investigations	e-Mail Journaling		2.00	3.00	2.00	7.00
21	BOSS	Compliance	Independent Audits		1.00	2.00	2.00	5.00
22	BOSS	Compliance	Third Party Audits		1.00	2.00	2.00	5.00
23	BOSS	Operational Risk Management	Business Impact Analysis		0.00	2.00	4.00	6.00
24	BOSS	Operational Risk Management	Business Continuity		0.00	1.00	2.00	3.00
25	BOSS	Operational Risk Management	Crisis Management		1.00	2.00	1.00	4.00
26	BOSS	Operational Risk Management	Risk Management		1.00	2.00	2.00	5.00
27	BOSS	Operational Risk Management	Independent Risk		1.00	2.00	2.00	5.00
28	BOSS	Security Monitoring Services	Database Monitoring		2.00	3.00	3.00	8.00
29	BOSS	Security Monitoring Services	Application Monitoring		2.00	3.00	3.00	8.00
30	BOSS	Security Monitoring Services	End-Point Monitoring		2.00	3.00	3.00	8.00
31	BOSS	Security Monitoring Services	Cloud Monitoring		2.00	3.00	3.00	8.00
32	BOSS	Data Governance	Secure Disposal of Data		3.00	3.00	3.00	9.00

20



NIST Security Reference Architecture

- Cloud-adapted Risk Management Framework and the FedRAMP A&A Process -



CloudSecurity < CloudComputing < TWiki - Windows Internet Explorer

http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/CloudSecurity

CloudSecurity < CloudComputing < TWiki

NIST Cloud Computing Collaboration Site

Reference Architecture | SAJACC | Security | Standards Roadmap | Business Use Cases | Documents and Resources | Koala Project

CloudComputing

Log In

CloudComputing Web

- Create New Topic
- Index
- Search
- Changes
- Notifications
- RSS Feed
- Statistics
- Preferences

Webs

- CloudComputing
- Main
- Sandbox
- TWiki

Cloud Security

Description

The formation of NIST Cloud Computing Security Working Group (NCC-SWG) is an integral part of the overall NIST effort to facilitate secure adoption of cloud services for United State Government (USG).

Objectives

Cloud computing has the potential to offer good cost savings both in terms of capital expenses (CAPEX) and operational expenses (OPEX) as well as leverage leading-edge technologies to meet the information processing needs of USG. However, the change in control dynamics (both in terms of ownership and management) with respect to IT resources poses security challenges. The objectives of NCC-SWG are:

1. Gather input from all stakeholders (both within USG and Industry) regarding security concerns in Cloud Computing services.
2. Analyze/prioritize a list of challenging security requirements that may delay or prevent adoption of Cloud Computing services by federal agencies.
3. Provide, when available, a description of practical approaches for mitigation and/or pointers to existing works that can lead to mitigation for each challenging security requirement.
4. Define a Security Reference Architecture that supplements the NIST Reference Architecture and Taxonomy described in the NIST SP 500-293.

Deliverables

1. The ["Challenging Security Requirements for US Government Cloud Computing Adoption"](#) document ([NIST SP 500-296](#)).
2. [Security Reference Architecture document.](#)

Target Date

1. The completion date for the "Challenging Security Requirements for US Government Cloud Computing Adoption" document is June 1, 2012.

Local intranet 100%

NIST Security Reference Architecture – what's next

1. *SP 500-299 (draft): posted for public comments (deadline for comments - July12, 2013)*
2. *Address public comments*
3. *Publish SP 500-299*

Other current work

Key Management is a Cloud Computing Environment

Other possible work (future)

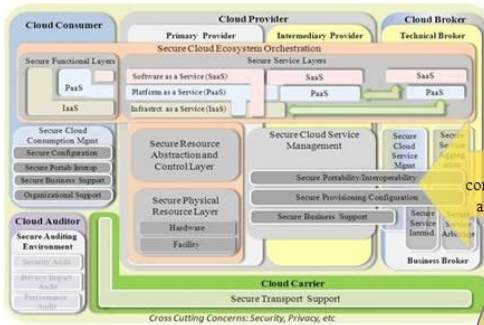
Determine if necessary to collect, aggregate, validate, analyze data and present the findings in the SRA or supplemental documents all types of deployment models :

- *Private Cloud instance*
- *Hybrid Cloud instance*
- *Community Cloud instance*

Cloud Security - future related work

NIST SP 800-53 SECURITY CONTROLS

NIST Security Reference Architecture – formal model

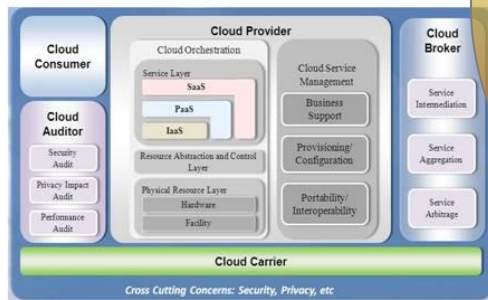


NIST Security Reference Architecture – security components

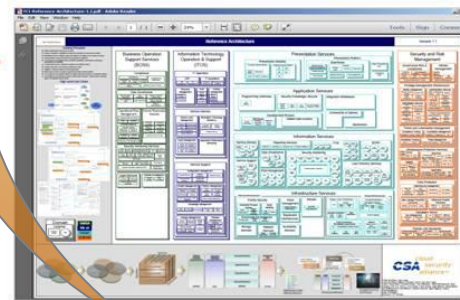
This table maps security components to the SRA architecture. It lists various security controls and their corresponding SRA components.

Component	Security Component	Control	Control ID	Control Title	Control Description	Control Type	Control Status	Control Version	Control Date	Control Author	Control Reviewer	Control Approval	Control Comments
Cloud Consumer	Secure Functional Layers	Secure Cloud Consumption Mgmt	CSA-1	Secure Cloud Consumption Mgmt	Secure Cloud Consumption Mgmt	Control	Active	1.0	2013-01-01	NIST	NIST	Approved	
Cloud Provider	Secure Cloud Ecosystem Orchestration	Secure Service Layers	CSA-2	Secure Service Layers	Secure Service Layers	Control	Active	1.0	2013-01-01	NIST	NIST	Approved	
Cloud Broker	Secure Cloud Service Mgmt	Secure Portability/Interoperability	CSA-3	Secure Portability/Interoperability	Secure Portability/Interoperability	Control	Active	1.0	2013-01-01	NIST	NIST	Approved	
Cloud Carrier	Secure Transport Support	Secure Provisioning Configuration	CSA-4	Secure Provisioning Configuration	Secure Provisioning Configuration	Control	Active	1.0	2013-01-01	NIST	NIST	Approved	

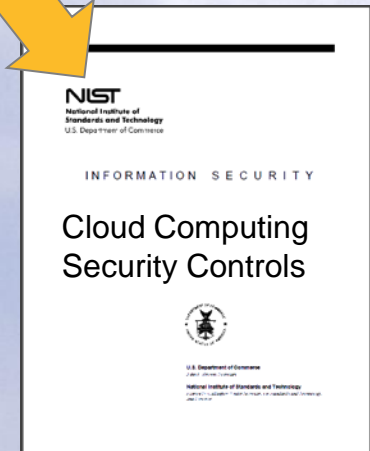
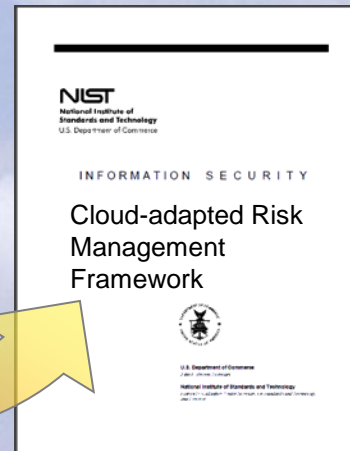
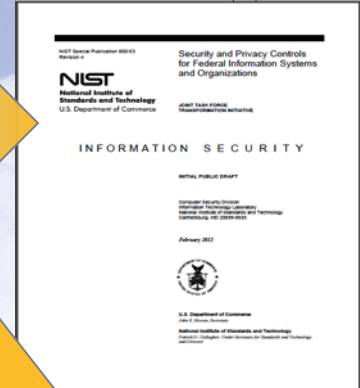
Mapping components to architecture



NIST Reference Architecture



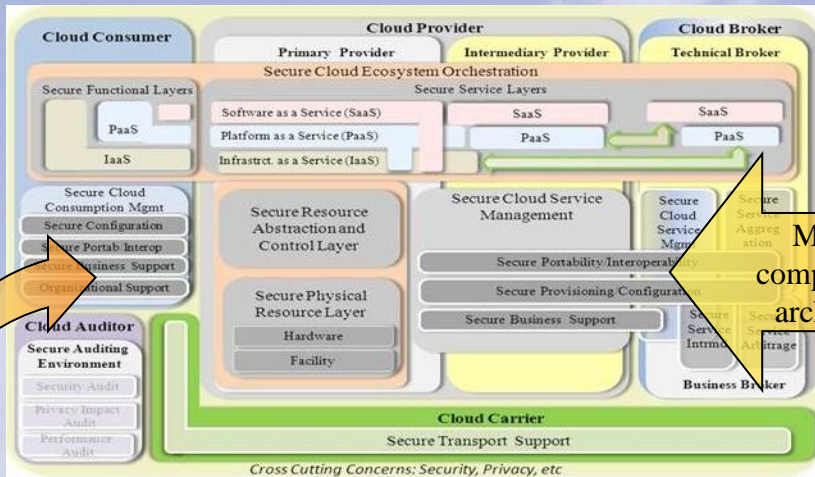
TCI Reference Architecture



NIST CC Security Reference Architecture – is **Modular** and **Adaptable**

25

NIST Security Reference Architecture – formal model

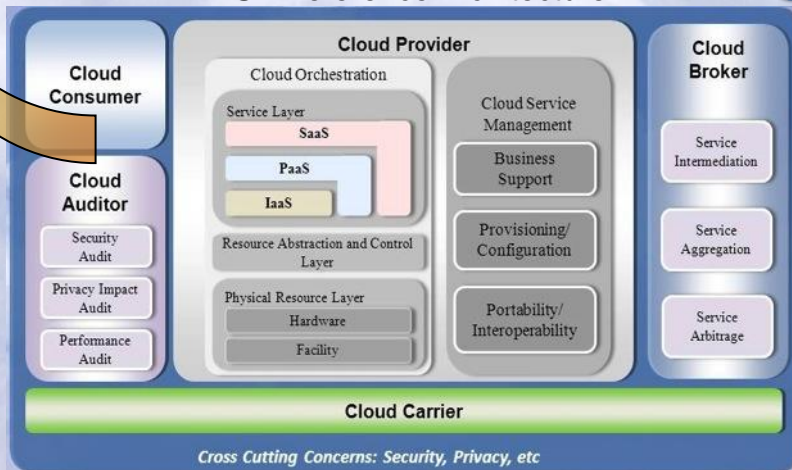


NIST Security Reference Architecture – security components

				Risk Index System			
				C	I	A	CIA
2							
4	BOSS	Compliance	Intellectual Property	2.00	2.00	2.00	6.00
5	BOSS	Data Governance	Handling/ Labeling/ Security	3.00	2.00	1.00	6.00
6	BOSS	Data Governance	Clear Desk Policy	1.00	0.00	1.00	2.00
7	BOSS	Data Governance	Rules for Information	2.00	3.00	2.00	7.00
8	BOSS	Human Resource Security	Employee Awareness	2.00	3.00	2.00	7.00
9	BOSS	Security Monitoring Services	Market Threat Intelligence	1.00	1.00	1.00	3.00
10	BOSS	Security Monitoring Services	Knowledge Base	1.00	2.00	2.00	5.00
11	BOSS	Compliance	Audit Planning	2.00	2.00	2.00	6.00
12	BOSS	Compliance	Internal Audits	2.00	2.00	2.00	6.00
13	BOSS	Security Monitoring Services	Event Mining	2.00	2.00	2.00	6.00
14	BOSS	Security Monitoring Services	Event Correlation	2.00	3.00	2.00	7.00
15	BOSS	Security Monitoring Services	Email Journaling	2.00	3.00	2.00	7.00
16	BOSS	Security Monitoring Services	User Behaviors and Profile	3.00	2.00	2.00	7.00
17	BOSS	Legal Services	E-Discovery	1.00	2.00	2.00	5.00
18	BOSS	Legal Services	Incident Response Legal	1.00	2.00	1.00	5.00
19	BOSS	Internal Investigations	Forensic Analysis	1.00	1.00	1.00	3.00
20	BOSS	Internal Investigations	e-Mail Journaling	2.00	3.00	2.00	7.00
21	BOSS	Compliance	Independent Audits	1.00	2.00	2.00	5.00
22	BOSS	Compliance	Third Party Audits	1.00	2.00	2.00	5.00
23	BOSS	Operational Risk Management	Business Impact Analysis	0.00	2.00	4.00	6.00
24	BOSS	Operational Risk Management	Business Continuity	0.00	1.00	2.00	3.00
25	BOSS	Operational Risk Management	Crisis Management	1.00	2.00	1.00	4.00
26	BOSS	Operational Risk Management	Risk Management	1.00	2.00	2.00	5.00
27	BOSS	Operational Risk Management	Independent Risk	1.00	2.00	2.00	5.00
28	BOSS	Security Monitoring Services	Database Monitoring	2.00	3.00	3.00	8.00
29	BOSS	Security Monitoring Services	Application Monitoring	2.00	3.00	3.00	8.00
30	BOSS	Security Monitoring Services	End-Point Monitoring	2.00	3.00	3.00	8.00
31	BOSS	Security Monitoring Services	Cloud Monitoring	2.00	3.00	3.00	8.00
32	BOSS	Data Governance	Secure Disposal of Data	3.00	3.00	3.00	9.00

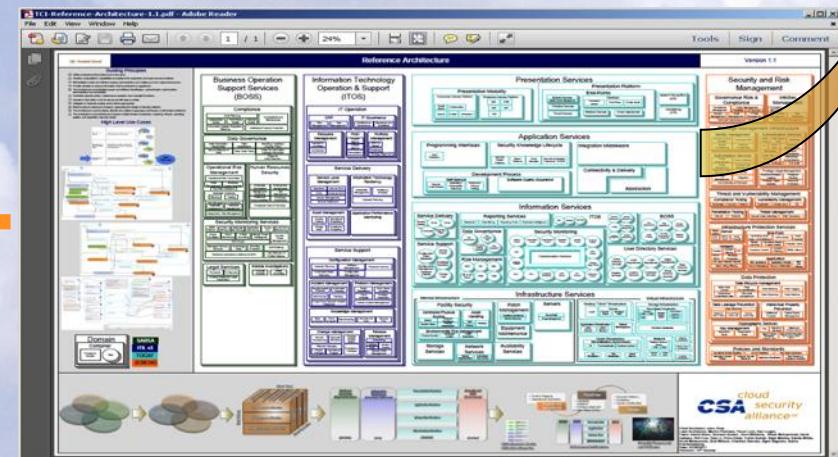
Mapping components to architecture

NIST Reference Architecture



CRMF

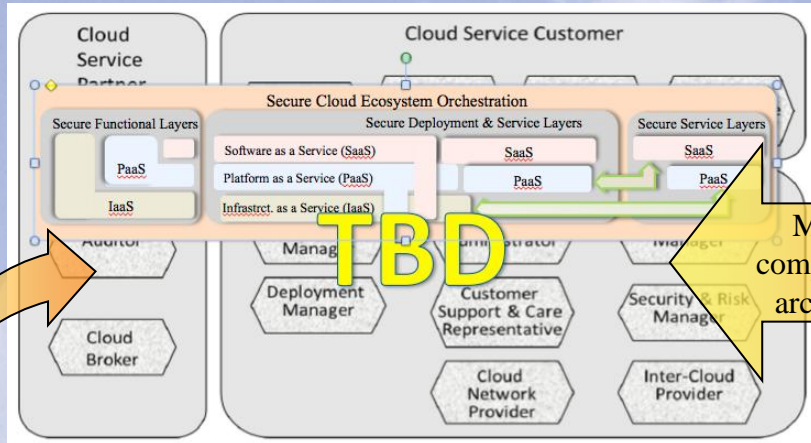
TCI Reference Architecture



ISO/IEC based CC Security Reference Architecture

ISO/IEC Security Reference Architecture – formal model

ISO/IEC Security Reference Architecture – security components

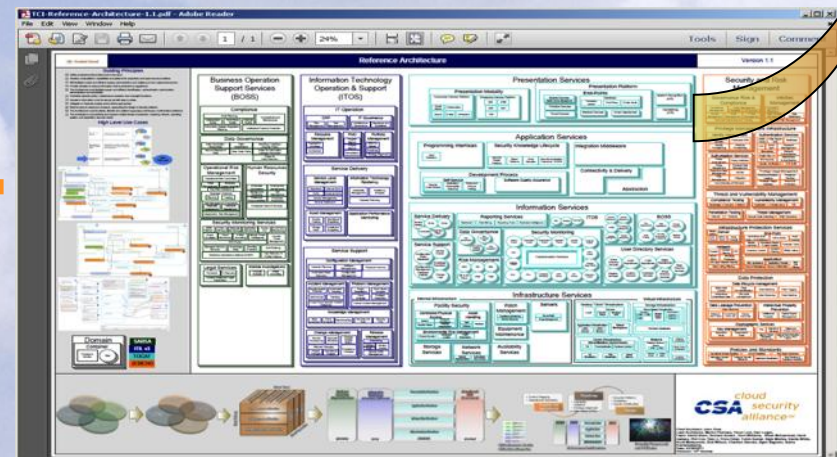
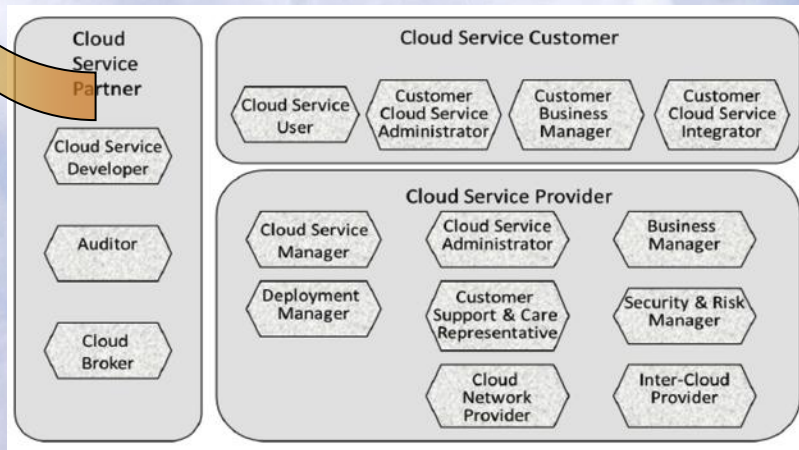


				Risk Index System			
				C	I	A	CIA
4	BOSS	Compliance	Intellectual Property	2.00	2.00	2.00	6.00
5	BOSS	Data Governance	Handling/ Labeling/ Security	3.00	2.00	1.00	6.00
6	BOSS	Data Governance	Clear Desk Policy	1.00	0.00	1.00	2.00
7	BOSS	Data Governance	Rules for Information	2.00	3.00	2.00	7.00
8	BOSS	Human Resource Security	Employee Awareness	2.00	3.00	2.00	7.00
9	BOSS	Security Monitoring Services	Market Threat Intelligence	1.00	1.00	1.00	3.00
10	BOSS	Security Monitoring Services	Knowledge Base	1.00	2.00	2.00	5.00
11	BOSS	Compliance	Audit Planning	2.00	2.00	2.00	6.00
12	BOSS	Compliance	Internal Audits	2.00	2.00	2.00	6.00
13	BOSS	Security Monitoring Services	Event Mining	2.00	2.00	2.00	6.00
14	BOSS	Security Monitoring Services	Event Correlation	2.00	3.00	2.00	7.00
15	BOSS	Security Monitoring Services	Email Journaling	2.00	3.00	2.00	7.00
16	BOSS	Security Monitoring Services	User Behaviors and Profile	3.00	2.00	2.00	7.00
17	BOSS	Legal Services	E-Discovery	1.00	2.00	2.00	5.00
18	BOSS	Legal Services	Incident Response Legal	1.00	1.00	1.00	3.00
19	BOSS	Internal Investigations	Forensic Analysis	1.00	1.00	1.00	3.00
20	BOSS	Internal Investigations	e-Mail Journaling	2.00	3.00	2.00	7.00
21	BOSS	Compliance	Independent Audits	3.00	2.00	2.00	7.00
22	BOSS	Compliance	Third Party Audits	1.00	1.00	1.00	3.00
23	BOSS	Operational Risk Management	Business Impact Analysis	0.00	2.00	4.00	6.00
24	BOSS	Operational Risk Management	Business Continuity	0.00	1.00	2.00	3.00
25	BOSS	Operational Risk Management	Crisis Management	1.00	2.00	1.00	4.00
26	BOSS	Operational Risk Management	Risk Management	1.00	2.00	2.00	5.00
27	BOSS	Operational Risk Management	Independent Risk	1.00	2.00	2.00	5.00
28	BOSS	Security Monitoring Services	Database Monitoring	2.00	3.00	3.00	8.00
29	BOSS	Security Monitoring Services	Application Monitoring	2.00	3.00	3.00	8.00
30	BOSS	Security Monitoring Services	End-Point Monitoring	2.00	3.00	3.00	8.00
31	BOSS	Security Monitoring Services	Cloud Monitoring	2.00	3.00	3.00	8.00
32	BOSS	Data Governance	Secure Disposal of Data	3.00	3.00	3.00	9.00

CRMF + methodology

ISO/IEC Reference Architecture

TCI Reference Architecture



27

ISO/IEC Security Reference Architecture – security components

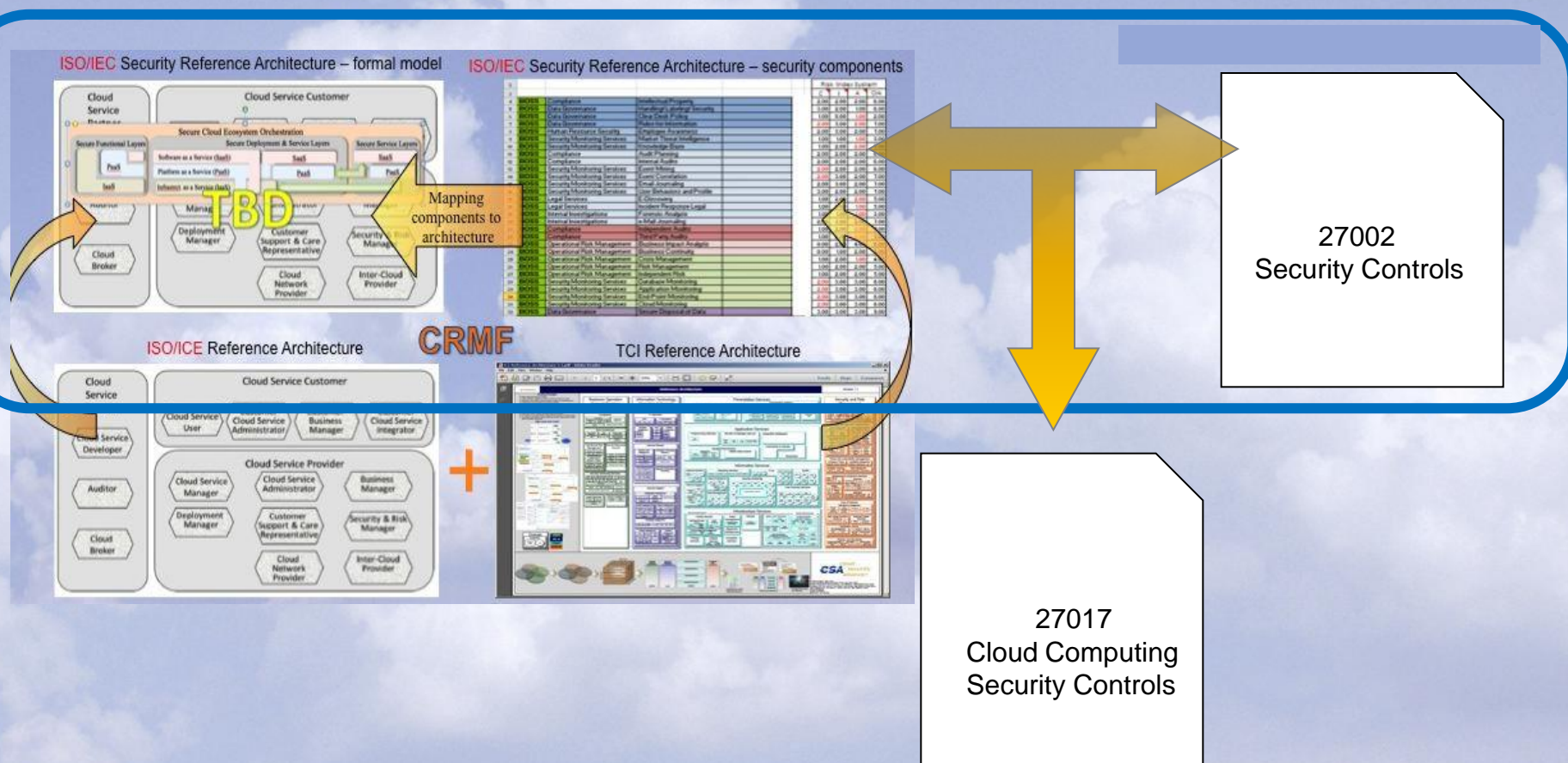


Proprietary Set of Components



How Cloud Computing Security Reference Architecture Relates to Other Standards

28



Additional Information

Dr. Michaela Iorga,

NIST, ITL, CSD

Senior Security Technical Lead for CC

Chair, NIST Cloud Computing Security WG

Co-Chair NIST Cloud Computing Forensic Science WG

michaela.iorga@nist.gov

301-975-8431



NIST Cloud Computing Collaborative Twiki:

<http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/CloudSecurity>

NIST Cloud Home Page: <http://www.nist.gov/itl/cloud>

Questions?

Thank you !

