NIST
National Institute of Standards and Technology

A RISK-BASED APPROACH TO CLOUD COMPUTING INFORMATION SYSTEMS

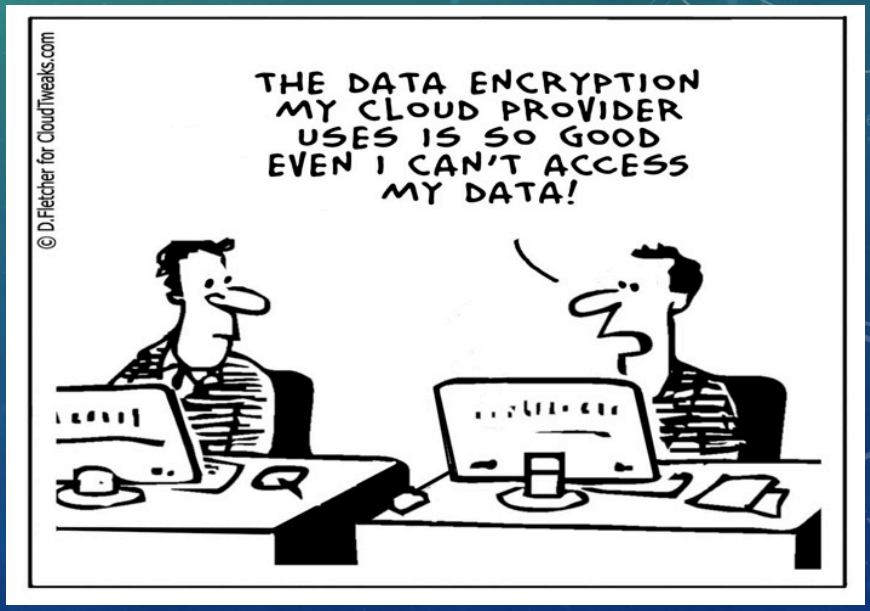
Dr. Michaela Iorga
Cloud Computing Security Technical Lead
NIST, ITL

MARCH 2018

NIST
National Institute of Standards and Technology

THE KEYS TO THE CLOUD KINGDOM: THE 3Ts

- Transparency
- Traceability
- Trustworthiness



NIST
National Institute of Standards and Technology

TODAY'S CHALLENGES

- Making the correct choice for your business (SaaS, PaaS or IaaS ?);
- Understanding the complexity of the Information Systems, especially cloud-based solutions;
- Risk Management is few orders of magnitude more complex;
  - Loss of control (trust issues not security issues, data owner & data custodian),
  - Vendor's transparency,
  - Security and Compliance,
    - Regulatory Frameworks are burdensome,
    - Security Vulnerabilities are everywhere,
  - Availability, Resilience and Reliability,
- System updates trigger documentation (SSP) to become outdated.

“INDUSTRY SHOULD STEAL FEDRAMP CLOUD SECURITY BASELINES”

"You need good security requirements around procuring cloud? Look what FedRAMP's done. Not some industry-driven consortium.”

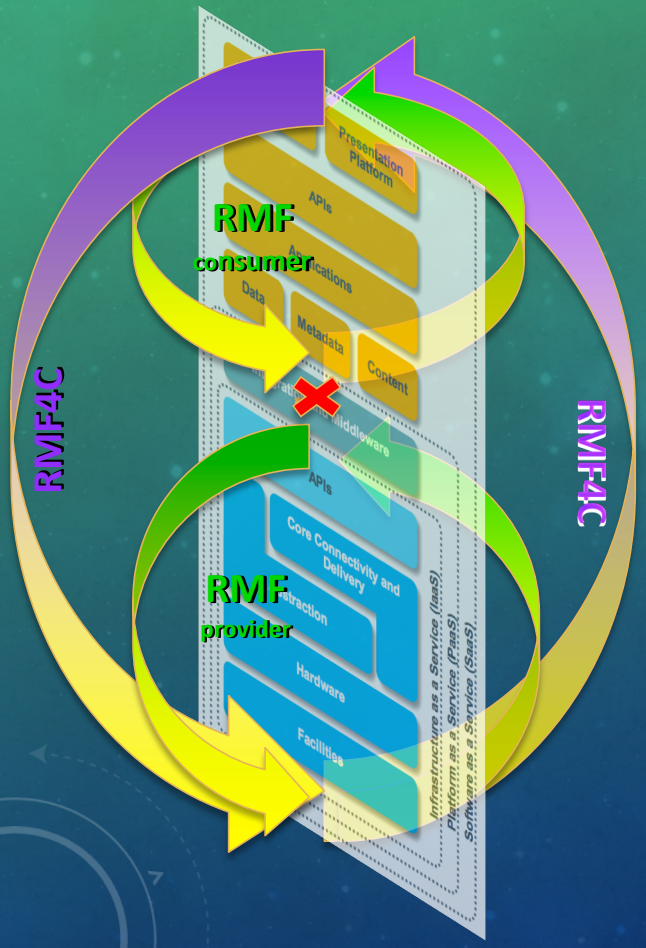
John Pescatore, Director SANS @ CyberCon

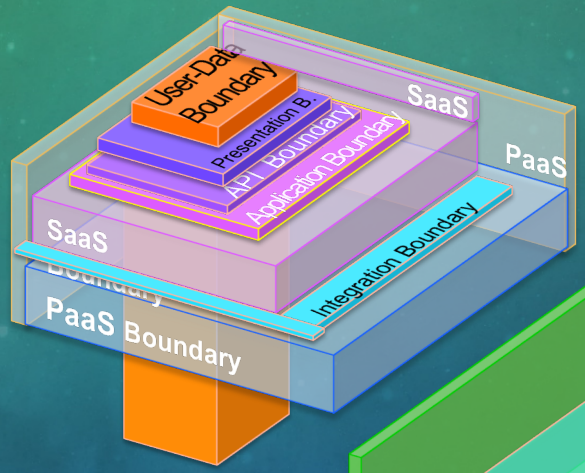
John Pescatore, Director of Emerging Security Trends at the SANS Institute speaks at CyberCon 2015 Conference at the Ritz-Carlton Pentagon City in Arlington, Va., on Wednesday, November 18, 2015.
(Photo: Mike Morones/Staff)

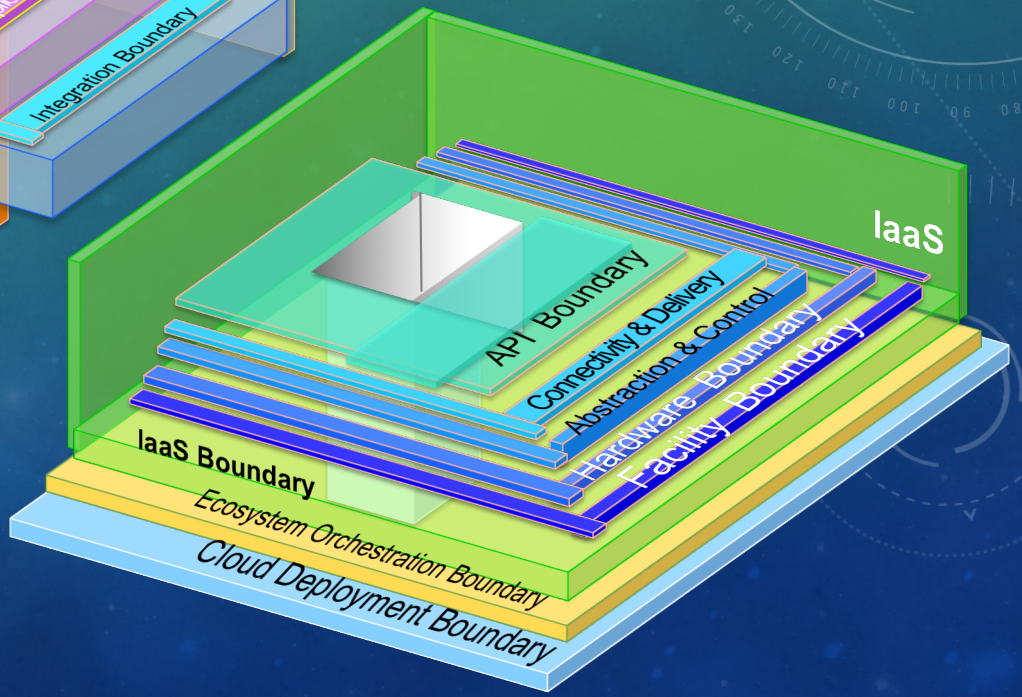
Pescatore, speaking at the *Federal Times'* CyberCon conference on Nov. 18, cited this as an area where the government has solved a problem that the private sector can take advantage of.

"For example, the GSA FedRAMP program for cloud — at Gartner, I found myself pointing private industry customers toward that," he said. "You need good security requirements around procuring cloud? Look what FedRAMP's done. Not some industry-driven consortium."

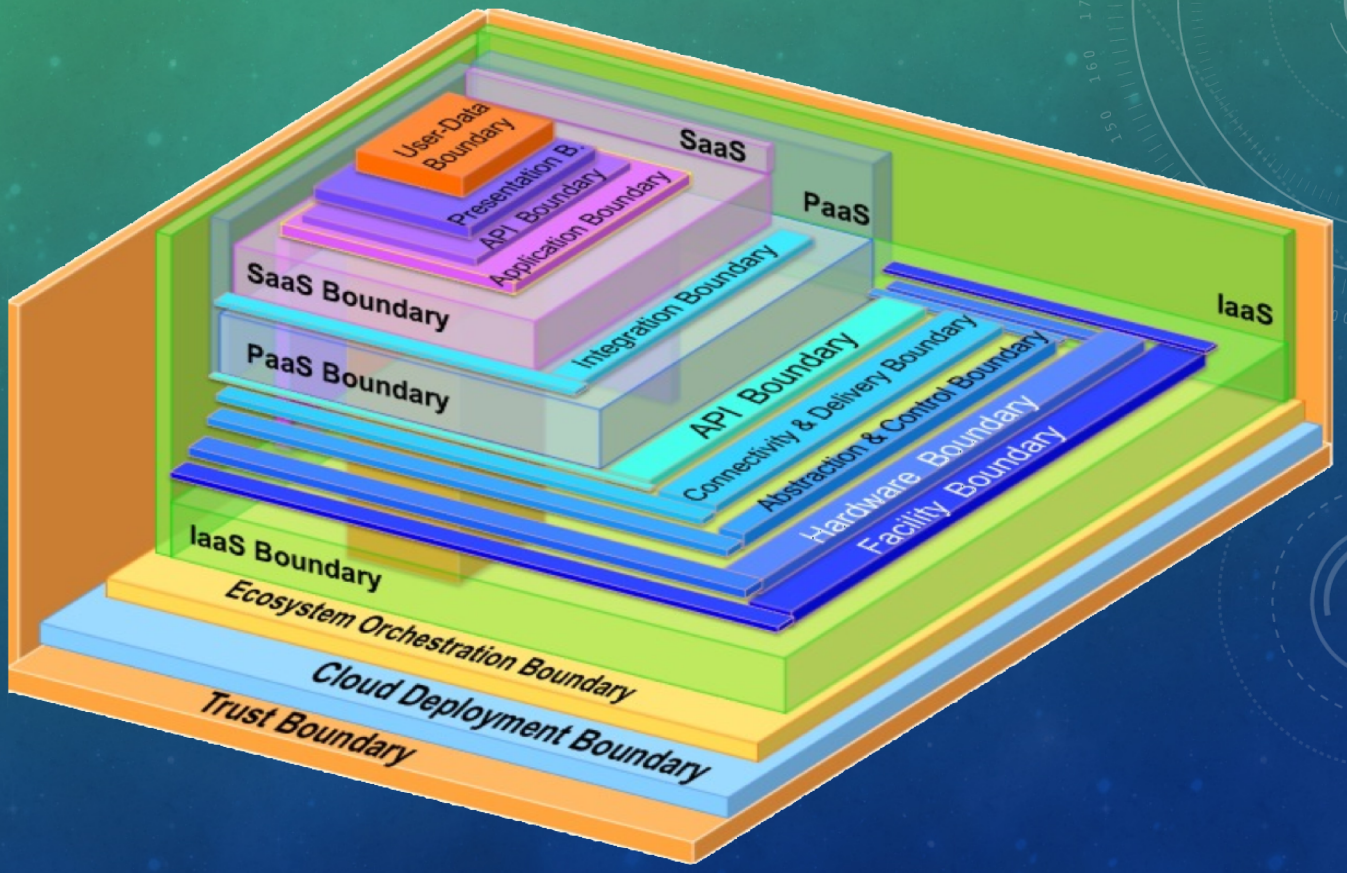
UNDERSTANDING THE CLOUD-BASED SYSTEM'S BOUNDARIES

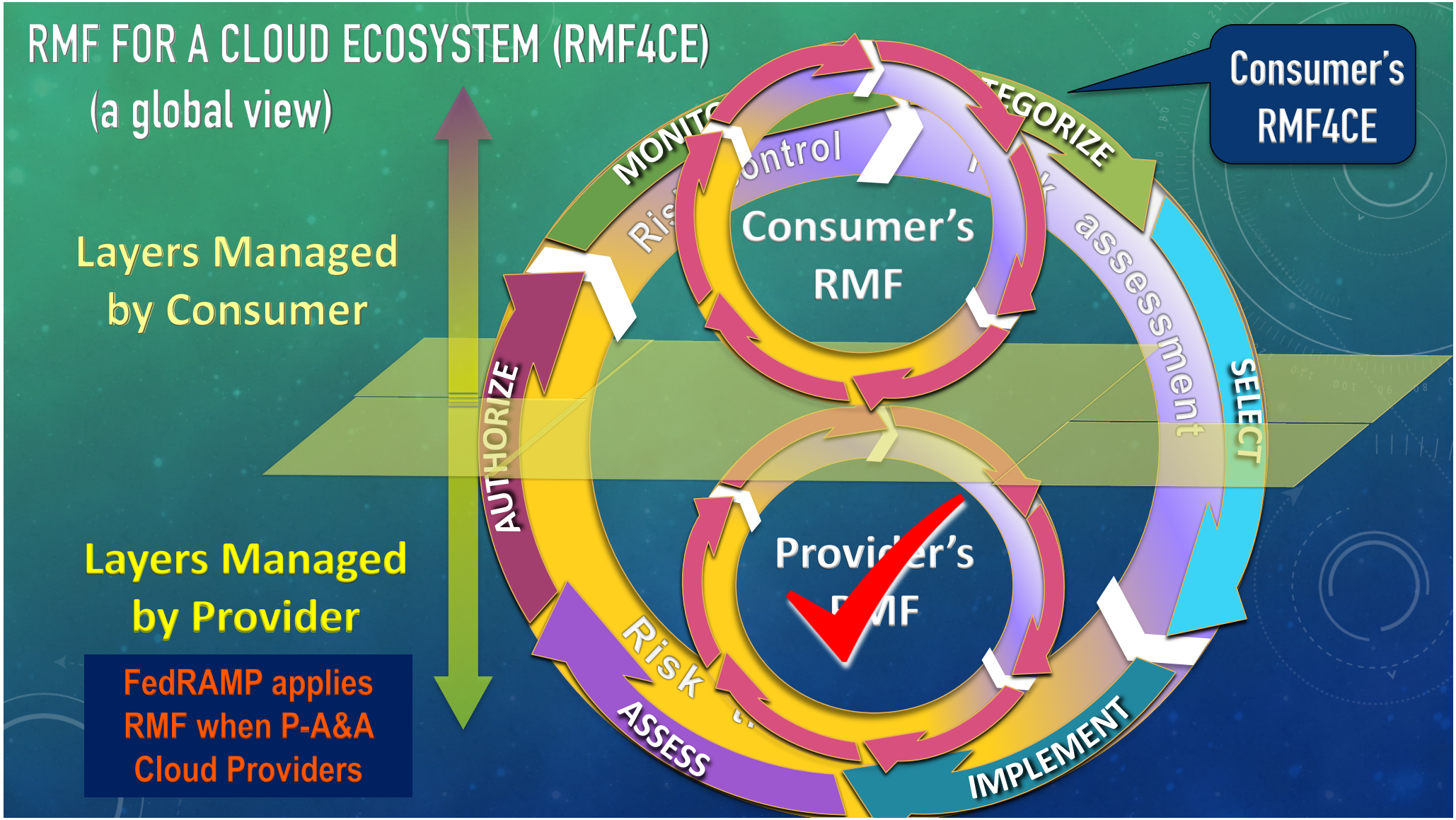




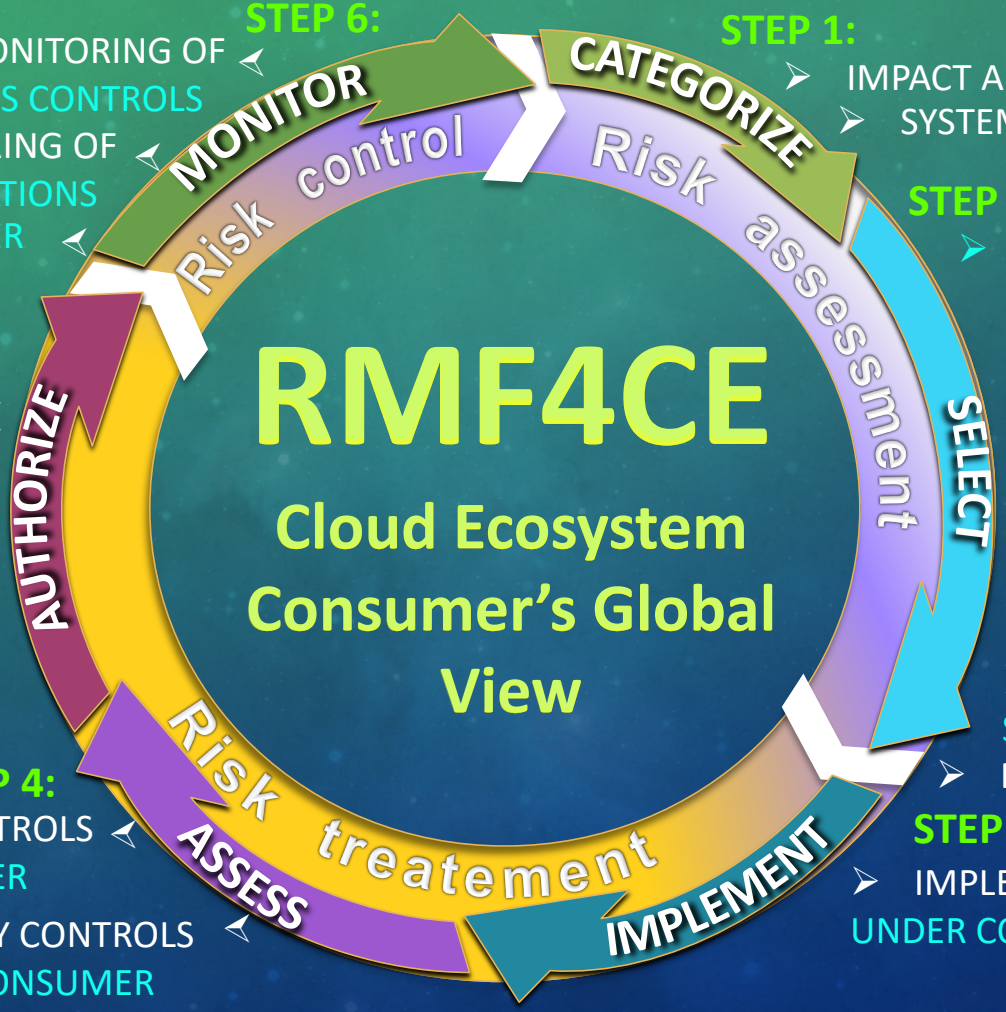


THE TRUST BOUNDARY




RMF FOR A CLOUD ECOSYSTEM (RMF4CE)
(a global view)
Layers Managed by Consumer
Layers Managed by Provider
FedRAMP applies RMF when P-A&A Cloud Providers
Consumer's RMF4CE
Consumer's RMF
Provider's RMF
CATEGORIZE
assessment
SELECT
IMPLEMENT
ASSESS
AUTHORIZE
MONITOR

RMF FOR THE CLOUD ECOSYSTEM



STEP 1:
- IMPACT ANALYSIS
- SYSTEM CATEGORIZATION

STEP 2:
- IDENTIFY & SELECT CAPABILITIES
- SELECT BASELINE CONTROLS
- TAILOR & SUPPLEMENT CONTROLS
- IDENTIFY & SELECT BEST-FITTING CLOUD ARCHITECTURE
- SELECT CLOUD PROVIDER
- NEGOTIATE SLA, METRICS, SIGN CONTRACT
- DEVELOP SECURITY PLAN

STEP 3:
- IMPLEMENT SECURITY CONTROLS UNDER CONSUMER'S MANAGEMENT

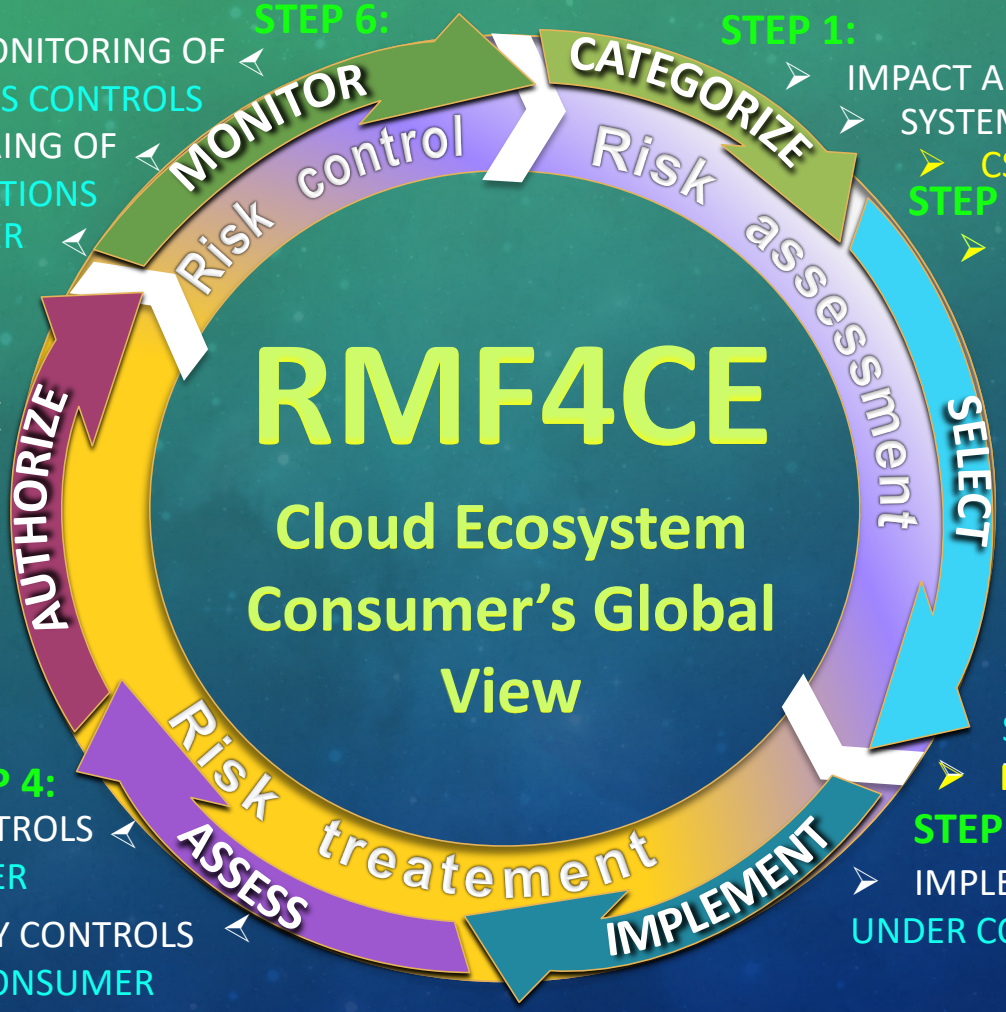
STEP 4:
- ASSESS SECURITY CONTROLS MANAGED BY PROVIDER
- ASSESS SECURITY CONTROLS MANAGED BY CONSUMER

STEP 5:
- AUTHORIZE CLOUD-BASED INFORMATION SYSTEM (BASED UPON RESIDUAL RISK & RISK TOLERANCE)

STEP 6:
- ONGOING MONITORING OF CONSUMER'S CONTROLS
- ONGOING MONITORING OF PROVIDER'S OPERATIONS
- RE-AUTHORIZE PROVIDER

RMF FOR THE CLOUD ECOSYSTEM

CLOUD SECURITY RUBIK'S CUBE



STEP 1:

- IMPACT ANALYSIS
- SYSTEM CATEGORIZATION
- CSF QUESTIONNAIRE

STEP 2:

- IDENTIFY & SELECT CAPABILITIES
- SELECT BASELINE CONTROLS
- TAILOR & SUPPLEMENT CONTROLS
- IDENTIFY & SELECT BEST-FITTING CLOUD ARCHITECTURE
- SELECT CLOUD PROVIDER
- NEGOTIATE SLA, METRICS, SIGN CONTRACT
- **DEVELOP SECURITY PLAN**

STEP 3:

- IMPLEMENT SECURITY CONTROLS UNDER CONSUMER'S MANAGEMENT

STEP 4:

- ASSESS SECURITY CONTROLS MANAGED BY PROVIDER
- ASSESS SECURITY CONTROLS MANAGED BY CONSUMER

STEP 5:

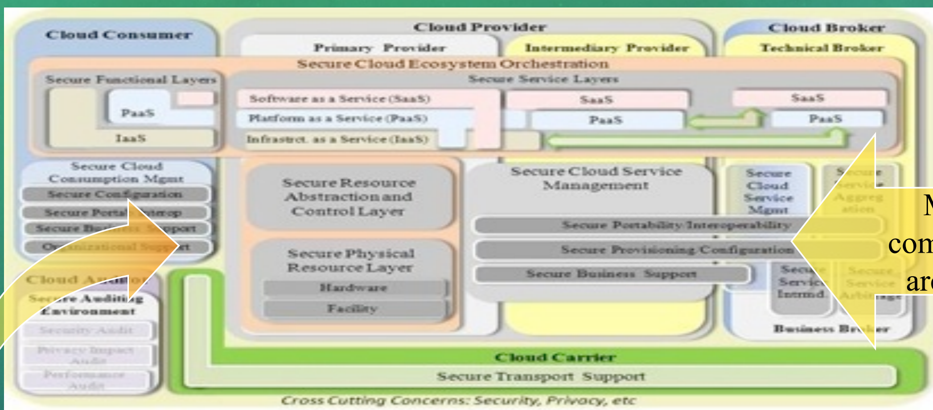
- AUTHORIZE CLOUD-BASED INFORMATION SYSTEM (BASED UPON RESIDUAL RISK & RISK TOLERANCE)

STEP 6:

- ONGOING MONITORING OF CONSUMER'S CONTROLS
- ONGOING MONITORING OF PROVIDER'S OPERATIONS
- RE-AUTHORIZE PROVIDER

NIST CC SECURITY REFERENCE ARCHITECTURE – THE APPROACH

NIST Security Reference Architecture – formal model

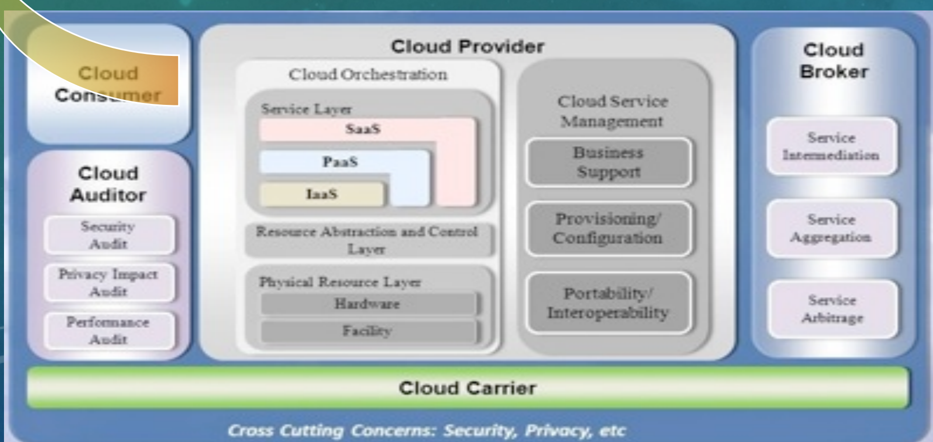


NIST Security Reference Architecture – security components

					Risk Index System			
3					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	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	[illegible]	[illegible]
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	[illegible]
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

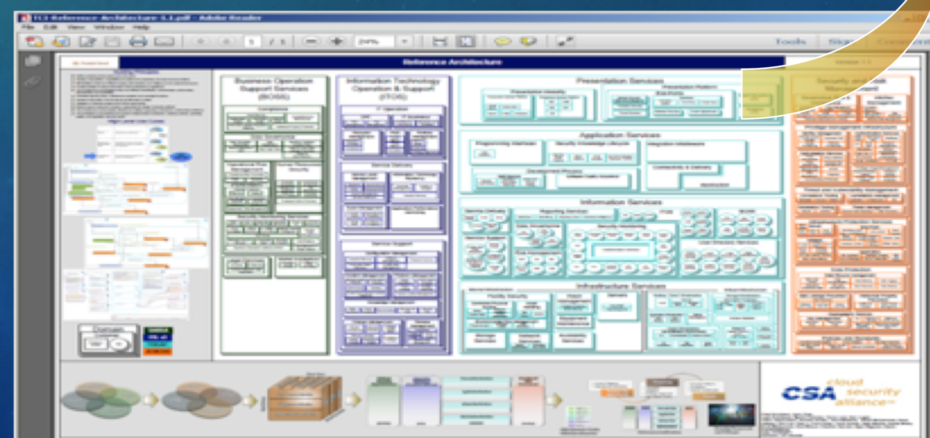
Mapping components to architecture

NIST Reference Architecture

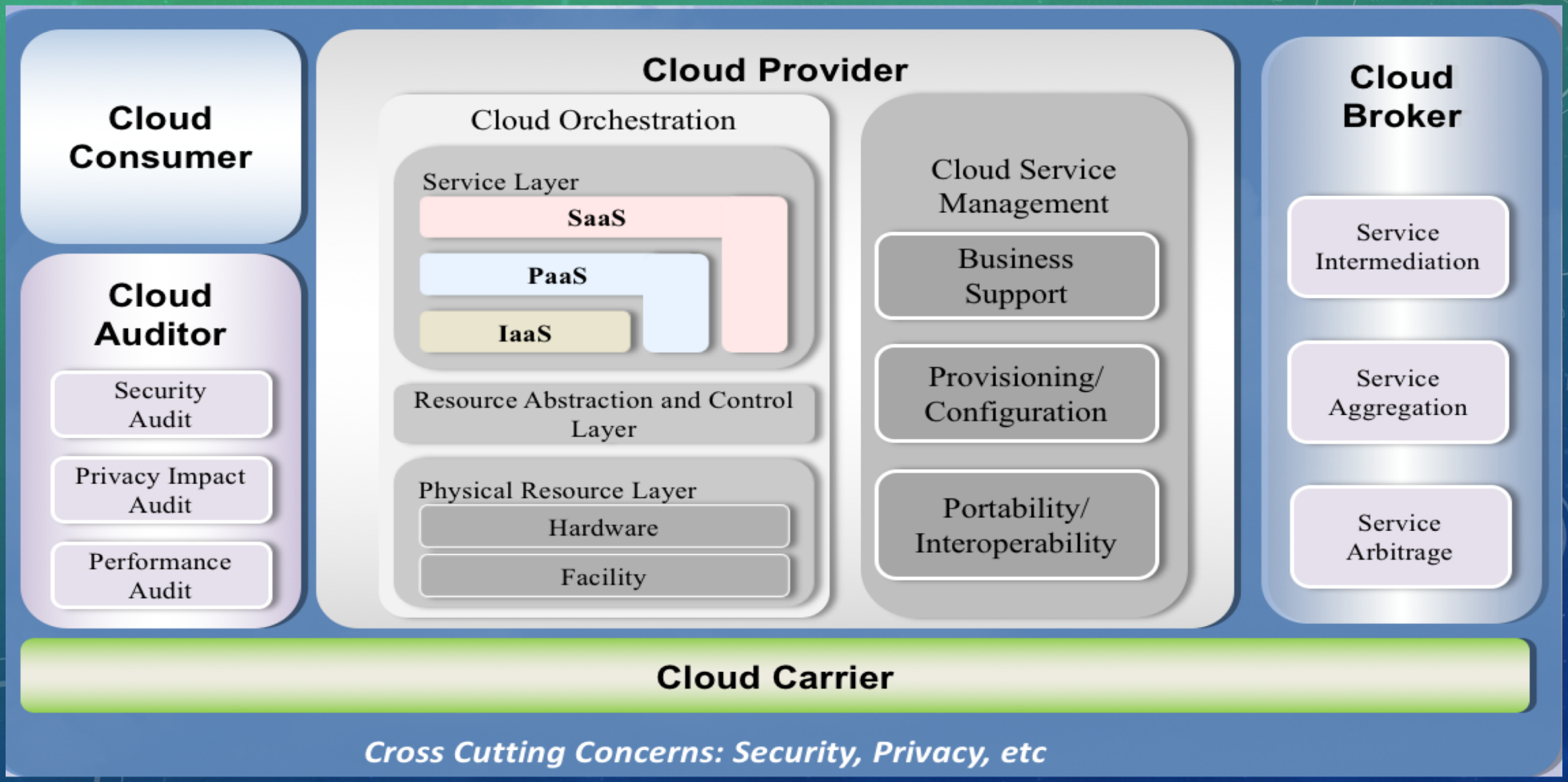


+

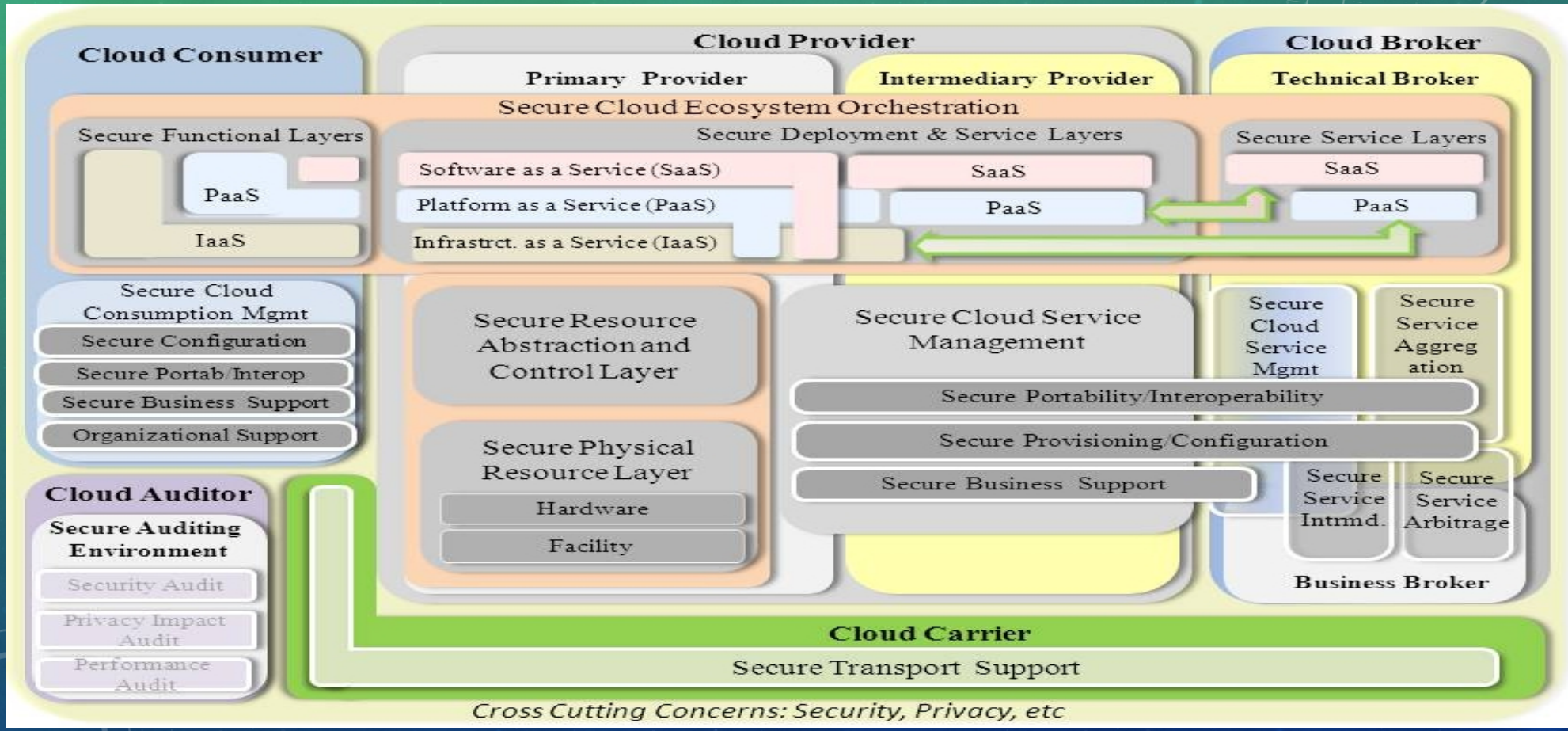
CSA's TCI Reference Architecture



SP 500-292: NIST CLOUD COMPUTING REFERENCE ARCHITECTURE

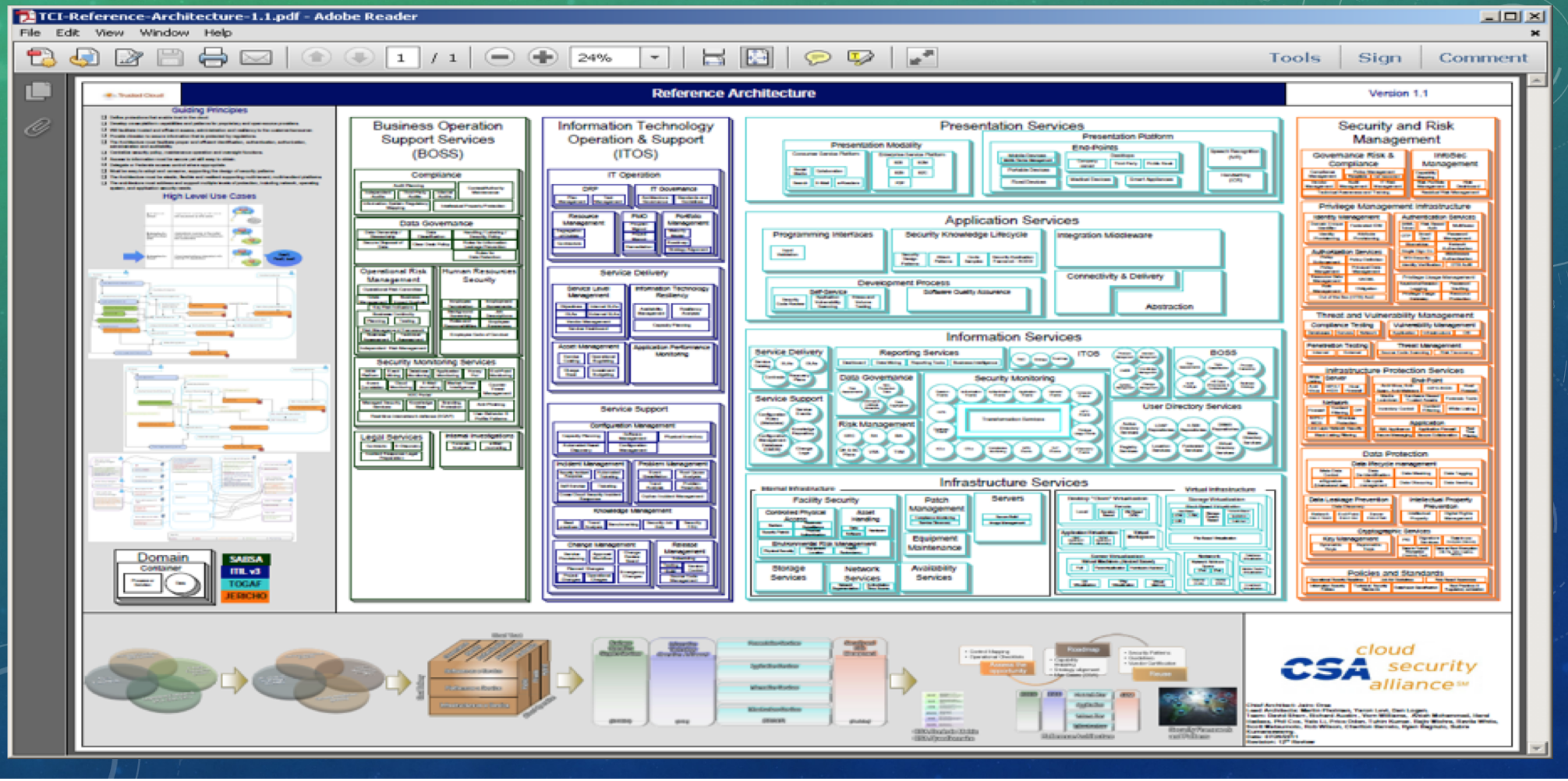


SP 500-299: NIST CLOUD SECURITY REFERENCE ARCHITECTURE



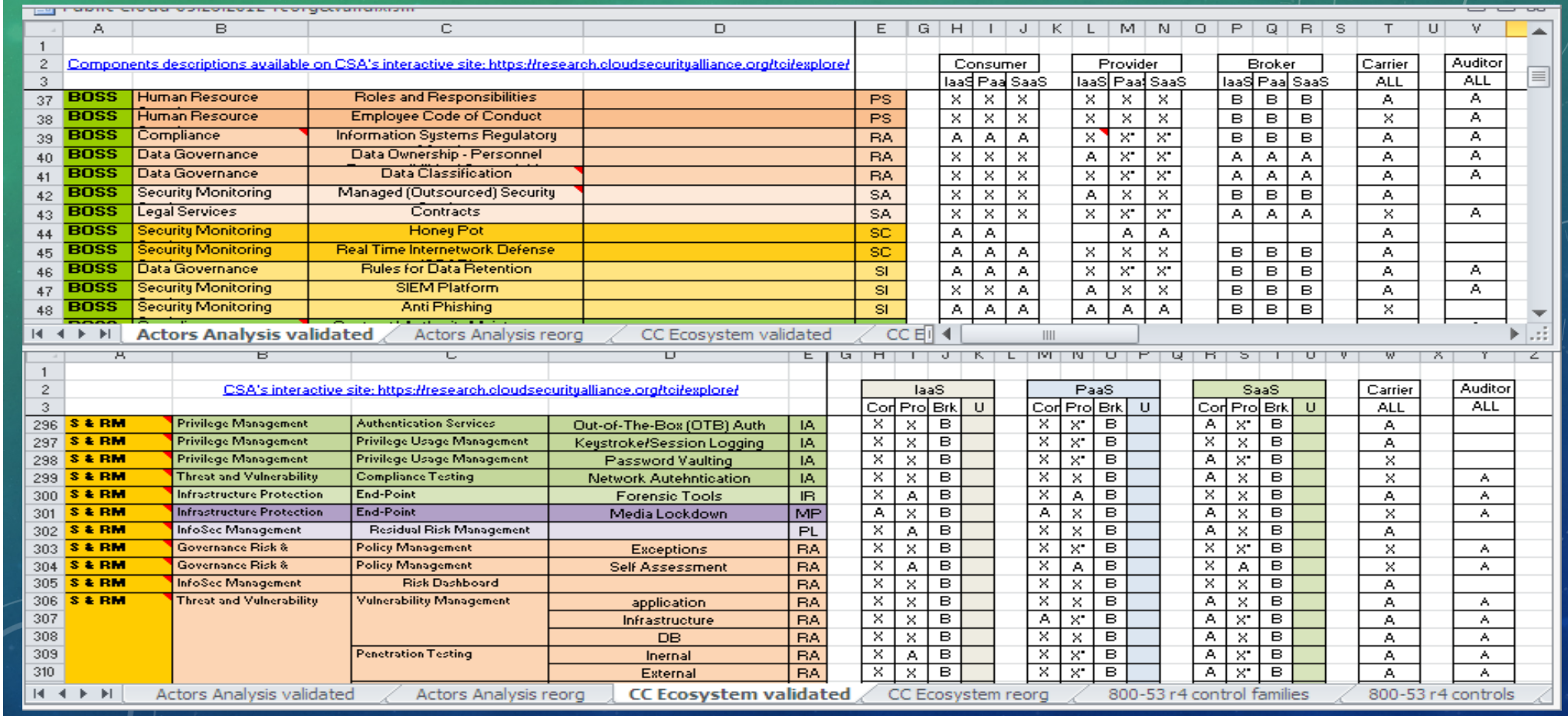
Cloud Security Alliance's TCI Reference Architecture

https://cloudsecurityalliance.org/wp-content/uploads/2011/10/TCI-Reference-Architecture-v1.1.pdf



SP 500-299: NIST CLOUD SECURITY REFERENCE ARCHITECTURE

- FUNCTIONAL CAPABILITIES -



Components descriptions available on CSA's interactive site: https://research.cloudsecurityalliance.org/tci/explore/

						Consumer			Provider			Broker			Carrier	Auditor
						IaaS	PaaS	SaaS	IaaS	PaaS	SaaS	IaaS	PaaS	SaaS	ALL	ALL
37	BOSS	Human Resource	Roles and Responsibilities		PS	X	X	X	X	X	X	B	B	B	A	A
38	BOSS	Human Resource	Employee Code of Conduct		PS	X	X	X	X	X	X	B	B	B	X	A
39	BOSS	Compliance	Information Systems Regulatory		RA	A	A	A	X	X*	X*	B	B	B	A	A
40	BOSS	Data Governance	Data Ownership - Personnel		RA	X	X	X	A	X*	X*	A	A	A	A	A
41	BOSS	Data Governance	Data Classification		RA	X	X	X	X	X*	X*	A	A	A	A	A
42	BOSS	Security Monitoring	Managed (Outsourced) Security		SA	X	X	X	A	X	X	B	B	B	A	
43	BOSS	Legal Services	Contracts		SA	X	X	X	X	X*	X*	A	A	A	X	A
44	BOSS	Security Monitoring	Honey Pot		SC	A	A			A	A				A	
45	BOSS	Security Monitoring	Real Time Internetwork Defense		SC	A	A	A	X	X	X	B	B	B	A	
46	BOSS	Data Governance	Rules for Data Retention		SI	A	A	A	X	X*	X*	B	B	B	A	A
47	BOSS	Security Monitoring	SIEM Platform		SI	X	X	A	A	X	X	B	B	B	A	A
48	BOSS	Security Monitoring	Anti Phishing		SI	A	A	A	A	A	A	B	B	B	X	

Actors Analysis validated | Actors Analysis reorg | CC Ecosystem validated | CC E

CSA's interactive site: https://research.cloudsecurityalliance.org/tci/explore/

						IaaS				PaaS				SaaS				Carrier	Auditor
						Cor	Pro	Brk	U	Cor	Pro	Brk	U	Cor	Pro	Brk	U	ALL	ALL
296	S & RM	Privilege Management	Authentication Services	Out-of-The-Box (OTB) Auth	IA	X	X	B		X	X*	B		A	X*	B		A	
297	S & RM	Privilege Management	Privilege Usage Management	Keystroke/Session Logging	IA	X	X	B		X	X*	B		X	X	B		A	
298	S & RM	Privilege Management	Privilege Usage Management	Password Vaulting	IA	X	X	B		X	X*	B		A	X*	B		X	
299	S & RM	Threat and Vulnerability	Compliance Testing	Network Autehntication	IA	X	X	B		X	X	B		A	X	B		X	A
300	S & RM	Infrastructure Protection	End-Point	Forensic Tools	IR	X	A	B		X	A	B		X	X	B		A	A
301	S & RM	Infrastructure Protection	End-Point	Media Lockdown	MP	A	X	B		A	X	B		A	X	B		X	A
302	S & RM	InfoSec Management	Residual Risk Management		PL	X	A	B		X	X	B		A	X	B		A	
303	S & RM	Governance Risk &	Policy Management	Exceptions	RA	X	X	B		X	X*	B		X	X*	B		X	A
304	S & RM	Governance Risk &	Policy Management	Self Assessment	RA	X	A	B		X	A	B		X	A	B		X	A
305	S & RM	InfoSec Management	Risk Dashboard		RA	X	X	B		X	X	B		X	X	B		A	
306	S & RM	Threat and Vulnerability	Vulnerability Management	application	RA	X	X	B		X	X	B		A	X	B		A	A
307				Infrastructure	RA	X	X	B		A	X*	B		A	X*	B		A	A
308				DB	RA	X	X	B		X	X	B		A	X	B		A	A
309			Penetration Testing	Inernal	RA	X	A	B		X	X*	B		A	X*	B		A	A
310				External	RA	X	X	B		X	X*	B		A	X*	B		A	A

Actors Analysis validated | Actors Analysis reorg | CC Ecosystem validated | CC Ecosystem reorg | 800-53 r4 control families | 800-53 r4 controls

NIST SP 800-174: SECURITY AND PRIVACY CONTROLS FOR CLOUD-BASED FEDERAL INFORMATION SYSTEMS

Components descriptions also available on CSA's interactive sit
https://research.cloudsecurityalliance.org/tci/

SP800-53 Rev4 Security Controls for Implementing Functional Capabilities

Domain	Container	Capability (process or solution)	Capability (process or solution)	SP 800-53 R4 security controls for LOW-IMPACT SYSTEMS: NIST Baseline	Additional Suggested Controls	FedRAMP Baseline	Additional Suggested Controls	SP 800-53 R4 security controls for MODERATE-IMPACT SYSTEMS: NIST Baseline	Additional Suggested Controls	FedRAMP Baseline	Additional Suggested Controls	SP 800-53 R4 security controls for HIGH-IMPACT SYSTEMS: NIST Baseline	Additional Suggested Controls	FedRAMP Baseline	Additional Suggested Controls	PM Controls	Information Protection (NOTE: Other capabilities might generate data that needs to be protected by applying the set of controls listed below) SP800-53 Rev4: Low (info protection)	Moderate (info protection)	High (info protection)	Security Index System (SIS) (Example of how to use SIS): C	I	A	CIA	Consumer: IaaS	PaaS	SaaS
BOSS	Compliance	Intellectual Property Protection		AC-1,AC-2,AC-3,AC-	CM-3,CM-5,MA-3,MP-	AC-1,AC-2,AC-3,AC-	CM-3,CM-5,MA-3,MP-	AC-2(1),AC-2(2),AC-	AC-2(5),AC-2(7),AC-	AC-2(1),AC-2(2),AC-	AC-19,CM-3(2),CM-6	AC-2(11),AC-2(12),AC-	AC-6(7),AC-6(8),AC-	AC-2(11),AC-2(13),AC-	AC-6(7),AC-21(2),AU-		AC-1, AC-2, AC-3,	AC-2(1), AC-2(2), AC-	AC-2(11), AC-2(13),	2.00	2.00	2.00	6.00	X	X	X
BOSS	Data Governance	Handling/ Labeling/ Security		AC-1,AC-3,AT-1,AU-	AC-4	AC-1,AC-3,AT-1,AU-	AC-4	MP-3,MP-5,MP-5(4)		MP-3,MP-5,MP-5(4)		AC-16		AC-16						4.00	2.00	2.00	8.00	X	X	X
BOSS	Data Governance	Clear Desk Policy		MP-1,MP-2,MP-7		MP-1,MP-2,MP-7		MP-4,MP-5,MP-		MP-4,MP-5,MP-										1.00	0.00	1.00	2.00	A	A	A
BOSS	Data Governance	Rules for Information Leakage		AC-1,CP-1,IA-1,IR-		AC-1,CP-1,IA-1,IR-										PM-11	AC-1, AC-2, AC-3,	AC-2(1), AC-2(2), AC-	AC-2(11), AC-2(13),	2.00	3.00	2.00	7.00	X	A	A
BOSS	Human Resource Se	Employee Awareness		AT-1,AT-2		AT-1,AT-2		AT-2(2)		AT-2(2)						PM-13, PM-14				2.00	3.00	2.00	7.00	A	A	A
BOSS	Security Monitoring S	Threat Intelligence		AU-6,CA-2,IR-4,IR-5		AU-6,CA-2,IR-4,IR-5		AU-6(1),AU-6(3)	CA-2(2)	AU-6(1),AU-6(3),CA-		AU-6(5),AU-6(6),IR-	IR-4(6),IR-4(7),IR-	AU-6(5),AU-6(6),IR-	SI-4(19),AU-6(9)	PM-12				1.00	1.00	1.00	3.00	A	A	A
BOSS	Security Monitoring S	Knowledge Base		PL-2,SA-5		PL-2,SA-5		PL-8	PL-7	PL-8	PL-7									1.00	2.00	2.00	5.00	A	A	A
BOSS	Compliance	Audit Planning		CA-2,CA-7,PL-2	CA-2(1)	CA-2,CA-2(1),CA-7,PL-		CA-7(1),PL-2(3)	CA-2(2)	CA-2(2),CA-7(1),PL-			PL-8(1),PL-8(2)		PL-8(1),PL-8(2)		AC-1, AC-2, AC-3,	AC-2(1), AC-2(2), AC-	AC-2(11), AC-2(13),	2.00	2.00	2.00	6.00	A	A	A
BOSS	Compliance	Internal Audits		CA-2,CA-7,PL-2	CA-2(1)	CA-2,CA-2(1),CA-7,PL-		CA-7(1),PL-2(3)	CA-2(2),CA-8,CA-8(1)	CA-2(2),CA-7(1),CA-			CA-7(3)	CA-7(3)			AC-1, AC-2, AC-3,	AC-2(1), AC-2(2), AC-	AC-2(11), AC-2(13),	2.00	2.00	2.00	6.00	A	A	A
BOSS	Security Monitoring S	Event Mining		AU-6,CA-7,RA-5,SI-4		AU-6,CA-7,RA-5,SI-4		AU-6(3),SI-4(2)	RA-5(6),RA-5	AU-6(3),RA-5(6),SI-			AU-6(4),CA-7(3),SI-	CA-7(3),SI-4(11),SI-	AU-6(4)		AC-1, AC-2, AC-3,	AC-2(1), AC-2(2), AC-	AC-2(11), AC-2(13),	2.00	2.00	2.00	6.00	X	X	A
BOSS	Security Monitoring S	Event Correlation		AU-6,CA-7,IR-4,RA-		AU-6,CA-7,IR-4,RA-		AU-6(3)	SI-4(16)	AU-6(3),SI-4(16)		AU-6(6),IR-4(4)	AU-6(9),IR-4(8),RA-	AU-6(6),IR-4(4),IR-	AU-6(9)		AC-1, AC-2, AC-3,	AC-2(1), AC-2(2), AC-	AC-2(11), AC-2(13),	2.00	3.00	2.00	7.00	X	X	A
BOSS	Security Monitoring S	Email Journaling		SI-3,SI-4		SI-3,SI-4		SI-4(5)	SI-3(7)	SI-3(7),SI-4(5)			SI-4(10),SI-4(12)		SI-4(10),SI-4(12)		AC-1, AC-2, AC-3,	AC-2(1), AC-2(2), AC-	AC-2(11), AC-2(13),	2.00	3.00	2.00	7.00	X	X	A
BOSS	Security Monitoring S	User Behaviors and Profile		AC-2,AU-1,AU-2,AU-		AC-2,AU-1,AU-2,AU-		AU-2(3),AU-3(1)	AC-2(12),AU-6(7)	AC-2(12),AU-2(3),AU-	AU-6(7)		AU-6(6)	AU-6(6)		PM-12, PM-13	AC-1, AC-2, AC-3,	AC-2(1), AC-2(2), AC-	AC-2(11), AC-2(13),	3.00	2.00	2.00	7.00	X	X	A
BOSS	Legal Services	E-Discovery		AU-1,AU-2,AU-3,AU-		AU-1,AU-2,AU-3,AU-		AU-3(1),AU-7,AU-	AU-9(2),IR-7(2)	AU-3(1),AU-7,AU-		AU-12(1),AU-12(3),IR-	AU-3(2),AU-9(3),AU-	AU-12(1),AU-12(3),IR-	AU-3(2),AU-9(3),AU-		AC-1, AC-2, AC-3,	AC-2(1), AC-2(2), AC-	AC-2(11), AC-2(13),	1.00	2.00	2.00	5.00	X	X	X
BOSS	Legal Services	Incident Response Legal		AU-1,IR-1		AU-1,IR-1		AU-10		AU-10		AU-10	AU-10(1),AU-10(3)	AU-10,AU-10(3)	AU-10(1)					1.00	3.00	1.00	5.00	X	X	X
BOSS	Internal Investigation	Forensic Analysis		AU-6,IR-5,IR-7		AU-6,IR-5,IR-7		AU-6(1),AU-6(3),AU-		AU-6(1),AU-6(3),AU-		AU-6(5),AU-6(6),IR-	AU-6(7),AU-6(8)	AU-6(5),AU-6(6),AU-			AC-1, AC-2, AC-3,	AC-2(1), AC-2(2), AC-	AC-2(11), AC-2(13),	1.00	1.00	1.00	3.00	X	X	X
BOSS	Internal Investigation	e-Mail Journaling		AU-1,AU-2,AU-3,AU-	AU-8(1)	AU-1,AU-2,AU-3,AU-	AU-8(1)	AU-3(1),AU-7,AU-		AU-3(1),AU-7,AU-		AU-12(1),AU-12(3)	AU-9(2),AU-9(3),AU-	AU-12(1),AU-12(3)	AU-9(2),AU-9(3),AU-		AC-1, AC-2, AC-3,	AC-2(1), AC-2(2), AC-	AC-2(11), AC-2(13),	2.00	3.00	2.00	7.00	A	A	A
BOSS	Compliance	Independent Audits		CA-1,CA-2,CA-7,RA-	CA-2(1)	CA-1,CA-2,CA-		CA-7(1),RA-5(1),RA-	CA-2(2),CA-8,CA-	CA-2(2),CA-7(1),CA-			CA-7(3),SA-11(3)	CA-7(3)	SA-11(3)		AC-1, AC-2, AC-3,	AC-2(1), AC-2(2), AC-	AC-2(11), AC-2(13),	1.00	2.00	2.00	5.00	A	A	A
BOSS	Compliance	Third Party's Compliance		AC-20,CA-3,PS-7,SA-	SA-12	AC-20,CA-3,PS-7,SA-	SA-12	AC-20(1),SA-9(2)	SA-9(1),SA-9(3),SA-	AC-20(1),SA-9(1),SA-	SA-9(3)						AC-1, AC-2, AC-3,	AC-2(1), AC-2(2), AC-	AC-2(11), AC-2(13),	1.00	2.00	2.00	5.00	A	A	A
BOSS	Operational Risk Mar	Business Impact Analysis		CM-4,CP-2,RA-1,RA-		CM-4,CP-2,RA-1,RA-		CM-3,CM-9,CP-		CM-3,CM-9,CP-		CP-2(4),CP-2(5)	SA-14	CP-2(4),CP-3(5)	SA-14	PM-4, PM-7, PM-9	AC-1, AC-2, AC-3,	AC-2(1), AC-2(2), AC-	AC-2(11), AC-2(13),	0.00	1.00	2.00	3.00	A	A	A
BOSS	Operational Risk Mar	Business Continuity	Planning & Testing	CP-1,CP-2,CP-3,CP-		CP-1,CP-2,CP-3,CP-		CP-2(1),CP-2(3),CP-	CP-9	CP-2(1),CP-2(3),CP-	CP-9	CP-2(2),CP-2(4),CP-	CP-2(7),IR-4(3)	CP-2(4),CP-2(5),CP-	CP-2(2),CP-9(3)	PM-9				0.00	2.00	4.00	6.00	X	A	A
BOSS	Operational Risk Mar	Crisis Management		CP-1,CP-2,CP-3,CP-		CP-1,CP-2,CP-3,CP-		CP-2(1),CP-2(3),CP-		CP-2(1),CP-2(3),CP-		CP-3(1),CP-10(4),IR-	IR-3(1),IR-4(3),IR-	CP-3(1),CP-10(4),IR-	IR-3(1),IR-4(10),IR-					1.00	2.00	1.00	4.00	A	A	A
BOSS	Operational Risk Mar	Risk Management Framework	Business & Technical	RA-3		RA-3							SA-14		SA-14	PM-9, PM-10, PM-				1.00	2.00	2.00	5.00	A	A	A
BOSS	Operational Risk Mar	Independent Risk Management		CA-2,CA-7,RA-3		CA-2,CA-7,RA-3		CA-2(1),CA-7(1)		CA-7(1)	CA-2(1)	CA-8	CA-8(1)		CA-8,CA-8(1)	PM-9				1.00	2.00	2.00	5.00	A	A	A
BOSS	Security Monitoring S	Database Monitoring		AU-1,AU-2,AU-3,AU-		AU-1,AU-2,AU-3,AU-		AU-2(3),AU-3(1),AU-	SI-4(1)	AU-2(3),AU-3(1),AU-		AU-12(1),AU-12(3)	AU-3(2),SI-4(14),SI-	AU-12(1),AU-12(3),CA-	AU-3(2),SI-4(14),SI-		AC-1, AC-2, AC-3,	AC-2(1), AC-2(2), AC-	AC-2(11), AC-2(13),	2.00	3.00	3.00	8.00	X	A	
BOSS	Security Monitoring S	Application Monitoring		AU-1,AU-2,AU-3,AU-		AU-1,AU-2,AU-3,AU-		AU-2(3),AU-3(1),AU-	SI-4(1)	AU-2(3),AU-3(1),AU-		AU-12(1),AU-12(3)	AU-3(2),SI-4(14),SI-	AU-12(1),AU-12(3),CA-	AU-3(2),SI-4(14),SI-		AC-1, AC-2, AC-3,	AC-2(1), AC-2(2), AC-	AC-2(11), AC-2(13),	2.00	3.00	3.00	8.00	X	X	X
BOSS	Security Monitoring S	End-Point Monitoring		AU-1,AU-2,AU-3,AU-		AU-1,AU-2,AU-3,AU-		AU-2(3),AU-3(1),AU-	SI-4(1)	AU-2(3),AU-3(1),AU-		AU-12(1),AU-12(3)	AU-3(2),SI-4(14),SI-	AU-12(1),AU-12(3),CA-	AU-3(2),SI-4(14),SI-		AC-1, AC-2, AC-3,	AC-2(1), AC-2(2), AC-	AC-2(11), AC-2(13),	2.00	3.00	3.00	8.00	X	X	X
BOSS	Security Monitoring S	Cloud Monitoring		AU-1,AU-2,AU-3,AU-		AU-1,AU-2,AU-3,AU-		AU-2(3),AU-3(1),AU-	SI-4(1)	AU-2(3),AU-3(1),AU-		AU-12(1),AU-12(3)	AU-3(2),SI-4(14),SI-	AU-12(1),AU-12(3),CA-	AU-3(2),SI-4(14),SI-		AC-1, AC-2, AC-3,	AC-2(1), AC-2(2), AC-	AC-2(11), AC-2(13),	2.00	3.00	3.00	8.00	X	X	X
BOSS	Data Governance	Secure Disposal of Data		SA-3,MP-6		SA-3,MP-6		MP-6(2)		MP-6(2)		MP-6(1)	AC-4(13),MP-6(8)	MP-6(1)	AC-4(13),MP-6(8)					3.00	3.00	3.00	9.00	X	A	A
BOSS	Human Resource Se	Employee Termination		AC-2,PE-2,PS-4,PS-5		AC-2,PE-2,PS-4,PS-5						PS-4(2)	PS-4(1)	PS-4(2)	PS-4(1)					2.00	3.00	2.00	7.00	X	X	X
BOSS	Human Resource Se	Employment Agreements		AC-20,AT-2,CA-3,PL-		AC-20,AT-2,CA-3,PL-		AC-6,AC-20(1),AC-		AC-6,AC-20(1),AC-		SA-12	SA-12(12)	SA-12	SA-12(12)					2.00	2.00	2.00	6.00	X	X	X
BOSS	Human Resource Se	Background Screening		PS-2,PS-3,PS-7,SA-9		PS-2,PS-3,PS-7,SA-9			PS-3(3)	PS-3(3)			PS-3(1),SA-21		PS-3(1),SA-21					2.00	2.00	2.00	6.00	X	X	X
BOSS	Human Resource Se	Job Descriptions		AC-1,AT-1,AU-1,CA-		AC-1,AT-1,AU-1,CA-		CM-9		CM-9						PM-1, PM-10				1.00	1.00	1.00	3.00	X	X	X
BOSS	Human Resource Se	Roles and Responsibilities						AC-5,AC-6		AC-5,AC-6										1.00	1.00	1.00	3.00	X	X	X
BOSS	Human Resource Se	Employee Code of Conduct		PL-4,PS-6,PS-8		PL-4,PS-6,PS-8		PL-4(1)		PL-4(1)						PM-1				2.00	2.00	2.00	6.00	X	X	X
BOSS	Compliance	Information Systems Regulatory		AC-1,AT-1,AU-1,CA-		AC-1,AT-1,AU-1,CA-										PM-1, PM-9				1.00	1.00	1.00	3.00	A	A	A
BOSS	Data Governance	Data Ownership / Stewardship		AC-1,AC-2,AC-3,AC-		AC-1,AC-2,AC-3,AC-		AC-4,AC-6,AC-12,CM-	AC-4(5),AC-4(6),AC-	AC-4,AC-6,AC-10,AC-	AC-4(5),AC-4(6),AC-	SI-7(2)	AC-9,AC-3(7),AC-	AC-9,SI-7(2),AC-3(9)	AC-3(7),AC-3(8),AC-	PM-1				3.00	3.00	3.00	9.00	X	X	X
BOSS	Data Governance	Data Classification		RA-2,RA-3		RA-2,RA-3										PM-9, PM-11				3.00	1.00	1.00	5.00	X	X	X
BOSS	Security Monitoring S	Managed (Outsourced) Security		AC-20,PS-7,SA-4,SA-		AC-20,PS-7,SA-4,SA-		AC-20(1),SA-4(1),SA-		AC-20(1),SA-4(1),SA-			SA-4(5),SA-9(3),SA-		SA-4(5),SA-9(3),SA-					1.00	1.00	1.00	3.00	X	X	X
BOSS	Legal Services	Contracts		SA-1,SA-4,SA-9		SA-1,SA-4,SA-9		SA-4(1),SA-4(2),SA-		SA-4(1),SA-4(2),SA-		SA-12	SA-4(3),SA-4(5),SA-	SA-12,SA-12(2),SA-	SA-4(3),SA-4(5),SA-					3.00	3.00	3.00	9.00	X	X	X
BOSS	Security Monitoring S	Honey Pot											SC-26,SC-35		SC-26,SC-35		AC-1, AC-2, AC-3,	AC-2(1), AC-2(2), AC-	AC-2(11), AC-2(13),	2.00	1.00	2.00	5.00	A	A	
BOSS	Security Monitoring S	Real Time Internetwork		CA-7,SI-4		CA-7,SI-4		CA-7(1),SI-4(2),SI-4(4)		CA-7(1),SI-4(2),SI-4(4)			SI-4(11),SI-4(12),SI-	SI-4(11),SI-4(18),SI-	SI-4(12)		AC-1, AC-2, AC-3,	AC-2(1), AC-2(2), AC-	AC-2(11), AC-2(13),	3.00	3.00	3.00	9.00	A	A	A
BOSS	Data Governance	Rules for Data Retention		AU-11,MP-6,SA-3,SI-		AU-11,MP-6,SA-3,SI-										PM-11	AC-1, AC-2, AC-3,	AC-2(1), AC-2(2), AC-	AC-2(11), AC-2(13),	1.00	2.00	3.00	6.00	A	A	A
BOSS	Security Monitoring S	Security Information and Event		AU-6,AU-12,SI-4		AU-6,AU-12,SI-4		AU-6(1),AU-6(3),SI-		AU-6(1),AU-6(3),SI-		AU-6(5),AU-6(6),AU-	AU-6(9),SI-4(3),SI-	AU-6(5),AU-6(6),AU-	AU-6(9),SI-4(3),SI-		AC-1, AC-2, AC-3,	AC-2(1), AC-2(2), AC-	AC-2(11), AC-2(13),	3.00	3.00	3.00	9.00	X	X	A
BOSS	Security Monitoring S	Anti Phishing		SC-7,SI-4	SI-8	SC-7,SI-4	SI-8	SI-8(1),SI-8(2)		SI-8(1),SI-8(2)			SC-7(11),SI-4(10),SI-		SC-7(11),SI-4(10),SI-					2.00	2.00	2.00	6.00	A	A	A
BOSS	Compliance	Contract/ Authority Maintenance		AC-2,AU-1,AU-2,AU-	SI-7	AC-2,AU-1,AU-2,AU-	SI-7	AC-2(4),AC-6,AC-		AC-2(4),AC-6,AC-		AC-2(12),AU-6(5),AU-	AU-3(2),AU-6(4),AU-	AU-6(5),AU-6(6),AU-	AC-2(12),AU-3(2),CM-	PM-4				2.00	2.00	2.00	6.00	X	X	A
BOSS	Operational Risk Mar	Operational Risk Committee		CA-2,RA-1,RA-2,RA-		CA-2,RA-1,RA-2,RA-			CA-2(2)	CA-2(2)						PM-9, PM-10, PM-				1.00	2.00	1.00	4.00	X	A	A
BOSS	Operational Risk Mar	Key Risk Indicators		RA-1,RA-3		RA-1,RA-3							RA-6,SA-14		RA-6,SA-14	PM-6, PM-9				1.00	2.00	1.00	4.00	X	X	A
BOSS	Security Monitoring S	Counter Threat Management		CA-7,RA-3		CA-7,RA-3		CA-7(1)	CA-8,CA-8(1)	CA-7(1),CA-8,CA-8(1)			CA-7(3)	CA-7(3)		PM-9, PM-12, PM-	AC-1, AC-2, AC-3,	AC-2(1), AC-2(2), AC-	AC-2(11), AC-2(13),	1.00	1.00	1.00	3.00	A	A	A
BOSS	Security Monitoring S	Security Operation Center		AU-12,CA-7,SI-4		AU-12,CA-7,SI-4		CA-7(1),SI-4(5)		CA-7(1),SI-4(5)		AU-12(1),AU-12(3)	SI-4(3),SI-4(16),SI-	AU-12(1),AU-12(3)	SI-4(3),SI-4(16),SI-		AC-1, AC-2, AC-3,	AC-2(1), AC-2(2), AC-	AC-2(11), AC-2(13),	1.00	1.00	1.00	3.00	A	A	A
BOSS	Security Monitoring S	Branding Protection											AU-13,AU-13(1),AU-		AU-13,AU-13(1),AU-					2.00	3.00	3.00	8.00	A	A	A
ITOS	IT Operations	Resource Management	Segregation of duties					AC-5		AC-5										1.00	1.00	2.00	4.00	X	X	X
ITOS	IT Operations	Resource Management	Contractors	AC-2,AC-3,AC-20,AT-		AC-2,AC-3,AC-20,AT-		AC-6,AC-20(1),CM-		AC-6,AC-20(1),CM-		AC-2(11),AC-2(12)	CM-5(5),SA-21,SC-43	AC-2(11)	AC-2(12),CM-5(5),SA-					1.00	1.00	2.00	4.00	A	A	A
ITOS	Service Delivery	Information Technology	Resiliency Analysis	CP-1,CP-2,CP-3,CP-		CP-1,CP-2,CP-3,CP-		CP-2(3),CP-2(8),CP-	CP-2(2)	CP-2(2),CP-2(3),CP-		PE-11(1),CP-2(4),CP-	AU-15,CP-2(6),CP-	PE-11(1),CP-2(4),CP-	CP-2(6),CP-11,CP-	PM-3, PM-9				1.00	0.00	2.00	3.00	X	A	A
ITOS	Service Delivery	Information Technology	Capacity Planning	AU-4,CP-2,SA-2,SC-5		AU-4,CP-2,SA-2,SC-5		PE-11	CP-2(2)	CP-2(2),PE-11		PE-11(1)	SC-5(2),AU-4(1),PE-	PE-11(1),SC-5(2)	AU-4(1),PE-11(2)					1.00	2.00	3.00	6.00	X	A	A
ITOS	Service Support	Configuration Management	Automated Asset Discovery	CA-7,CM-2,CM-8	CM-3	CA-7,CM-2,CM-8	CM-3	CA-7(1),CM-2(1),CM-		CA-7(1),CM-2(1),CM-	CM-3(2)	CM-2(2),CM-3(1),CM-	CM-8(7)	CM-3(1),CM-8(2),CM-	CM-2(2),CM-8(7)	PM-5	AC-1, AC-2, AC-3,	AC-2(1), AC-2(2), AC-	AC-2(11), AC-2(13),	2.00	1.00	1.00	4.00	A	A	A
ITOS	Service Support	Problem Management	Event Classification	AU-1,AU-2,AU-3,AU-		AU-1,AU-2,AU-3,AU-		AU-2(3),AU-3(1),AU-		AU-2(3),AU-3(1),AU-		AU-6(5)	AU-3(2),AU-12(2)	AU-6(5),AU-12(2)	AU-3(2)		AC-1, AC-2, AC-3,	AC-2(1), AC-2(2), AC-	AC-2(11), AC-2(13),	1.00	2.00	2.00	5.00	X	X	X
ITOS	Service Support	Problem Management	Root Cause Analysis	IR-4		IR-4											AC-1, AC-2, AC-3,	AC-2(1), AC-2(2), AC-	AC-2(11), AC-2(13),	2.00	2.00	1.00	5.00	A	A	A
ITOS	IT Operations	Portfolio Management	Maturity Model													PM-1, PM-5, PM-6	AC-1, AC-2, AC-3,	AC-2(1), AC-2(2), AC-	AC-2(11), AC-2(13),	1.00	1.00	2.00	4.00	A	A	A

NIST SP 800-174: SECURITY AND PRIVACY CONTROLS FOR CLOUD-BASED FEDERAL INFORMATION SYSTEMS

NIST Interactive Questionnaire

Role	Question	Response
CIO	Does the organization maintain an up-to-date inventory of all IT hardware assets?	
Sysadmin	Does the system provide location services reporting the physical location of assets, resources, facilities, people, etc.?	
CIO	Does the organization maintain an up-to-date inventory of all IT software and virtual machine assets?	
CISO	Does the organization categorize/classify and label its data, servers, endpoints, and other assets based on their sensitivity and value in accordance with organizational policy?	
Sysadmin	Does the system assign, use, and manage data tags for specific pieces of information to facilitate data classification?	
Contracts	Does the organization have processes and resources in place to support contracts, including standard clauses for system security and privacy?	
CIO	Does the organization document its business goals, objectives, and processes, then analyze that information to help determine IT, security, and risk management strategies and priorities?	
CISO	Does the organization document its information security program's capabilities and map these capabilities to what the business does?	
CISO	Does the organization use documented processes for developing, documenting, disseminating, reviewing, updating, and handling exceptions to its information security policies?	
CISO	Does the organization establish contracts, service level agreements (SLA), or other formal agreements with internal groups and external parties regarding the security of their systems and/or services delivered by those groups or parties, as well as the consequences of failure to meet those agreements?	
Legal	Are there standard agreements for the purpose of specifying terms and conditions, including a privacy policy, intellectual property agreements, acceptable use, a code of conduct, website terms and conditions, or non-disclosures and non-competes, prior to granting employees, contractors, third parties, and customers access to the organization's data, services, and systems?	
Sysadmin	Does the system associate a particular security policy with a certain role (data owner, custodian, delegate, etc.), in essence defining roles that each have a unique combination of privileges and rights?	
CISO	Does the organization manage the applicable legal and regulatory requirements involving security, including mapping these requirements to the organization's security best practices and storing them in a risk register?	
CISO	Does the organization define and measure objectives for security services and their delivery?	
CISO	Has the organization defined its approach to governance, risk, and compliance, and refines that approach as needed?	
Sysadmin	Does the system use an automation protocol (e.g. Security Content Automation Protocol (SCAP)) to detect vulnerabilities and verify and detect whether or not the system's configuration has changed for the purpose of detecting unauthorized changes?	
Sysadmin	Does the system receive threat and vulnerability management information from other sources, such as threat intelligence feeds, peer organizations, vulnerability databases, or security monitoring services?	
CISO	Does the organization manage information security threats, including identifying, categorizing, and characterizing known threats against each system?	
CISO	Does the organization use risk management principles to identify, assess, prioritize, and track risks?	
CISO	Does the organization determine how to counter threats through a systematic, repeatable, documented approach?	
CISO	Does the organization develop, implement, review, and update a comprehensive risk management strategy designed to manage risk to organizational operations and assets, individuals, and other organizations, with this strategy including the organization's risk management framework, risk assessment methodologies, risk mitigation strategies, risk monitoring approaches, and risk evaluation processes?	
CISO	Does the organization use testing, such as compliance testing or penetration testing, as part of managing risk?	
HR	Does the level of each background investigation align with the data classifications the person would be permitted to access, pursuant to laws, regulations, other requirements, and ethics?	

Yes
No
Not Sure

NIST Interactive Questionnaire

Role	Question	Response
CIO	Does the organization maintain an up-to-date inventory of all IT hardware assets?	Yes
Sysadmin	Does the system provide location services reporting the physical location of assets, resources, facilities, people, etc.?	Yes
CIO	Does the organization maintain an up-to-date inventory of all IT software and virtual machine assets?	Yes
CISO	Does the organization categorize/classify and label its data, servers, endpoints, and other assets based on their sensitivity and value in accordance with organizational policy?	Yes
Sysadmin	Does the system assign, use, and manage data tags for specific pieces of information to facilitate data classification?	Yes
Contracts	Does the organization have processes and resources in place to support contracts, including standard clauses for system security and privacy?	Yes
CIO	Does the organization document its business goals, objectives, and processes, then analyze that information to help determine IT, security, and risk management strategies and priorities?	Yes
CISO	Does the organization document its information security program's capabilities and map these capabilities to what the business does?	Yes
CISO	Does the organization use documented processes for developing, documenting, disseminating, reviewing, updating, and handling exceptions to its information security policies?	Yes
CISO	Does the organization establish contracts, service level agreements (SLA), or other formal agreements with internal groups and external parties regarding the security of their systems and/or services delivered by those groups or parties, as well as the consequences of failure to meet those agreements?	Yes
Legal	Are there standard agreements for the purpose of specifying terms and conditions, including a privacy policy, intellectual property agreements, acceptable use, a code of conduct, website terms and conditions, or non-disclosures and non-competes, prior to granting employees, contractors, third parties, and customers access to the organization's data, services, and systems?	Yes
Sysadmin	Does the system associate a particular security policy with a certain role (data owner, custodian, delegate, etc.), in essence defining roles that each have a unique combination of privileges and rights?	Yes
CISO	Does the organization manage the applicable legal and regulatory requirements involving security, including mapping these requirements to the organization's security best practices and storing them in a risk register?	Not Sure
CISO	Does the organization define and measure objectives for security services and their delivery?	Yes
CISO	Has the organization defined its approach to governance, risk, and compliance, and refines that approach as needed?	Yes
Sysadmin	Does the system use an automation protocol (e.g. Security Content Automation Protocol (SCAP)) to detect vulnerabilities and verify and detect whether or not the system's configuration has changed for the purpose of detecting unauthorized changes?	No
Sysadmin	Does the system receive threat and vulnerability management information from other sources, such as threat intelligence feeds, peer organizations, vulnerability databases, or security monitoring services?	No
CISO	Does the organization manage information security threats, including identifying, categorizing, and characterizing known threats against each system?	Yes
CISO	Does the organization use risk management principles to identify, assess, prioritize, and track risks?	Yes
CISO	Does the organization determine how to counter threats through a systematic, repeatable, documented approach?	Yes
CISO	Does the organization develop, implement, review, and update a comprehensive risk management strategy designed to manage risk to organizational operations and assets, individuals, and other organizations, with this strategy including the organization's risk management framework, risk assessment methodologies, risk mitigation strategies, risk monitoring approaches, and risk evaluation processes?	

Yes
No
Not Sure

NIST Interactive Questionnaire

Role	Question	Response
CIO	Does the organization maintain an up-to-date inventory of all IT hardware assets?	Yes
Sysadmin	Does the system provide location services reporting the physical location of assets, resources, facilities, people, etc.?	Yes
CIO	Does the organization maintain an up-to-date inventory of all IT software and virtual machine assets?	Yes
CISO	Does the organization categorize/classify and label its data, servers, endpoints, and other assets based on their sensitivity and value in accordance with organizational policy?	Yes
Sysadmin	Does the system assign, use, and manage data tags for specific pieces of information to facilitate data classification?	Yes
Contracts	Does the organization have processes and resources in place to support contracts, including standard clauses for system security and privacy?	Yes
CIO	Does the organization document its business goals, objectives, and processes, then analyze that information to help determine IT, security, and risk management strategies and priorities?	Yes
CISO	Does the organization document its information security program's capabilities and map these capabilities to what the business does?	Yes
CISO	Does the organization use documented processes for developing, documenting, disseminating, reviewing, updating, and handling exceptions to its information security policies?	Yes
CISO	Does the organization establish contracts, service level agreements (SLA), or other formal agreements with internal groups and external parties regarding the security of their systems and/or services delivered by those groups or parties, as well as the consequences of failure to meet those agreements?	Yes
Legal	Are there standard agreements for the purpose of specifying terms and conditions, including a privacy policy, intellectual property agreements, acceptable use, a code of conduct, website terms and conditions, or non-disclosures and non-competes, prior to granting employees, contractors, third parties, and customers access to the organization's data, services, and systems?	Yes
Sysadmin	Does the system associate a particular security policy with a certain role (data owner, custodian, delegate, etc.), in essence defining roles that each have a unique combination of privileges and rights?	Yes
CISO	Does the organization manage the applicable legal and regulatory requirements involving security, including mapping these requirements to the organization's security best practices and storing them in a risk register?	Yes
CISO	Does the organization define and measure objectives for security services and their delivery?	Yes
CISO	Has the organization defined its approach to governance, risk, and compliance, and refines that approach as needed?	Yes
Sysadmin	Does the system use an automation protocol (e.g. Security Content Automation Protocol (SCAP)) to detect vulnerabilities and verify and detect whether or not the system's configuration has changed for the purpose of detecting unauthorized changes?	Yes
Sysadmin	Does the system receive threat and vulnerability management information from other sources, such as threat intelligence feeds, peer organizations, vulnerability databases, or security monitoring services?	Yes

NIST Interactive Questionnaire Results

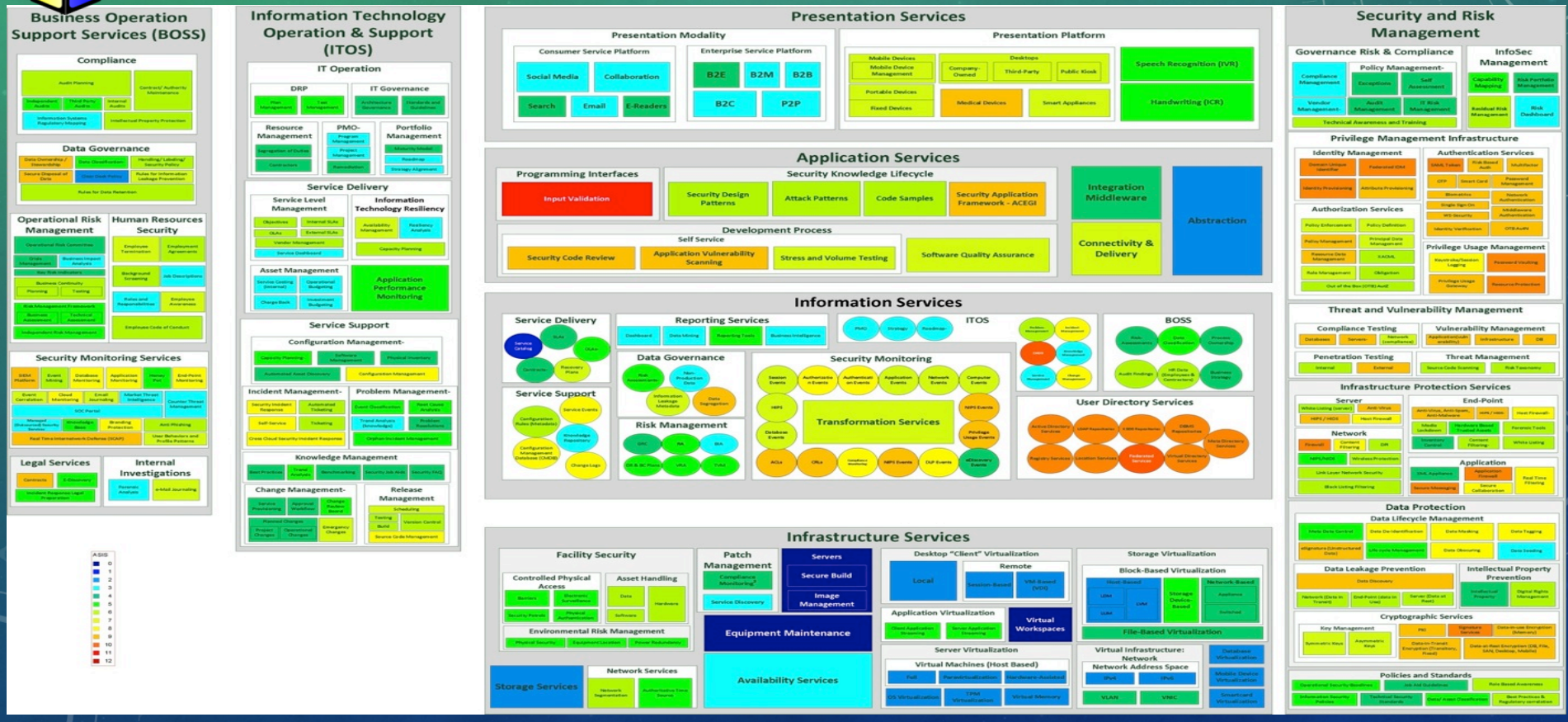
CSF Subcategory ID	CSF Subcategory Description	FY 2017 CIO FISMA Metrics	Domain	Container	Capability (process or solution)	Capability (process or solution)	Revised Description	Unique Identifier	NIST Baseline	Additional Suggested Controls	FedRAMP Baseline	Ad Su C
									SP 800-53 R4 security controls for LOW-IMPACT SYSTEMS			
ID.AM	Identify--Asset Management											
ID.AM-1	Physical devices and systems within the organization are inventoried	1.1, 1.2, 1.3, 1.4, 1.5, 3.16										
			ITOS	Service Support	Configuration Management	Automated Asset Discovery	The system's organization has a capability that identifies new and changing assets across the IT infrastructure and maintains an up-to-date inventory of configuration items.	Automated Asset Discovery	CA-7,CM-2,CM-8	CM-3	CA-7,CM-2,CM-8	CM-
			ITOS	Service Support	Configuration Management	Physical Inventory	The system's organization has a capability that tracks all IT assets, including their ownership and current custody.	Physical Inventory	CM-8		CM-8	
			S & RM	Infrastructure Protection Services	End-Point	Inventory Control	The system has a capability that manages and maintains inventory for its physical and digital assets, including virtual machines.	Inventory Control	CM-8		CM-8	
			Information Services	User Directory Services	Location Services		The system has a capability that provides location services reporting the physical location of assets, resources, facilities, people, etc.	Location Services	CM-8		CM-8	
ID.AM-2	Software platforms and applications within the organization are inventoried	2.3.1, 3.17										
			ITOS	Service Support	Configuration Management	Automated Asset Discovery	The system's organization has a capability that identifies new and changing assets across the IT infrastructure and maintains an up-to-date inventory of configuration items.	Automated Asset Discovery	CA-7,CM-2,CM-8	CM-3	CA-7,CM-2,CM-8	CM-
			ITOS	Service Support	Configuration Management	Physical Inventory	The system's organization has a capability that tracks all IT assets, including their ownership and current custody.	Physical Inventory	CM-8		CM-8	
			S & RM	Infrastructure Protection Services	End-Point	Inventory Control	The system has a capability that manages and maintains inventory for its physical and digital assets, including virtual machines.	Inventory Control	CM-8		CM-8	
ID.AM-5	Resources (e.g., hardware, devices, data, and software) are prioritized based on their											
			BOSS	Data Governance	Handling/ Labeling/ Security Policy		The system has a policy, enforced by a capability, that requires accurate labeling and identifiers for information and its associated media and data repositories. If virtual repositories	Handling/ Labeling/ Security	AC-1,AC-3,AT-1,AU-1,CA-1,CM-1,CP-	AC-4	AC-1,AC-3,AT-1,AU-1,CA-1,CM-1,CP-	AC-
			BOSS	Data Governance	Data Classification		The system's data is assigned classifications (e.g. controlled unclassified information, classified, sensitive) based on the sensitivity of the data and its value to the system owner. The	Data Classification-	RA-2,RA-3		RA-2,RA-3	
			Information Services	BOSS	Data Classification		The system's organization has a capability to categorize the organization's information to guide data handling.	Data Classification	RA-2		RA-2	
			S & RM	Policies and Standards	Data/ Asset Classification		The system's organization has a capability that defines a classification scheme for information, servers, endpoints, and other assets so that specific security policies can be applied to	Data/ Asset Classification	RA-2,RA-3		RA-2,RA-3	
			S & RM	Data Protection	Data Lifecycle Management	Data Tagging	The system has a capability that assigns, uses, and manages data tags for specific pieces of information to aid in browsing and searching activities.	Data Tagging		AC-4		AC-
ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party											
			BOSS	Legal Services	Contracts		The system's organization has processes and resources in place to support contracts. A contract template is in place that includes contract clauses for system security and privacy.	Contracts	SA-1,SA-4,SA-9		SA-1,SA-4,SA-9	
ID.BE	Identify--Business Environment											
ID.BE-3	Priorities for organizational mission, objectives, and activities are established and											
			BOSS	Operational Risk	Business Impact Analysis		The system's organization has a process for conducting a	Business	CM-4,CP-2,RA-		CM-4,CP-2,RA-	

NIST SP 800-174: SECURITY AND PRIVACY CONTROLS FOR CLOUD-BASED FEDERAL INFORMATION SYSTEMS

Suggested functional capabilities and security controls based on the answers to the Questionnaire

											K	L	M	N	O	P	Q	R	S	T		
											SP800-53 Rev4 Security Controls for Implementing Functional Capabilities											
											SP 800-53 R4 security controls for LOW-IMPACT SYSTEMS				SP 800-53 R4 security controls for MODERATE-IMPACT SYSTEMS				SP 800-53 R4 secur HIGH-IMPACT			
	CSF Subcategory ID	CSF Subcategory Description	FY 2017 CIO FISMA Metrics	Domain	Container	Capability (process or solution)	Capability (process or solution)	Revised Description	Unique Identifier	NIST Baseline	Additional Suggested Controls	FedRAMP Baseline	Additional Suggested Controls	NIST Baseline	Additional Suggested Controls	FedRAMP Baseline	Additional Suggested Controls	NIST Baseline	Additional Suggested Controls		
	ID.AM	Identify--Asset Management																				
	ID.AM-1	Physical devices and systems within the organization are inventoried	1.1, 1.2, 1.3, 1.4, 1.5, 3.16																			
				ITOS	Service Support	Configuration Management	Automated Asset Discovery	The system's organization has a capability that identifies new and changing assets across the IT infrastructure and maintains an up-to-date inventory of configuration items.	Automated Asset Discovery	CA-7,CM-2,CM-8	CM-3	CA-7,CM-2,CM-8	CM-3	CA-7(1),CM-2(1),CM-2(3),CM-		CA-7(1),CM-2(1),CM-2(3),CM-	CM-3(2)	CM-2(2),CM-3(1),CM-8(2),CM-8(4)	CM-8(7)	C 8	
				ITOS	Service Support	Configuration Management	Physical Inventory	The system's organization has a capability that tracks all IT assets, including their ownership and current custody.	Physical Inventory	CM-8		CM-8		CM-8(1),CM-8(3),CM-8(5)		CM-8(1),CM-8(3),CM-8(5)		CM-8(2),CM-8(4)	CM-8(8)	C 8	
				S & RM	Infrastructure Protection Services	End-Point	Inventory Control	The system has a capability that manages and maintains inventory for its physical and digital assets, including virtual machines.	Inventory Control	CM-8		CM-8						CM-8(2),CM-8(4)	CM-8(7)	C 8	
				Information Services	User Directory Services	Location Services		The system has a capability that provides location services reporting the physical location of assets, resources, facilities, people, etc.	Location Services	CM-8		CM-8							CM-8(8),PE-20		
	ID.AM-2	Software platforms and applications within the organization are inventoried	2.3.1, 3.17																			
				ITOS	Service Support	Configuration Management	Automated Asset Discovery	The system's organization has a capability that identifies new and changing assets across the IT infrastructure and maintains an up-to-date inventory of configuration items.	Automated Asset Discovery	CA-7,CM-2,CM-8	CM-3	CA-7,CM-2,CM-8	CM-3	CA-7(1),CM-2(1),CM-2(3),CM-		CA-7(1),CM-2(1),CM-2(3),CM-	CM-3(2)	CM-2(2),CM-3(1),CM-8(2),CM-8(4)	CM-8(7)	C 8	
				ITOS	Service Support	Configuration Management	Physical Inventory	The system's organization has a capability that tracks all IT assets, including their ownership and current custody.	Physical Inventory	CM-8		CM-8		CM-8(1),CM-8(3),CM-8(5)		CM-8(1),CM-8(3),CM-8(5)		CM-8(2),CM-8(4)	CM-8(8)	C 8	
				S & RM	Infrastructure Protection Services	End-Point	Inventory Control	The system has a capability that manages and maintains inventory for its physical and digital assets, including virtual machines.	Inventory Control	CM-8		CM-8						CM-8(2),CM-8(4)	CM-8(7)	C 8	
	ID.AM-5	Resources (e.g., hardware, devices, data, and software) are prioritized based on their																				
				BOSS	Data Governance	Handling/ Labeling/ Security Policy		The system has a policy, enforced by a capability, that requires accurate labeling and identifiers for information and its associated media and data repositories. If virtual repositories	Handling/ Labeling/ Security Policy	AC-1,AC-3,AT-1,AU-1,CA-1,CM-1,CP-	AC-4	AC-1,AC-3,AT-1,AU-1,CA-1,CM-1,CP-	AC-4	MP-3,MP-5,MP-5(4)		MP-3,MP-5,MP-5(4)			AC-16		
				BOSS	Data Governance	Data Classification		The system's data is assigned classifications (e.g. controlled unclassified information, classified, sensitive) based on the sensitivity of the data and its value to the system owner. The	Data Classification-	RA-2,RA-3		RA-2,RA-3									
				Information Services	BOSS	Data Classification		The system's organization has a capability to categorize the organization's information to guide data handling.	Data Classification	RA-2		RA-2									
				S & RM	Policies and Standards	Data/ Asset Classification		The system's organization has a capability that defines a classification scheme for information, servers, endpoints, and other assets so that specific security policies can be applied to	Data/ Asset Classification	RA-2,RA-3		RA-2,RA-3							AC-16,AC-16(1),AC-16(2),AC-		
				S & RM	Data Protection	Data Lifecycle Management	Data Tagging	The system has a capability that assigns, uses, and manages data tags for specific pieces of information to aid in browsing and searching activities.	Data Tagging		AC-4		AC-4						AC-4(6),AC-16,SC-16		
	ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party																				
				BOSS	Legal Services	Contracts		The system's organization has processes and resources in place to support contracts. A contract template is in place that includes contract clauses for system security and privacy.	Contracts	SA-1,SA-4,SA-9		SA-1,SA-4,SA-9		SA-4(1),SA-4(2),SA-4(9),SA-9(2)		SA-4(1),SA-4(2),SA-4(9),SA-9(2)		SA-12	SA-4(3),SA-4(5),SA-9(1),SA-	S 1	
	ID.BE	Identify--Business Environment																				

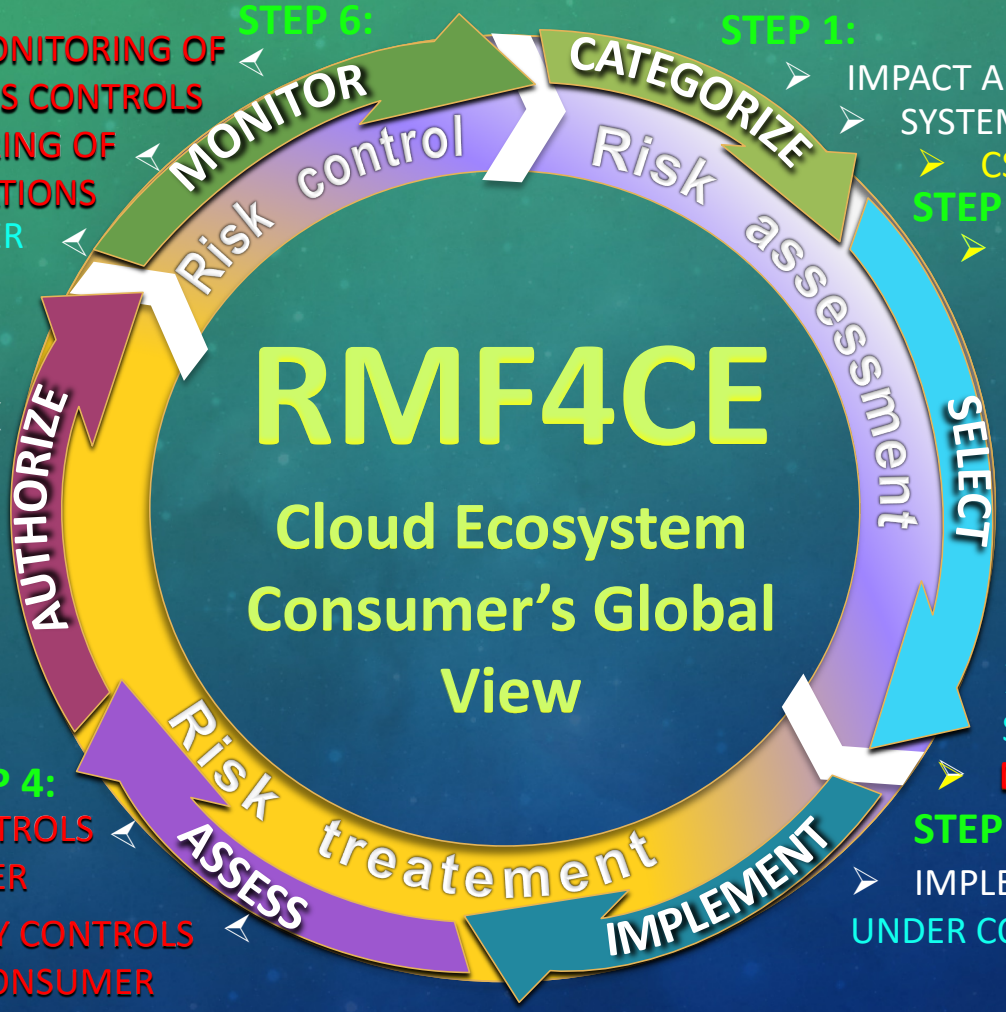
NIST SP 500-299/SP 800-200: NIST CLOUD COMPUTING SECURITY REFERENCE ARCHITECTURE



RMF FOR THE CLOUD ECOSYSTEM

CLOUD SECURITY RUBIK'S CUBE

OSCAL



STEP 1:

- IMPACT ANALYSIS
- SYSTEM CATEGORIZATION
- CSF QUESTIONNAIRE

STEP 2:

- IDENTIFY & SELECT CAPABILITIES
- SELECT BASELINE CONTROLS
- TAILOR & SUPPLEMENT CONTROLS
- IDENTIFY & SELECT BEST-FITTING CLOUD ARCHITECTURE
- SELECT CLOUD PROVIDER
- NEGOTIATE SLA, METRICS, SIGN CONTRACT
- DEVELOP SECURITY PLAN

STEP 3:

- IMPLEMENT SECURITY CONTROLS UNDER CONSUMER'S MANAGEMENT

STEP 4:

- ASSESS SECURITY CONTROLS MANAGED BY PROVIDER
- ASSESS SECURITY CONTROLS MANAGED BY CONSUMER

STEP 5:

- AUTHORIZE CLOUD-BASED INFORMATION SYSTEM (BASED UPON RESIDUAL RISK & RISK TOLERANCE)

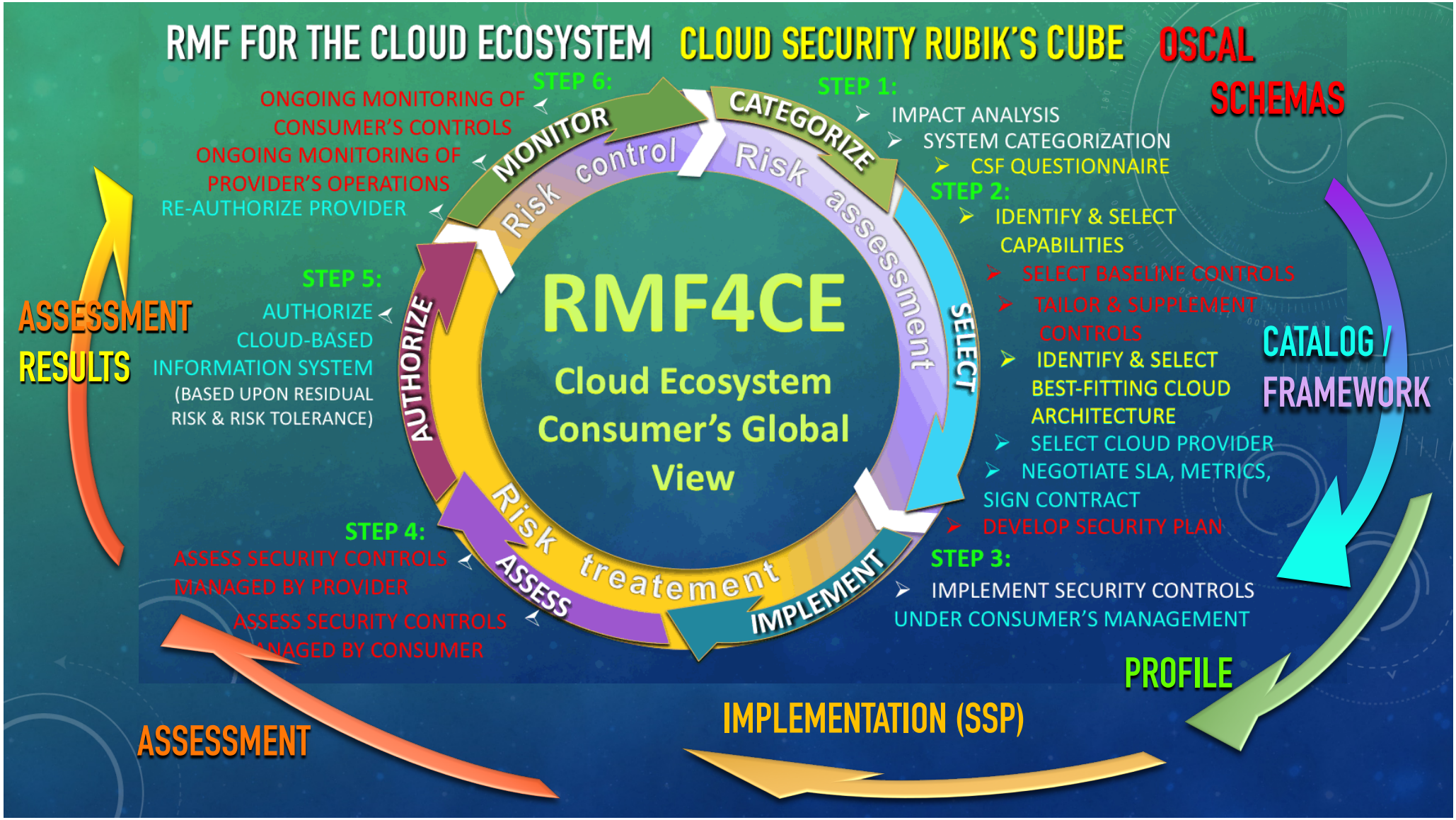
STEP 6:

- ONGOING MONITORING OF CONSUMER'S CONTROLS
- ONGOING MONITORING OF PROVIDER'S OPERATIONS
- RE-AUTHORIZE PROVIDER

NIST
National Institute of Standards and Technology

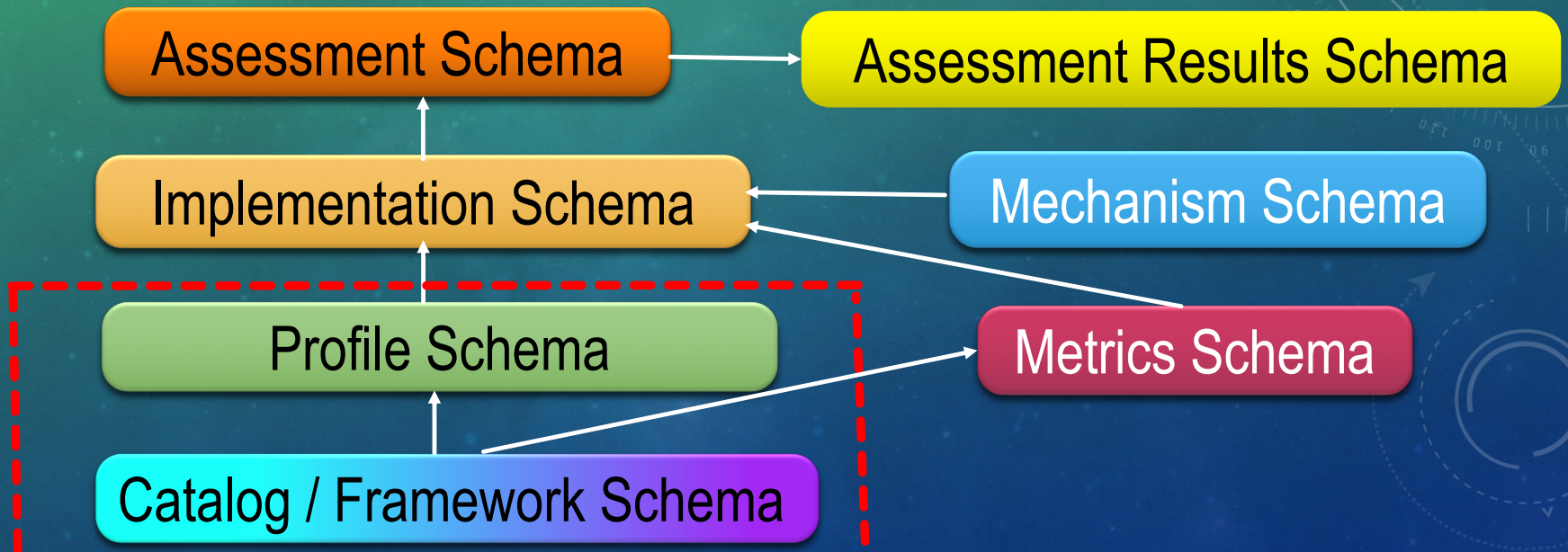
WHAT IS OSCAL?

- New "Standard of Standards" normalizing how system security controls and corresponding assessment information are represented;
- **OSCAL Project Goals:**
  - **Standardized:** Provide security control, control implementation, and assessment information in an open, standardized way that can be used by both humans and machines
  - **Interoperable:** Ensure OSCAL is well-defined so tools using OSCAL information are interoperable and use information consistently
  - **Easy to use:** Promote developer adoption of OSCAL so tools are available for organizations to build, customize, and use OSCAL information
- Improves the efficiency, accuracy, and consistency of system security assessments.


RMF FOR THE CLOUD ECOSYSTEM
CLOUD SECURITY RUBIK'S CUBE
OSCAL SCHEMAS
STEP 6:
ONGOING MONITORING OF CONSUMER'S CONTROLS
ONGOING MONITORING OF PROVIDER'S OPERATIONS
RE-AUTHORIZE PROVIDER
MONITOR
Risk control
CATEGORIZE
Risk assessment
SELECT
STEP 1:
IMPACT ANALYSIS
SYSTEM CATEGORIZATION
CSF QUESTIONNAIRE
STEP 2:
IDENTIFY & SELECT CAPABILITIES
SELECT BASELINE CONTROLS
TAILOR & SUPPLEMENT CONTROLS
IDENTIFY & SELECT BEST-FITTING CLOUD ARCHITECTURE
SELECT CLOUD PROVIDER
NEGOTIATE SLA, METRICS, SIGN CONTRACT
DEVELOP SECURITY PLAN
ASSESSMENT RESULTS
STEP 5:
AUTHORIZE CLOUD-BASED INFORMATION SYSTEM
(BASED UPON RESIDUAL RISK & RISK TOLERANCE)
AUTHORIZE
RMF4CE
Cloud Ecosystem Consumer's Global View
CATALOG / FRAMEWORK
Risk treatement
ASSESS
IMPLEMENT
STEP 4:
ASSESS SECURITY CONTROLS MANAGED BY PROVIDER
ASSESS SECURITY CONTROLS MANAGED BY CONSUMER
STEP 3:
IMPLEMENT SECURITY CONTROLS UNDER CONSUMER'S MANAGEMENT
PROFILE
ASSESSMENT
IMPLEMENTATION (SSP)

NIST
National Institute of Standards and Technology

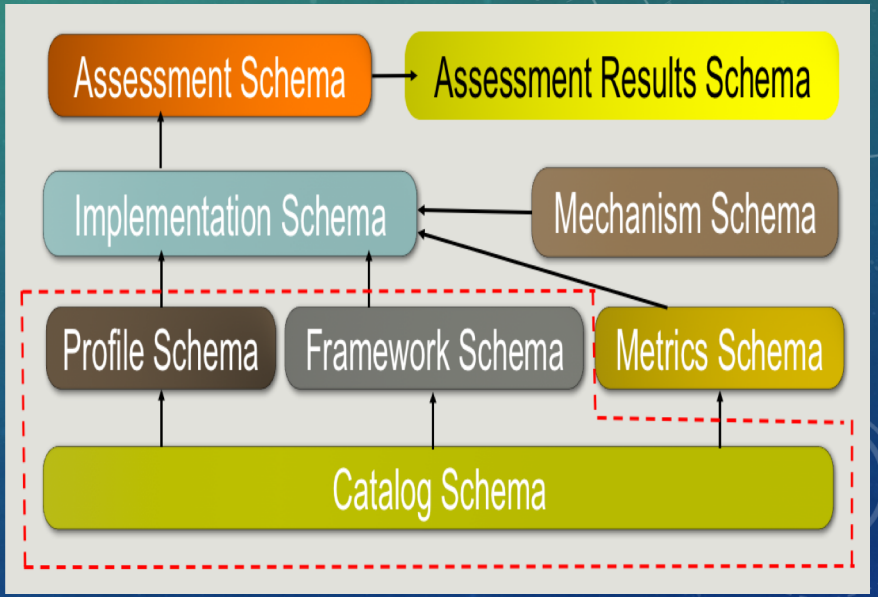
CURRENT FOCUS OF OSCAL DEVELOPMENT



NIST
National Institute of
Standards and Technology

DESCRIPTIONS OF CURRENT COMPONENTS

- **Catalog:** Defines a set of security controls (e.g., NIST SP 800-53 Appendix F); may also define objectives and methods for assessing the controls (e.g., NIST SP 800-53A)
- **Profile:** Defines a set of security requirements, where meeting each requirement necessitates implementing one or more security controls
- **Framework**: Defines a set of security requirements expressed at a higher level (e.g. Cybersecurity Framework)



PROSE VS. OSCAL CATALOG

Control Title

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the access control policy and associated access controls; and

b. Reviews and updates the current:

1. Access control policy [*Assignment: organization-defined frequency*]; and

2. Access control procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** AC-1	**MOD** AC-1	**HIGH** AC-1

```
<catalog xmlns="http://scap.nist.gov/schema/oscal">
  <title>NIST SP800-53</title>
  <declarations href="800-53-declarations.xml"/>
  <group class="family">
    <title>ACCESS CONTROL</title>
    <control class="SP800-53">
      <title>ACCESS CONTROL POLICY AND PROCEDURES</title>
      <prop class="number">AC-1</prop>
      <prop class="priority">P1</prop>
      <feat class="statement">
        <prop class="description">The organization:</prop>
        <feat class="statement">
          <prop class="number">AC-1a.</prop>
          <prop class="description">Develops, documents, and disseminates to <assign id="ac1a">
            organization-defined personnel or roles</assign></prop>
          <feat class="statement-item">
            <prop class="number">AC-1a.1.</prop>
            <prop class="description">An access control policy that addresses purpose, scope, roles,
responsibilities, management commitment, coordination among organizational …[snip]…</prop>
          </feat>
        </feat>
      </feat>
      …[snip]…
      <references>
        <ref>
          <citation href="http://csrc.nist.gov/publications/PubsSPs.html#800-12">NIST Special Publication
800-12</citation>
        </ref>
        …[snip]…
      </references>
    </control>
  </group>
</catalog>
```

National Institute of Standards and Technology

SP 800-53 BASELINE VS OSCAL PROFILE

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Access Control					
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)
AC-7	Unsuccessful Logon Attempts	P2	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	P0	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	P3	Not Selected	Not Selected	AC-10
AC-11	Session Lock	P3	Not Selected	AC-11 (1)	AC-11 (1)
AC-12	Session Termination	P2	Not Selected	AC-12	AC-12
AC-13	**Withdrawn**	---	---	---	---
AC-14	Permitted Actions without Identification or Authentication	P3	AC-14	AC-14	AC-14
AC-15	**Withdrawn**	---	---	---	---
AC-16	Security Attributes	P0	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	P1	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)
AC-18	Wireless Access	P1	AC-18	AC-18 (1)	AC-18 (1) (4) (5)
AC-19	Access Control for Mobile Devices	P1	AC-19	AC-19 (5)	AC-19 (5)
AC-20	Use of External Information Systems	P1	AC-20	AC-20 (1) (2)	AC-20 (1) (2)
AC-21	Information Sharing	P2	Not Selected	AC-21	AC-21
AC-22	Publicly Accessible Content	P3	AC-22	AC-22	AC-22
AC-23	Data Mining Protection	P0	Not Selected	Not Selected	Not Selected
AC-24	Access Control Decisions	P0	Not Selected	Not Selected	Not Selected
AC-25	Reference Monitor	P0	Not Selected	Not Selected	Not Selected

```
<profile xmlns="http://csrc.nist.gov/ns/oscal/1.0">
  <title>SP 800-53 Low Baseline</title>
  <invoke href="..snip..l">
    <call control-id="ac.1"/>

    <call control-id="ac.2"/>

   <call control-id="ac.3"/>

    <call control-id="ac.7"/>

    <call control-id="ac.8"/>

    <call control-id="ac.14"/>

    <call control-id="ac.17"/>

    <call control-id="ac.18"/>

    <call control-id="ac.19"/>

    <call control-id="ac.20"/>

    ...snip...
  </invoke>
</profile>
```

NIST
National Institute of Standards and Technology

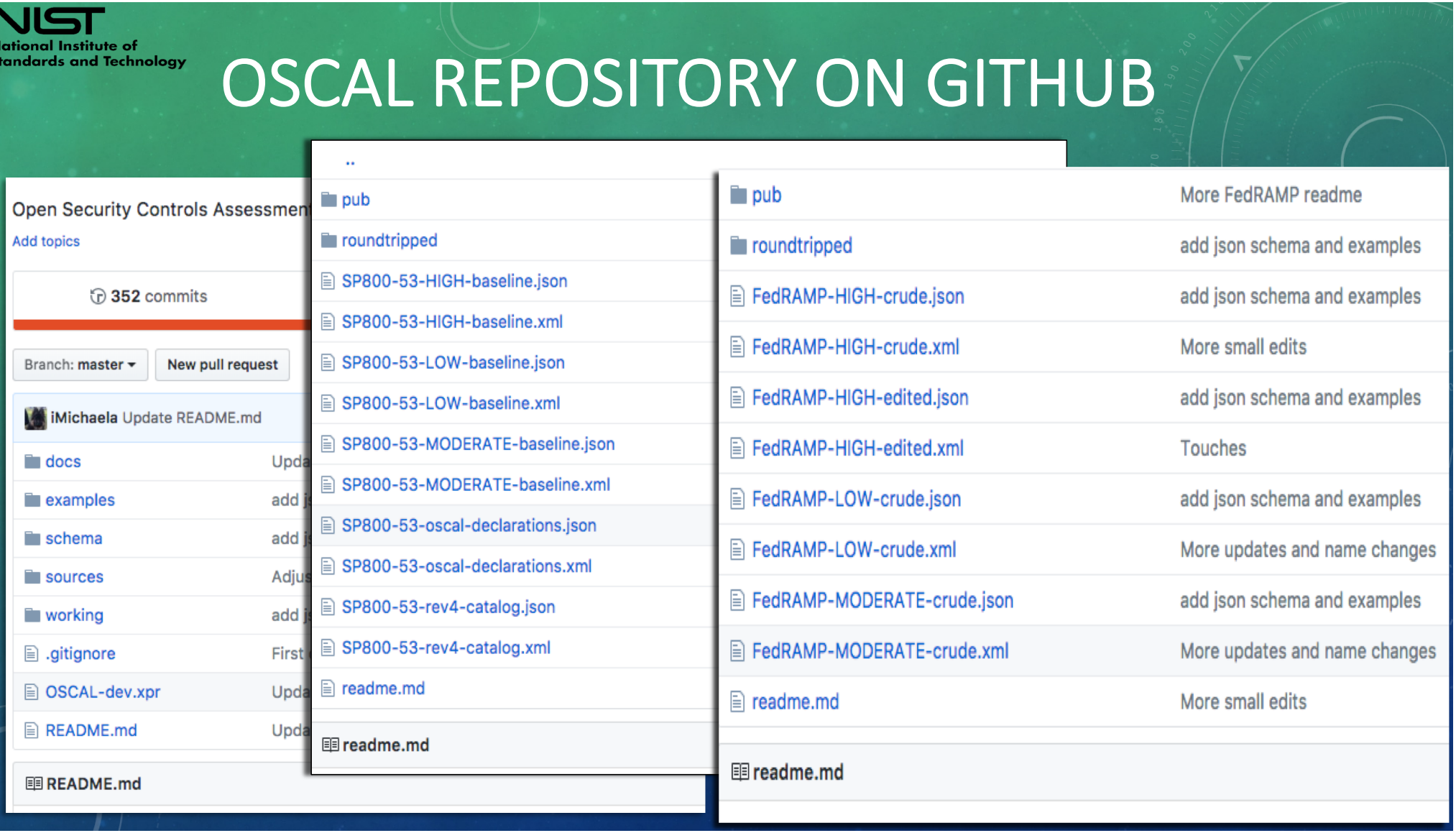
OSCAL DELIVERABLES

XML and JSON Schemas	Validate catalogs and profiles against constraints
XSL Templates	Produce human-readable versions (PDFs)
CSS	Edit OSCAL catalogs and profiles using XML tools
Documentation	Define the OSCAL specification Explain how organizations can convert existing catalogs and profiles into OSCAL formats

Posted to a NIST GitHub repo: https://github.com/usnistgov/OSCAL
Email oscal@nist.gov for access

NIST
National Institute of Standards and Technology

OSCAL REPOSITORY ON GITHUB



NIST
National Institute of
Standards and Technology

QUESTIONS?

FOR MORE GENERAL INFORMATION: MICHAELA.IORGA@NIST.GOV.

CLOUD SECURITY RUBIK'S CUBE IS ON GITHUB (WORK IN PROGRESS): HTTPS://GITHUB.COM/USNISTGOV/CLOUDSECURITYRUBIKSCUBE

FOR MORE INFORMATION REGARDING OSCAL: OSCAL@NIST.GOV.

OSCAL ON GITHUB (WORK IN PROGRESS): (EMAIL FIRST TO US FOR ACCESS TO THE PRIVATE REPOSITORY): HTTPS://GITHUB.COM/USNISTGOV/OSCAL

THANK YOU!

OSCAL TEAM WOULD LIKE TO INVITE YOUR TO COLLABORATE WITH US.