Building the Bionic Cloud

- Facts and Visions -

Dr. Michaela Iorga,
Senior Security Technical Lead for Cloud Computing
Co-Chair, NIST Cloud Security WG
Co-Chair, NIST Cloud Forensics Science WG

NIST

NIST Cloud Computing Program

Stats:

Stats courtesy of
Dr. David Bray, CIO, FCC

- in 2013 - 850 million web servers online
  for 7.1 billion humans that lived on Earth
- by 2022, 75-300 billion networked devices
  for 8 billion humans that will live on Earth

Every minute on the Internet:

204,000,000+ emails sent globally (2014)

4,000,000+ Google search queries

2,460,000+ pieces of Facebook content shared

72+ hours of new YouTube video uploaded

48,000+ iOS apps downloaded (per Domo.com)

Stats will grow exponentially in the years ahead

NIST Cloud Computing Program

2015 Identity Theft Stats: 707.5M Data Records lost or stolen

2015/2016 Increase of Government Breaches:

- OPM (23M);
- IRS (464K eFile PINs);
- US Voters Database (191M records)
- DoJ hack exposed 10K DHS and 20K FBI employees names, emails, job descriptions (1K intelligence analysts)

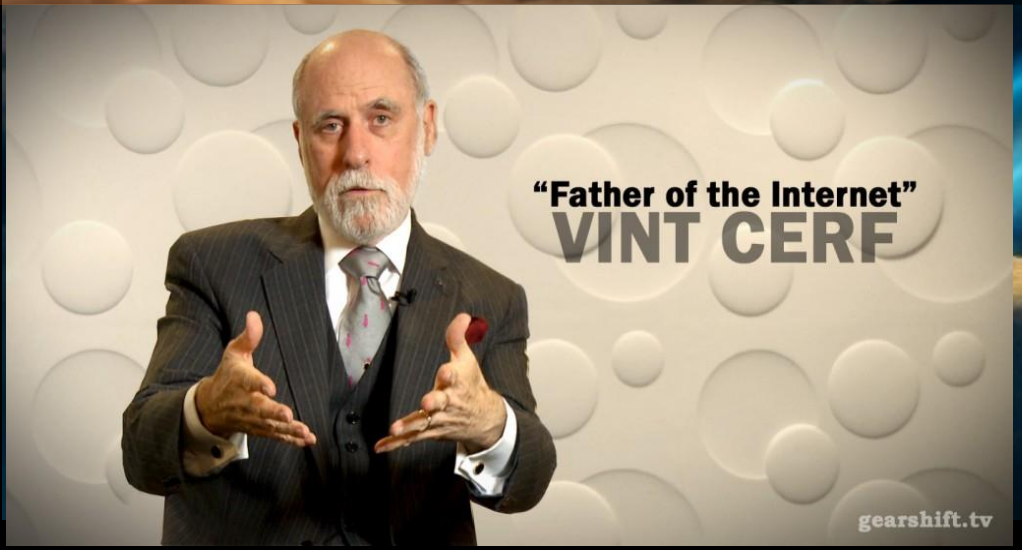
2016 Increase in Ransomware – Fully functional variant targeting OSX (Mac). It spreads through poisoned adds on major sites

Stats courtesy of Federal Bureau of Investigation- NIST's IT Security Day

Vint Cerf on the Security and Privacy of IoT

"You could have a situation where Bank of America succumbs to a DDoS attack from 100 million connected refrigerators in the U.S.,"

- Cerf said …

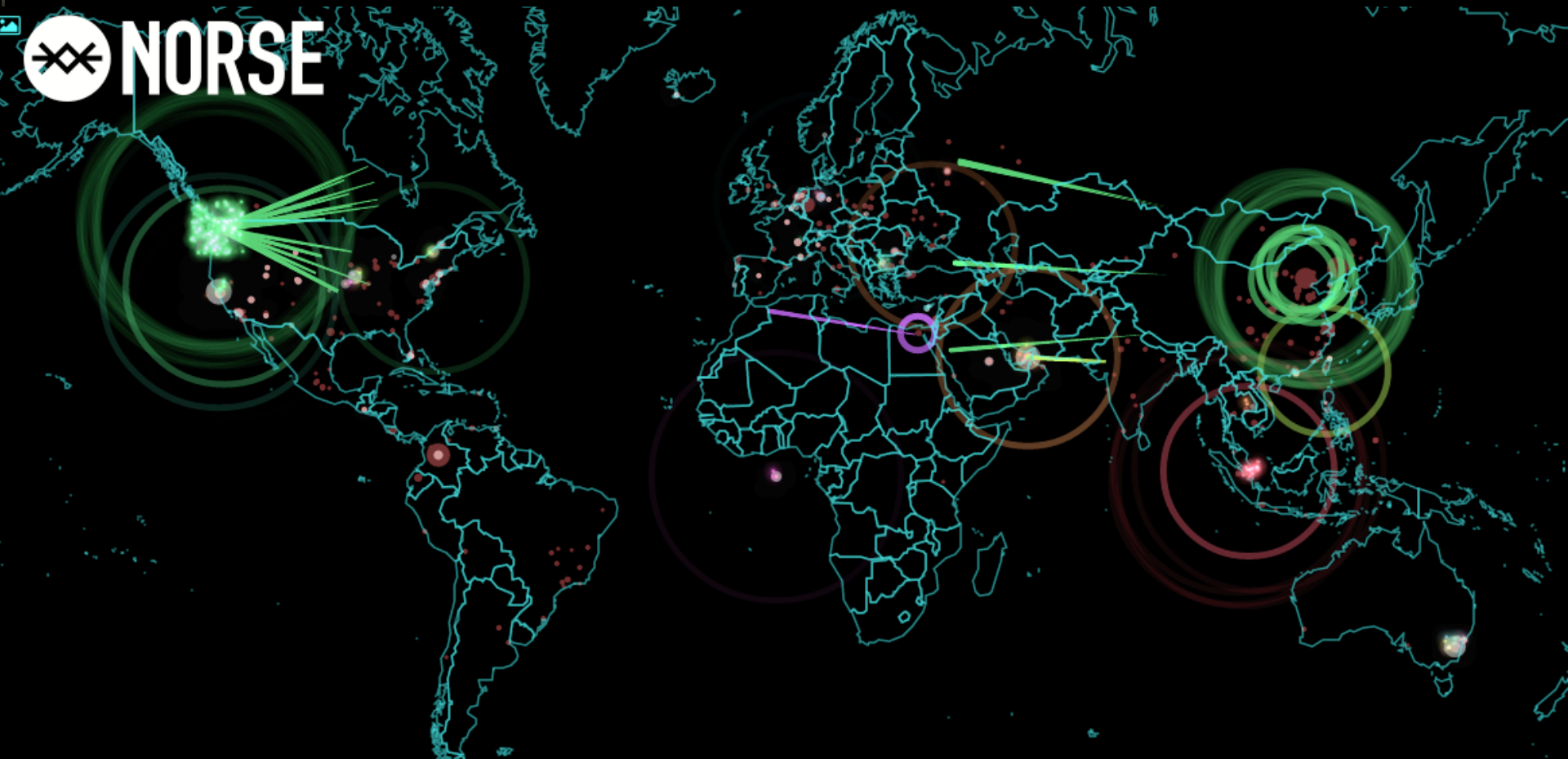


VINT CERF's POINT: The "processing power available for making those things accessible" is enough to make them plausible solders in a malicious bot army, once they have been successfully attacked.

https://securityledger.com/2014/04/vint-cerf-cs-changes-needed-to-address-iot-security-privacy/


Cyber Attacks in Real Time

Cyber Threats (real-time map) - http://map.norsecorp.com




NORSE
Ready, 1099 x 575
ATTACK ORIGINS
COUNTRY
449 China
311 South Korea
220 United States
80 Germany
ATTACK TYPES
PORT SERVICE TYPE
428 23 telnet
85 508... xsan-filesyste...
69 508... xsan-filesyste...
68 5900 rfb
ATTACK TARGETS
COUNTRY
1022 United States
299 United Arab ...
39 Germany
24 Portugal
LIVE ATTACKS
TIMESTAMP ATTACKER ATTACKER IP ATTACKER ... TARGET GEO ATTACK TYPE PORT
11:17:43.727 Chinanet Fujian Province Network 120.33.10... Fuzhou, CN Lynnwood... xsan-filesyst... 50...
11:17:43.618 Network For Pppoe Clients Termi... 109.184.1... Nizhny No... Lynnwood... microsoft-ds 445
11:17:43.190 Hknet Company Ltd. 202.67.23... Hong Kon... Kirksville, ... ssh 22
11:17:43.179 Stamnet Llc 185.93.18... Kharkiv, UA Braga, PT telnet 23


https://cybermap.kaspersky.com/
RUSSIA
CHINA
2603027
2215688
283944
60852
161966
31292
2363114
37
OAS
ODS
WAV
MAV
IDS
VUL
KAS
BAD

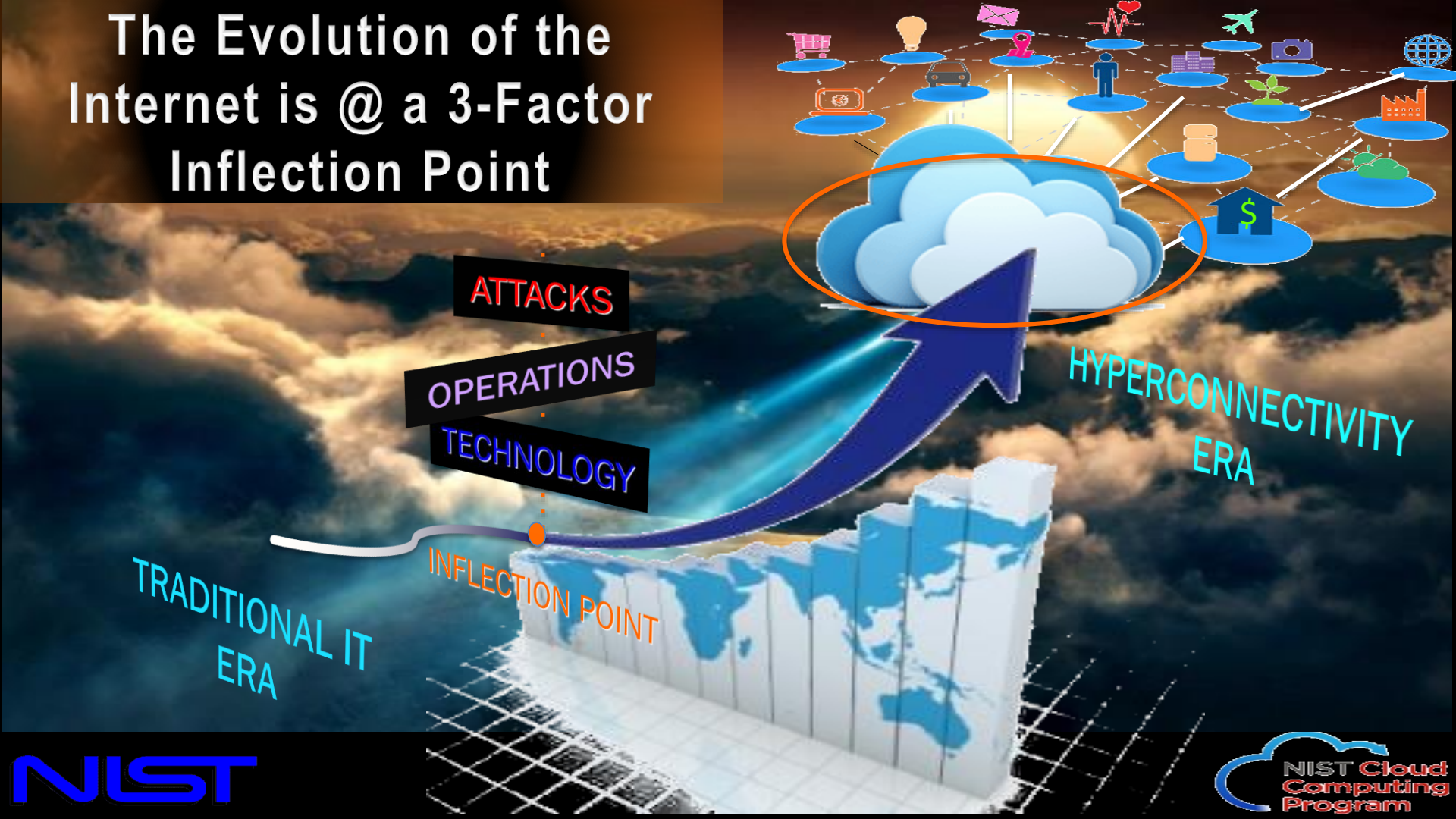
CYBERTHREAT REAL-TIME MAP

EN

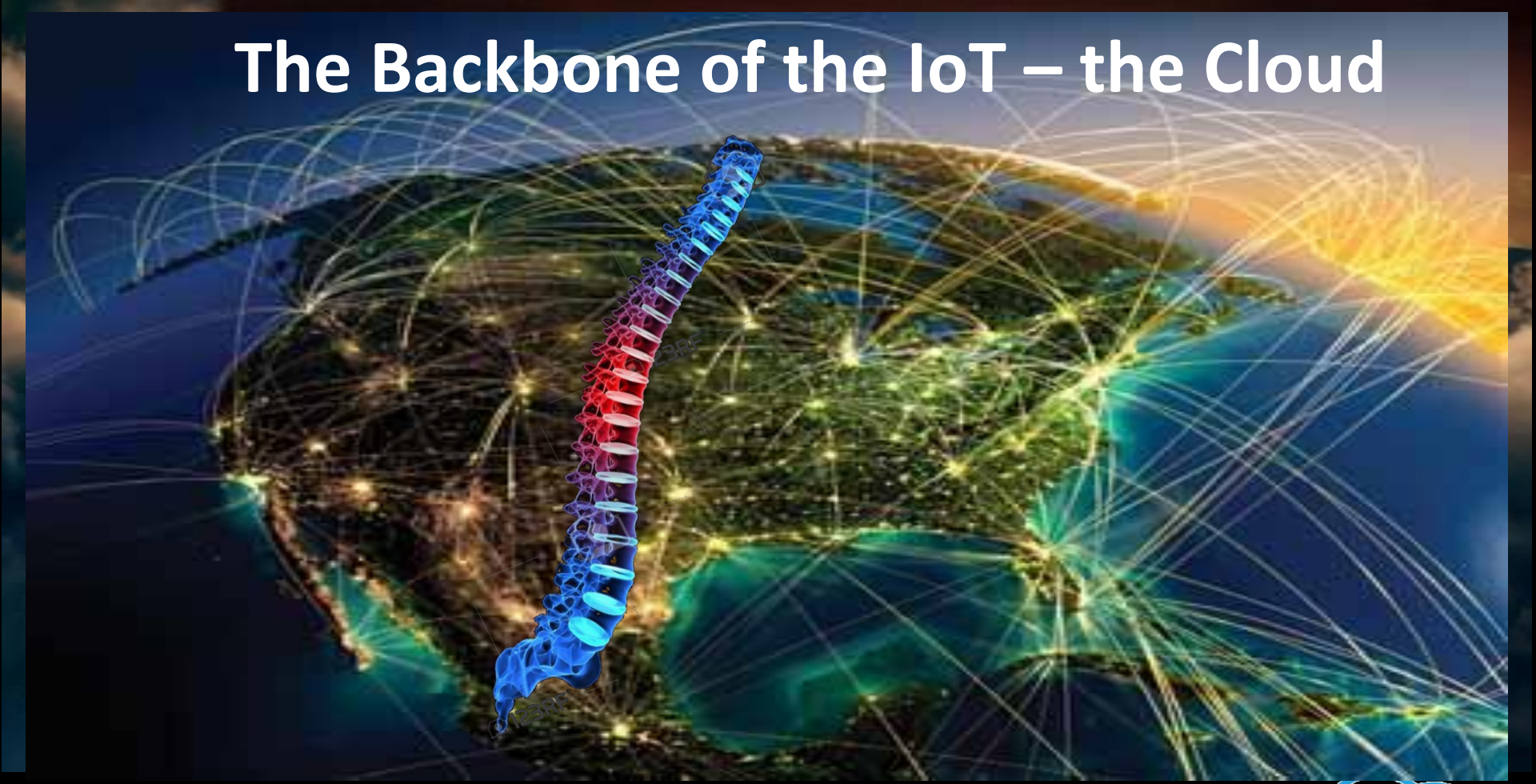
Download Trial

MAP STATISTICS DATA SOURCES BUZZ WIDGET

Share


The Evolution of the Internet is @ a 3-Factor Inflection Point
ATTACKS
OPERATIONS
TECHNOLOGY
TRADITIONAL IT ERA
INFLECTION POINT
HYPERCONNECTIVITY ERA
NIST
NIST Cloud Computing Program

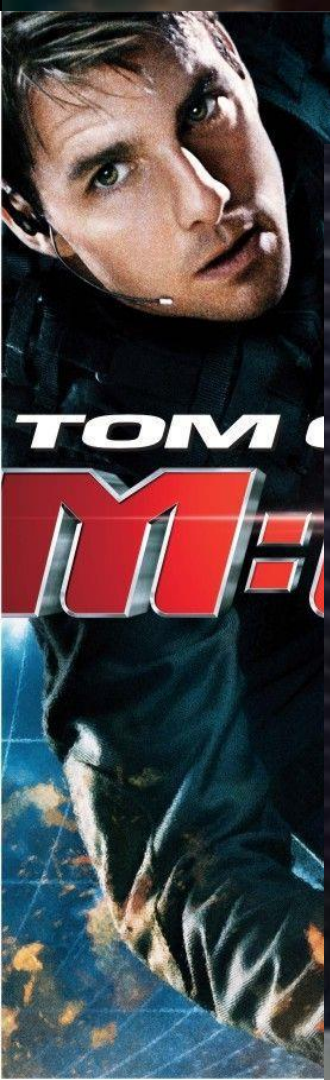
The Backbone of the IoT – the Cloud



NIST

NIST Cloud Computing Program

Mission Impossible 1



We offer three kinds of service:

GOOD - CHEAP - FAST

You can pick any two

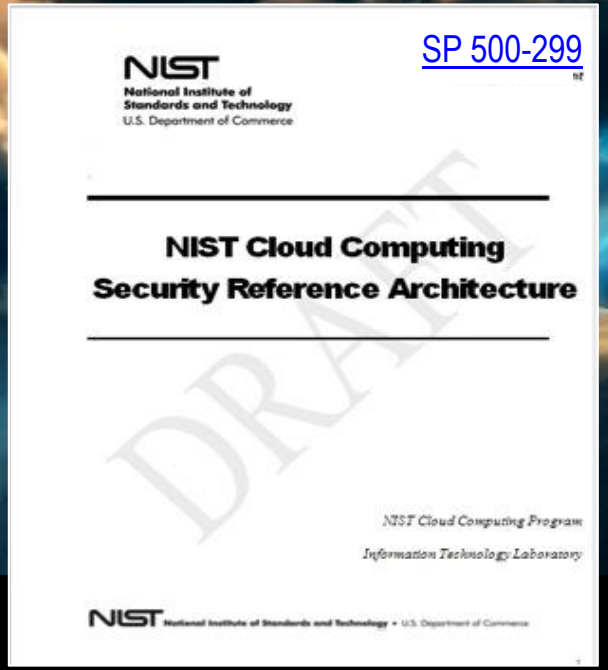
GOOD service CHEAP won't be FAST

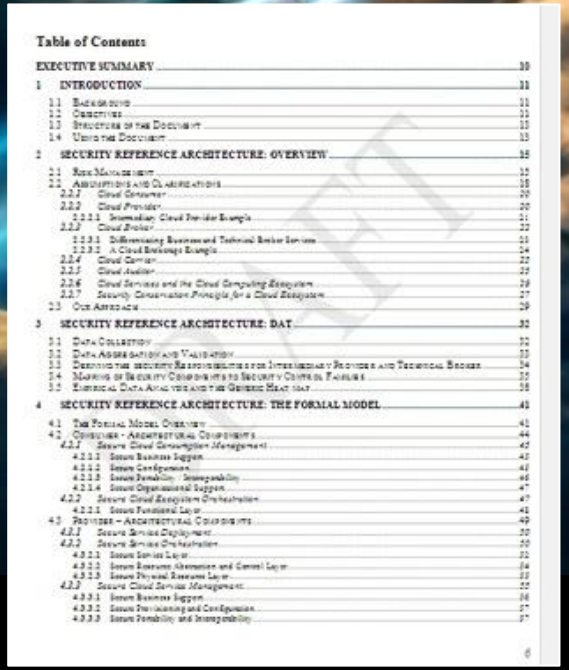
GOOD service FAST won't be CHEAP

FAST service CHEAP won't be GOOD

NIST Cloud Computing Security Reference Architecture

NIST SP 500-299 (draft reviewed by public)



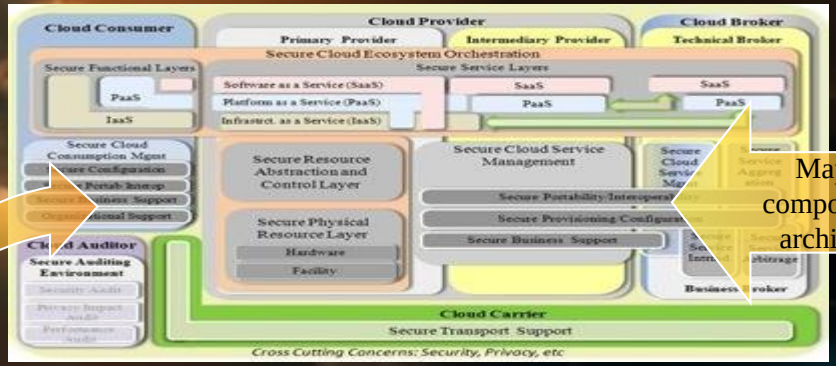


NIST

NIST Cloud Computing Program

NIST CC Security Reference Architecture – the Approach

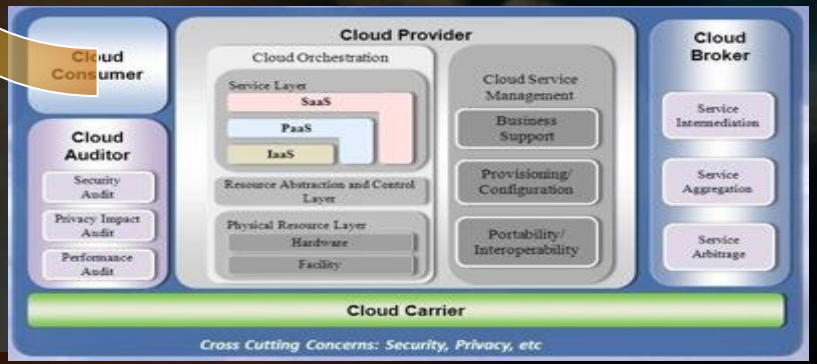
NIST Security Reference Architecture – formal model



Mapping components to architecture

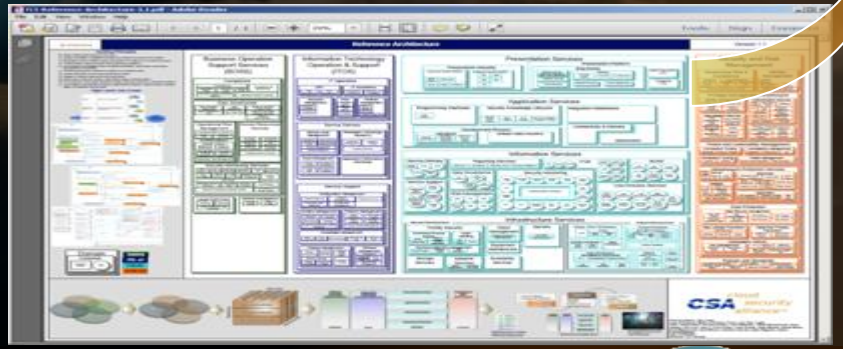
NIST Security Reference Architecture – security components

NIST Reference Architecture



+

CSA's TCI Reference Architecture

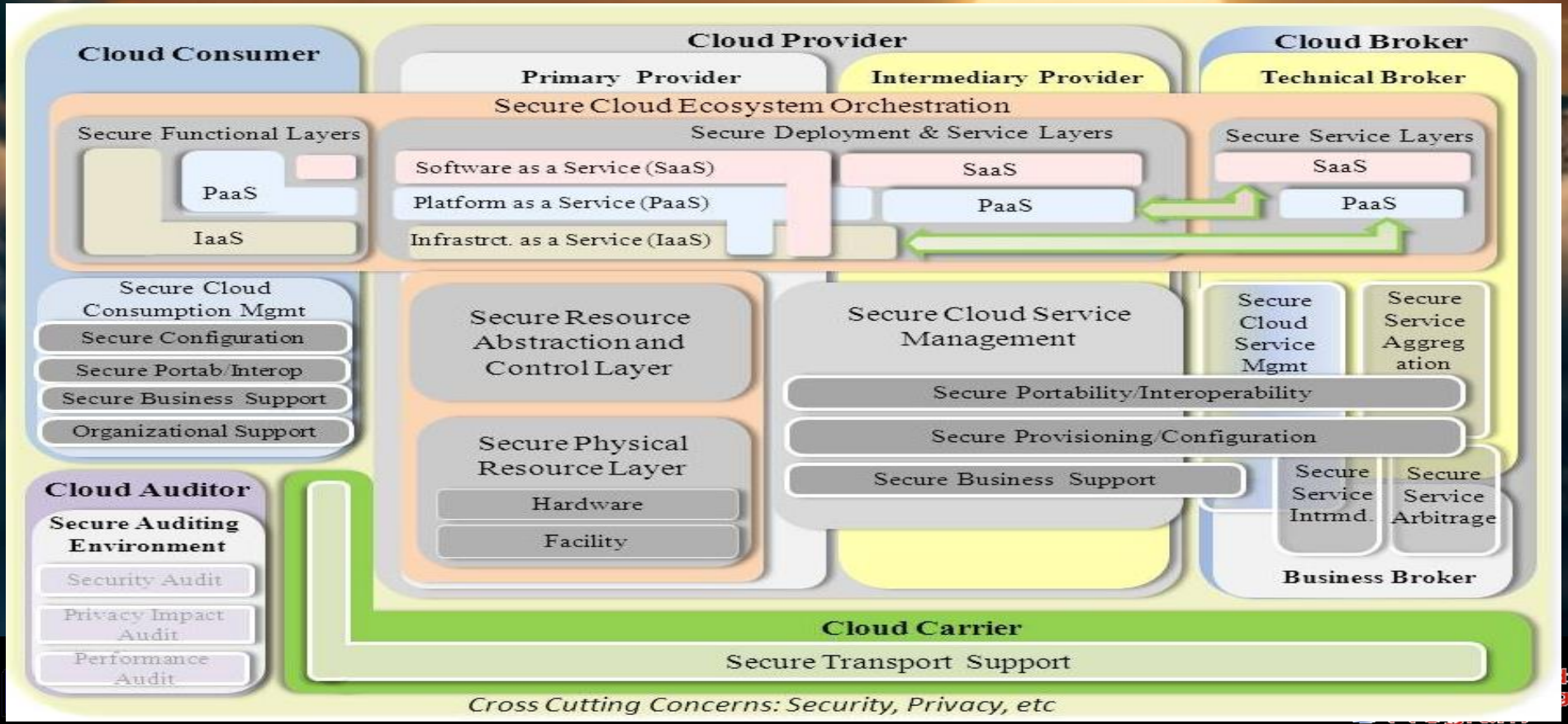


NIST

NIST Cloud Computing Program

NIST Security Reference Architecture (NIST SP 500-299)

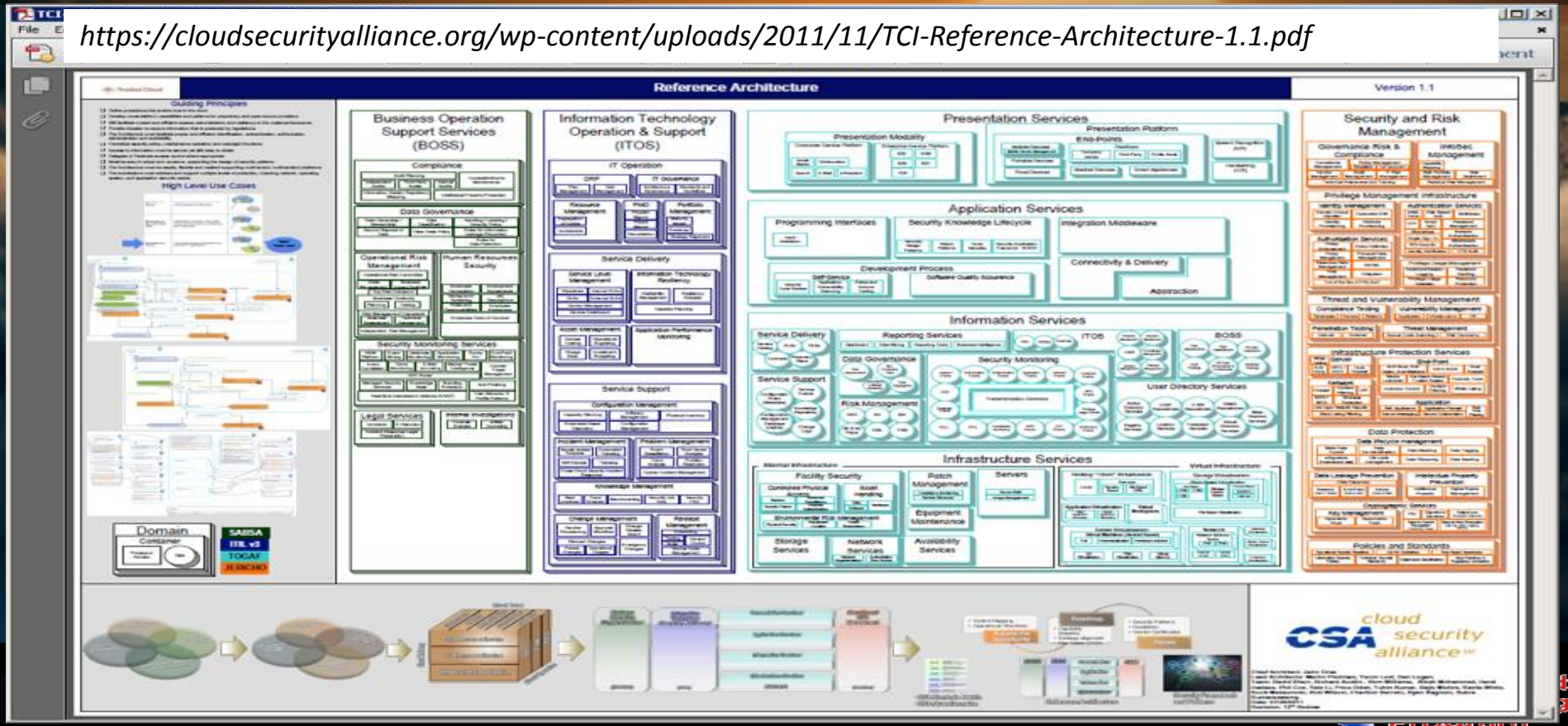
– the Formal Model -



Cloud Security Alliance's TCI Reference Architecture

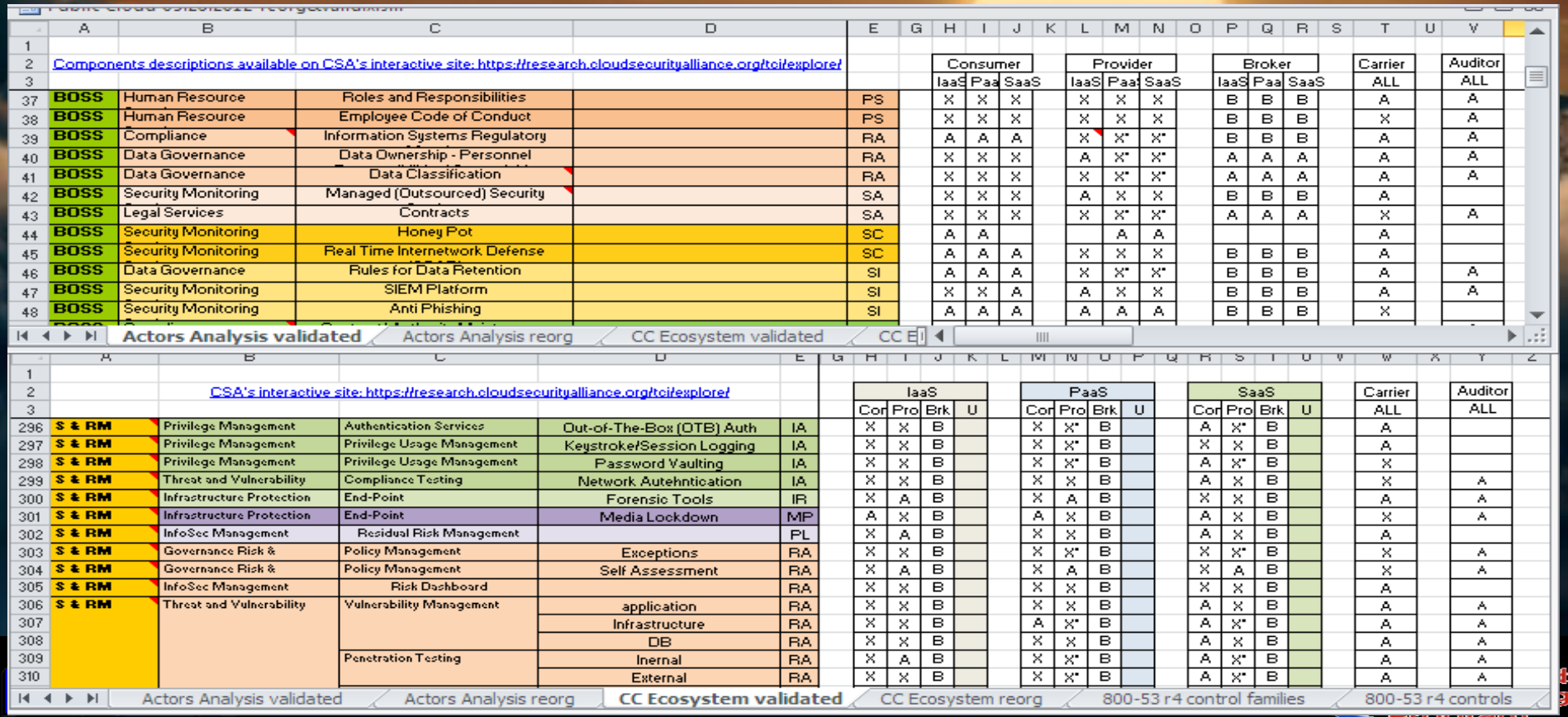
- NCC SWG leverages on Cloud Security Alliance's **Trusted Cloud Initiative - Reference Architecture**

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



NIST Security Reference Architecture (NIST SP 500-299)

– security components -



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

						Consumer			Provider			Broker			Carrier	Auditor
						IaaS	Paa	SaaS	IaaS	Paa	SaaS	IaaS	Paa	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

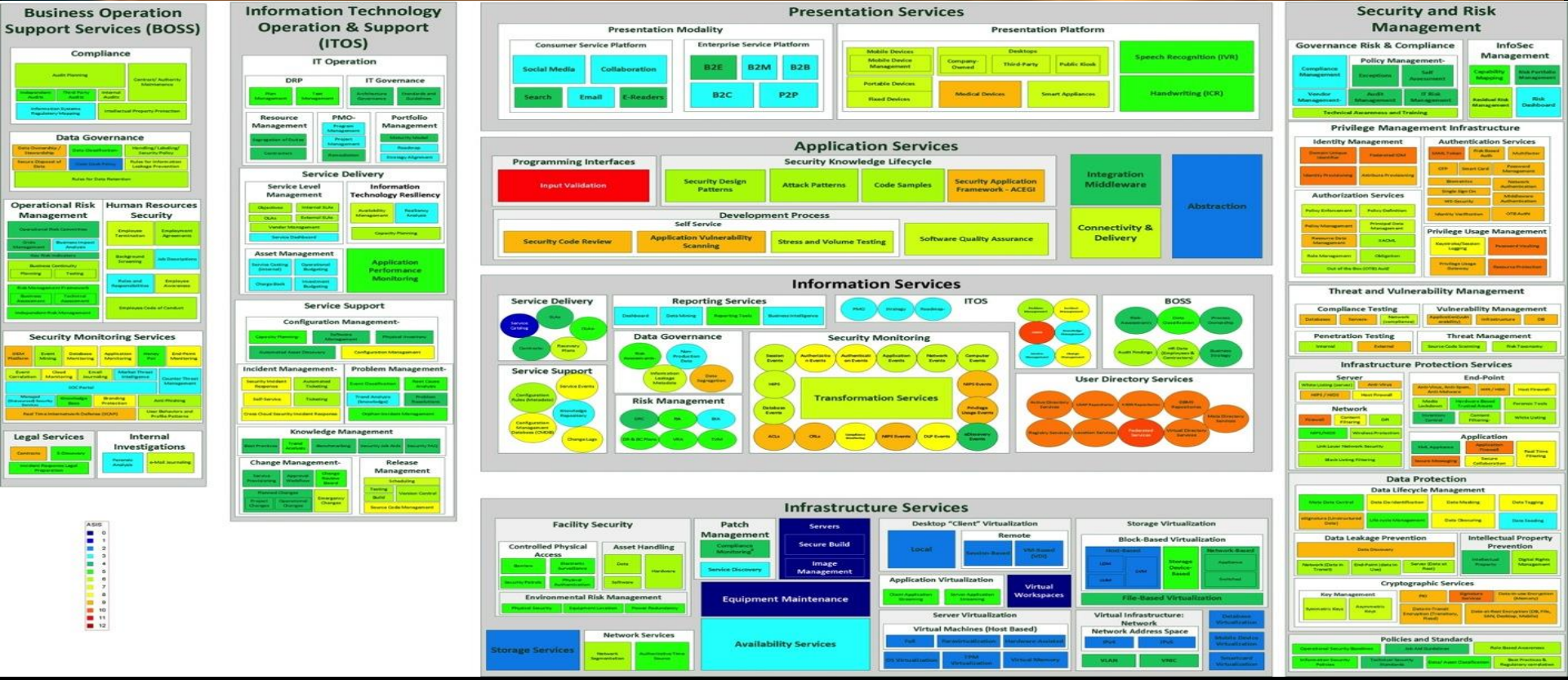
CSA's interactive site: https://research.cloudsecurityalliance.org/tci/explore/

						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

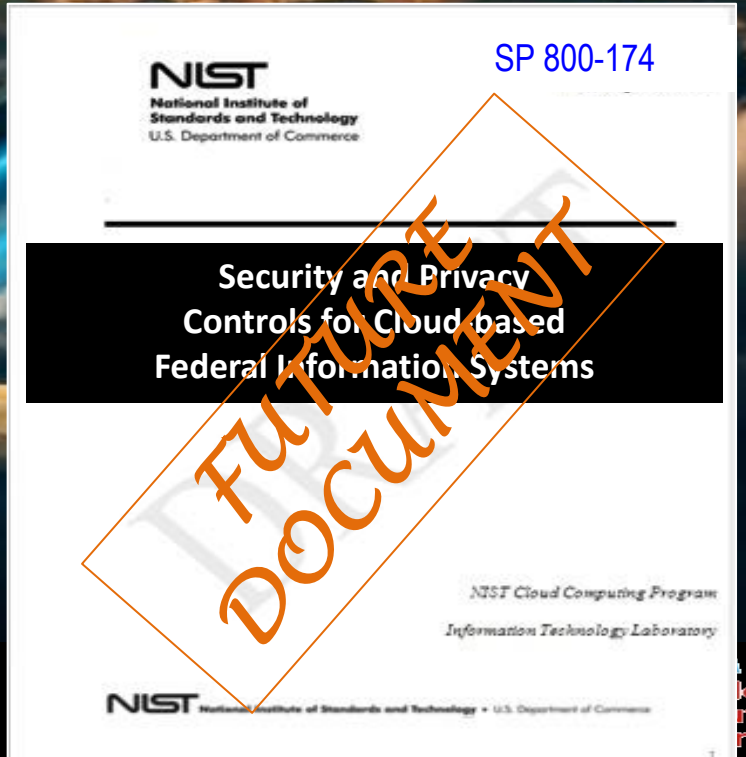
NIST Security Reference Architecture (NIST SP 500-299)

– Heat Map of the Aggregated-CIA Security Indexes –

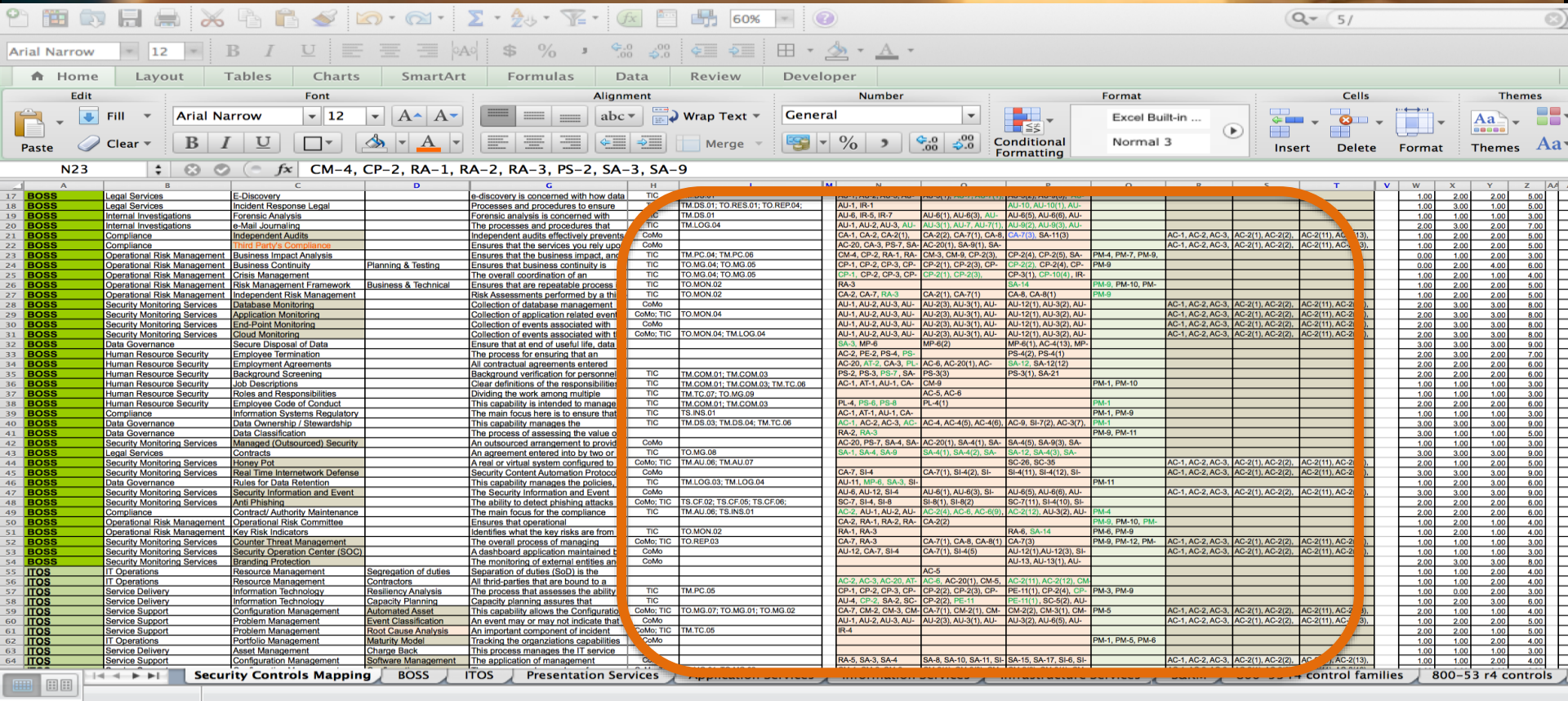


Security and Privacy Controls for Cloud-based Federal Information Systems.

NIST SP 800-174
-work in progress -

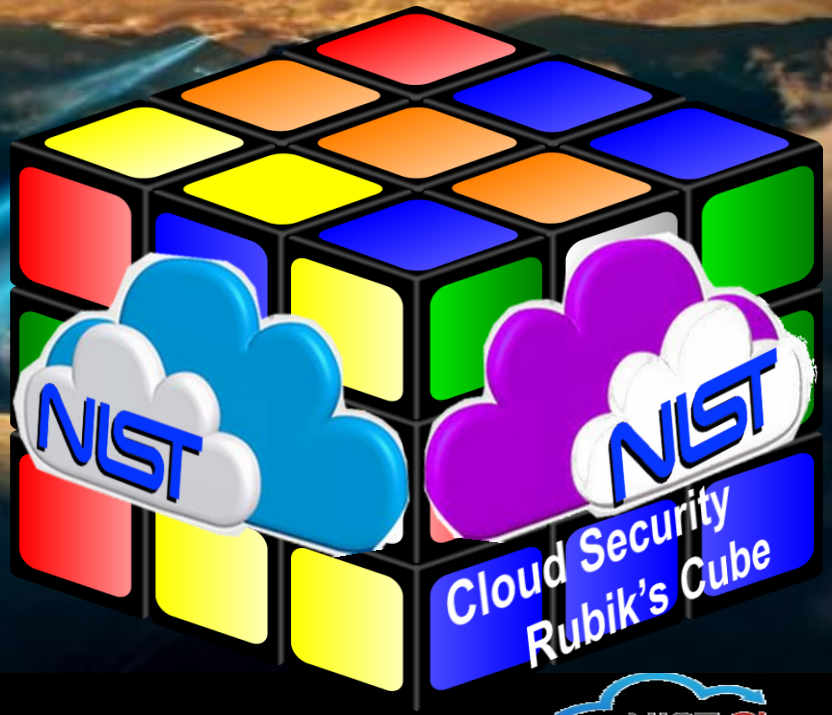


Security and Privacy Controls for Cloud-based Federal Information Systems



NIST Cloud Security Rubik's Cube (CSRC)

- CSRC is a tool that helps orchestrating a cloud ecosystem and analyzes the data aggregated in this process.
- The tool was implemented by NIST's summer 2015 SURF interns.



NIST

NIST Cloud Computing Program

Mission Impossible 2

We offer three kinds of service:

GOOD - CHEAP - FAST

You can pick any two

GOOD service CHEAP won't be FAST

GOOD service FAST won't be CHEAP

FAST service CHEAP won't be GOOD

Visibility & Trust

BUILD TRUST

The notion of “perimeter” becomes obsolete.
The old walls and moats can no longer defend us.

Dealing with an Iceberg Architecture

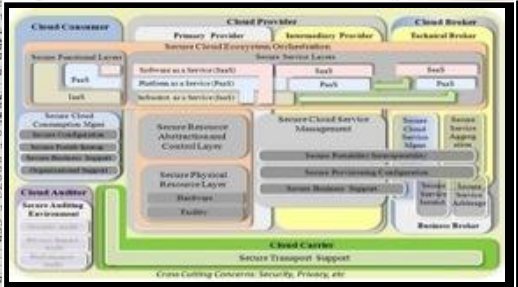
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

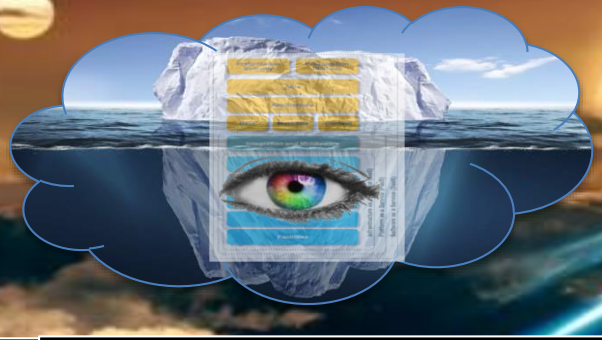
SP 500-299

NIST Cloud Computing Security Reference Architecture

Table of Contents

EXECUTIVE SUMMARY 30
1 INTRODUCTION 31
1.1 BACKGROUND 31
1.2 OBJECTIVES 31
1.3 STRUCTURE OF THE DOCUMENT 32

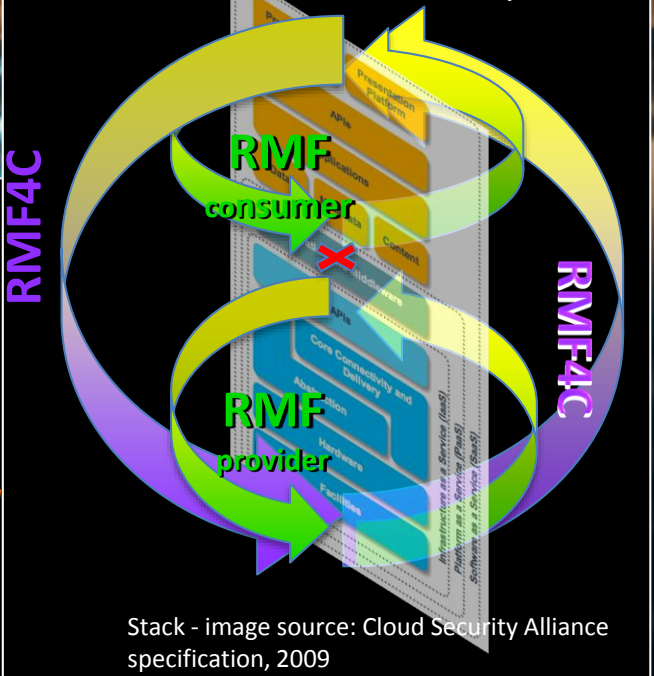




Risk Management Framework *(SP 800-37)*
Step 1: ***Categorize*** *Information System*
Step 2: ***Select*** *Security Controls*
Step 3: ***Implement*** *Security Controls*
Step 4 ***Assess*** *Security Controls*
Step 5: ***Authorize*** *Information System*
Step 6: ***Monitor*** *Security Controls*
(Repeat process as necessary)

Risk Management Framework in Cloud Env. *(SP 800-1*
Step 1: ***Categorize*** *Federal Information System*
Step 2: ***Select*** *Security Controls (Identify Security Requirements, perform a Risk Assessment)*
Step 3: ***Implement***
Step 4: ***Assess*** *Service Provider(s) & Controls*
Step 5: ***Authorize*** *Use of Service*
Step 6: ***Monitor*** *Service Provider (on-going, near-real- time);*
(Repeat process as necessary

NIST SP 800-173:
Guide for Applying Risk Management Framework to Cloud-based Federal Information Systems

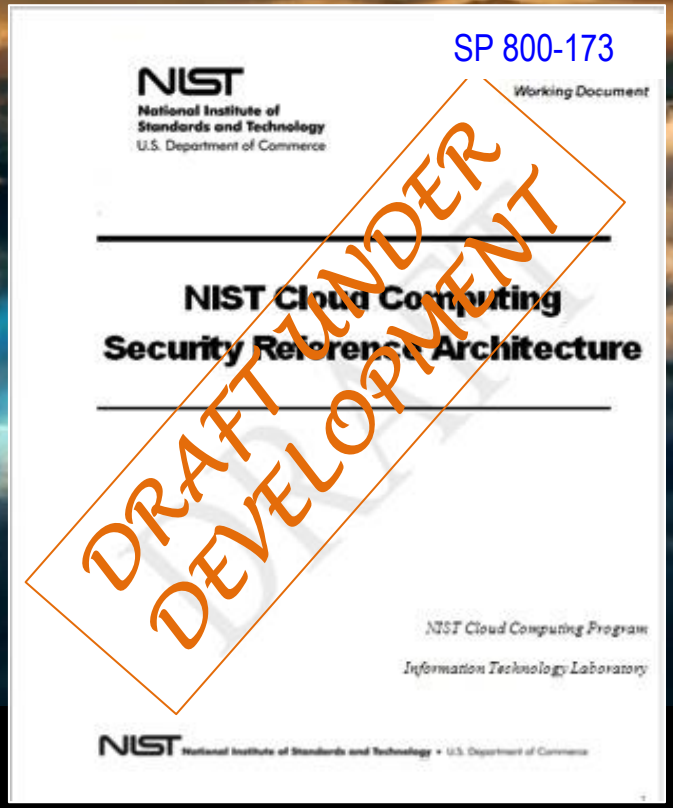


Stack - image source: Cloud Security Alliance specification, 2009

NIST Cloud Computing Program

Guide to Applying Risk Management Framework to Cloud-based Federal Information Systems.

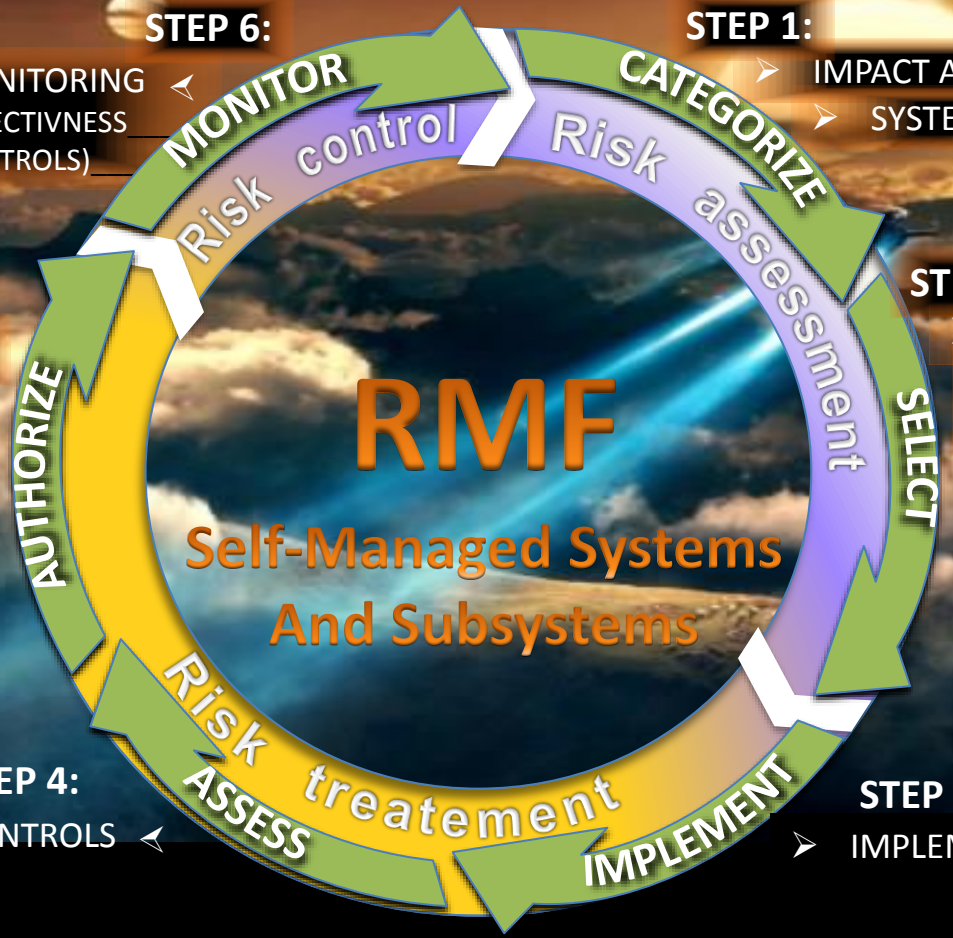
NIST SP 800-173
-draft-



NIST

NIST Cloud Computing Program

NIST SP 800-37 Rev1: **Risk Management Framework (RMF)**



STEP 6:

ONGOING MONITORING
(OPERATIONS & EFFECTIVNESS OF SECURITY CONTROLS)

STEP 1:

- IMPACT ANALYSIS
- SYSTEM CATEGORIZATION

STEP 2:

- SELECT BASELINE CONTROLS
- TAILOR & SUPPLEMENT CONTROLS
- DEVELOP SECURITY PLAN

STEP 5:

AUTHORIZE OPERATIONS
(BASED UPON RESIDUAL RISK & RISK TOLERANCE)

STEP 4:

ASSESS SECURITY CONTROLS

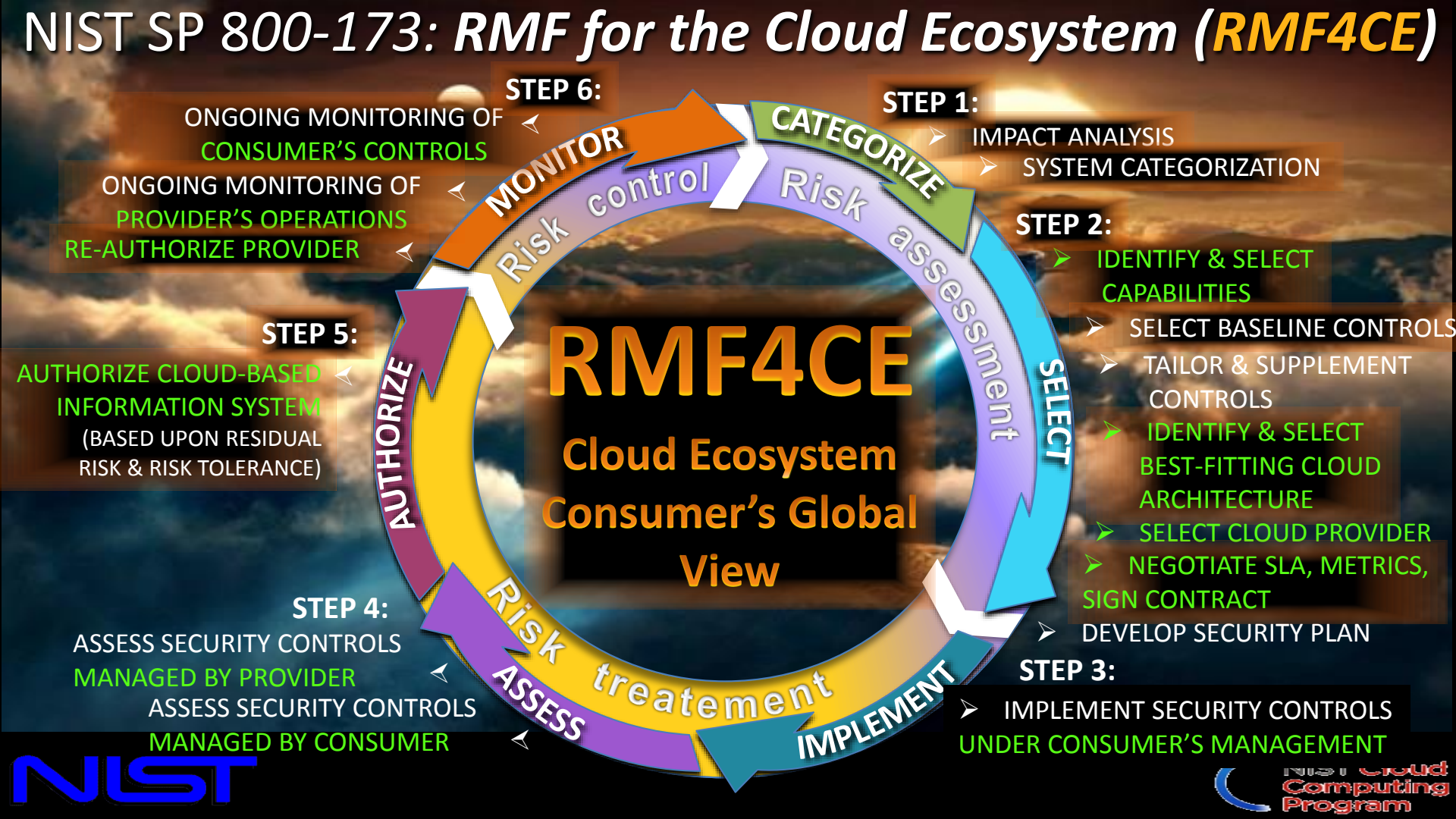
STEP 3:

- IMPLEMENT SECURITY CONTROLS

NIST

NIST Cloud Computing Program

NIST SP *800-173*: *RMF for the Cloud Ecosystem (RMF4CE)*



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

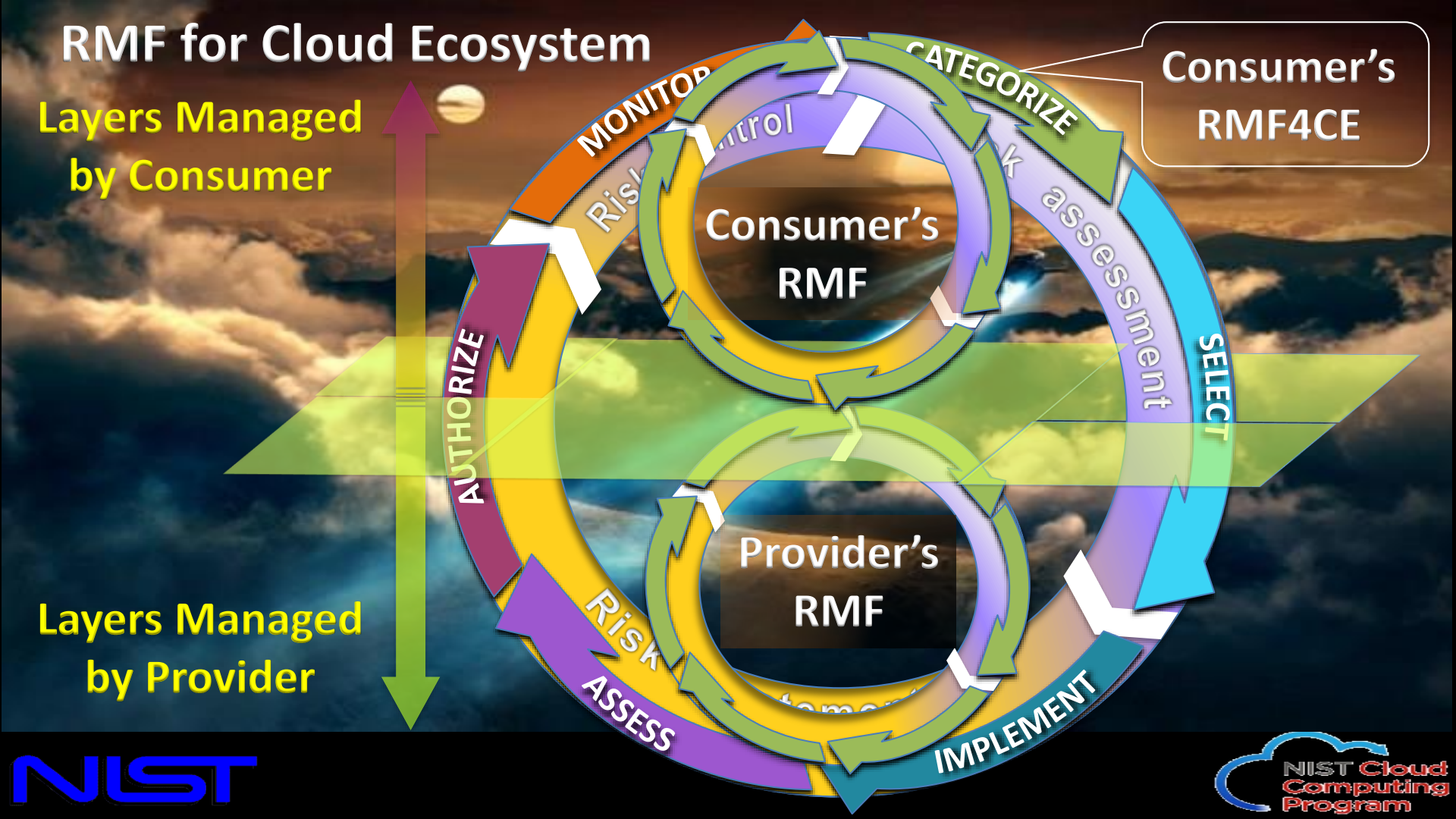
STEP 4:
- ASSESS SECURITY CONTROLS MANAGED BY PROVIDER
- ASSESS SECURITY CONTROLS MANAGED BY CONSUMER

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

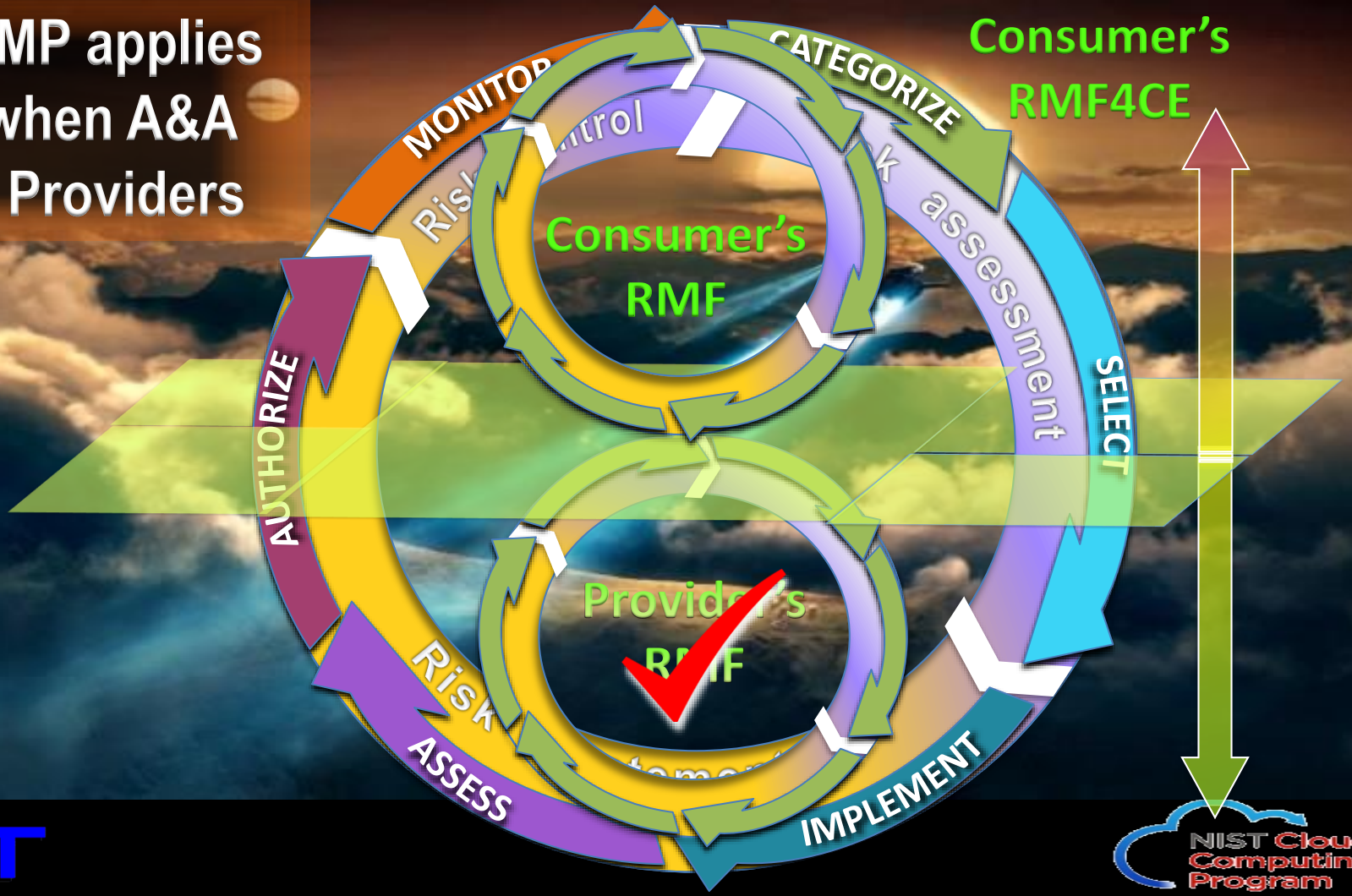
STEP 6:
- ONGOING MONITORING OF CONSUMER'S CONTROLS
- ONGOING MONITORING OF PROVIDER'S OPERATIONS
- RE-AUTHORIZE PROVIDER

NIST

NIST Cloud Computing Program


RMF for Cloud Ecosystem
Layers Managed by Consumer
Layers Managed by Provider
Consumer's RMF4CE
Consumer's RMF
Provider's RMF
CATEGORIZE
SELECT
IMPLEMENT
ASSESS
AUTHORIZE
MONITOR
NIST
NIST Cloud Computing Program

FedRAMP applies RMF when A&A Cloud Providers



NIST

NIST Cloud Computing Program

“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

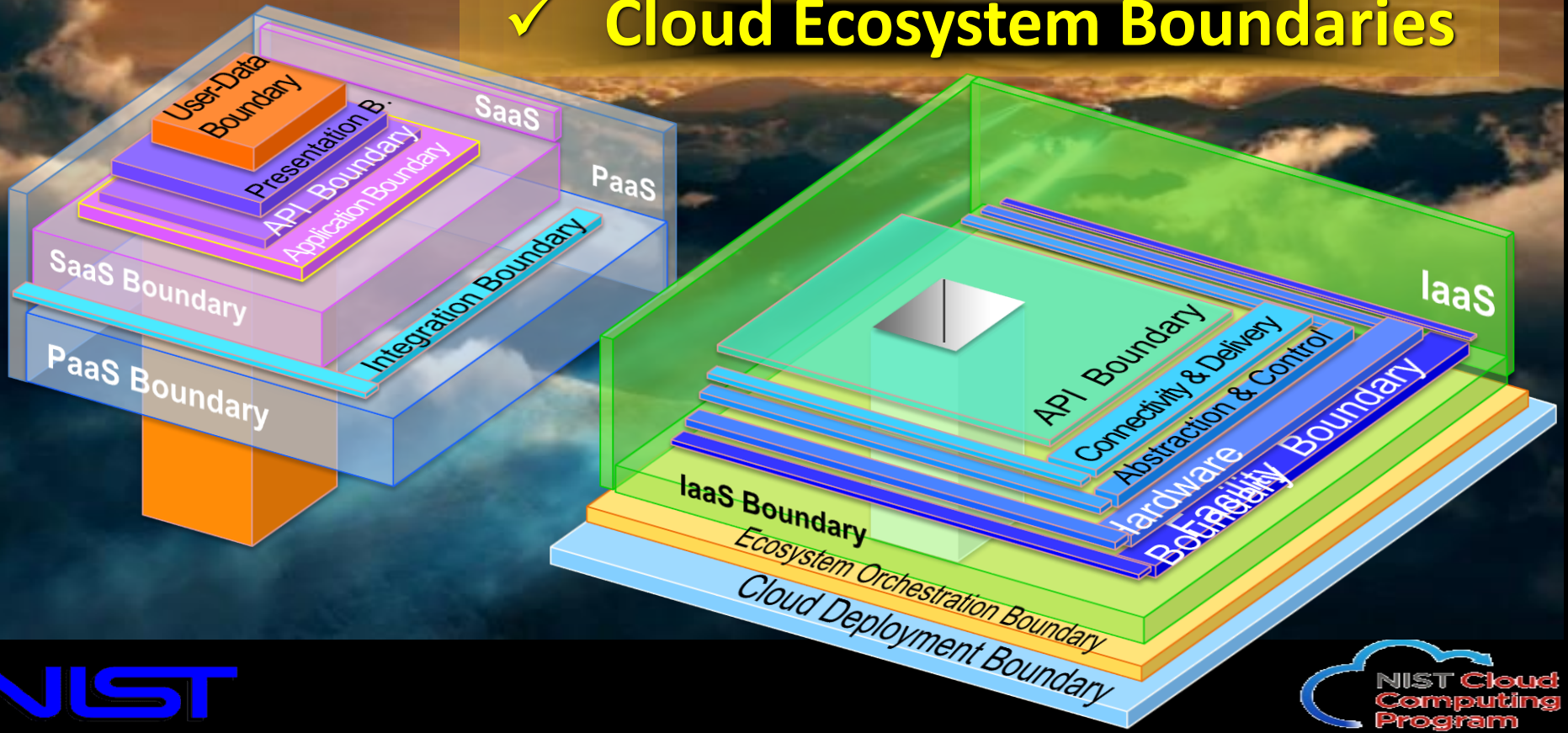
John Pescatore, Director of Emerging Security Trends at the SANS Institute speaks at CyberCon 2015 Conference at the Ritz-Carlton Pentagon City in Arlington, Va., on Wednesday, November 18, 2015.
(Photo: Mike Morones/Staff)

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."

Guide to Applying Risk Management Framework to Cloud-based Federal Information Systems

✓ Cloud Ecosystem Boundaries

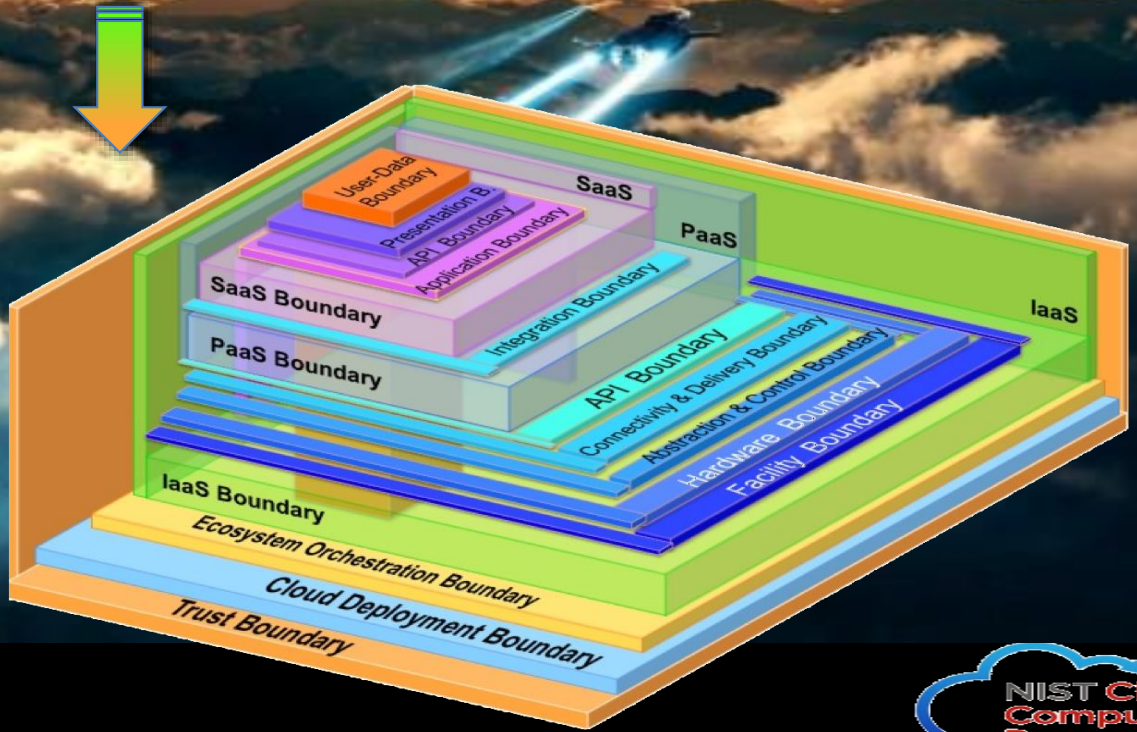


NIST

NIST Cloud Computing Program

Guide to Applying Risk Management Framework to Cloud-based Federal Information Systems –cont.

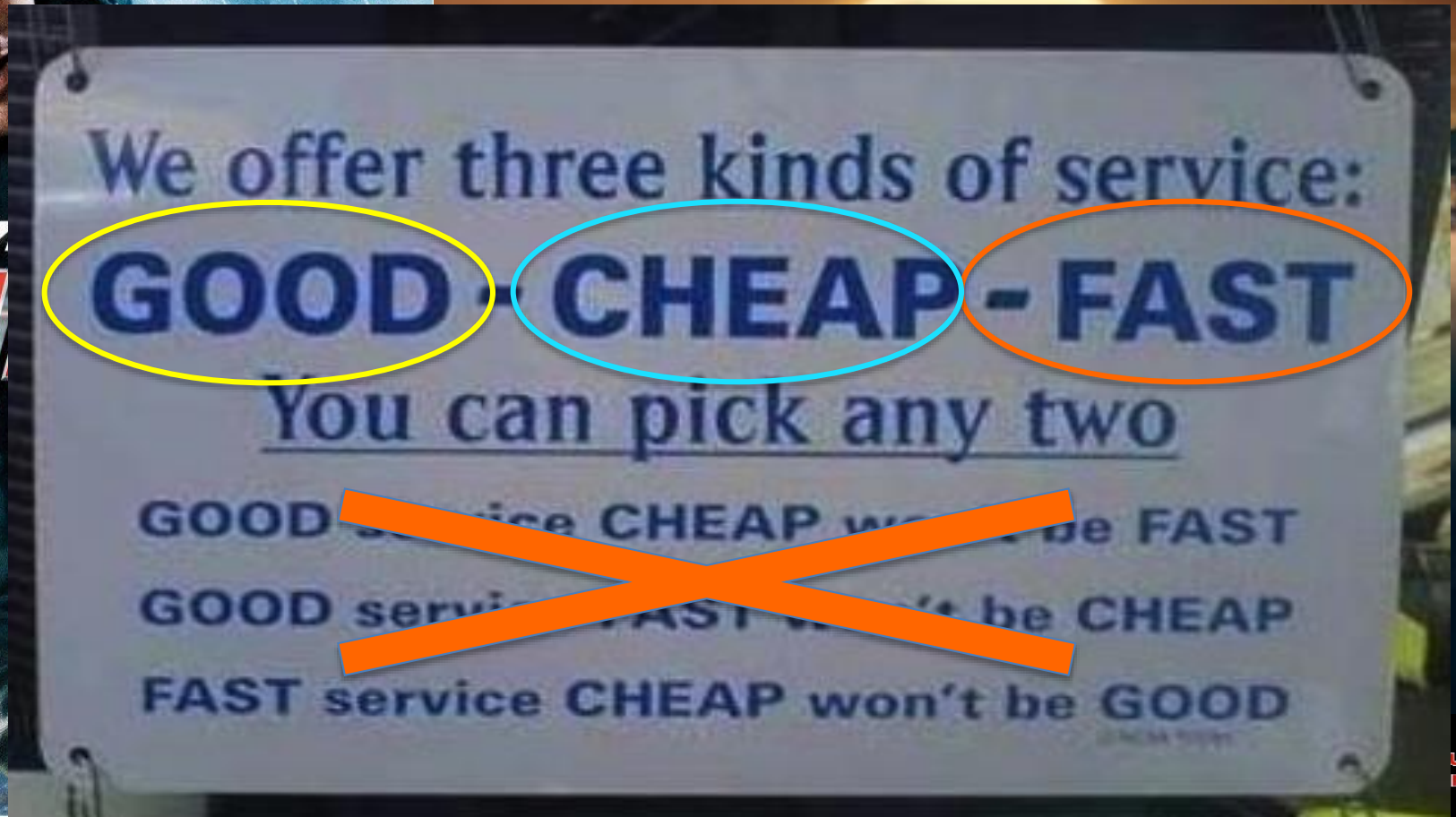
Building Trust & Trust Boundary



NIST

NIST Cloud Computing Program

Mission Impossible 3



Structured Formats

I, the sender, want to send a letter to Addressee .  Here is my stamp

They live at the house with Street Number on First Street in Some City.
In case you are unable to deliver please return the letter to Street Address in City and State.

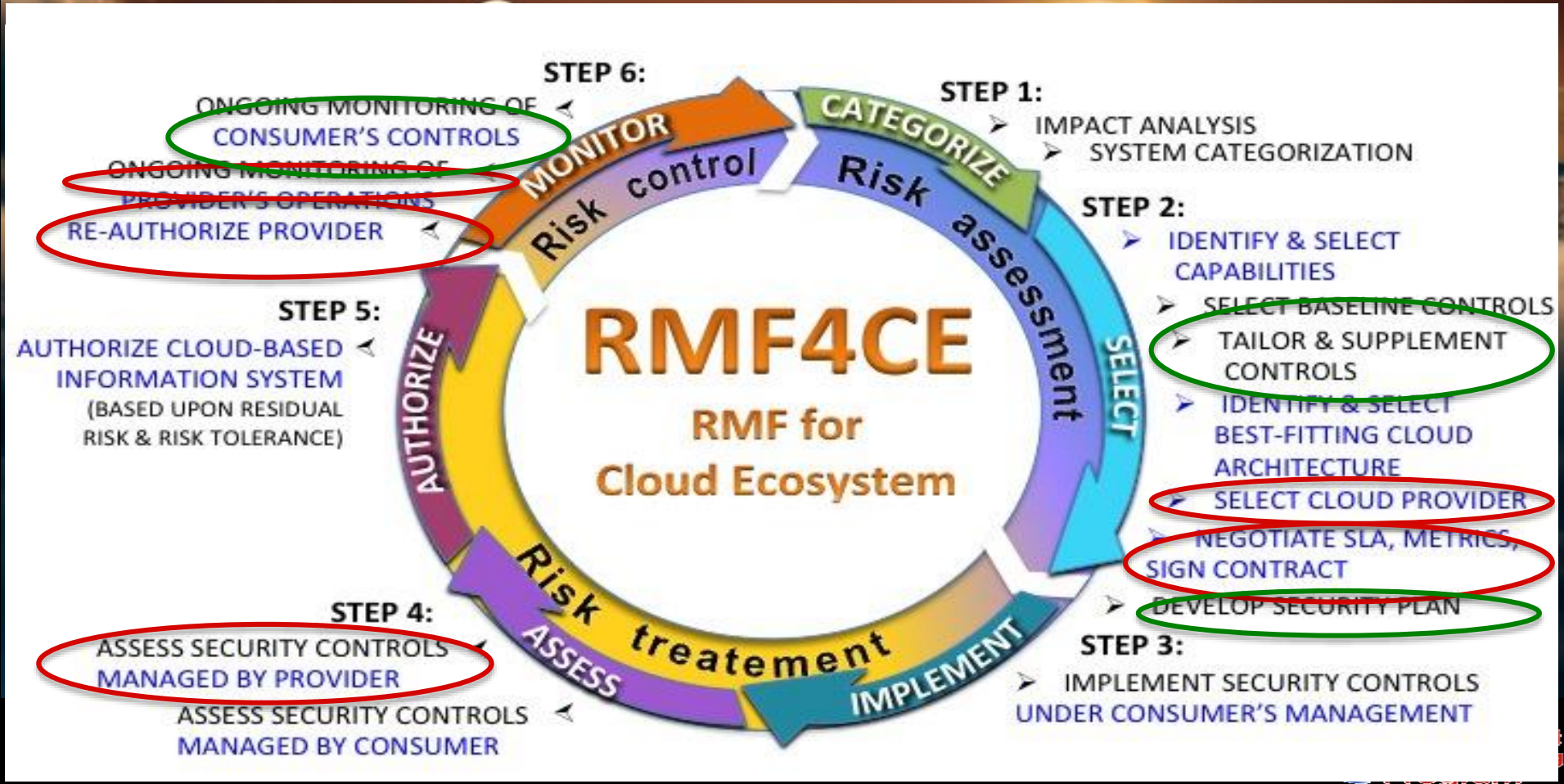
Sender
Street Address
City, State ZIP

Addressee
Street Address
City, State ZIP
||||||||||||

NIST

NIST Cloud Computing Program

Transforming Automation Dream into Reality



Transforming Automation Dream into Reality - cont.

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

DOMAIN	CONTAINER	CAPABILITY (process or solution)	CAPABILITY (process or solution	SCOPE	TIC CAPABILITIES mapping	Capability Implementation SP800-53 Rev4 Reviewed Low(Capability implementation)	Reviewed Moderate(Capability implementation)	Reviewed High(Capability implementation)
BOSS	Compliance	Intellectual Property Protection				AC-1, AC-2, AC-3, AC-	AC-2(1), AC-2(2), AC-	AC-2(11), AC-2(13), AC-
BOSS	Data Governance	Handling/ Labeling/ Security		TIC	TM.DS.05	AC-1, AC-3, AC-4, AT-1,	MP-3, MP-5, MP-5(4)	AC-16
BOSS	Data Governance	Clear Desk Policy				MP-1, MP-2, MP-7	MP-4, MP-5, MP-5(4),	
BOSS	Data Governance	Rules for Information Leakage		TIC	TM.LOG.04;	AC-1, CP-1, IA-1, IR-1,		
BOSS	Human Resource Security	Employee Awareness			TO.MG.10	AT-1, AT-2, AR-5	AT-2(2)	
BOSS	Security Monitoring Services	Market Threat Intelligence		TIC	TS.INS.01;	AU-6, CA-2, IR-4, IR-5	AU-6(1), AU-6(3), CA-	AU-6(5), AU-6(6), IR-
BOSS	Security Monitoring Services	Knowledge Base		TIC	TM.DS.05;	PL-2, SA-5	PL-7, PL-8	
BOSS	Compliance	Audit Planning		CoMo		CA-2, CA-2(1), CA-7,	CA-2(2), CA-7(1), PL-	PL-8(1), PL-8(2)
BOSS	Compliance	Internal Audit		CoMo; TIC	TO.MON.03	CA-2, CA-2(1), CA-7,	CA-2(2), CA-7(1), CA-8,	CA-7(3)
BOSS	Security Monitoring Services	Event Mi g		CoMo; TIC	TM.DS.01;	AU-6, CA-7, RA-5, SI-	AU-6(3), RA-5(6), RA-	AU-6(4), CA-7(3), SI-
BOSS	Security Monitoring Services	Event Correlation		CoMo; TIC	TM.DS.01	AU-6, CA-7, IR-4, RA-5,	AU-6(3), SI-4(16)	AU-6(6), AU-6(9), IR-
BOSS	Security Monitoring Services	Email Journaling		CoMo; TIC	TS.CF.05; TS.CF.06;	SI-3, SI-4	SI-3(7), SI-4(5)	SI-4(10), SI-4(12)
BOSS	Security Monitoring Services	User Behaviors and Profile		CoMo		AC-2, AU-1, AU-2, AU-	AC-2(12),	AU-6(8)
BOSS	Legal Services	E-Disco		TIC	TM.DS.01	AU-1, 2, AU-3, AU-	AU-3(1), AU-7, AU-7(1),	AU-3(2), AU-9(3), AU-
BOSS	Legal Services	Incident Res se Legal		TIC	TM.DS.01;	AU, IR-1		AU-10, AU-10(1), AU-
BOSS	Internal Investigations	Forensic Analysis		TIC	TM.DS.01	AU-6, IR-5, IR-7	AU-6(1), AU-6(3), AU-7,	AU-6(5), AU-6(6), AU-
BOSS	Internal Investigations	e-Mail Journaling		TIC	TM.LOG.04	AU-1, AU-2, AU-3, AU-	AU-3(1), AU-7, AU-7(1),	AU-9(2), AU-9(3), AU-
BOSS	Compliance	Independent Audits		CoMo		CA-1, CA-2, CA-2(1),	CA-2(2), CA-7(1), CA-8,	CA-7(3), SA-11(3)
BOSS	Compliance	Third Party's Compliance		CoMo		AC-20, CA-3, PS-7, SA-	AC-20(1), SA-9(1), SA-	
BOSS	Operational Risk Management	Business Impact Analysis		TIC	TM.PC.04;	CM-4, CP-2, RA-1, RA-	CM-3, CM-9, CP-2(3),	CP-2(4), CP-2(5), SA-
BOSS	Operational Risk Management	Business Continuity	Planning & Testing	TIC	TO.MG.04;	CP-1, CP-2, CP-3, CP-	CP-2(1), CP-2(3), CP-	CP-2(2), CP-2(4), CP-
BOSS	Operational Risk Management	Crisis Management		TIC	TO.MG.04;	CP-1, CP-2, CP-3, CP-	CP-2(1), CP-2(3),	CP-3(1), CP-10(4), IR-
BOSS	Operational Risk Management	Risk Management Framework	Business & Technical	TIC	TO.MON.02	RA-3		SA-14
BOSS	Operational Risk Management	Independent Risk Management		TIC	TO.MON.02	CA-2, CA-7, RA-3	CA-2(1), CA-7(1)	CA-8, CA-8(1)
BOSS	Security Monitoring Services	Database Monitoring		CoMo		AU-1, AU-2, AU-3, AU-	AU-2(3), AU-3(1), AU-	AU-12(1), AU-3(2), AU-
BOSS	Security Monitoring Services	Application Monitoring		CoMo; TIC	TO.MON.04	AU-1, AU-2, AU-3, AU-	AU-2(3), AU-3(1), AU-	AU-12(1), AU-3(2), AU-

Format of a Structured Security Control

- Hierarchical
- Standards-based (e.g. NIST SP 800-53, ISO 27001/2)
  - Description and Metadata:
    - Overlay ->Technology (Cloud, ICS, Mobile, etc…)
      - ❖Scope (functional capability)
        - » Implementation
        - » Assessment
        - » Metrics
        - » Other related information

NIST

NIST Cloud Computing Program

Open Security Controls Automation Language (OSCAL)

- OSCAL aims to provide a structured representation of the security controls for Overlays that would:
  - Allow Consumers to compare cloud services from different Providers
  - Speed up FedRAMP's assessment process
  - Support security SLA & metrics
  - Make possible the automation of continuous monitoring

NIST

NIST Cloud Computing Program

Questions?

NIST

NIST Cloud Computing Program

For additional information :

Michaela Iorga:
michaela.iorga@nist.gov

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

THANK YOU!

NIST

NIST Cloud Computing Program