NIST Standards to Balance Security and Risk in a Cloud-Connected Enterprise

Anil Karmel
Co-Chair, NIST Cloud Security Working Group
Founder and CEO, C2 Labs. Inc.
akarmel@c2labs.com

© Ian Powell / Barcroft Media

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

C2 labs

NIST Cloud Computing Program

Evolution of Computing Resources

2010s

1960s

Cloud Computing

On-demand, Self-service

Broad network access

Resource pooling

Rapid elasticity

Measured services

IBM: Time-Sharing

***2012**: Vivek Kundra's quote in "Cloud First": "**Cloud computing will not just be more innovative than we imagine; it will be more innovative than we can imagine**".*

© Ian Powell / Barcroft Media

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

2 labs

NIST Cloud Computing Program

Many Shades of Cloud Views….

© Ian Powell / Barcroft Media

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

2 labs

NIST Cloud Computing Program

Balancing Cloud Benefits and Risks …

… is not easy but it CAN be done.

- Reduce Capital Cost
- Improve Business Agility
- Increase Productivity & Collaboration
- Increase Competitiveness
- Lower Staff Cost

- Preserve Security Posture
- Improve Security
- Minimize Business Risk
- Increase Availability
- Preserve Privacy

NIST Risk Management Standards

- *Standards for Security Categorization of Federal Information and Information Systems (FIPS 199); Feb 2004*
- *Guide for Mapping Types of Information and Information Systems to Security Categories (SP 800-60 Rev. 1); Aug 2008*
- *Minimum Security Requirements for Federal Information and Information Systems (FIPS 200); Mar 2006*
- *Security Considerations in the System Development Life Cycle (SP 800-64 Rev. 2); Oct 2008*
- *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach (SP 800-37, Rev. 1); Feb 2010*
- *Managing Information Security Risk: Organization, Mission, and Information System View (SP 800-39); Mar 2011*
- *Guide for Conducting Risk Assessments (SP 800-30 Rev. 1); Sep 2012*
- *Security and Privacy Controls for Federal Information Systems and Organizations (SP 800-53 Rev. 4); Apr 2013*

© Ian Powell / Barcroft Media

Other Related NIST Standards

- Performance Measurement Guide for Information Security (SP 800-55 Rev. 1); Jul 2008
- Contingency Planning Guide for Federal Information Systems (SP 800-34 Rev. 1); May 2010
- Information Security Continuous Monitoring for Federal Information Systems and Organizations (SP 800-137); Sep 2011
- Computer Security Incident Handling Guide (SP 800-61 Rev. 2); Aug 2012

New NIST Standards Drafts

- DRAFT Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems (SP 800-160 Draft); May 12, 2014
- DRAFT Supply Chain Risk Management Practices for Federal Information Systems and Organizations SP 800-161 (Second Draft); Jun. 3, 2014
- **Cloud-Adapted Risk Management Framework: Guide for Applying the Risk Management Framework to Cloud-based Federal Information Systems (SP 800-163); *In Development***
- **Security and Privacy Controls for Cloud-based Federal Information Systems (SP 800-174); *In Development***

© Ian Powell / Barcroft Media

Security may mean different things to different people…

Navy

Army

Marines

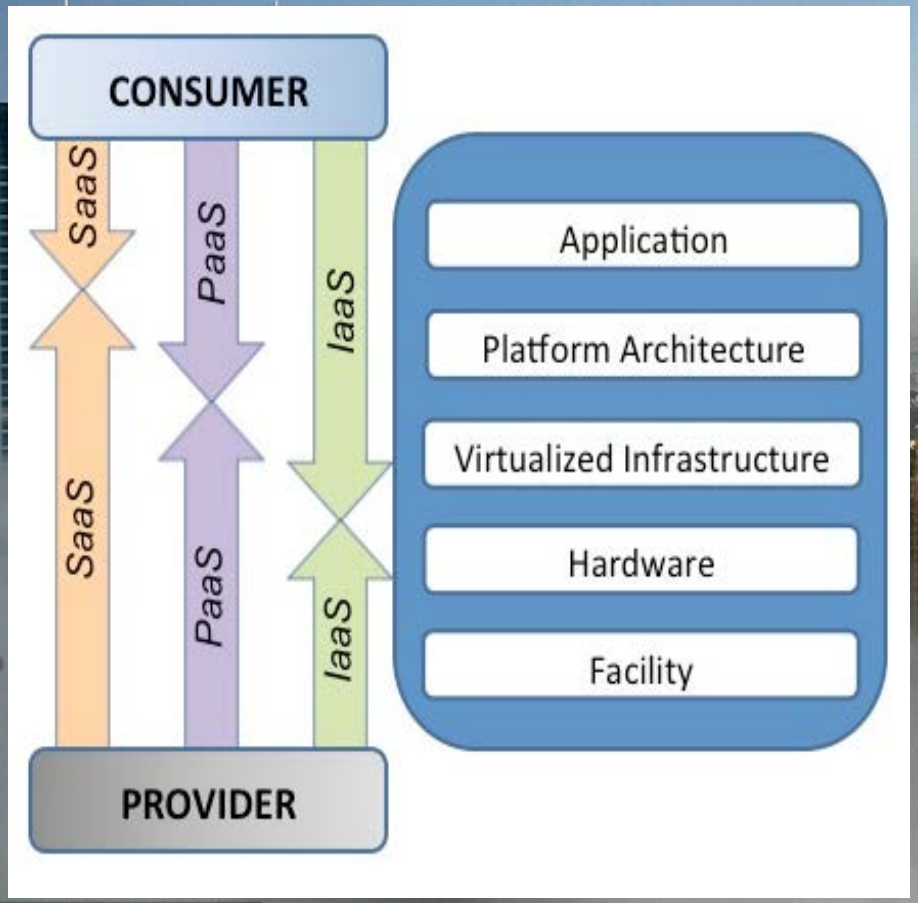
Air Force

Courtesy of Bill Murray, AWS, Amazon

© Ian Powell / Barcroft Media

Distributed Architecture = Split Control / Responsibilities

Security Conservation Principle



CLOUD ECOSYSTEM

Cloud Clients
(Browsers, Mobile Apps, etc.)

CLOUD ENVIRONMENT

Software as a Service (SaaS)
(Application , Services)

Platform as a Service (PaaS)
(APIs, Pre-built components)

Infrastructure as a Service
(VMs, Load Balancers, DB, etc.)

Physical Hardware
(Servers, Storage, Networking)

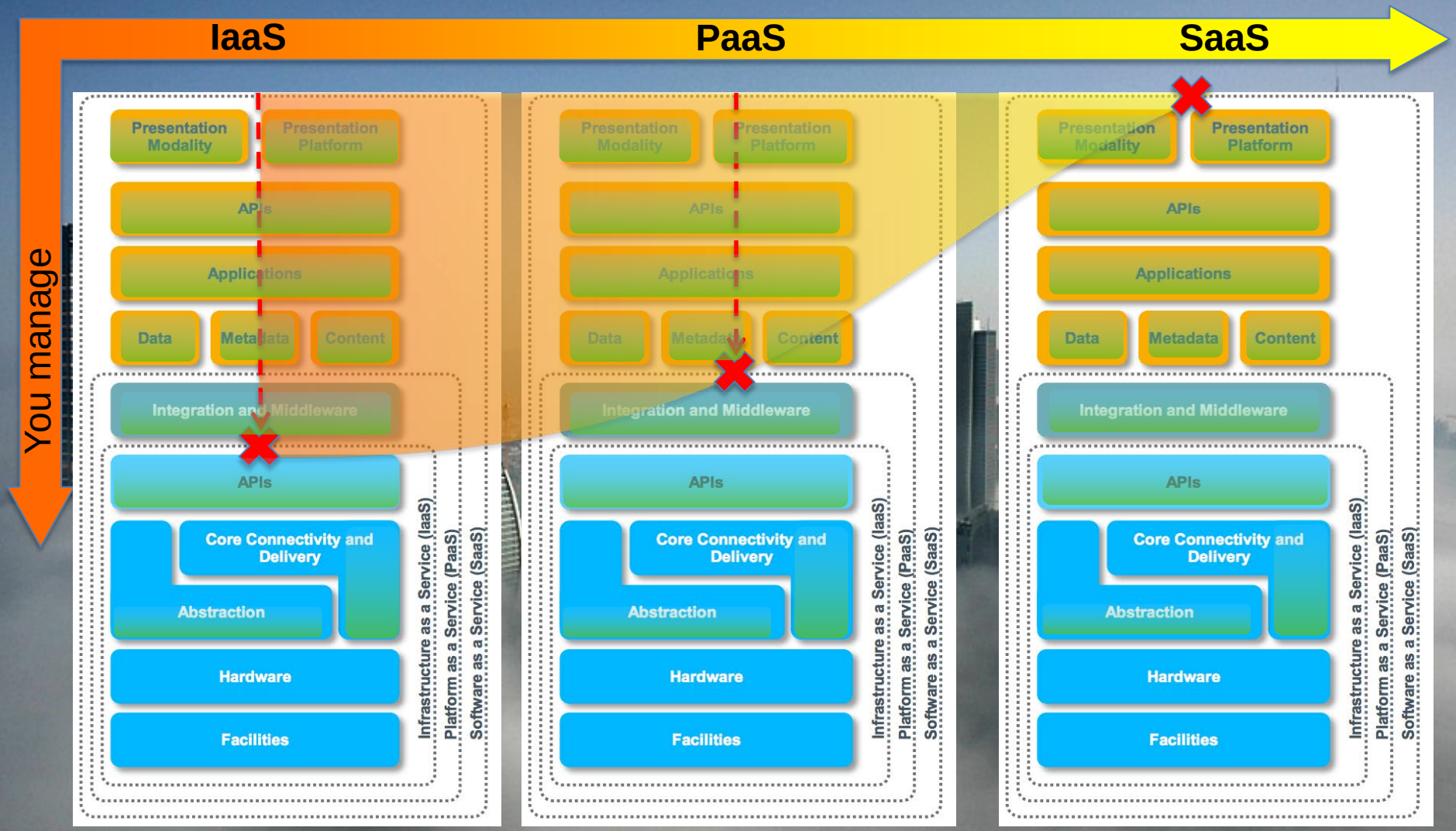
© Ian Powell / Barcroft Media

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

2 labs

NIST Cloud Computing Program

What You can manage matters…



Stack image source: Cloud Security Alliance specification, 2009

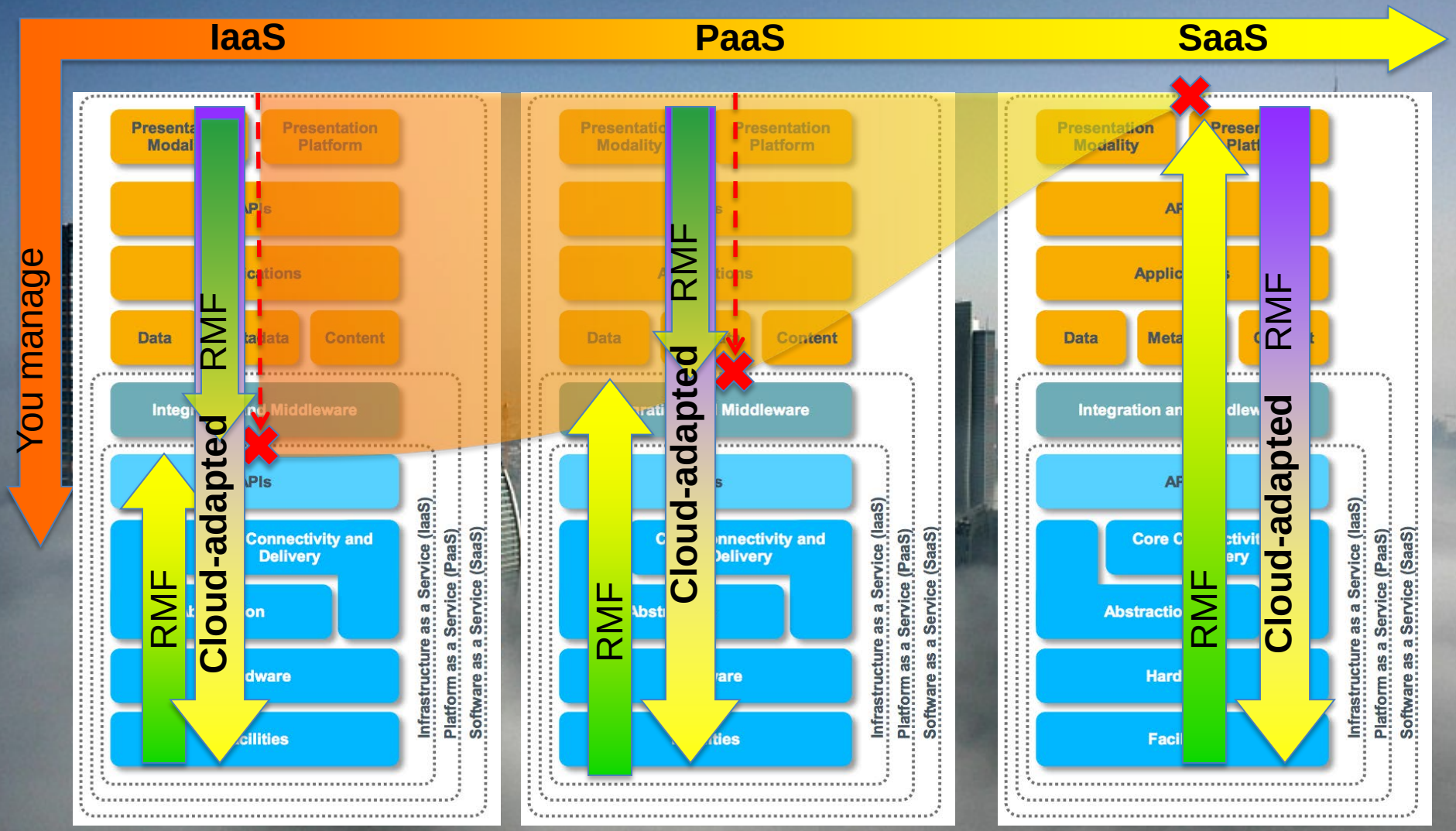
© Ian Powell / Barcroft Media

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

2 labs

NIST Cloud Computing Program

Consumer's Risk Assessment & Management



Stack image source: Cloud Security Alliance specification, 2009

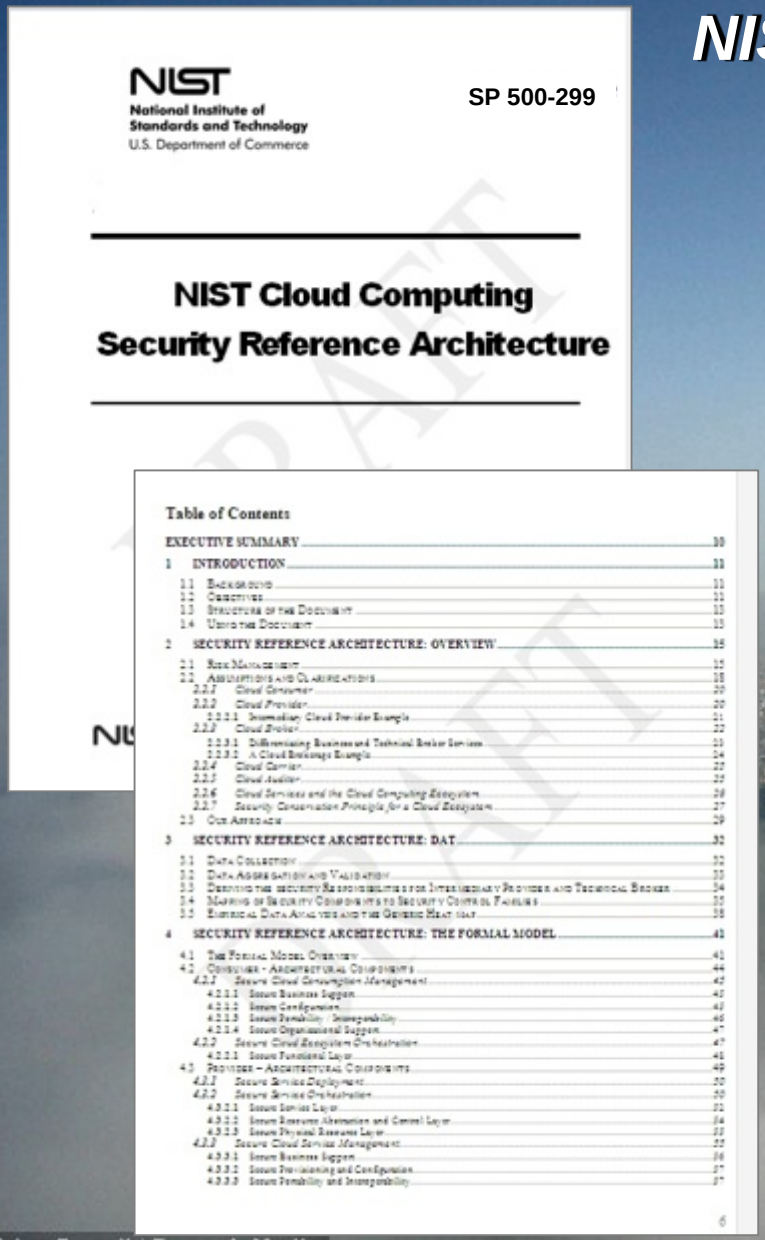
© Ian Powell / Barcroft Media

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

2 labs

NIST Cloud Computing Program

NIST Security Reference Architecture SP 500-299 Draft


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 33
1.4 Using the Document 33
2 SECURITY REFERENCE ARCHITECTURE: OVERVIEW 35
2.1 Risk Management 35
2.2 Assumptions and Clarifications 38
2.2.1 Cloud Consumer 39
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: DAT 32
3.1 Data Collection 32
3.2 Data Aggregation and Validation 33
3.3 Deriving the Security Responsibilities for Intermediary Providers and Technical Brokers 34
3.4 Mapping of Security Components to Security Control Families 35
3.5 Empirical Data Analysis and the Generic Heat Map 38
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 52
4.3.2.2 Secure Resource Abstraction 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

6

© Ian Powell / Barcroft Media

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)

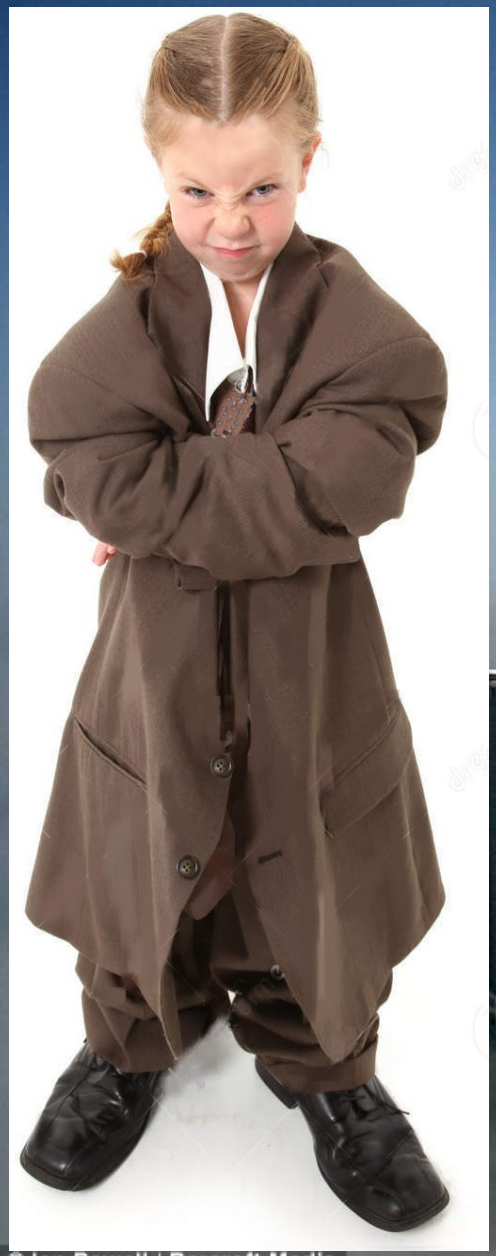
Cloud-adapted Risk Management Framework :

Step 1: Categorize System to be migrated
Step 2: Identify Security Requirements, perform a Risk Assessment & select Security Controls
Step 3: Select best-fitting Cloud Architecture
Step 4: Assess Service Provider(s) & Controls
Step 5: Authorize Use of Service
Step 6: Monitor Service Provider (on-going, near-real-time)

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

2 labs

NIST Cloud Computing Program



© Ian Powell / Barcroft Media

Not All Clouds Are Equal !

Step 3:

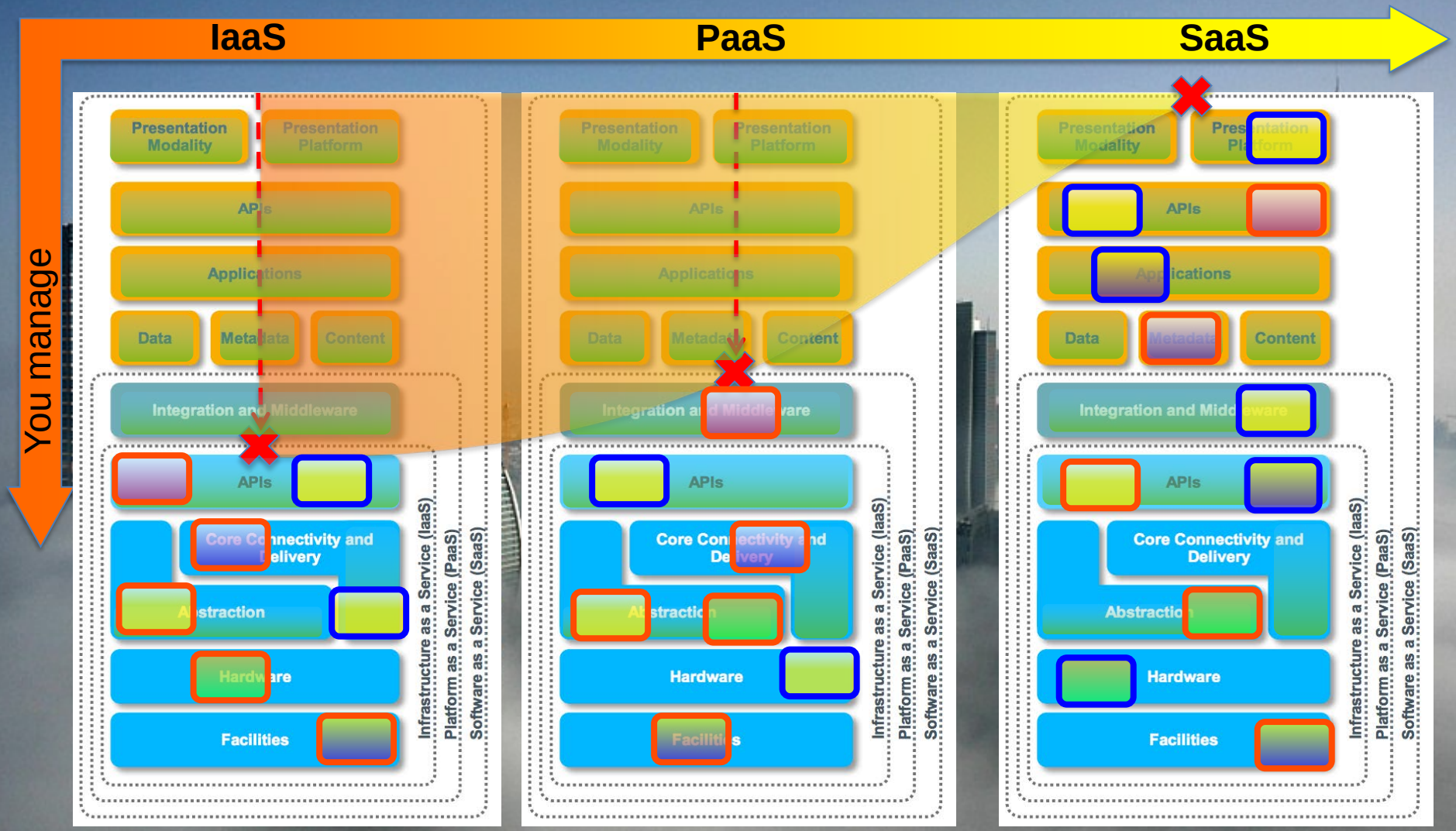
Select Best-fitting Architecture for the System

And remember:

One–size–fits–All Approach

DOES NOT WORK…

A & A – Controls' Allocation Matters...



Stack image source: Cloud Security Alliance specification, 2009

© Ian Powell / Barcroft Media

A & A baseline

Consumer's needs

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

NIST Cloud Computing Program

Not All Clouds Are Equal !

Step 4: Assess Service Provider(s) & Their Controls

FedRAMP CAN HELP:
leverage issued P-ATOs

REMEMBER: not all the controls are implemented the same

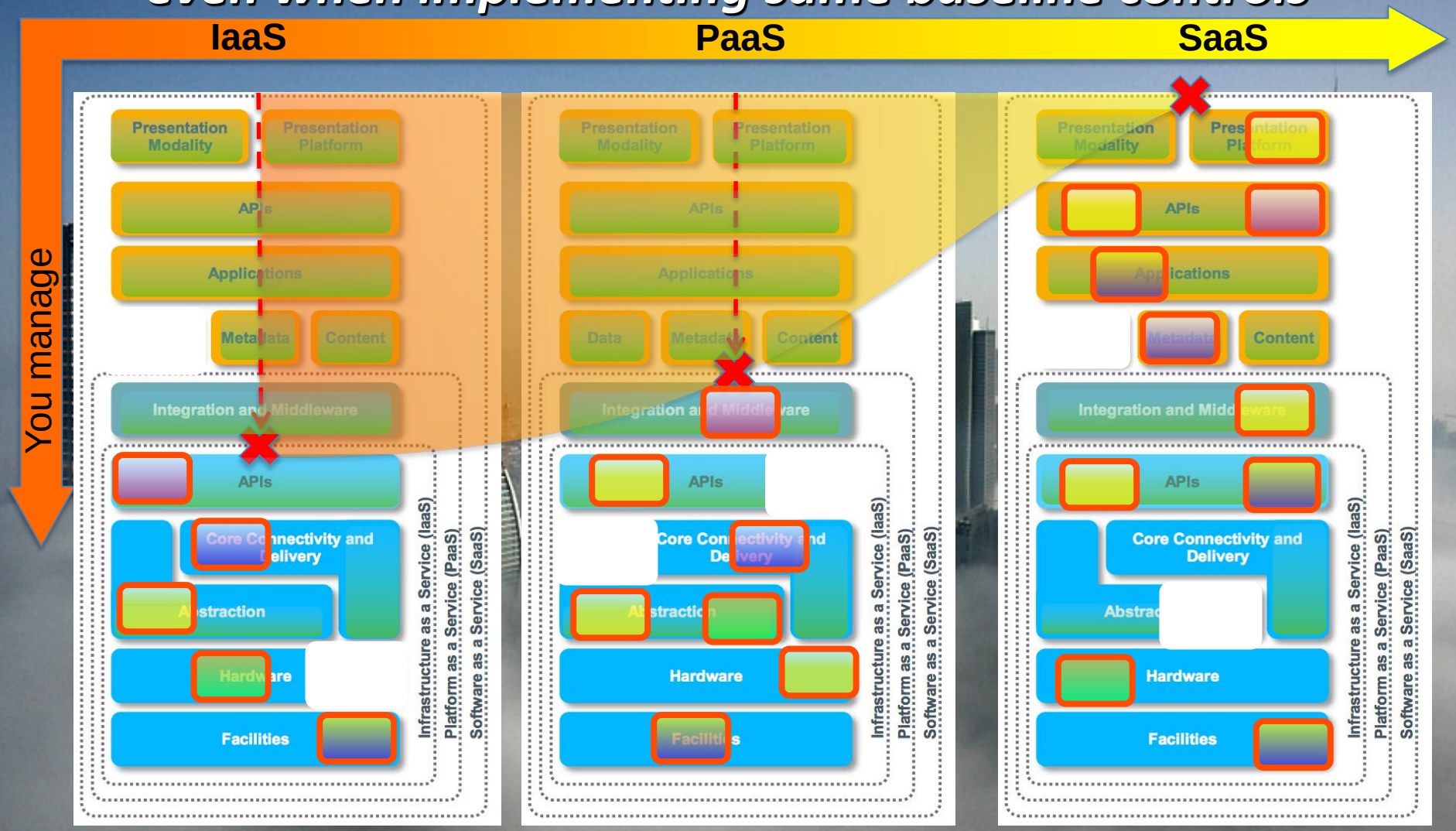
So do your homework

1. *READ ALL FedRAMP's A&A documentation*
2. *IDENTIFY controls that need to be tailored,*
3. *NEGOTIATE them &*
4. *ASSESS them*

© Ian Powell / Barcroft Media

Clouds are not identical …

even when implementing same baseline controls



Stack image source: Cloud Security Alliance specification, 2009

© Ian Powell / Barcroft Media

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

A & A baseline

NIST Cloud Computing Program

The Final Decision

Step 5: Authorize the Use of Service

- but not before you negotiate the Service Level Objectives (SLO) and agreed on the Service Level Agreement (SLA)

© Ian Powell / Barcroft Media

On-going Work...

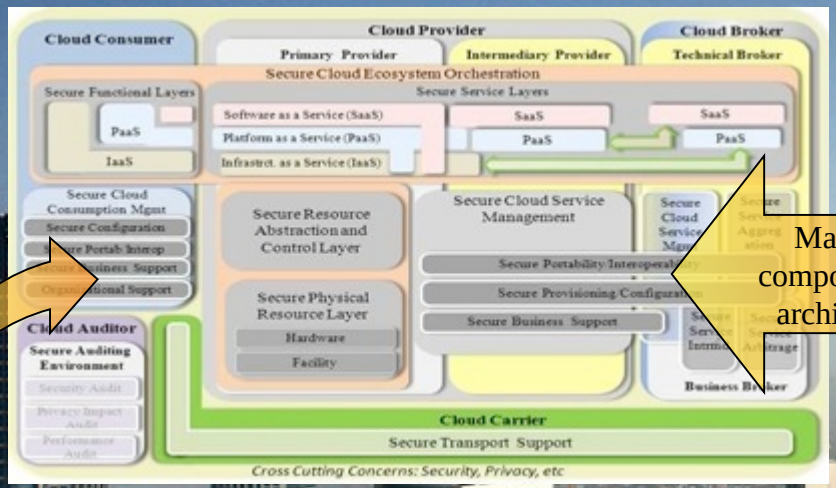
Step 6: Monitor the Service
(on-going, near-real-time) –

- *the controls implemented in house (by you) &*
- *the Provider (the controls implemented by them)*

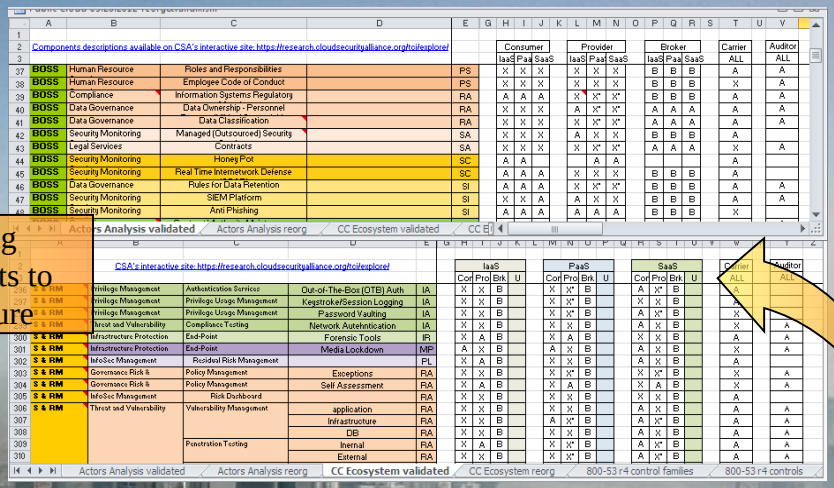
© Ian Powell / Barcroft Media

Need help? – Check out SP 500-299: NIST Cloud Security Reference Architecture

NIST Security Reference Architecture – formal model

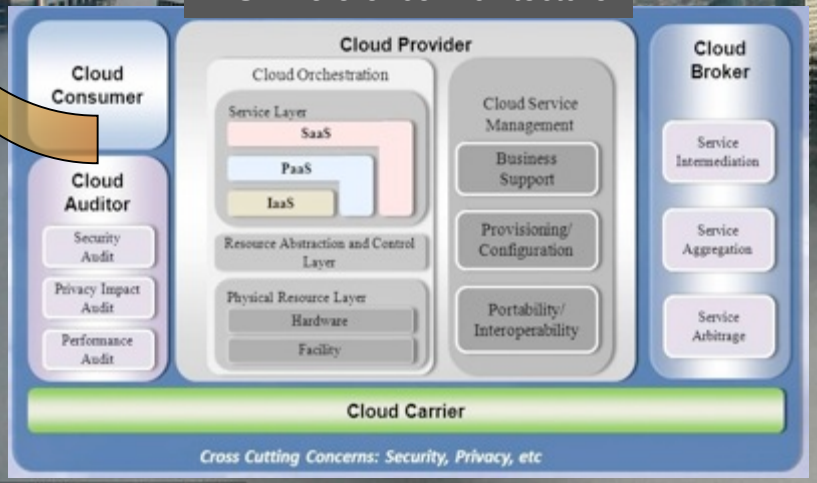


NIST Security Reference Architecture – security components



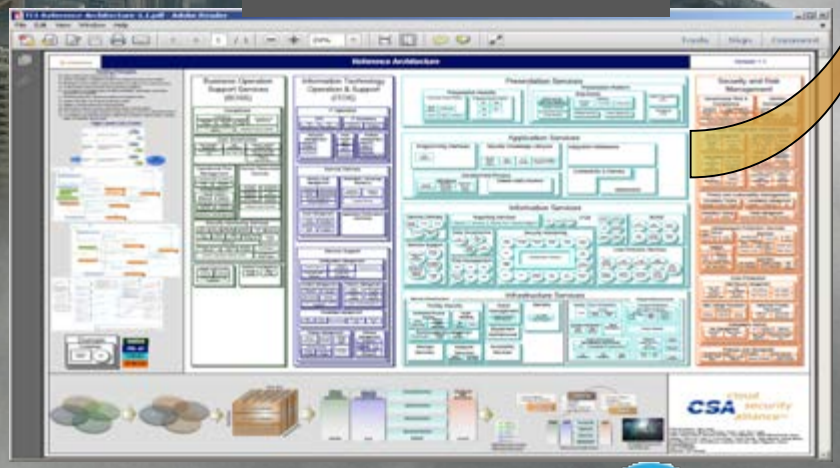
Mapping components to architecture

NIST Reference Architecture



+

TCI Reference Architecture



© Ian Powell / Barcroft Media

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

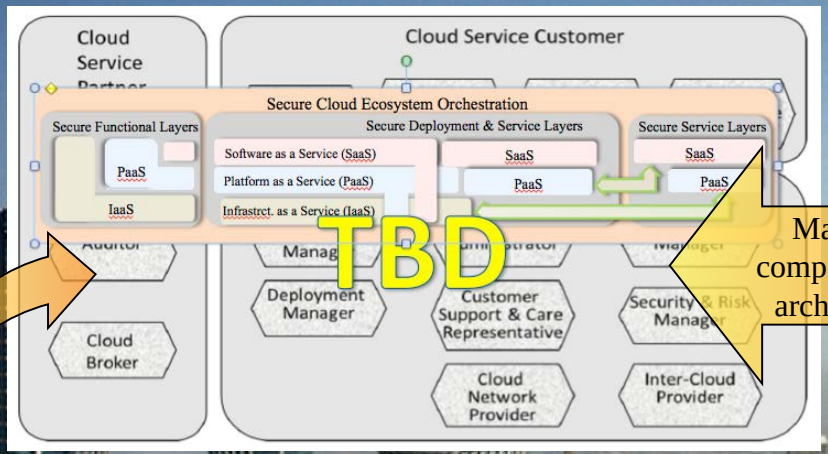
2 labs

NIST Cloud Computing Program

OUR APPROACH IS MODULAR – YOU CAN SUBSTITUTE COMPONENTS

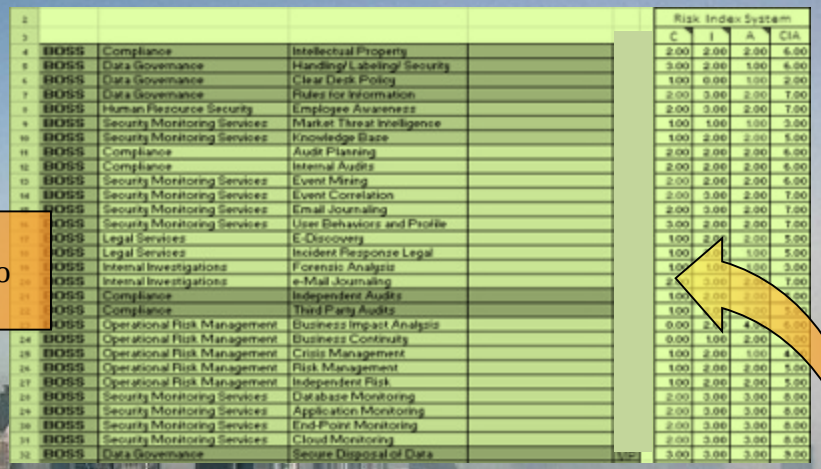
E.g. ISO/IEC based CC Security Reference Architecture -

ISO/IEC Security Reference Architecture – formal model



Mapping components to architecture

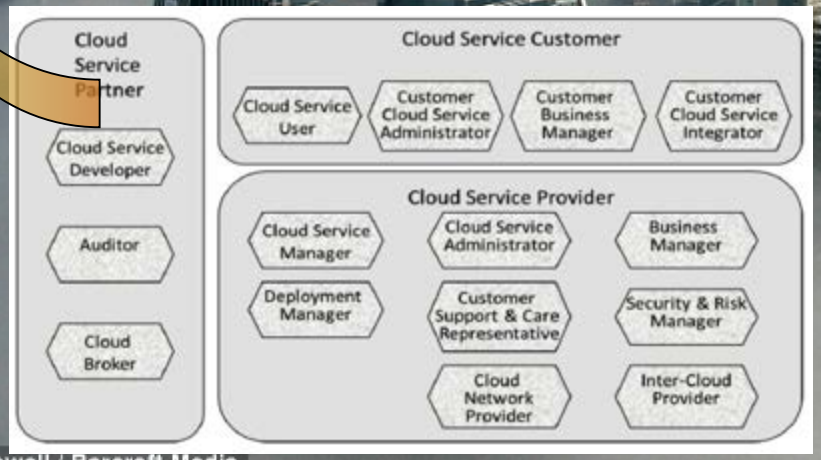
ISO/IEC Security Reference Architecture – security components



				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	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

CRMF + methodology

ISO/ICE Reference Architecture



+

Proprietary Set of Components

YOUR OWN SET OF COMPONENTS

© Ian Powell / Barcroft Media

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

2 labs

NIST Cloud Computing Program

Software-Defined IT

Balancing Security, Privacy and Functionality

- Technical
  - Validate that your architecture respects multi-tenancy and scales with an established root of trust
  - Embrace Identity and Access Management to authenticate and authorize users to context aware applications and systems
  - Redefine your network perimeter
  - Build intelligence into your application, not the end point
  - Fork your logs to multiple entities with a baseline timestamp
  - Manage your application security while quantifying the risk to the same
  - Encryption
    - Compute: In-Memory Encryption
    - Network: Software Defined Perimeter
    - Storage: VM and File-Level Encryption

© Ian Powell / Barcroft Media

Software-Defined IT

Balancing Security, Privacy and Functionality

- Legal
  - Establish Clear Contract Terms and Conditions with Cloud Service Providers
  - Update Policies and Procedures
  - Understand Jurisdiction for Forensics Analysis
  - Define your Data Retention Periods

© Ian Powell / Barcroft Media

Software-Defined IT

Balancing Security, Privacy and Functionality

- Organization
  - Design with the user in mind with security baked in, not bolted on
  - Redefine your system boundaries
  - Ensure people that have access to government data have the appropriate clearance level

© Ian Powell / Barcroft Media

Thank you!

Anil Karmel, CEO
akarmel@c2labs.com
@anilkarmel