

National Aeronautics and Space Administration



Enterprise Management of Software as a Service (SaaS)

Office of the Chief Information Officer

Karen Petraska
March 9, 2016

www.nasa.gov





An Enterprise Approach To Cloud Computing



An enterprise approach results in faster adoption, greater consistency, managed risks, and lower Agency costs

Key Elements of an Enterprise Approach

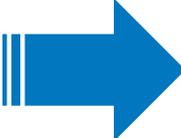
- Standardized Agency governance
- Standards and guidance for technical integration with Agency infrastructure, processes, and services
 - Networking
 - Security operations
 - Authentication services
- Integrated hierarchical approach to FedRAMP compliance
- Common procurement vehicles with proper terms, conditions, best practices
- Payment mechanisms to accommodate the many SaaS pricing models
- Integration with Agency IT service catalog and help desk (ordering and renewals)



Case for an Enterprise Approach

If each NASA community or project addresses the wide array of Requirements for Cloud Computing:

- Projects may interpret and fulfill requirements differently
- Unknown security posture and risks
- Inconsistencies in policies, processes, and implementations
- Highly inefficient approach that results in large Agency spend
- Chaos

Strategy 

Do the “heavy lifting” once for the Agency and enable projects to leverage the capabilities we’ve created.



SaaS Enterprise Implementation Strategy

Driving concern: We do not know how many SaaS products are already deployed in our environment and how much data we have at risk because of the unmanaged use of those SaaS products

Deploy Security Framework

- A&A processes and guidance
- Cloud Access Security Broker tool (CASB)
- Establish technical integrations including authentication, networking, security operations



Enables centers to onboard new SaaS in a safe and compliant way

Begin Cleanup Of Existing SaaS

- Triage the list to prioritize biggest risks
- Audit usage
- Establish any special rules or constraints
- Establish center ownership and who will perform assessment



Brings existing SaaS into compliance and reduces Agency risk

Develop SaaS Business Environment

- Identify SaaS vendor business models
- Define ownership and curation requirements
- Determine best procurement approach
- Define ordering and payment and renewal mechanism



Enables enterprise management of SaaS business aspects



What is A Cloud Access Security Broker?

Cloud Access Security Brokers (CASB) are on-premise or cloud-hosted software that act as a control point to secure cloud services. Range of capabilities may include:

- **Visibility:** Dashboards, identification of approved vs unapproved applications, analytics, incident reporting, policy control, automated alerting and reporting, license counts and usage, identification of “shadow IT”
- **Compliance:** Role based auditing, file content monitoring for compliance to PII, HIPAA, etc., policy enforcement
- **Data Security:** DLP, Encryption, Tokenization
- **Threat Protection:** inbound/outbound content monitoring, user behavior analytics, prevent prohibited devices and locations from accessing network, anomaly detection
- **Enterprise Integration:** ICAM, centralized log management, secure web gateway/ proxies

By 2016, 25% of enterprises will secure access to cloud-based services using a CASB platform, up from less than 1% in 2012, reducing the cost of securing access by 30%.
– Gartner, The Growing Importance of Cloud Access Security Brokers



Discovery and Clean Up Phase

- Lab tested one CASB with 30 days of log files from each of two centers.
 - » 2500 and 3100 SaaS products identified in use
 - » Variety of risk ratings and risk factors
- As we deploy a CASB and begin to get information about what SaaS products are running in the environment then we can:
 - » Identify which products represent the most risk and prioritize
 - » Work on getting assessments done and ATOs issued
 - » Audit the data managed by these products and correct problems
 - » Ban or eliminate from our environment products that represent excessive or unmanageable risk
 - » Establish/refine policies, governance and constraints
 - » Educate our customers about new practices, risks and requirements related to SaaS



FedRAMP Background

- The purpose of the Federal Risk and Authorization Management Program (FedRAMP) is to:
 - » Assess and approve the set of NIST 800-53 controls that are implemented by each cloud service provider (CSP)
 - » Issue a provisional authorization to operate (PATO) for those controls that can be used by all agencies to insure consistent interpretation
 - » Reduce agency costs by enabling agencies to leverage the FedRAMP assessment and build on it for the shared and agency specific controls
- Effective June 2014, FedRAMP certification became a requirement for any cloud computing products utilized by the government



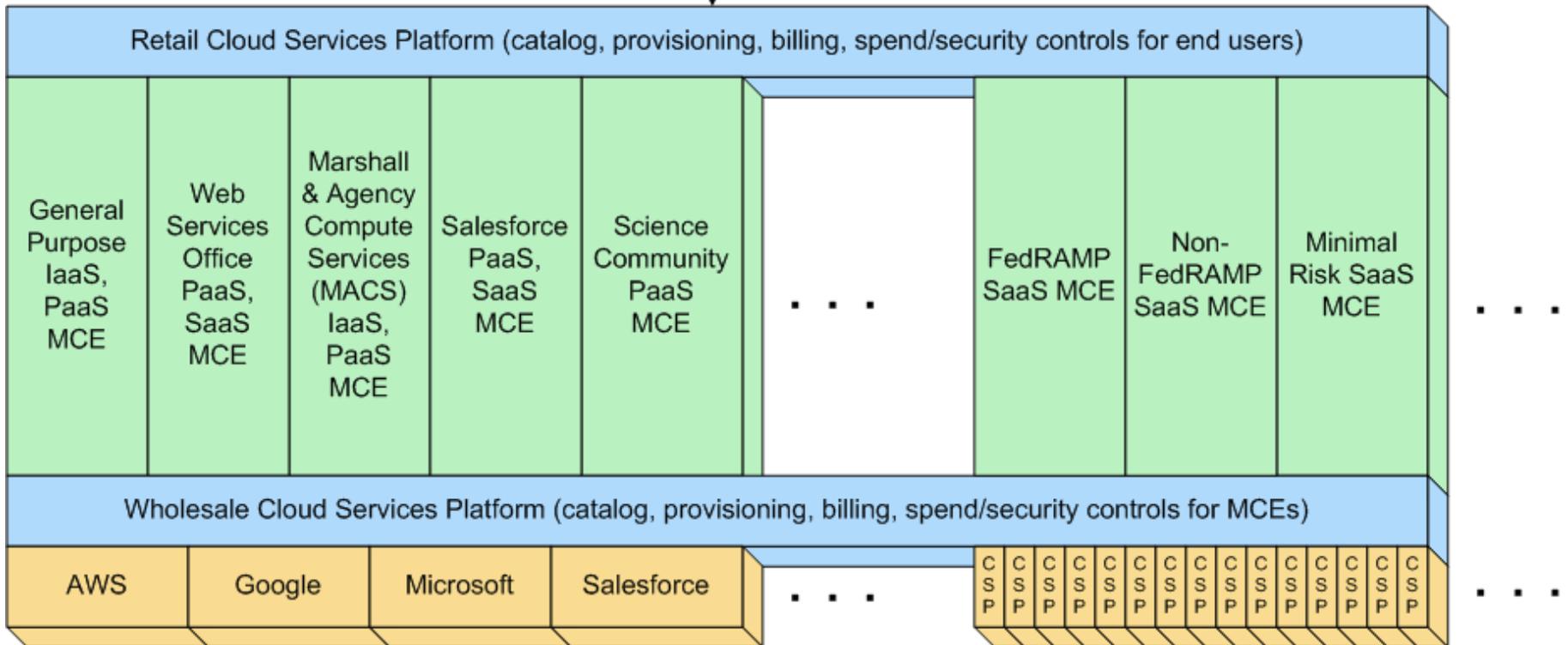
FedRAMP Challenge

- The FedRAMP process has been morbidly slow at processing vendor requests for certification. Fifteen months after the mandate took effect there are only 48 FedRAMP certified CSPs and 38 more listed as “In Progress” on www.fedramp.gov site.
- There are substantially more than 10,000 different CSPs available in the market place across IaaS, PaaS and SaaS delivery models. Approximately 90% of these are SaaS products.
- NASA employees have need for tools from MANY of the CSPs that are NOT FedRAMP certified, are NOT on a path for certification (and will likely never be) and CANNOT even get a reasonable place in the FedRAMP queue.
- Many SaaS and PaaS products without FedRAMP certification are already deployed and in use around NASA.

PROPOSAL: Waive the FedRAMP compliance requirement and accept that risk for low risk CSPs that are required for the conduct of NASA business.

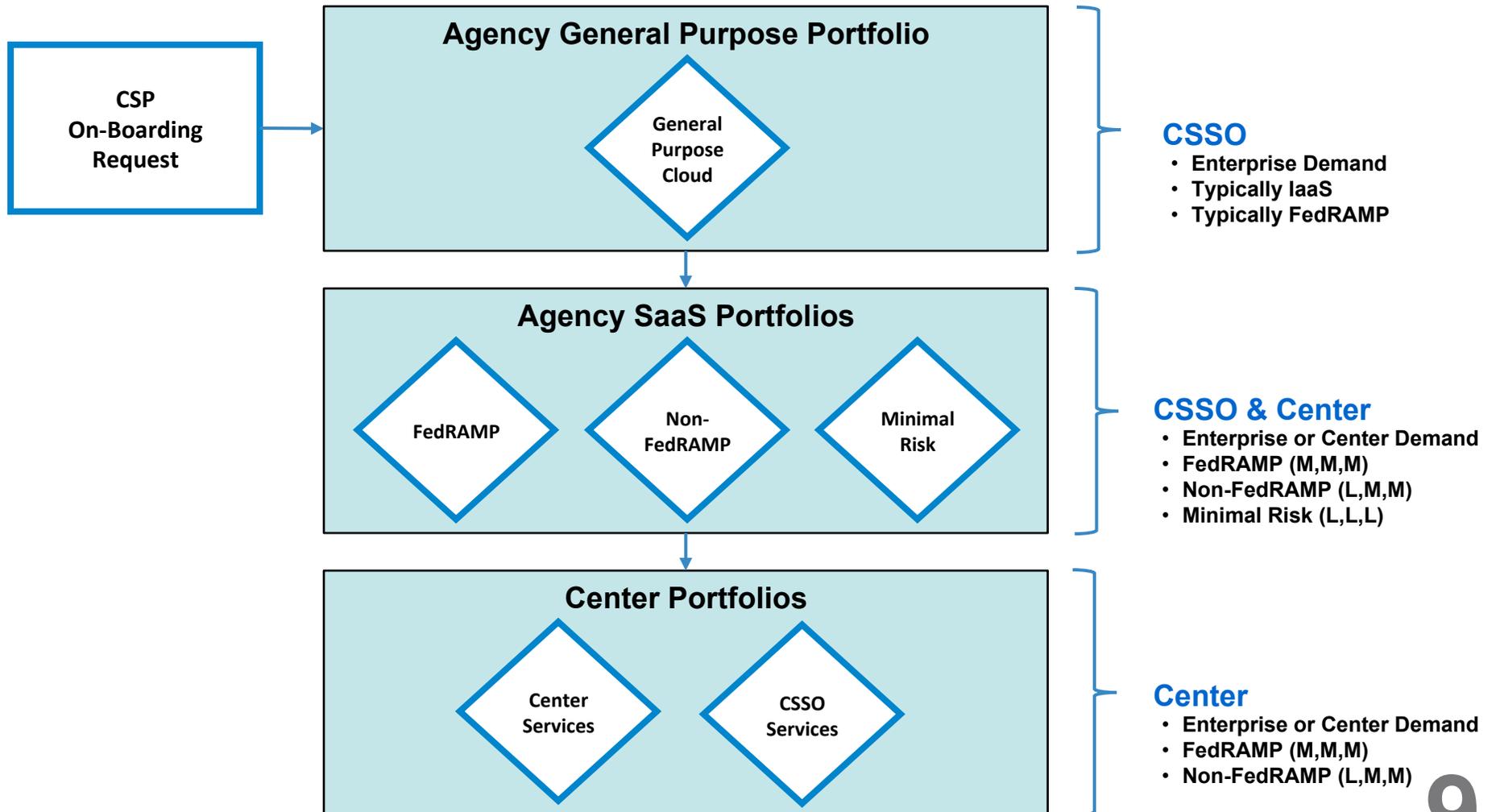


Tiered Cloud Services Architecture





NCAA Framework Summary





Risk & Resource Balanced Approach

Establish Agency SaaS Managed Cloud Environment (MCE)s

- » Agency Level AO, SO, CISO, & AAO
- » Three Agency ATOs, each supported by a “wrap-around” SSP
 1. Low: C, I, & A = Low, Low, Low – a.k.a. Minimal Risk Portfolio (MRP)
 - Highly tailored A&A (risk acceptance)
 - Minimal CSP security vetting (risk acceptance)
 - For low risk, “need it now” scenarios
 2. Moderate: C, I, & A = Low, Mod, Mod
 - NIST Moderate baseline
 - Full Security Assessment Review Process (SARP) for CSP (Non-FedRAMP)
 - Not suitable for sensitive data
 - Designed to address prevalence of non-FedRAMP SaaS CSP demand
 3. Moderate: C, I, & A = Mod, Mod, Mod
 - NIST Moderate baseline
 - Full SARP for CSP (FedRAMP)
 - Suitable for sensitive data



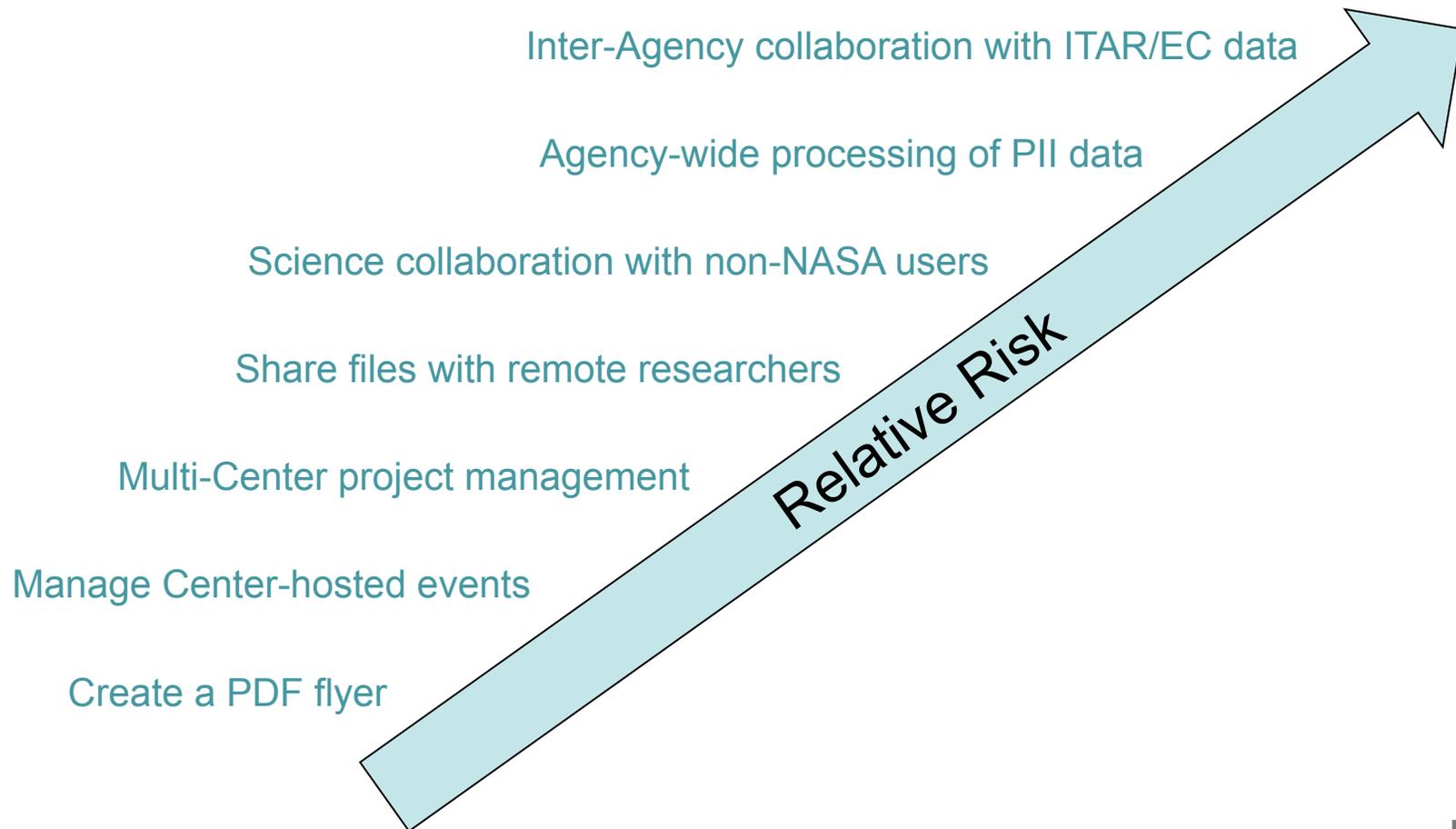
NCAA Framework Summary

- Requests for SaaS move automatically to an Agency SaaS MCE
 - One of three SaaS MCEs
 - EMCC & Sponsoring Center share CSP on-boarding & ConMon tasks
 - Minimal Risk MCE facilitates quick response for low risk scenarios
- Result is:
 - Centralized Governance & Management Oversight
 - Distributed burden
 - Optimal balance of risk and resources



Concept of Operations

Broad spectrum of SaaS Use Cases





Business Aspects Phase

If we can manage these aspects elegantly then the users will have a better experience and we will reduce the Agency's administrative overhead created by SaaS tremendously

- Acquisition: Ideally we could set up a “marketplace” with BPA(s) to make NASA-approved SaaS products easy to obtain.
- Pricing and payments: There are numerous pricing models in use for different SaaS products:
 - » Per use e.g., Go-To-Meeting
 - » Annual, monthly or other recurring interval individual license
 - » Purchase fixed quantities (bands defined by vendor) for annual or other recurring payments
 - » Costs for data stored at the remote site
 - » Others?
- End user ordering, provisioning and renewals: managing all the stops and starts and expirations



Roles for Centers In Delivery Cloud Computing

- On-boarding and Full Lifecycle Support of PaaS/SaaS
 - » Review of FedRAMP or other security assessment and issuance of ATOs
 - » Curatorship of center-sponsored PaaS and SaaS, with availability to Agency-wide customer base
 - » Review center cloud requests and refer to best provisioning option across Agency
 - » Potential role in one or more of acquisition, management and user provisioning
 - » Cleanup of existing legacy center SaaS/PaaS environments
- Facilitating center projects and people into the cloud
 - » Develop cloud skills in architecture, programming, administration
 - » Help customers understand how to structure and implement their systems in the cloud
 - » Help customers with cost estimating in the cloud



Benefits Of Center Participation

- Enables the center workforce to develop cloud skills that will enable them to bridge the transition to what the future center IT workloads will look like
 - » Reduction in traditional data center based technologies and a shift of a substantial portion of the traditional data center workloads into the cloud
 - » Most new applications will be born in the cloud and most commercial software will be served to you from a commercial cloud.
- Coordinating the Agency effort to on-board each tool ONCE saves NASA money and increases the throughput of tools to approval. There are clear reciprocal participation benefits for all centers.
- Allowing CSSO to retain primarily a role of enterprise governance, guidance and framework contains OCIO cost

Having more skilled hands will facilitate faster adoption of cloud for NASA



Summary

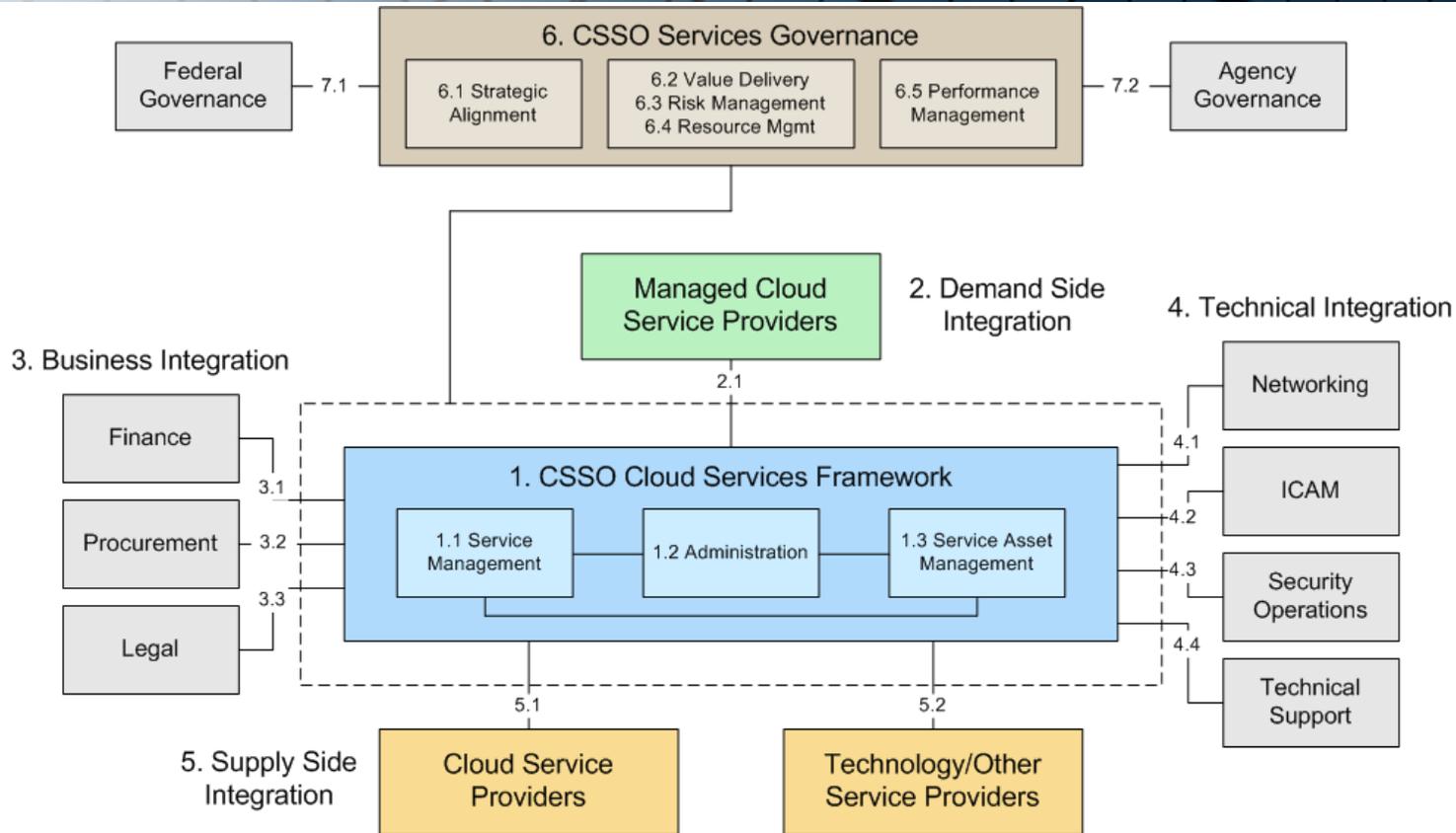
- Initiate Implementation of Enterprise Management of SaaS
 - » Governance for center on-boarding of CSPs to roll out shortly
 - » Lab tested CASB on real data with excellent results
- Support Centers in taking on new roles to onboard SaaS
 - » Provide processes and guidance
 - » Help transition Center customers and workforce to cloud skills
 - » Many center CIO teams already engaging!!!!!!!
- Incorporate new methods and tools as marketplace evolves
 - » Much about the business aspects yet to be resolved
 - » The marketplace is still figuring out what it means to do enterprise management of cloud and new kinds management tools will continue to emerge quarter by quarter



Office of the
Chief Information Officer



Framework – Contextual View



The Cloud Services Framework consists of capabilities and resources (e.g., people, processes, information, technology, other services) that are integrated to provide Services to Managed Cloud Service Providers.