



*THE SHORTEST DISTANCE BETWEEN MISSION AND SUCCESS*

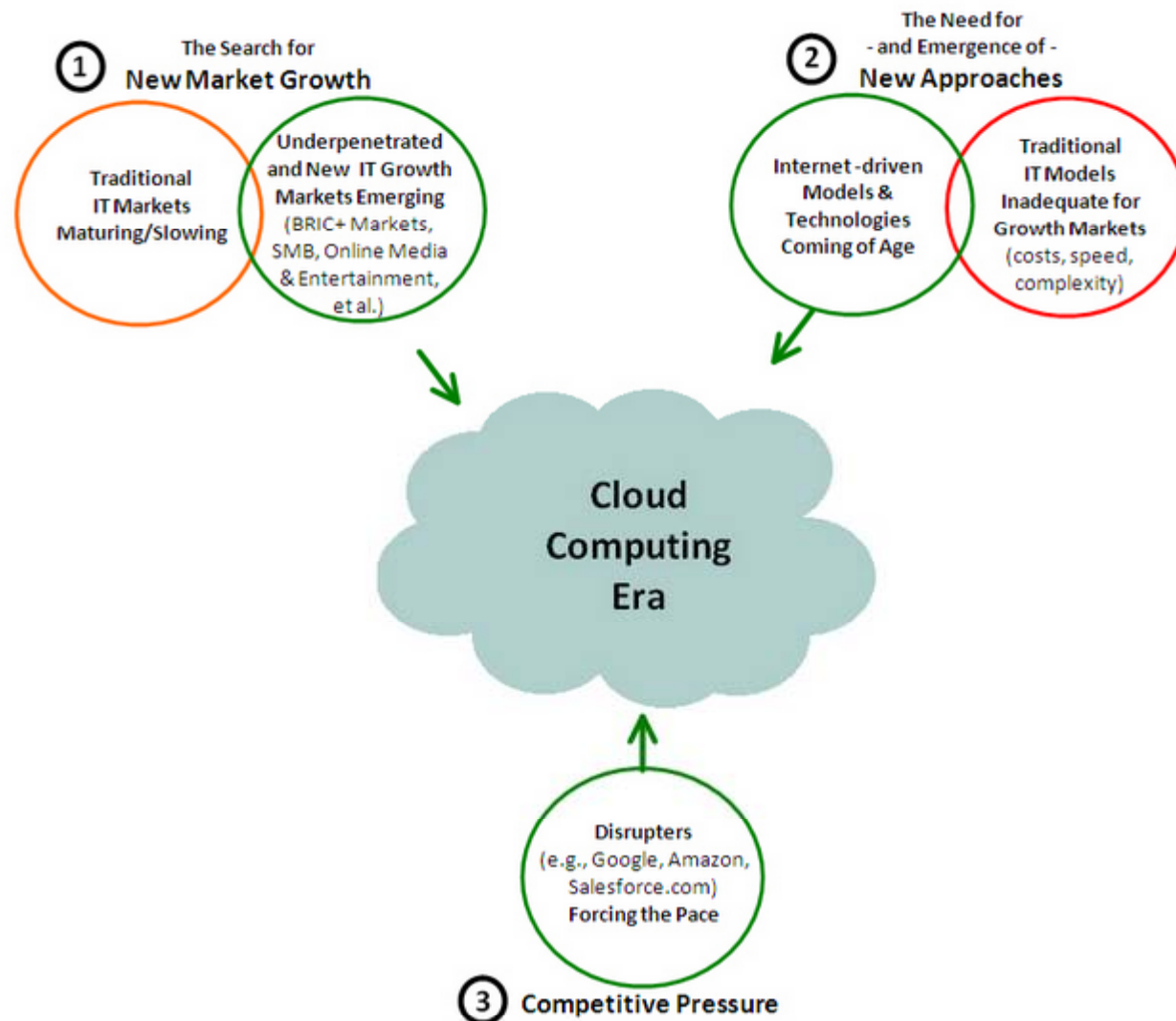
# Secure Cloud Computing:

## An Architecture Ontology Approach

KEVIN JACKSON



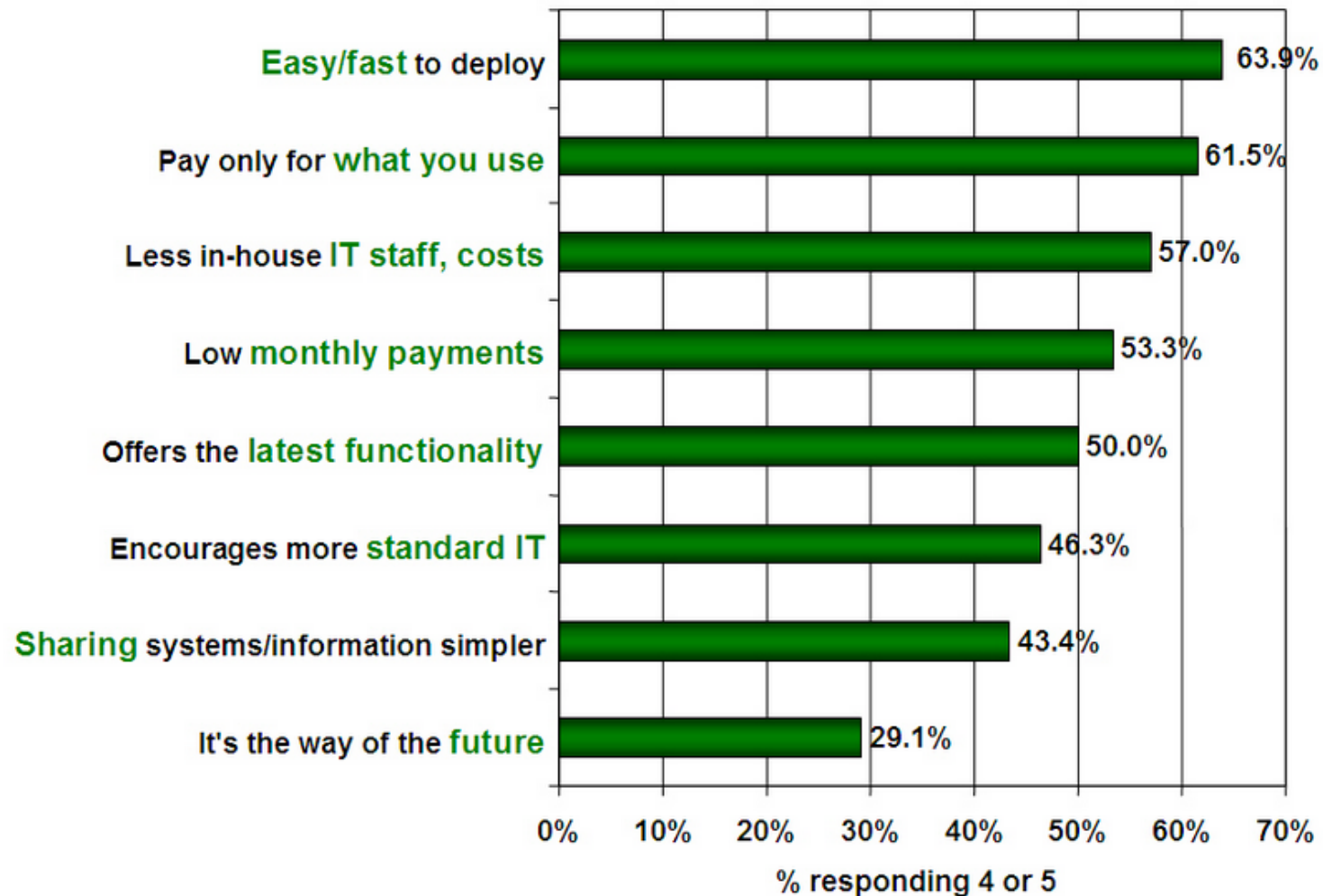
# Forces Driving Cloud Computing - The New IT Era



Source: IDC, September 2008

# Cloud Computing Value

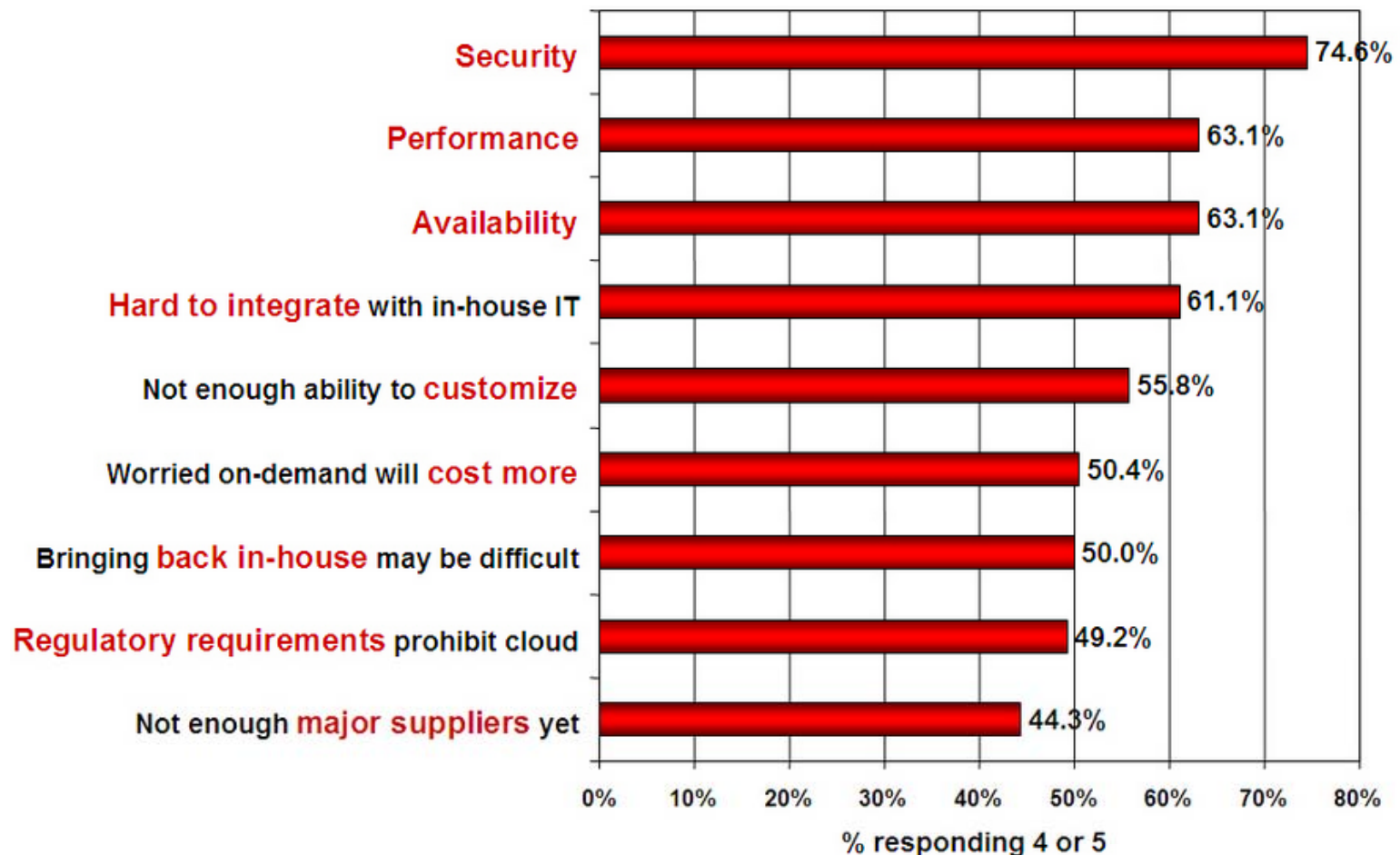
Q: Rate the **benefits** commonly ascribed to the 'cloud'/on-demand model  
(1=not important, 5=very important)



Source: IDC Enterprise Panel, August 2008 n=244

# Cloud Computing Challenge

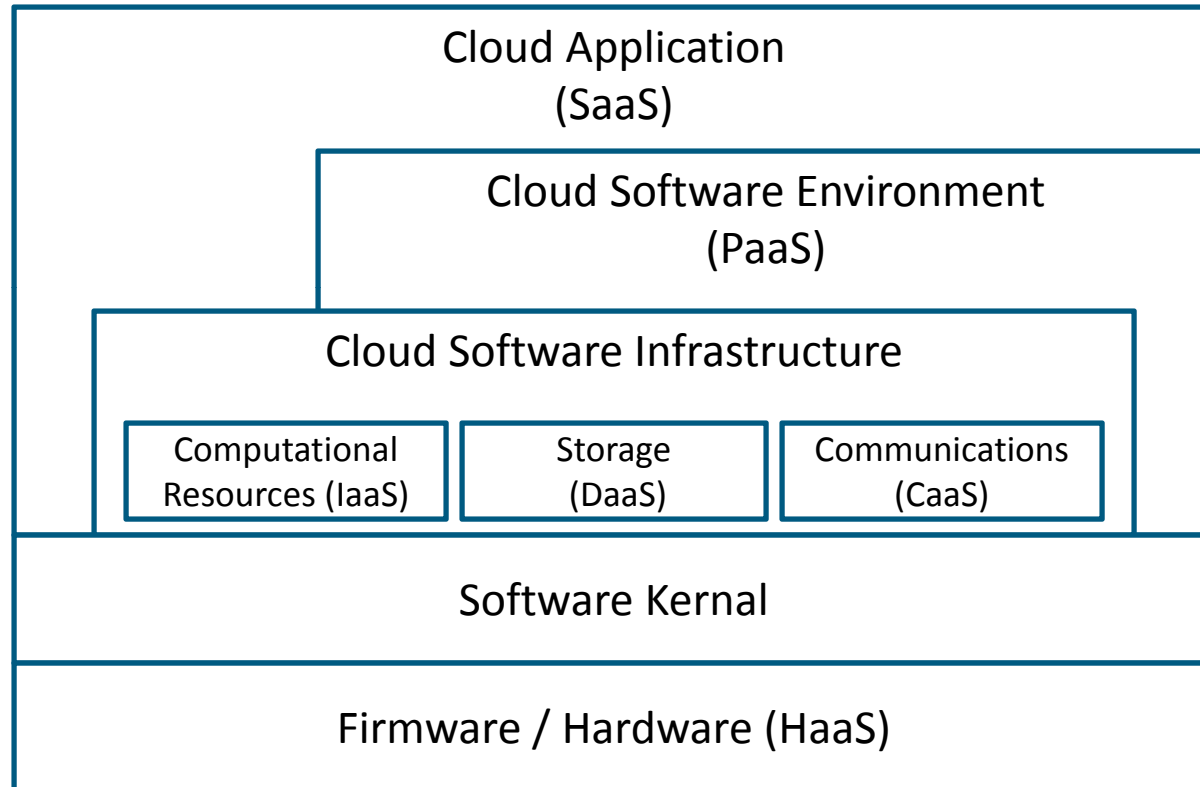
Q: Rate the **challenges/issues** ascribed to the 'cloud'/on-demand model  
(1=not significant, 5=very significant)



Source: IDC Enterprise Panel, August 2008 n=244

# Unified Ontology of Cloud Computing

(<http://www.cs.ucsb.edu/~lyouseff/CCOntology/CloudOntology.pdf>)



Lamia Youseff  
University of California, Santa Barbara

Maria Butrico, Dilma Da Silva  
IBM T.J. Watson Research Center

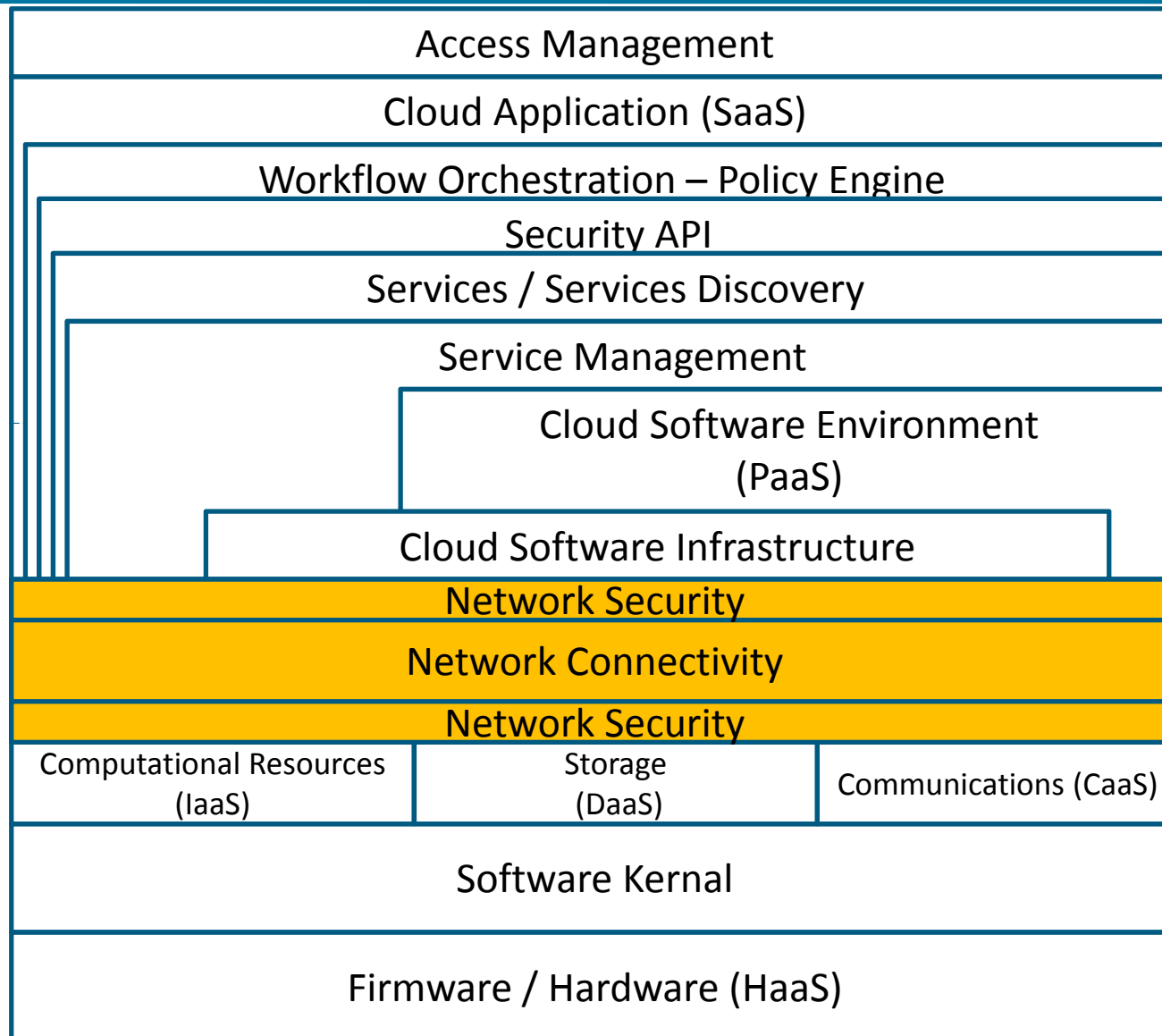


# Tactical Employment Issues

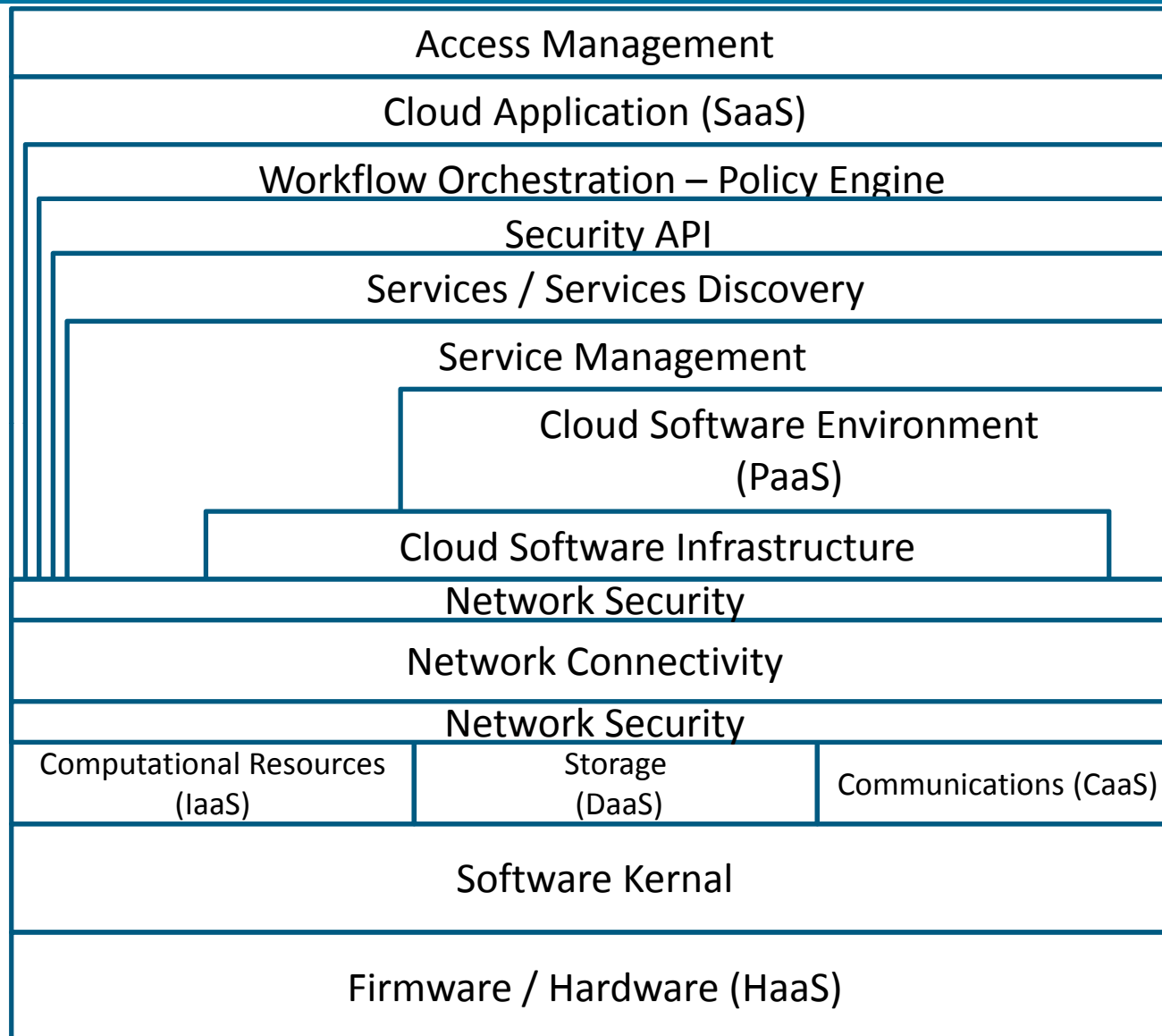
---

- Internet connectivity assumed
- SOA platform
  - Security management
  - Application service discovery and management
  - Workflow orchestration
- Access management

# Ontology Modifications for Tactical Cloud Computing

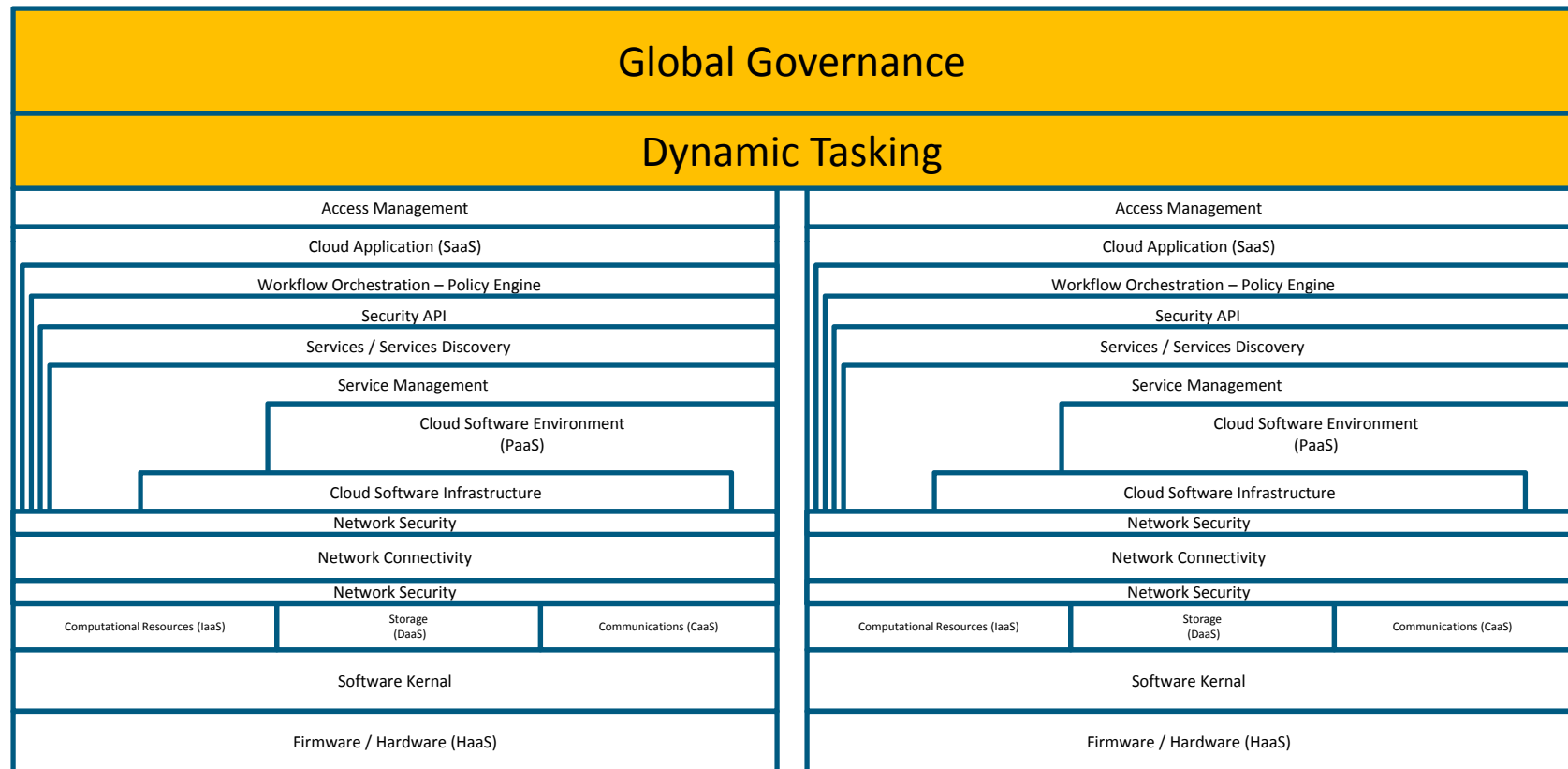


# Tactical Cloud Computing Ontology



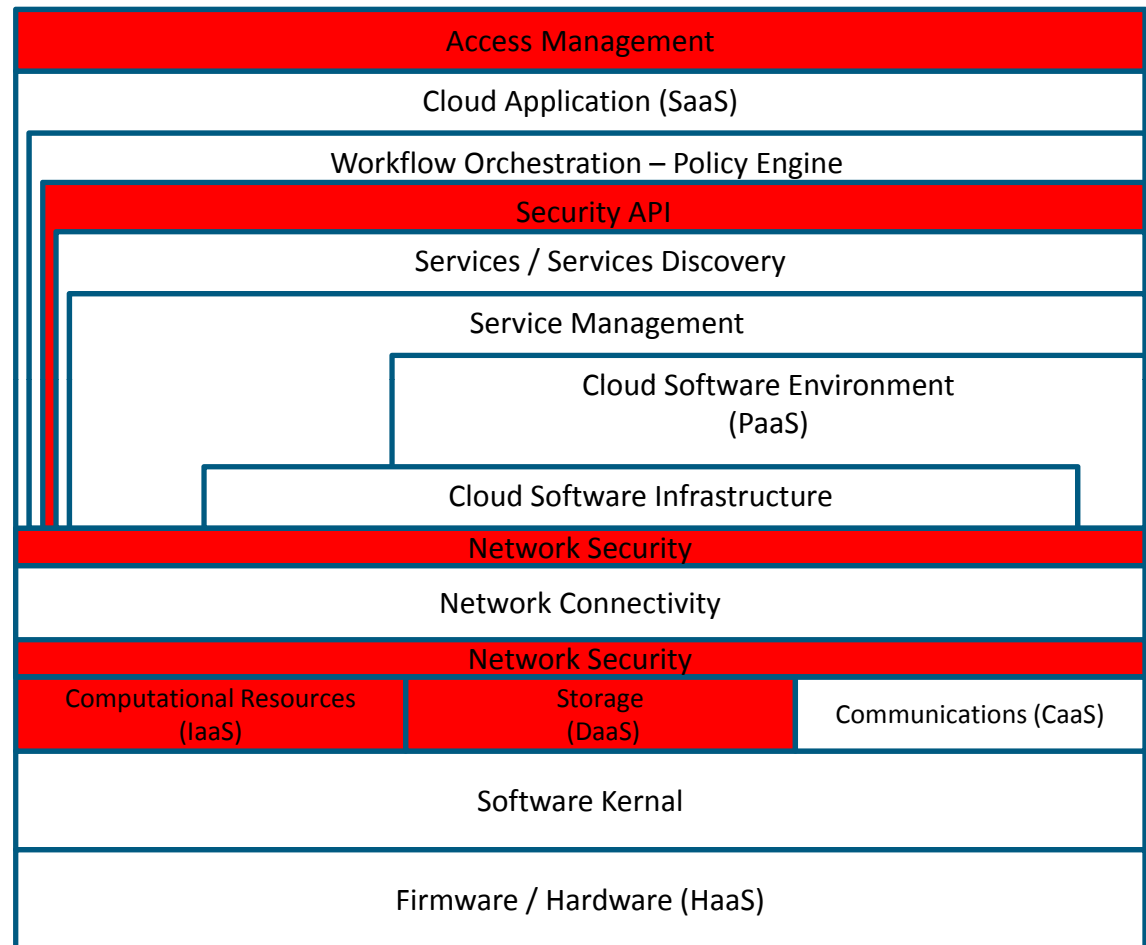


# Ontology Modification – Federated SOA

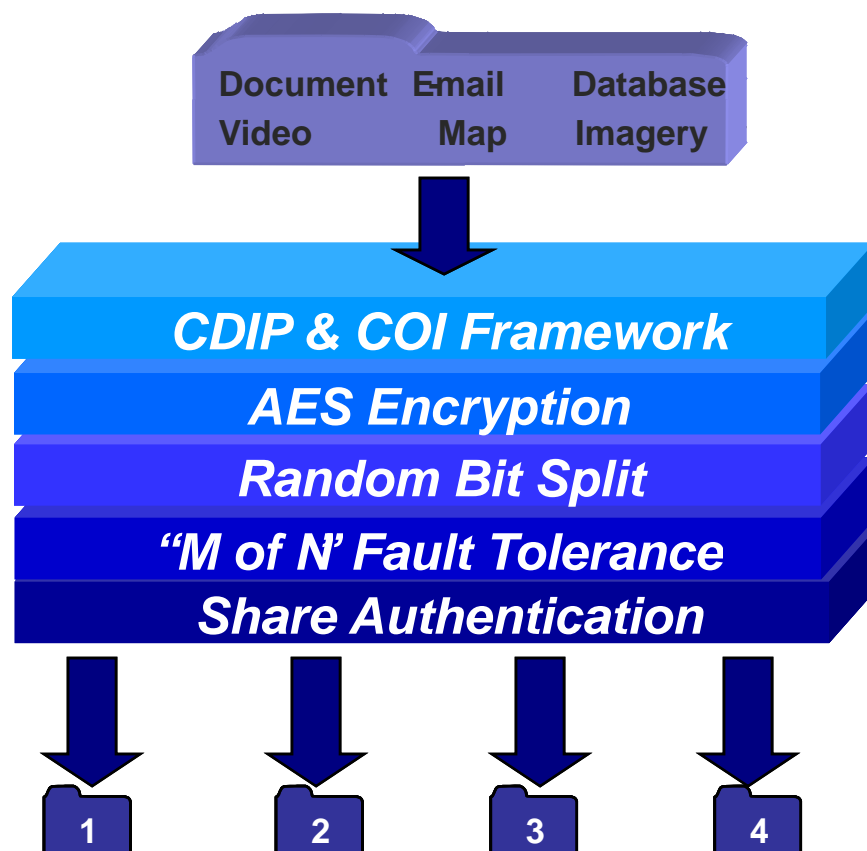


# Secure Cloud Computing – An Approach

- Access Management
  - “Out of Band” authentication
- Security API
  - Use of services
  - Binding of service
  - COI driven management
- Network Security
  - No VPN
  - “Data in Motion” security
- Computational Resources
  - VM management
  - Data-centric security model
- Storage
  - “Data at Rest” security
  - COI driven access



# SecureParser®



**Cryptographically splits data**  
**Creates physically separate fault tolerant Shares**

## High-efficiency cryptographic module:

- Provably-secure Computational Secret Sharing
- Cryptographic Data Splitting
- Data Integrity Protection
- Modules can be change out, e.g. AES could be changed with a TYPE I encryption as requirement called for

## Physically Separate Shares

- Written to Storage – Data at Rest
- Written to Networks – Data in Motion
- Created at any IO Point in the system

## User Definable

- Number of Shares
- Fault Tolerance
- Key Management

# Independent Testing and Evaluation

2005 CWID: AFCA assessment & AF C2 Battle Lab demo

**"...as demonstrating the potential to be labeled as an MLS/PL-4 System..."**

2005 DISA: Technical Information Panel (TIP)

**"...found to have merit for further evaluation and consideration for use as an information assurance technology...potential to fundamentally alter the way storing and securing of data is approached."**

2006 SOCOM: National Center for the Study of Counter-terrorism and Cybercrime

**IV&V completed successfully for SOCOM MLS Pilot Project**

2006 EUCOM Combined Endeavor: Joint Interoperability Test Center (JITC)

**"...value of the SecureParser was obvious. This capability not only offers increased security of data, but reduces costs by eliminating the need for redundant resources."**

2008 Selected by DISA as a demonstration solution for CWID'08 - June 08

Selected by NSA for HAP Trade Study as a Crypto Service and for DAR



## Network Centric Operations Industry Consortium

---

### ▶ Mission

- ▶ Our mission is to facilitate global realization of the benefit inherent in Network Centric Operations. To that end, we seek to enable continuously increasing levels of interoperability across the spectrum of joint, interagency, intergovernmental, and multinational industrial and commercial operations. We will execute this mission in good faith as a global organization with membership open to all enterprises in quest of applying the vast potential of network centric technology to the operational challenges faced by our nations and their citizens.

### ▶ Past successes

- Network Centric Analysis Tool (NCAT)
- NCOIC Interoperability Framework (NIF)

### ▶ Future

- Develop “operational art” in support of netcentric operations
- Support operational art advances through collaboration (Government, Industry, Non-profits, Interest Groups)
- Provide value to members
  - Use of NCOIC developed process provided differentiator in recent European procurement for a member company
  - NCOIC Patterns addressing interoperability concerns of member government agencies



# Cloud Computing Operational Art

---

- Embrace collaboration
  - OSD – tactical Cloud Computing
  - TIGR – Government Cloud Computing
  - Cloud Interoperability Forum
- Use Operational and Capability pattern process to develop Cloud Computing Technical Patterns
- Identify key netcentric operations interoperability requirements and preferences within identified technical patterns
- Iterate with NCOIC stakeholder companies and government organizations
- Use Capability and Operational patterns to validate operational impact of reduced cloud interoperability
- Leverage analysis to drive cloud interoperability recommendations and best practices

# Cloud Musings by Kevin L. Jackson

PERSONAL COMMENTS AND INSIGHT ON CLOUD COMPUTING RELATED TECHNOLOGIES THEIR USE IN THE PUBLIC SECTOR TO SUPPORT NET-CENTRIC OPERATIONS.

Showing posts for query **DHS**. [Show all posts](#)

TUESDAY, DECEMBER 16, 2008

## The Tactical Cloud

When cloud computing first came in vogue, there was a rather serious discussion about the private cloud concept. The whole idea of cloud computing seemed to argue against implementing such a capability behind a "private" firewall. The idea of a "private cloud" is being subject of this week's discussions at the Network Center of Excellence. It's a different cloud concept - the "tactical cloud".

Now before you shout foul, please hear me out.

First of all, the discussion was centered on possibly leverage cloud computing to create a "private" or "enterprise" cloud for the private internets (NIPRnet, SIPRnet).

 **DATALINE**

DAILY SUBSCRIBERS

289 readers  
BY FEEDBURNER

Visitors

[Performancing Metrics](#)

<http://kevinljackson.blogspot.com/>

# Thank You !



[Kevin.jackson@dataline.com](mailto:Kevin.jackson@dataline.com)







<http://cloudcomputing.dataline.com>

<http://govcloud.ulitzer.com>

## Cloud Computing for Government Efficiency and Transparency

# Government Cloud Computing

Subscribe to Government Cloud Computing:  Email Alerts  Weekly Newsletters

Get Government Cloud Computing:  Homepage  Mobile  RSS  Facebook  Twitter  LinkedIn

EDITOR

Kevin  
Jackson



FOUNDER:

Kevin Jackson

CONTRIBUTORS:

Kevin Jackson

Maureen O'Gara

Salvatore Genovese

Patrick Sweeney

Fuat Kircaali

Reuven Cohen

Nicole Schepker

James G. ...

## Top Stories

### 100 Players in the Cloud Computing Ecosystem



In periods of economic uncertainty IT managers turn to look at what other options might enable them to continue to meet end-user and business demands for IT services. What new cloud technologies and techniques are coming over the horizon? Which vendors are driving the most Enterprise-relevant

innovation? SYS-CON's Cloud Computing Journal here expands its list of most active players in the fast-emerging Cloud Ecosystem. Whether what you need is to achieve higher scale at lower costs than possible before, or to eliminate data center capital in favor of a "pay-as-you-go" model, C... [\(more\)](#)

### US CIO Reinstated After FBI Raid



America's first federal CIO, Obama appointee Vivek Kundra, was briefly put on leave right after the FBI raided his old offices and arrested two ex-Kundra staffers, charging one of them, Washington, DC's information system security officer no less, with bribery, money laundering, wire fraud and conflict of interest for

 **DATALINE**