

Networks & Telecom SIG
“Modernizing Government”

March Membership Meeting

Chair – Roxane Rucker, Qwest Government Services, Inc.

Vice Chair – Chris Chroniger, NetStar-1

Agenda



10:00 Welcoming/Introduction

10:05 Ed O'Hare, GSA FAS ITS Assistant Commissioner,
*"GSA Integrated Technology Services - What's
Ahead in 2010?"*

11:00 Business Meeting

12:00 Adjourn



American Council for Technology



Industry Advisory Council

Government and Industry IT: one vision, one community

Business Meeting

www.actgov.org

N&T Overview



- Focus for 2010 - Federal Infrastructure Modernization
 - Cloud Computing
 - National Broadband
 - Network Transition/MTIPS/Transformation
 - Wireless Sub-Committee
 - Wireless in Health IT
 - Land-Mobile Radio

N&T Overview



- Plan to foster working across industry and government in this community
 - Actively engaging other service providers in program planning
 - Added new GAP member, DOL CTO
 - Broadly define N&T SIG programs based on evolving role and definition of Network and Telecom services – “Not just pipes...”
 - Speaker’s Program targeting senior industry and government participation
 - Expanded usage of Web 2.0 tools

N&T Overview



- Target Community – Infrastructure Delivery & Operations
 - Civilian Agencies: CIO Office, Telecom/Enterprise Services
 - DOD/DISA: Network Services, Military Departments
 - Health IT: TriCare, Veterans Affairs, HHS
 - Regulatory Agencies: FCC
 - Emergency Responders: DHS, Interior, and State/Local
 - Program Office, Engineering and Technical Community in industry and government

Announcements



- *New!* N&T SIG Communications Officer – Harry Perper, CavTel
- *New!* Government Advisory Panel Member – Hamid Ouyachi, Department of Labor – Chief Technology Officer
- March 24 - IAC Community Fair
- April 9 – Washington Capitals Fun Night!
- April 19 – Erik Garr, Federal Communications Commission, National Broadband Strategy
- Mid June - ACT IAC Cloud Computing Day - A panel of five Government participants addressing their achievements, current challenges, and future opportunities relating to creating and successfully deploying a cloud or virtualization strategy.

N&T SIG Upcoming Activities



American Council for Technology



Industry Advisory Council

Government and Industry IT: one vision, one community

Project	Gov Sponsor	Objective	Deliverable	Time	Collab.
ITS 2010	Ed O'Hare, Asst. Comm. GSA FAS	Plans ahead for GSA Network Services, GWACs, and GSA Schedules	Speaker & Presentation	March 05	N/A
DOL Modernization	Hamid Ouyachi, DOL CTO	Agency modernization objectives & execution	Speaker & Presentation	April 05	N/A
Emergency Communications	Jeff King - Branch Chief, Office of Emergency Communications, DHS	Current trends in Emergency Communications including Land Mobile Radio – Speaker and Presentation	Panel Discussion	April 13	N/A
National Broadband Plan	Erik Garr, FCC, General Mgr - NBP	National Broadband Plan Rollout	Speaker & Presentation	April 19	N/A
GSA Network Services Conference	Karl Krumbholz, Director GSA FAS	Networx Transition / Transformation Update	Speaker & Presentation	June 21	N/A

Government and Industry IT: one vision, one community



American Council for Technology



Industry Advisory Council

Government and Industry IT: one vision, one community

Cloud Computing Initiative

www.actgov.org

Background



- ACT-IAC Cloud Computing Cross SIG working group was formed to leverage expertise of each SIG to support Industry and Governments Cloud Computing initiatives.

Use Case Approach



- There are numerous Cloud Computing Use Cases or other Cloud Computing documents available.
- Most if not all of this material is focused on the CXO level providing high-level concepts and strategic and financial benefits of using the Cloud.
- ACT-IAC's goal is to develop a Use Case that helps GSA further prepare the Federal Government for Cloud adoption by:
 - Developing a Use Case that focuses on the Federal Environment
 - Targets the Operational details of Cloud Computing within the Federal environment

Use Case Approach



- Messaging Services (Specifically Microsoft Exchange) was chosen as the first specific Use Case as it is a critical application to all Federal entities with MS achieving an estimated 80%+ usage rate.
- An Operational View was taken to prepare Federal Operations for Cloud implementation.
- GSA can leverage the Operational details within the Use Case to ensure that any/all RFP's issued for Cloud Services have a provision to address the operational requirements

Use Case Approach



- Critical Operational Areas include:
 - Service Level Agreements (SLA)
 - End to End Service Management (ITSM)
 - Security, FISMA Compliance
 - Enterprise Architecture (EA)
 - Linkage to External Components and Systems
 - Standards required to prevent vendor lock-in
 - Integration points required to provide service
 - Procurement Process
 - Policy
 - Operational Concerns

Use Case Approach



- Use Case provides Four Views of Messaging Services:
 - Current – typical view of messaging services being provided internally by a agency
 - IAAS – provides a view and impact if IAAS services is used to provide the messaging services
 - PAAS – provides a view and impact if PAAS services is used to provide the messaging services
 - SAAS – provides a view and impact if SAAS services is used to provide the messaging services

Use Case - Current



Operational View of Cloud Computing Services
 Cloud Computing Use Case - Microsoft Exchange E-mail
 Public Cloud Computing Service

Key:

Internal/Existing Federal Network
Cloud Provider
New Interface

Cloud Computing Service Description Category	Service Provider	Service Level Agreements (SLA)	IT Service Management (ITSM)	Security	Enterprise Architecture (EA)	Linkage to External Components and Systems	Procurement Process	Policy	Operational Concerns
Software as a Service (SaaS)	Delivers a business service to consumers, owns configuration of system based on requirements and end to end delivery of system and all SLA defined	Possibilities: System Uptime, Account Mgmt (adds, changes, deletions), Application availability, Disaster Recovery, Capacity Mgmt, Reporting and Metrics, Licensing	Users call agency help desk. Help Desk escalates to internal ops team	Full FISMA Compliance with ATO as part of the overall General Support System (GSS)		Active Directory integration is required to provide standardized single sign-on and user administration	Users are added/deleted as needed based on an enterprise level agreement. True-Up process is utilized annually to establish the license costs based on # of users, # of servers, etc. Operational approval for users and associated costs are performed as part of the new user request process. Alternately, peruse licensing is available from provider with no minimum term for use of shared services	Internal policy has to synch with Service Provider controls. Service provider compliance must be evaluated regularly. The sensitivity of data processed by the service must be aligned to the level of trust and policy compliance to client standards.	Capacity Planning, Operational risk, some security risk all assumed by service provider. Some security risk is shared. Processes and Controls for Capacity Planning, Operational risk, some security risk all implemented by service provider. Consumer is ultimately responsible for impact to the business/mission.
Platform as a Service (PaaS)	Service Owner - owns the installation, setup, maintenance, patching, etc. of the Application Provides a platform service that supports development of a business service. Owns the installation, setup, maintenance, patching, etc. of the software and SLA's and configuration management of the API to deliver functionality promised	Uptime Restore OS and App Restore specific inbox, calendar Proactive Capacity Mgmt - Storage, Memory	Systems and Network teams own Tier-2/3 problem identification and resolution. Maintenance/Licensing agreements provide access to support through Microsoft to include system patches, configuration reviews and audits, etc.	Application Patch Management Operational Security Procedures, SOPs Security Monitoring of Application activity		Active Directory integration is required to allow standard system management and administration to include the use fo standardized system images, patch and anti-virus management. Catalog integration to request and change services DNS integration for mail routing	Support costs to include (HW, SW, Personnel, etc.) are procured and established annually based on historical trends and future estimates. Daily operational personnel work to manage the environment based on new requests, but do not have hard costs approval or measurements included in the daily process.	Internal policy has to synch with Service Provider controls. Service provider compliance must be evaluated regularly. The sensitivity of data processed by the service must be aligned to the level of trust and policy compliance to client standards.	Capacity Planning, Operational risk, some security risk assumed by service provider. Processes and Controls for Capacity Planning, Operational risk, some security risk all implemented by service provider. Consumer is ultimately responsible for impact to the business/mission.
Infrastructure as a Service (IaaS)	Service Provider - owns the installation, setup, maintenance, patching of the Operating System and the physical servers, data center, storage, etc. Provides a platform component from which systems can be built. Owns the installation, setup, maintenance, patching of the Operating System and the physical servers, data center, storage, deployed applications, and possibly etc. limited control of select networking components (e.g., host firewalls).	Uptime Restore OS Restore DB Proactive Capacity Mgmt - CPU, Network	Systems and Network teams own Tier-2/3 problem identification and resolution. Hardware Maintenance is procured from the appropriate vendor based on server models (i.e. Dell, HP, etc.)	Server OS Patch Management Operational Procedures, Security SOPs, Security Monitoring of System, Network, NIST/DISA checklists		Storage is provided through a SAN with the appropriate performance and storage scalability characteristics VM Management integration Catalog integration to request and change services	Users are added/deleted as needed based on capacity of the physical infrastructure. Physical Infrastructure capacity is estimated based on historical trends, future estimates and is procured as appropriate once or twice a year utilizing a well defined Federal procurement process.	Internal policy has to synch with Service Provider controls. Service provider compliance must be evaluated regularly. The sensitivity of data processed by the service must be aligned to the level of trust and policy compliance to client standards.	Capacity Planning, some Operational risk assumed by service provider. Processes and Controls for Capacity Planning, Operational risk, some security risk all implemented by service provider. Consumer is ultimately responsible for impact to the business/mission.

Use Case - IaaS

Cloud Computing Service Description Category	Service Provider	Service Level Agreements (SLA)	IT Service Management (ITSM)	Security	Enterprise Architecture (EA)	Linkage to External Components and Systems	Procurement Process	Policy	Operational Concerns
Software as a Service (SaaS)	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.	Delivers a business service to consumers, owns configuration of system based on requirements and end to end delivery of system and all SLA defined	Possibilities: System Uptime, Account Mgmt (adds, changes, deletions), Application availability, Disaster Recovery, Capacity Mgmt, Reporting and Metrics, Licensing	Users call agency help desk. Help Desk escalates to internal ops team	Full FISMA Compliance with ATO as part of the overall General Support System (GSS)	Active Directory integration is required to provide standardized single sign-on and user administration	Users are added/deleted as needed based on an enterprise level agreement. True-Up process is utilized annually to establish the license costs based on # of users, # of servers, etc. Operational approval for users and associated costs are performed as part of the new user request process. Alternately, peruse licensing is available from provider with no minimum term for use of shared services	Internal policy has to synch with Service Provider controls compliance must be evaluated regularly. The sensitivity of data processed by the service must be aligned to the level of trust and policy compliance to client standards.	Capacity Planning, Operational risk, some security risk all assumed by service provider. Some security risk is shared. Processes and Controls for Capacity Planning, Operational risk, some security risk all implemented by service provider. Consumer is ultimately responsible for impact to the business/mission.
Platform as a Service (PaaS)	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.	Service Owner - owns the installation, setup, maintenance, patching, etc. of the Application Provides a platform service that supports development of a business service. Owns the installation, setup, maintenance, patching, etc. of the software and SLA's and configuration management of the API to deliver functionality promised	Uptime Restore OS and App inbox, calendar Proactive Capacity Mgmt - Storage, Memory	Systems and Network teams own Tier-2/3 problem identification and resolution. Maintenance/Licensing agreements provide access to support through Microsoft to include system patches, configuration reviews and audits, etc.	Application Patch Management Operational Security Procedures, SOPs Security Monitoring of Application activity	Active Directory integration is required to allow standard system management and administration to include the use fo standardized system images, patch and anti-virus management. Catalog integration to request and change services DNS integration for mail routing	Support costs to include (HW, SW, Personnel, etc.) are procured and established annually based on historical trends and future estimates. Daily operational personnel work to manage the environment based on new requests, but do not have hard costs approval or measurements included in the daily process.	Internal policy has to synch with Service Provider controls Service provider compliance must be evaluated regularly. The sensitivity of data processed by the service must be aligned to the level of trust and policy compliance to client standards.	Capacity Planning, Operational risk assumed by service provider. Processes and Controls for Capacity Planning, Operational risk, some security risk all implemented by service provider. Consumer is ultimately responsible for impact to the business/mission.
New Service Management Interface		Tools will be required to monitor and report on SLAs	E-Bonding Systems, SOPs and other Service Management mechanisms must be updated to integrate and provide end to end service management	Audit and validation methodologies must be detailed in MOU/ISA documentation		Need defined rules as to who is authorized to acquire new services or expand capacity. Requires operational changes and integration with financial management processes			
Infrastructure as a Service (IaaS)	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).	Service Provider - owns the installation, setup, maintenance, patching of the Operating System and the physical servers, data center, storage, etc. Provides a platform component from which systems can be built. Owns the installation, setup, maintenance, patching of the Operating System and the physical servers, data center, storage,	Uptime Restore OS Restore DB Proactive Capacity Mgmt - CPU, Network	Systems and Network teams own Tier-2/3 problem identification and resolution. Hardware Maintenance is procured from the appropriate vendor based on server models (i.e. Dell, HP, etc.)	Server OS Patch Management Operational Procedures, SOPs, Security Monitoring of System, Network, NIST/DISA checklists	Storage is provided through a SAN with the appropriate performance and storage scalability characteristics VM Management integration Catalog integration to request and change services	Users are added/deleted as needed based on capacity of the physical infrastructure. Physical Infrastructure capacity is estimated based on historical trends, future estimates and is procured as appropriate once or twice a year utilizing a well defined Federal procurement process.	Internal policy has to synch with Service Provider controls Service provider compliance must be evaluated regularly. The sensitivity of data processed by the service must be aligned to the level of trust and policy compliance to client standards.	Capacity Planning, some Operational risk assumed by service provider. Processes and Controls for Capacity Planning, Operational risk, some security risk all implemented by service provider. Consumer is ultimately responsible for impact to the business/mission.

Use Case Next Steps



- Once Model is reviewed and approved, the Cloud Computing Cross SIG group can quickly adapt the Use Case for other specific services or views to include:
 - Specific Services example:
 - Development Environments
 - Major Applications (Financial Systems, HR Systems, etc.)
 - Data Center Services
 - Specific Views examples:
 - CIO View
 - CFO View
 - Procurement View