



State Information Technology Advisory Committee (SITAC)

**March 12, 2015
Pioneer Room
State Capitol Building**



AGENDA		
Time	Topic	Presenter
3:30	Welcome / Opening Comments	Mike Ressler
3:35	Enterprise Architecture Update	Jeff Quast
3:45	Cyber Insurance	Tag Anderson
3:55	Mobile Applications Demo	Eli Cornell
4:20	Vendor Application Hosting ITD Services / Fees	Dan Sipes
4:40	Large Project Reporting Veteran's Home – Electronic Medical System Adjutant General – State Records Mgmt System	Justin Data Justin Data Mike Lynk
4:55	Open Discussion / Closing Comments	Mike Ressler



Welcome / Opening Comments



**Jeff Quast,
Program
Administrator**

**Enterprise
Architecture**





Enterprise Architecture Update

- EA has now transitioned to “EA 2.0”
 - Creation of the Information Technology Coordinators Council ([ITCC](#))
 - Creation of four Architecture Teams
 - Application
 - Data
 - Security
 - Technology
 - Eliminated previous Architecture Review Board (ARB), Architecture Team (AT), and nine Domain Teams



Enterprise Architecture Update

- ITCC membership is a subset of IT Coordinators from all state agencies
 - Initially almost the same membership as the ARB
 - Will continue to participate in EA process as before
 - Now includes ownership of several “business” standards and policies
 - Adds the ability to address non-EA topics and initiatives
 - Provides a collective voice for IT Coordinators that didn't exist previously
 - Meets the second Wednesday of each month at ITD



Enterprise Architecture Update

- Architecture Teams
 - Responsibilities from previous Domain Teams have been distributed to the appropriate Architecture
 - No designated membership, anyone can participate
 - Meets monthly at ITD and as needed
 - Data Architecture will be an area that has not been addressed actively in the past
- Next steps:
 - Establish scope of each Architecture
 - Review existing standards
 - Develop a Future State, Current State, and Gap Analysis



Enterprise Architecture Update

- Process Model changes
 - All teams (including the ITCC) will participate at the same level, vs. the hierarchical model used previously
 - Participants will not “vote” at a team level; each participant will optionally complete a short survey for every decision point
 - The benefits include the ability to gather feedback beyond yea or nay
 - The results of the survey will be a recommendation to the CIO for a final decision



Questions?

Thanks!



Tag Anderson, Director of Risk Management

Cyber Insurance





**Elijah Cornell,
ITD Enterprise
Architect**

**Mobile
Landscape and
Opportunities**





Dan Sipes Deputy CIO





ITD's Role in Brokering Cloud Services

- ITD will serve in a “Cloud Broker” role as agencies evaluate cloud services to meet business needs.
- Aligned with ITD's hosting responsibilities in NDCC 54-59-22.
 - Software as a Service (SaaS) solutions hosted in the cloud require a waiver from OMB and ITD.
 - ITD will partner with agencies to broker the on-going contract/relationship with the agency and the vendor that results from an approved waiver.



Brokering - an ITD/Agency partnership

- SaaS - Cloud Service Risk Assessment Process
- SaaS - Cloud Contracts
- Cloud Service Inventory/Integration Points
- Funding the Cloud Broker role



Broker Value - Risk Assessment Process

- ITD is developing a rubric to help assess the risk associated a cloud based solution (SaaS)
- Assessment Areas
 - IT Architecture/Vendor Capability
 - Identity
 - Active Directory integration for state agency users
 - Security
 - Data
 - Strategic Impact
 - Cost



Cloud Risk Assessment



Risk Control Area		Agency Assessment	ITD Assessment	Enterprise Tolerance
Architecture	Networking	Very low	Low	Low
	Storage	Very low	Low	Moderate
	Software	Very low	Very low	Low
	Integration	Low	Low	Moderate
	Capacity Management	Very low	Very low	Moderate
	High Availability	Low	Very low	Moderate
	IT Agility	Very low	Very low	Very low
	Portability	Very low	Very low	Very low
	Service Termination	Very low	Very low	Low
	Security	Data Center Operations	Low	Low
Identity		Low	Moderate	Low
Audit and Compliance		Very low	Very low	Low
Logging and Tracing		Very low	Low	Very low
Malicious Activities from Within		Low	Low	Low
Data	Data Classification	Low	Low	Moderate
	Data Migration	Low	Low	Low
	Data backup	Very low	Very low	Moderate
	Data Sanitization	Very low	Low	Moderate
	Records Management	Very low	Low	Low
	Electronic Discovery	Very low	Low	Moderate
Strategy	Mission Criticality	Low	Low	Low
	User Expectations	Low	Low	Low
	Customer-facing Implications	Low	Low	Low
	Availability	Low	Low	Low
	Provider Selection	Low	High	Low
	Organizational Readiness	Low	Low	Very low
	Incident Management	Low	Low	Very low
	Ongoing Maintenance	Low	Low	Very low
	IT Skillsets	Low	Low	Very low
	Disaster Recovery	High	Low	Very low
	Finance	Very low	Low	Very low
	3rd-Party Involvement	Very low	Low	Low

Risk Control Areas

- Architecture
- Security
- Data
- Strategy

Perspectives

- Agency Assessment
- ITD Assessment
- Enterprise Tolerance



Cloud Risk Assessment



Risk Control Area		Agency Assessment	ITD Assessment	Enterprise Tolerance
Architecture	Networking	Very low	Low	Low
	Storage	Very low	Low	Moderate
	Software	Very low	Very low	Low
	Integration	Low	Low	Moderate
	Capacity Management	Very low	Very low	Moderate
	High Availability	Low	Very low	Moderate
	IT Agility	Very low	Very low	Very low
	Portability	Very low	Very low	Very low
	Service Termination	Very low	Very low	Low
Security	Data Center Operations	Low	Low	Low
	Identity	Low	Moderate	Low
	Audit and Compliance	Very low	Very low	Low
	Logging and Tracing	Very low	Low	Very low
	Malicious Activities from Within	Low	Low	Low
Data	Data Classification	Low	Low	Moderate
	Data Migration	Low	Low	Low
	Data backup	Very low	Very low	Moderate
	Data Sanitization	Very low	Low	Moderate
	Records Management	Very low	Low	Low
	Electronic Discovery	Very low	Low	Moderate
Strategy	Mission Criticality	Low	Low	Low
	User Expectations	Low	Low	Low
	Customer-facing Implications	Low	Low	Low
	Availability	Low	Low	Low
	Provider Selection	Low	High	Low
	Organizational Readiness	Low	Low	Very low
	Incident Management	Low	Low	Very low
	Ongoing Maintenance	Low	Low	Very low
	IT Skillsets	Low	Low	Very low
	Disaster Recovery	High	Low	Very low
	Finance	Very low	Low	Very low
	3rd-Party Involvement	Very low	Low	Low

Risk Likelihood

- Slight
- Not likely
- Likely
- Highly likely
- Expected

Risk Impact

- Low
- Mild
- Serious
- Severe
- Catastrophic



Cloud Risk Assessment



Architecture	Networking	Insufficient controls and/or incompatible architecture to securely provide network connectivity/capacity
	Storage	Insufficient controls and/or incompatible architecture to securely store data
	Software	Insufficient controls and/or incompatible architecture to securely integrate with other business applications
	Integration	Insufficient controls and/or incompatible architecture to securely integrate with other business applications
	Capacity Management	Unable to proactively load-test, monitor (by State), and/or scale application performance
	High Availability	Insufficient architecture to provide geographically distributed high-availability
	IT Agility	Latency or overall difficulty in implementing/adjusting system architecture to address technical and/or business requirements
	Portability	Technical and/or non-technical dependencies create vendor lock-in and/or limit future options for migrating service elsewhere
	Service Termination	Insufficient control/confidence with regard to either party terminating service and the State's ability to transfer functionality elsewhere



Cloud Risk Assessment



Strategy	Mission Criticality	Unable to provide critical government services if the provider experiences a loss of service
	User Expectations	Inability to fulfill user expectations, especially with regard to performance and/or ease-of-use
	Customer-facing Implications	Unable to maintain a positive stakeholder perception and/or State reputation
	Availability	Insufficient uptime guarantees and/or reliability
	Provider Selection	Insufficient confidence with regard to the provider's completeness of vision and ability to execute; in the past, present, and future
	Organizational Readiness	Insufficient preparation with regard to strategic alignment, workforce readiness, cultural impact, and/or stakeholder buy-in
	Incident Management	Insufficient controls in place detect, report, and resolve disruptions in service
	Ongoing Maintenance	Insufficient control over the process, frequency, scheduling, and functionality of maintenance/enhancements
	IT Skillsets	Insufficient IT resources/training to properly implement/manage the application and/or an unclear shift in IT roles/responsibilities
	Disaster Recovery	Insufficient control/capability/confidence with regard to handling natural disasters and maintaining business continuity
	Finance	Insufficient preparation within accounting/budgeting procedures to shift from capital to operational expenditures
3rd-Party Involvement	Insufficient control and/or over-dependency upon 3rd party hosting providers	



Cloud Risk Assessment



Security	Data Center Operations	Insufficient controls/testing of data center redundancy/security
	Identity	Insufficient controls and/or incompatible architecture to provide proper identity and access management
	Audit and Compliance	Insufficient controls in place to properly measure and meet regulatory requirements/certifications
	Logging and Tracing	Insufficient controls and/or access to properly manage operational logs for troubleshooting and regulatory compliance
	Malicious Activities from Within	Insufficient control/confidence with regard to privileged users performing unauthorized/unlawful activities such as data theft, tampering, leakage, etc.
Data	Data Classification	Unclear classification of data and/or insufficient control/confidence with regard to safeguarding sensitive/confidential data
	Data Migration	Difficulty in moving legacy data into a new environment
	Data backup	Insufficient backup/recovery procedures, lack of geographical separation of media, and/or misplacement or theft of backup information
	Data Sanitization	Insufficient control/confidence with regard to properly identifying and physically destroying sensitive media
	Records Management	Insufficient control/confidence with regard to data being stored, retained, and purged to a compliant level
	Electronic Discovery	Insufficient access to data upon request and/or insufficient control with regard to subpoenas, jurisdiction, and confiscation of data



Cloud Risk Assessment



Architecture	Networking	Insufficient controls and/or incompatible architecture to securely provide network connectivity/capacity
	Storage	Insufficient controls and/or incompatible architecture to securely store data
	Software	Insufficient controls and/or incompatible architecture to securely integrate with other business applications
	Integration	Insufficient controls and/or incompatible architecture to securely integrate with other business applications
	Capacity Management	Unable to proactively load-test, monitor (by State), and/or scale application performance
	High Availability	Insufficient architecture to provide geographically distributed high-availability
	IT Agility	Latency or overall difficulty in implementing/adjusting system architecture to address technical and/or business requirements
	Portability	Technical and/or non-technical dependencies create vendor lock-in and/or limit future options for migrating service elsewhere
	Service Termination	Insufficient control/confidence with regard to either party terminating service and the State's ability to transfer functionality elsewhere



Broker Value - Contracts/Vendor Mgmt

- Contract negotiations and key terms and conditions
 - Cost drivers
 - Escalation caps
 - Hosting location
- On-going Vendor Relationship
 - Periodic architecture reviews
 - Certification reviews
 - Prior approval of material changes to the cloud architecture environment



Broker Value - Inventory & Integration

- Statewide Inventory of Cloud Based Solutions
 - Helps to manage risk
 - Helps to ensure consistent contract terms
- Documentation of Integration Points
 - Identify key integration points to the state infrastructure (e.g. Active Directory)
 - Promote common standards based integration where possible



Broker Value - Approving and Funding

- On-premise solutions vs. cloud based solutions
 - Near-term, on-premise solutions will be preferred to maintain economies of scale in the data center.
- Funding
 - Agencies with approved waivers will fund the broker role and the associated infrastructure investments
 - Monthly add-on fee to vendor fees
 - Applied to new waivers starting this biennium
 - Legacy waivers - no later than 7/1/2017



Justin Data, ITD Project Management

Large Project Reporting





Large Project Reporting

- Currently there are 18 projects being monitored via oversight - 11 are executing, 7 are planning
- **NDCC 54-59-23. ...**
 2. During the life of the project, the agency shall notify the state information technology advisory committee if:
 - a. At a project milestone, the amount expended on project costs exceeds the planned budget for that milestone by twenty percent or more; or
 - b. At a project milestone, the project schedule extends beyond the planned schedule to attain that milestone by twenty percent or more.
 3. A report under subsection 2 must specify corrective measures being undertaken to address any cost or time of completion issue. If the agency has not taken adequate corrective measures within ninety days after the report, the agency shall submit a report to the legislative management's information technology committee regarding the project.



North Dakota Veterans Home

Software Contract with HealthMEDX

Variance Report



Causal Factors

- 1) The schedule variance has been caused by vendor's inability to integrate state auditors requirements into the software package.



Lessons Learned

- 1) When evaluating software companies, a higher value should have been placed on companies that had software systems already working in ND.
- 2) This is the first computer system that we have ever done, therefore, benchmark time frames were not controlled like they could have been.



Recovery Strategy

- 1) Withhold the remaining contract dollars until reliable report can be produced which will meet auditors standards.
- 2) Work with ITD, Attorney General Office, Project Manager and HealthMEDX to bring contract to a positive resolution.
- 3) Hiring an individual, who knows the software program to develop reports that meet facility expectations is not possible without great expense as HealthMEDX will not allow access until extensive training is completed.



**Mike Lynk,
Director of State Radio

Division of State Radio
and
Criminal Justice
Information Sharing (CJIS)**

CAD2/Statewide Records
Management System

Variance Report





Causal Factors

- Product went into production on-schedule, providing service to the state per the original baseline dates
- Although the post-production bug fix timeline was aggressive, the project team felt it was attainable
- During this timeline unforeseen fixes arose that took additional time to correct
- Because the “execution” phase of the project was only a few months long, extending the deadline caused variance to increase quickly
- Prior to the unexpected fixes being required, variance was on target to finish at 10.5% under budget and 9% behind schedule (both “green” indicators)



Lessons Learned

- Allow for a reasonable amount of time for post-production fixes in any contract to account for “unexpected” fixes
- Consider similar past project experiences to encompass more scheduling lessons learned
- If a project team realizes post-production fixes will take so long, consider pursuing a formal re-plan



Recovery Strategy

- The team has analyzed current progress, and has estimated a completion date in late March for the one remaining “core” update
- The final payment of \$125,351 (15% of the total contract cost) is being held until the core update is accepted by the state
- As the team is confident of this date being hit, no further recovery strategy is required



Open Discussion / Closing Comments



THANK YOU!!!