SMART LEAN GOVERNMENT
NASCIO

Direction, State Experiences and Federated Identity Management

April 29, 2014

Eric Sweden, Program Director, Enterprise Architecture & Governance
Overview

• Enterprise . . . . Federation . . . . Ecosystem
• Cross-Jurisdictional Joining Up
• Enablers – Identity Management – Smart Lean
• Rationalize – Optimize – Simplify
A. Priority Strategies, Management Processes and Solutions

1. Security
2. Consolidation / Optimization
3. Cloud Services
4. Project and Portfolio Management
5. Strategic IT Planning
6. Budget and Cost Control
7. Mobile Services / Mobility
8. Shared Services
9. Interoperable Nationwide Public Safety Broadband Network (FirstNet)
10. Health Care

Source: NASCIO State CIO Survey, November 2013
A. Priority Strategies, Management Processes and Solutions

Security:

- risk assessment, governance, budget and resource requirements, security frameworks, data protection, training and awareness, insider threats, third party security practices as outsourcing increases, determining what constitutes “due care” or “reasonable”
Project and Portfolio Management:

project management discipline, enterprise portfolio management (EPM), oversight, portfolio review, IT Investment Management (ITIM), training/certification of staff, traceability to mission and strategy, scope management, execution
A. Priority Strategies, Management Processes and Solutions

Project and Portfolio Management:

project management discipline, enterprise portfolio management (EPM), oversight, portfolio review, IT Investment Management (ITIM), training/certification of staff, traceability to mission and strategy, scope management, execution.
B. Priority Technologies, Applications and Tools

Top 10 Final Ranking

1. Cloud computing: software as a service
2. Security enhancement tools: continuous diagnostic monitoring (CDM), digital forensics
3. Mobile Workforce: technologies and solutions
4. Enterprise Resource Planning (ERP)
5. Virtualization: servers, desktop, storage, applications, data center
6. Legacy application modernization / renovation
7. Business Intelligence (BI) and Business Analytics (BA): applications, big data
8. Disaster Recovery / Business Continuity
9. Identity and access management
10. Networking: voice and data communications, unified
IT Project and Portfolio Management

• Widely implemented but generally not effective
• Need enterprise-wide governance
• Good at monitoring ongoing projects
• Ineffective in driving IT investment
IT Project and Portfolio Management

Figure 1
How effective are your state’s practices for oversight of large IT projects?

- 0%: No formal project oversight practices
- 4%: Not at all effective
- 52%: Somewhat effective
- 31%: Effective
- 13%: Very effective

Figure 2
Do you use a formal IT enterprise portfolio management process to support decisions regarding planned initiatives, projects, or ongoing IT services such as application support?

- 63%: Yes
- 28%: No
- 2%: Do not know
- 7%: Does not apply
- 0%: Other
IT Project and Portfolio Management

Figure 3
How effectively do your IT portfolio management practices help drive IT investment decisions? Please rate this effectiveness on the scale below.

<table>
<thead>
<tr>
<th>Rating</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not use portfolio management</td>
<td>23%</td>
</tr>
<tr>
<td>Use portfolio management</td>
<td>77%</td>
</tr>
<tr>
<td>Not at all effective</td>
<td>7%</td>
</tr>
<tr>
<td>Somewhat ineffective</td>
<td>56%</td>
</tr>
<tr>
<td>Effective</td>
<td>32%</td>
</tr>
<tr>
<td>Very effective</td>
<td>5%</td>
</tr>
</tbody>
</table>
IT Project and Portfolio Management

37% of State CIOs - Portfolio Management Practices are Effective

Keys to Effective IT Investment Management

- Statewide Standards for Business Cases
- Stronger Executive-Level Engagement
- Strong Enterprise-wide Oversight Role by CIO
Introduction - A Balancing Act for the State CIO

The state CIO is required to manage a vast array of relationships, needs, demands and solutions. From both the demand and supply sides, the state CIO is the primary promoter, communicator and facilitator for enterprise wide perspectives. In that role, the CIO is required to continually balance business needs coming in from across government—presented by government customer partners, and the many possible solutions and services coming in from the solution providers—presented by internal organizations, industry partners and cross-jurisdictional arrangements. A frustration shared by many state CIOs is the lack of a shared vision about the enterprise and the difficulties in managing a diverse issues and investment portfolio.

Matching up those needs with the right solutions requires the business acumen and technical expertise to address problems and surface opportunities that lead to delivering effective government services. In that process, the CIO enlists staff, industry partners, various management disciplines and technologies to:

- evaluate options
- reduce risk
- maintain, apply, and sometimes reevaluate enterprise standards
- reduce complexity and redundancy
- manage customer relationships
- manage vendor relationships
- manage legislative relationships

NASCIO Staff Contact:
Eric Sweden, MSMS MBA
Program Director,
Enterprise Architecture & Governance
NASCIO

NASCIO represents state chief information officers and information technology executives and managers from state governments across the United States. For more information visit www.nascio.org.

201 East Main Street, Suite 1405
Lexington, KY 40507
Phone: (859) 514-9213
Fax: (859) 514-9266
NASCIO@AMReR.com
www.NASCIO.org

Copyright © 2013 NASCIO
All rights reserved
State CIO Challenge – Balancing Needs and Resources

State CIO Portfolio

Business Needs
- Economic Development
- Jobs
- Education
- Public Safety
- Citizens' Demands
- Health
- eDemocracy

Statutory Requirements

Citizen Outcomes

Existing and Potential Resources and Capabilities
- Centralized IT
- Cross Agency
- Cross Jurisdictional
- Industry Partner
- Cloud Services
  - internal
  - external
  - ...

Enterprise Architecture - the path to Government Transformation
Many “Portfolios”
Enterprise Architecture Value Chain

Observe the Contextual Environment
- Fiscal Circumstances
- Macroeconomics
- Customer Expectations
- Customer Behavior
- Regulations
- New Technology
- Competition
- Mandate

Observe the Need or Opportunity (Market)
- SWOT Analysis
- Risks Analysis
- Assumptions
- Policies
- Stakeholders
- Supply / Demand
- Economics
- Access

Determine Strategic Business Intent
- Decisions
  - Mission
  - Vision
  - Goals
  - Objectives
  - Strategies
  - Performance

Enable Strategic Business Intent
- Business Relationships
- Processes
- Information
- Organizations
- Value Chains
- Management
- Initiatives
- Analytics / Six Sigma
- Balanced Scorecard
- Geospatial Capabilities
- Records Management
- Security

Capabilities
Issues Portfolio
Issues Portfolio

Observe the Contextual Environment

Fiscal Circumstances
Macroeconomics
Customer Expectations
Customer Behavior
Regulations
New Technology
Competition
Mandate

current issues
Emerging issues
Anticipated issues
Expanding issues

Surfaces Business Needs

Environmental
Natural Resources
Public Health
Economics
Public Safety
Defense
Education

Enterprise Architecture - the path to Government Transformation
Public Safety Portfolio

Protecting & Supporting Victims of Crime

Human Trafficking

Recidivism

Securing Borders

Crime Prevention

Pandemic / Emergency Preparedness

Substance Abuse

Substance abuse – what is happening here?
Inter-related Public Sector Spheres

- Economics
- Public Health
- Public Safety
- Education
NASCIO Rendering of the Issue Management Council’s Original Issue Management Process Model

Issue Identification

Issues Analysis

Issue change strategy

Issue action program

Evaluation of results

http://issuemanagement.org/learnmore/origins-of-issue-management/
IT Procurement

• Widespread adoption of reforms is slow
• Two Major Focus Areas for this survey
  • contract terms & conditions
  • the procurement process
IT Procurement Challenges

• Lengthy process
• Risk averse nature inhibits innovation
• Identify and mitigate all perceived risks
• Equitable sharing of risk
IT Procurement Recommendations

• Recommendations
  • Establish a reasonable cap on vendor financial exposure
  • Adopt “license” rather than “acquisition”
  • Limit indemnification obligations to tangible losses
    • injury
    • death
    • damage
IT Procurement

Figure 4
To what extent do you believe that the contract terms and conditions used by your state to procure IT goods and services are effective in sharing risk between the state and vendors?

- Very ineffective: 4%
- Somewhat effective: 48%
- Effective: 33%
- Very effective: 9%
- Don't know/does not apply: 6%

How would you rate the effectiveness of your IT procurement process?

- Very ineffective: 11%
- Somewhat ineffective: 49%
- Effective: 32%
- Very effective: 8%
# IT Procurement

**Figure 6**

What three (3) reforms in the procurement process would do the most to improve your state’s ability to procure IT goods and services?

<table>
<thead>
<tr>
<th>Reform</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide training to state staff involved with IT procurement so that they are better equipped to develop RFPs that balance risks between vendors and states.</td>
<td>72%</td>
</tr>
<tr>
<td>Implement rules for using competitive negotiations, which in turn serve to facilitate “give-and-take” between buyer and sellers so that obstacles, where presented by terms and conditions, can be addressed and resolved without derailing the procurement.</td>
<td>58%</td>
</tr>
<tr>
<td>Develop standard forms for procuring cloud and/or Software as a Service offerings.</td>
<td>54%</td>
</tr>
<tr>
<td>Institute a process to periodically review and scrub the current IT terms and conditions used by the state to see if they align with terms and conditions used by other states. Likewise, if no “model” set of terms and conditions exist, set about to establish a set of “standard” or recommended terms.</td>
<td>48%</td>
</tr>
<tr>
<td>For state contracts involving IT services and/or system implementation, include a dispute resolution process in the signed contract that involves successive escalation steps so that opportunities are available for resolution rather than litigation.</td>
<td>38%</td>
</tr>
<tr>
<td>Other</td>
<td>12%</td>
</tr>
</tbody>
</table>
Cybersecurity

• Most states have adopted continuous vulnerability testing

• Challenges
  • documenting program effectiveness
  • developing cybersecurity disruption response plans
Cybersecurity Threats

- Require formal strategy
- Adequate resources
- Constant vigilance
## Cybersecurity Threats

**Figure 9**

Please characterize the current status of the cybersecurity program and environment in state government.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adopted a cybersecurity framework based on national standards and guidelines</td>
<td>78%</td>
</tr>
<tr>
<td>Acquired and implemented continuous vulnerability monitoring capabilities</td>
<td>78%</td>
</tr>
<tr>
<td>Developed security awareness training for workers and contractors</td>
<td>78%</td>
</tr>
<tr>
<td>Established trusted partnerships for information sharing and response</td>
<td>75%</td>
</tr>
<tr>
<td>Created a culture of information security in your state government</td>
<td>73%</td>
</tr>
<tr>
<td>Adopted a cybersecurity strategic plan</td>
<td>61%</td>
</tr>
<tr>
<td>Documented the effectiveness of your cybersecurity program with metrics and testing</td>
<td>47%</td>
</tr>
<tr>
<td>Developed a cybersecurity disruption response plan</td>
<td>45%</td>
</tr>
<tr>
<td>Other</td>
<td>6%</td>
</tr>
</tbody>
</table>
Identity and Access Management

- Half of the states have an IAM model implemented or under way
- Some states are extended their IAM model to include citizens
Identity and Access Management

Figure 12
Has your state attempted to extend its IAM solution to identify and authenticate constituents seeking to access state services?

- 26% Yes, as a standalone capability
- 10% Yes, following the National Strategy for Trusted Identities in Cyberspace (NSTIC) federated ecosystem framework
- 6% Yes, following some other federated model
- 46% No
- 12% Other
Identity and Access Management

Figure 11
Which best describes the status of your state’s current approach to identity and access management?

<table>
<thead>
<tr>
<th>Status</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise model fully implemented in the executive branch</td>
<td>8%</td>
</tr>
<tr>
<td>Enterprise model under way - partial implementation</td>
<td>42%</td>
</tr>
<tr>
<td>Still investigating an enterprise model</td>
<td>21%</td>
</tr>
<tr>
<td>No plans for enterprise IAM implementation</td>
<td>2%</td>
</tr>
<tr>
<td>Decentralized IAM at agency level</td>
<td>17%</td>
</tr>
<tr>
<td>No IAM initiatives at all</td>
<td>6%</td>
</tr>
<tr>
<td>Other</td>
<td>4%</td>
</tr>
</tbody>
</table>
9. For identity and access management, how would you classify your state’s progress? (State Government only)

- **26%** A. My state has an enterprise approach to identify and access management.
- **40%** B. My state has a siloed and incompatible identity management systems, but we want to move to an enterprise approach.
- **23%** C. There have been discussions on identity management systems, but little progress has been made.
- **11%** D. It’s just not a priority at this time.
Cross Jurisdictional Collaboration

• Most states include on strategic agenda
• Challenges
  • governance
  • turf
**Cross Jurisdictional Collaboration**

**Figure 16**
What types of public sector organizations in your state are participating in an IT shared services model?

<table>
<thead>
<tr>
<th>Category</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other state executive agencies</td>
<td>88%</td>
</tr>
<tr>
<td>Local government entities other than education</td>
<td>55%</td>
</tr>
<tr>
<td>State colleges and universities</td>
<td>53%</td>
</tr>
<tr>
<td>State judicial agencies</td>
<td>45%</td>
</tr>
<tr>
<td>K-12 schools and school districts</td>
<td>43%</td>
</tr>
<tr>
<td>State legislative agencies</td>
<td>39%</td>
</tr>
<tr>
<td>Community colleges</td>
<td>39%</td>
</tr>
<tr>
<td>Entities outside my state</td>
<td>16%</td>
</tr>
<tr>
<td>Entities in my state other than those listed above</td>
<td>10%</td>
</tr>
<tr>
<td>Special districts</td>
<td>8%</td>
</tr>
<tr>
<td>Other</td>
<td>4%</td>
</tr>
</tbody>
</table>
Cross Jurisdictional Collaboration

Types of services states are providing – particularly to local government

Figure 17

<table>
<thead>
<tr>
<th>Service</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network services</td>
<td>63%</td>
</tr>
<tr>
<td>Data center hosting</td>
<td>61%</td>
</tr>
<tr>
<td>Security</td>
<td>51%</td>
</tr>
<tr>
<td>Email/office productivity</td>
<td>47%</td>
</tr>
<tr>
<td>GIS</td>
<td>47%</td>
</tr>
<tr>
<td>Telephony</td>
<td>45%</td>
</tr>
<tr>
<td>Cloud solutions/hosting</td>
<td>41%</td>
</tr>
<tr>
<td>Co-location</td>
<td>41%</td>
</tr>
<tr>
<td>IT training</td>
<td>35%</td>
</tr>
<tr>
<td>Portal/website hosting</td>
<td>29%</td>
</tr>
<tr>
<td>Storage and backup</td>
<td>28%</td>
</tr>
<tr>
<td>Video conferencing</td>
<td>26%</td>
</tr>
<tr>
<td>Applications development/support</td>
<td>24%</td>
</tr>
<tr>
<td>Business intelligence/business analytics</td>
<td>14%</td>
</tr>
<tr>
<td>Enterprise resource planning</td>
<td>12%</td>
</tr>
<tr>
<td>Mobile apps</td>
<td>12%</td>
</tr>
<tr>
<td>Digital archiving and preservation</td>
<td>10%</td>
</tr>
<tr>
<td>Imaging</td>
<td>10%</td>
</tr>
<tr>
<td>None</td>
<td>10%</td>
</tr>
<tr>
<td>Records management</td>
<td>6%</td>
</tr>
</tbody>
</table>
Cross Jurisdictional Collaboration

**Figure 18**
What are the major barriers when considering or initiating a cross-jurisdictional collaboration?

<table>
<thead>
<tr>
<th>Barriers</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance</td>
<td>69%</td>
</tr>
<tr>
<td>Turf issues</td>
<td>58%</td>
</tr>
<tr>
<td>Cost sharing</td>
<td>52%</td>
</tr>
<tr>
<td>Federal funding/cost allocation restrictions</td>
<td>33%</td>
</tr>
<tr>
<td>Legal/statutory restrictions</td>
<td>23%</td>
</tr>
<tr>
<td>Other</td>
<td>17%</td>
</tr>
<tr>
<td>Procurement rules</td>
<td>13%</td>
</tr>
</tbody>
</table>
Cybersecurity continues to be one of the most pressing challenges facing State Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) today.

Security threats to states have been widely reported, however the nature of the game has changed.

Cybercriminals and hacktivists — a new breed of hacker with a political or social agenda — use increasingly sophisticated methods involving rapidly evolving technologies to target cyber infrastructure for monetary gain and to make political statements.
Cybersecurity

States at risk – A call for action

Cybersecurity challenges continue in 2012 amidst escalating threats

- 92% State officials feel cybersecurity is very important for the state
- 50% Only 14% CISOs manage a team of one to five cybersecurity professionals only
- Only 70% CISOs have reported a breach
- Only 24% CISOs are very confident in protecting state's assets against external threats
- Only 32% CISOs feel that staff have the required cybersecurity competency
- 86% CISOs feel that "Lack of sufficient funding" is the key barrier to address cybersecurity
- 82% CISOs feel "phishing and pharming" as their top cybersecurity threat

2012 Deloitte-NASCIO Cybersecurity Study
State governments at risk: a call for collaboration and compliance
Cybersecurity

An urgent call to execute on a robust cybersecurity strategy, with strong governance and compliance monitoring measures.

1. Assess your risk and share results with business stakeholders
2. Strategize to address risks and threats
3. Invest in cybersecurity solutions
4. Educate on cybersecurity
5. Measure and report Share your story

Partner with business, agency and across jurisdictions.
Cybersecurity

94 million

The number of Americans’ files in which personal information has been exposed to potential identity theft through data breaches at government agencies since 2009.4

680%

The increase in significant cybersecurity threats against U.S. government systems from 2006 to 2011.6
10. Which security risk concerns you the most? (State Government only)

A. End-user downloads of non-approved apps 7%
B. Insider threats 15%
C. Email – malware and phishing 11%
D. Mobile devices and BYOD 15%
E. Sophisticated, pre-meditated attacks by hackers 9%

59%
Identity and Access Management
Scaling Interoperable Trust through a Trustmark Marketplace

John Wandelt
john.wandelt@gtri.gatech.edu
Georgia Tech Research Institute
October 2013
Smart Lean Government (SLG)

21st Century Collaborative Solutions
Serving Customers
More Responsively, Quickly, Efficiently

April 29, 2014

Presented by:
Eric Sweden
NASCIO
Resources

• Cyberspace Law: Identity Management Legal Task Force
  https://apps.americanbar.org/dch/committee.cfm?com=CL320041

• CyberSecurity Newsbriefs
  http://www.infoinc.com/NASCIO_CyberSecurity/mailinglist.cfm?FORMID=1&SERVICEID=466

• EA Newsbriefs

• The Heart of the Matter: A Core Services Taxonomy for State IT Security Programs
  October 2011  www.nascio.org/publications
Connect with NASCIO...

Eric Sweden  MSIH MBA
Program Director,
Enterprise Architecture & Governance
NASCIO
201 East Main Street, Suite 1405,
Lexington, KY 40507 USA
859.514.9189
esweden@nascio.org

Thank You!