Statewide IT Risk Assessment

Pacific Northwest/Western Intergovernmental Audit Forums Joint Meeting

September 2, 2015

Troy Niemeyer, Deputy Director of State Audit
Susan Hoffman, Principal, Performance Audit

What will we cover?

- Why we conducted a risk assessment
- What we did
- Our results
- What's next?

Why we conducted a risk assessment

Why conduct a statewide IT risk assessment?

- Priority of the State Auditor
- Known high-risk area in the state
- Current approach is fragmented and lacks strategic direction

What we did

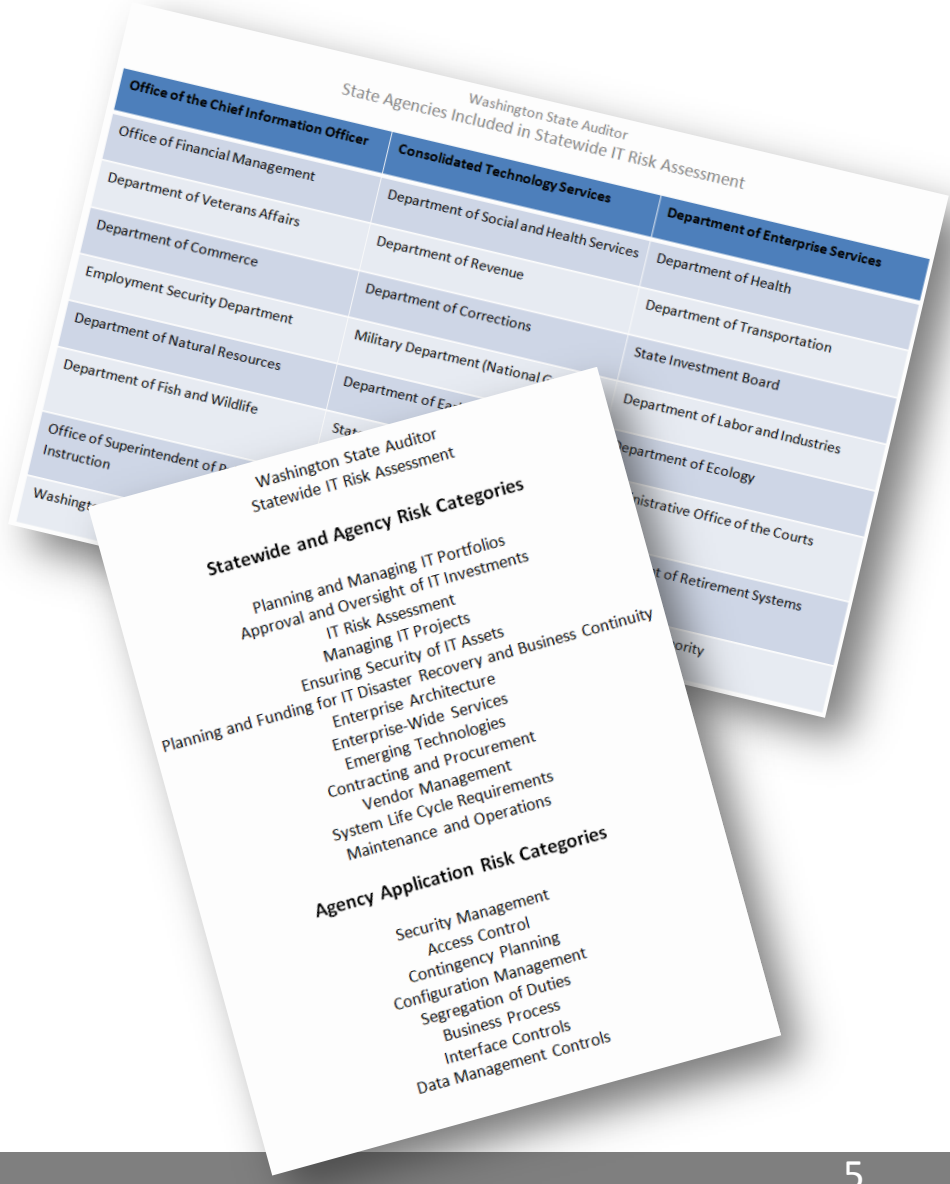
Asked our consultants to:

1. Develop an inventory of the state's information technology audit universe
2. Develop an approach to identify and assess those areas presenting the highest risk
3. Evaluate the role of State Auditor's Office in auditing the state's IT programs, functions, and systems
4. Evaluate how our efforts could be best organized to effectively audit the state's IT programs, functions and systems

What we did

Risk Assessment Tool

- Selected 25 state agencies
- Developed risk categories
  - Statewide
  - Agency-specific?
  - Agency applications
- Populated the tool with information gathered from Washington's OCIO and state agencies through structured interviews and document review



What we did

Structured interview questions for all agencies:

Annual IT budget?	Mobile devices used?
Number of users? (internal, external)	Wearable technology?
Any security breaches in the last year?	Last test of DRP?
Number of IT staff?	IT projects in process?
Formal IT risk assessment process?	

What we did

Interview questions specific to agency applications

Last security assessment?	Where physically hosted?
Categories of data in system?	Security event logs monitored?
Last vulnerability assessment?	Number of transactions monthly?
Last penetration test?	Does this support other applications?
Last review of access controls?	Processing controls in place?

What were the results?

IT Risk Assessment

- Risk ratings at state, agency, and agency application level
- Detailed explanations of ratings for each risk category
- Suggested audit topics for the next 3 years prioritized by level of risk
- Risk assessment tool that can be periodically updated by SAO to update and re-prioritize our IT audit workplan

What we did

Our role and organization for IT audits

- Interviewed state agency managers and staff
- Interviewed SAO executives, managers, and staff
- Gathered information from 17 state auditor offices on their roles in performing IT audits and their organization structure

What were the results?

Our role and organization for IT audits

- Consensus from our executives, managers and staff – as well as state OCIO and CISO – that we should play a major role in auditing the state's IT programs, functions and systems
- Our management and staff agreed that an IT audit team requires adequate funding to:
  - cover costs
  - pay market salaries
  - provide training
  - support certifications
  - engage third-party vendors as needed to provide technical expertise

What were the results?

Other states' results:

- Majority have a separate dedicated IT audit team
- Half have a separate budget for IT audit projects
- Most use external IT experts and consultants as needed
- Many would like more IT audit resources so they can perform more IT-related audit work

What were the results?

Recommendations from our consultant regarding our Office:

- Take the lead role as the independent auditor of the state's IT programs, functions, and systems
- IT audit resources should be organized and managed as a single team
- Use the risk assessment tool to perform continuous IT risk assessment
- Use the results of the initial risk assessment to develop a risk-based audit plan and potential projects

What's next?

SAO has established a IT Audit Committee to provide strategic direction and oversight for IT audit, including:

- Developing a comprehensive IT audit work plan based on the results of the IT risk assessment
- Determining which IT audits will be conducted
- Making staffing, hiring and training decisions related to IT audit
- Providing input to SAO executive management on how to further develop our IT expertise and audit function

QUESTIONS?

Troy Niemeyer
Deputy Director of State Audit
Troy.Niemeyer@sao.wa.gov

Susan Hoffman
Principal, Performance Audit
Susan.Hoffman@sao.wa.gov