OPEGA
REVIEW

INTERIM REPORT

State-Wide Information Systems Planning and Management

DECEMBER
2005

a report by

the Office of Program Evaluation & Government Accountability

About the Review

Purpose

OPEGA Seeks to Answer the Question…

Are information systems and technology being planned for and managed in a way that:

- maximizes the effectiveness and efficiency of State government; and
- keeps the State's exposure to associated risks at an acceptable level?

Method

To answer this question, OPEGA …….

- Hired a firm with IT auditing expertise to conduct a Risk Assessment
- Conducted research on:
  - State's history related to IS/IT
  - Current organization and plans for IS/IT
  - Role of IS/IT in government
  - Models and best practices related to the planning and management of IS/IT in government

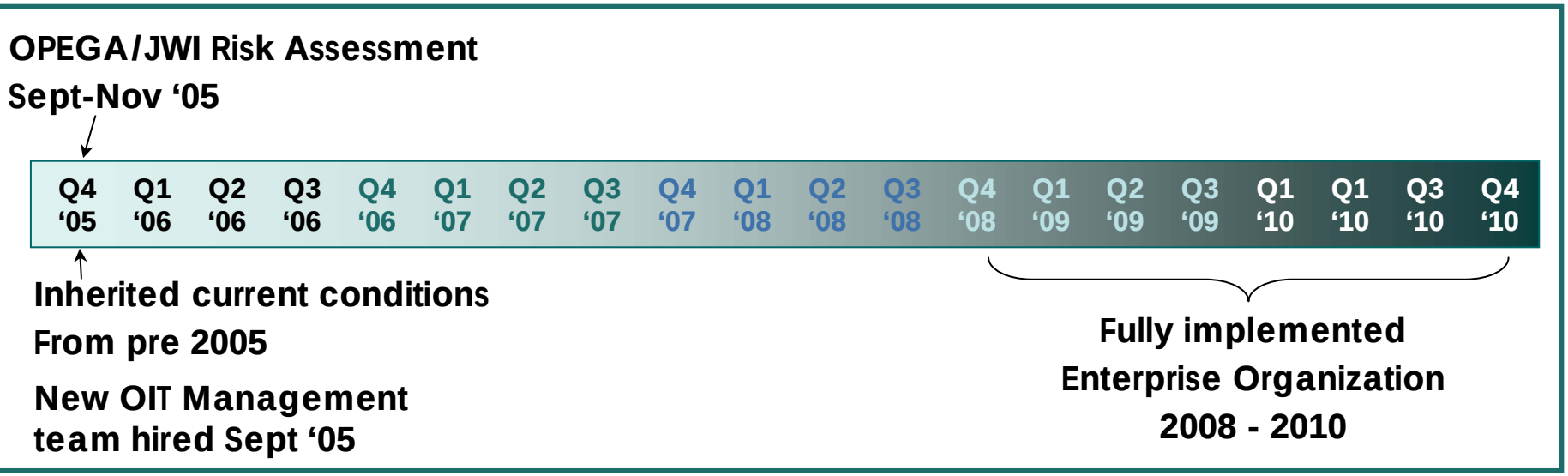
Status

- Risk Assessment complete
- Additional research complete
- Interim report today on:
  - Risk Assessment results
  - OPEGA and OIT Plans for Risk Assessment results
- Findings and Recommendations being finalized
- Final report being drafted; expected January

Background

OIT Transformation

- Involves consolidation & integration of fragmented, relatively independent IT "universes" with varying resources and priorities
- Effort to move the state toward an IT structure that allows planning & managing from an "enterprise" perspective
- OPEGA Review & JWI Risk Assessment took place just as the reorganization was beginning.
- Can expect 3-5 years before transformation is complete



What is a Risk Assessment?

Government/Quality Objectives

What are we trying to achieve?

Risks or Threats to Achievement

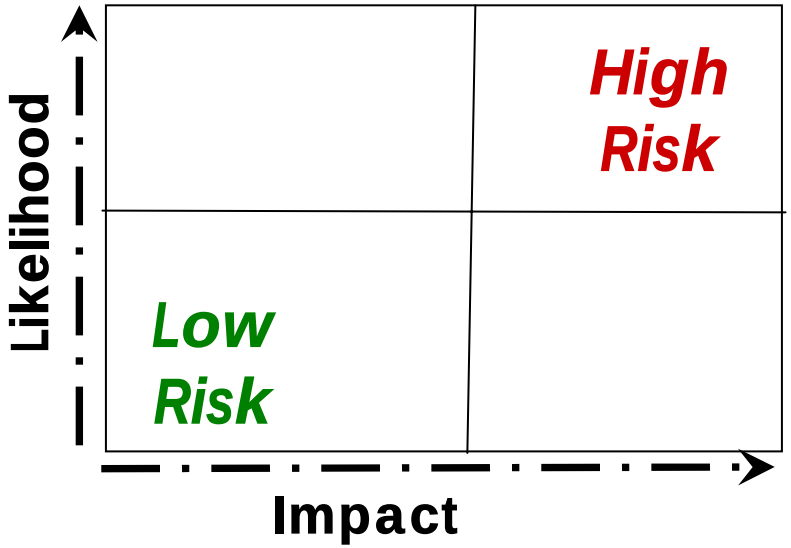
What could go wrong? How likely is it? What's the potential impact?

Controls

How do we prevent it, detect it or reduce its impact?

Exposure

What's the likelihood and impact with controls in place?



Is it Acceptable?

Categories of Controls

- Purpose: Definition and Communication
- Commitment
- Planning & Risk Assessment
- Capability/Continuous Learning
- Direct Controls
- Indicator/Measurement
- Employee Well-Being & Morale
- Process Oversight

Who is Jefferson Wells?

- International consulting firm specializing in internal audits.
- Highly qualified professionals perform information technology audits.
- Performed over 800 IT audits in the past 5 years.
- The JWI specialists assigned to work with OPEGA on this review: Mike Flowers and Jeff Bamberger

JEFFERSON WELLS
A Manpower Company

JWI Risk Assessment Results

- ✓ JWI delivered a detailed report of their results to OPEGA in November 2005
- ✓ Details were shared with CIO & key staff
- ✓ The detailed report and other deliverables are working papers for the OPEGA audit and as such remain confidential
- ✓ Deliverables included detailed Risk Matrix and recommended 3-5 year audit plan

Jefferson Wells Presentation

State of Maine / Results of OPEGA IT Risk Assessment

Sunrise on Cobbossee Lake

JEFFERSON WELLS
A Manpower Company

State of Maine / Results of OPEGA IT Risk Assessment

Jefferson Wells International was contracted by OPEGA to provide:

- An IT Risk Assessment for the Executive Branch IT environment
- A Proposed IT audit schedule
- An Information Systems Map of key business systems

State of Maine / Results of OPEGA IT Risk Assessment

OPEGA directed Jefferson Wells to also broadly focus on the areas of:

- Planning and management processes
- Change management practices and processes
- Organizational structure
- Performance monitoring
- Use of billing and charge back
- Use of current technology solutions
- Systems standardization and interfaces

State of Maine /
Results of OPEGA IS/IT Risk Assessment

Sunset on Cobbossee Lake

JEFFERSON WELLS
A Manpower Company

Jefferson Wells used the following methods to perform the IT Risk Assessment:

- Solicited specific information and documents from OIT and agencies
- Interviewed key IT directors and managers
- Visited the OIT data center
- Logged and analyzed the information received
- Tested information received against selected Control Objectives for Information and Related Technologies (CobiT) standards
- Compiled and evaluated the test results
- Prepared Risk Assessment deliverables

High-Risk: The IT Culture

- IT culture is one of 'operational expediency'
- "If it does not help me deliver IT services better, faster, cheaper, right now, then I don't have time for it!"
- Technical craftsmen & artisans
- Budget and manpower constraints most frequently cited factor
- The first casualties of this culture are documentation, procedures and controls

State of Maine / Results of OPEGA IT Risk Assessment

Pemaquid Lighthouse

JEFFERSON WELLS
A Manpower Company

High-Risk: The IT Culture

- IT documentation needs significant improvement
- Policies should be updated using 'best practices'
- Procedures implementing these policies and ensuring compliance should be developed and implemented
- A goal of the IT consolidation is a transition to 'process-driven' culture

OIT Management Staff

- Competent and committed managers
- Enthusiastic about IT consolidation
- Spend far more than 40 hours a week delivering IT services
- Hold the IT 'organizational memory'
- Are the agency's IT 'surge capacity'
- Represent a part of hidden IT costs
- Significant experience in IT and the State
- May benefit from additional professional development opportunities

State of Maine /
Results of OPEGA IT Risk Assessment

In Camden Harbor

High-Risk: IT Consolidation

- Goals are service efficiencies and cost benefits
- Estimated to take 3 – 5 years to fully realize benefits
- Critically dependent on the CIO's skill set
- CIO appointed by the Commissioner of the Department of Administrative and Financial Services
- Change at the CIO level could adversely impact the outcome

IT Consolidation

- New OIT organization logically follows IT functional areas
- Lines of authority and communication are clearly defined
- Areas of responsibility are well defined
- Key management positions are filled
- No structural impediments were observed
- Long-term effectiveness yet to be determined

State of Maine /
Results of OPEGA IT Risk Assessment

At Harvey Pond

JEFFERSON WELLS
A Manpower Company

High-Risk: Business Continuity Planning (BCP)

- IT Business Continuity Planning inadequate
- Most likely will fail in a real emergency
- Plans fail most CobiT tests
- No meaningful testing of recovery plans
- Insufficient resources allocated to plans and recovery

High-Risk: Business Continuity Planning (BCP), continued

- Immediate development of OIT BCP and integration with agency BCP's strongly recommended
- Risks must be assessed against actual threats

State of Maine / Results of OPEGA IT Risk Assessment

Mooselookmeguntic Lake

JEFFERSON WELLS
A Manpower Company

High-Risk: Security

- Physical and system access security was found to be inadequate for many network, WAN and stand alone computer systems
- This does NOT mean the State is vulnerable to hackers. In fact, protection against hackers was noted as a positive in this assessment
- A number of specific high and medium risk exposures related to security were noted
- OPEGA and OIT have been provided detail of exposure areas and recommended actions
- At OPEGA's direction, specifics will not be released to public

High-Risk: Project Management

- IT culture of 'operational expediency' not always adaptable to managing capital IT projects
- No IT-wide SDLC process or Project Management methodology in place as a standard
- Capital IT projects in past depended on at least one outstanding project manager from IT, business or vendor
- Business end-user management must own capital IT projects as they will own the resulting system
- IT provides technology support to the business project

State of Maine /
Results of OPEGA IT Risk Assessment

At Small Falls

JEFFERSON WELLS
A Manpower Company

High-Risk: Project Management

- Proven SDLC methodologies should be analyzed
- An effective SDLC methodology should be adopted and integrated into procurement process
- Project Management Institute (PMI) methodology should be adopted and integrated into procurement process
- Project Management Professional (PMP) fast becoming industry standard for Project Managers
- IT Capital Project Managers should be PMP certified

High-Risk: Procedures and Documentation

- Procedures and documentation across the IT environment need immediate attention
- Frequently disorganized & fragmented
- Often lack basic identifying information
- Little evidence of document control procedures
- Little evidence of formal review process
- Some necessary documentation is missing
- Many policies lack documented procedures to implement and monitor

State of Maine /
Results of OPEGA IT Risk Assessment

At Small Falls

High-Risk: Procedures and Documentation

- IT should implement basic document format and content standards which will ensure the completeness, identification and protection of documents
- IT should establish minimum documentation requirements for systems, policies and procedures
- At a minimum, basic document control procedures should be implemented for key IT documents
- Procedures for timely and regular management review and approval of key plans and strategy documents should be immediately implemented

State of Maine / Results of OPEGA IT Risk Assessment

Positives:

- The IT Directors and Managers interviewed were very committed to providing quality IT services
- An IT Steering Committee, known as the CIO Council, has begun to hold regular meetings
- Some large-scale IT capital projects have been successful and should serve as instructive examples
- An Information Security policy exists and has been adopted by many agencies
- Business Continuity Plan documents exist for many agencies
- Network diagrams are generally up to date

State of Maine /
Results of OPEGA IT Risk Assessment

At Sand Pond

State of Maine / Results of OPEGA IT Risk Assessment

Positives:

- In the agencies with significant IT resources, many sound practices are in use
- Background checks are conducted for all employees
- Some backup tapes are created for critical systems on a daily, weekly and monthly basis
- Test restores are performed for some critical system backup tapes
- Strong Authentication is used for dial up remote access and VPN access to the network
- For the most part, current versions of Operating Systems & relatively new hardware are in use

State of Maine / Results of OPEGA IT Risk Assessment

Summary:

- Benefits in terms of reduction in costs and increases in service can be realized through IT consolidation
- An IT consolidation of this size and complexity can reasonably be expected to require between three to five years to fully realize the benefits
- To fully succeed, the IT consolidation effort needs continuing IT management focus and strong support from business management within the State of Maine's Executive Branch agencies
- As IT is consolidated, opportunities are created for a more process-driven IT environment with standardized service offerings

State of Maine / Results of OPEGA IT Risk Assessment

Summary:

- Address the high-risk exposures immediately
- Address the medium-risk exposures in the course of the IT consolidation
- Implement the recommended audit schedule, if possible, with an internal IT audit staff or OPEGA
- IT Consolidation will not be universally popular, but it is the right thing to do
- Stay the course – IT is heading in the right direction
- Protect the IT consolidation process so the State of Maine can reap the benefits
- "Support your local CIO"

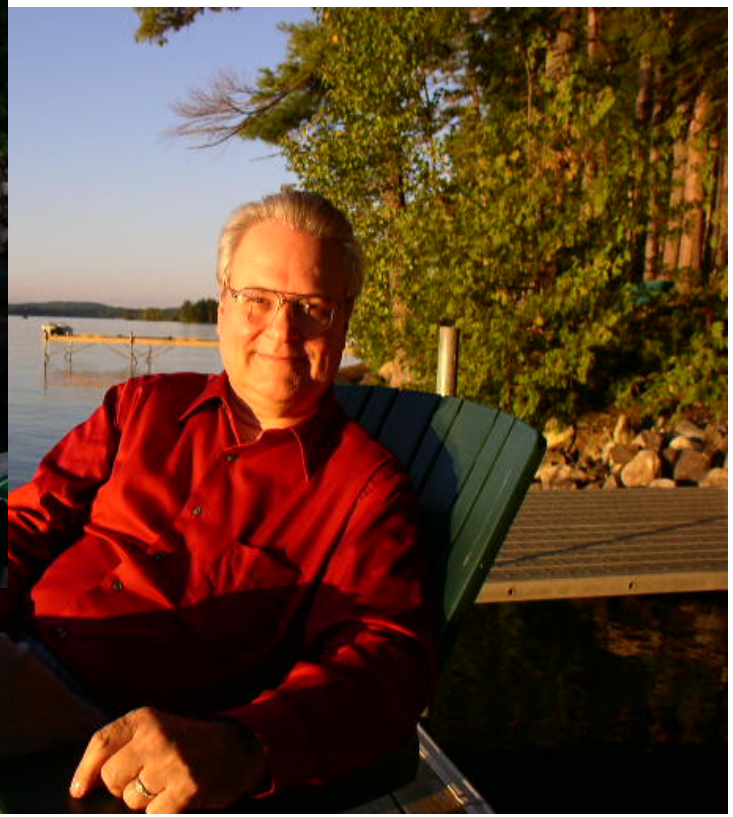
State of Maine /
Results of OPEGA IT Risk Assessment

A Bright Sunrise for OIT

JEFFERSON WELLS
A Manpower Company

State of Maine / Results of OPEGA IS/IT Risk Assessment

Thank you for all your support …



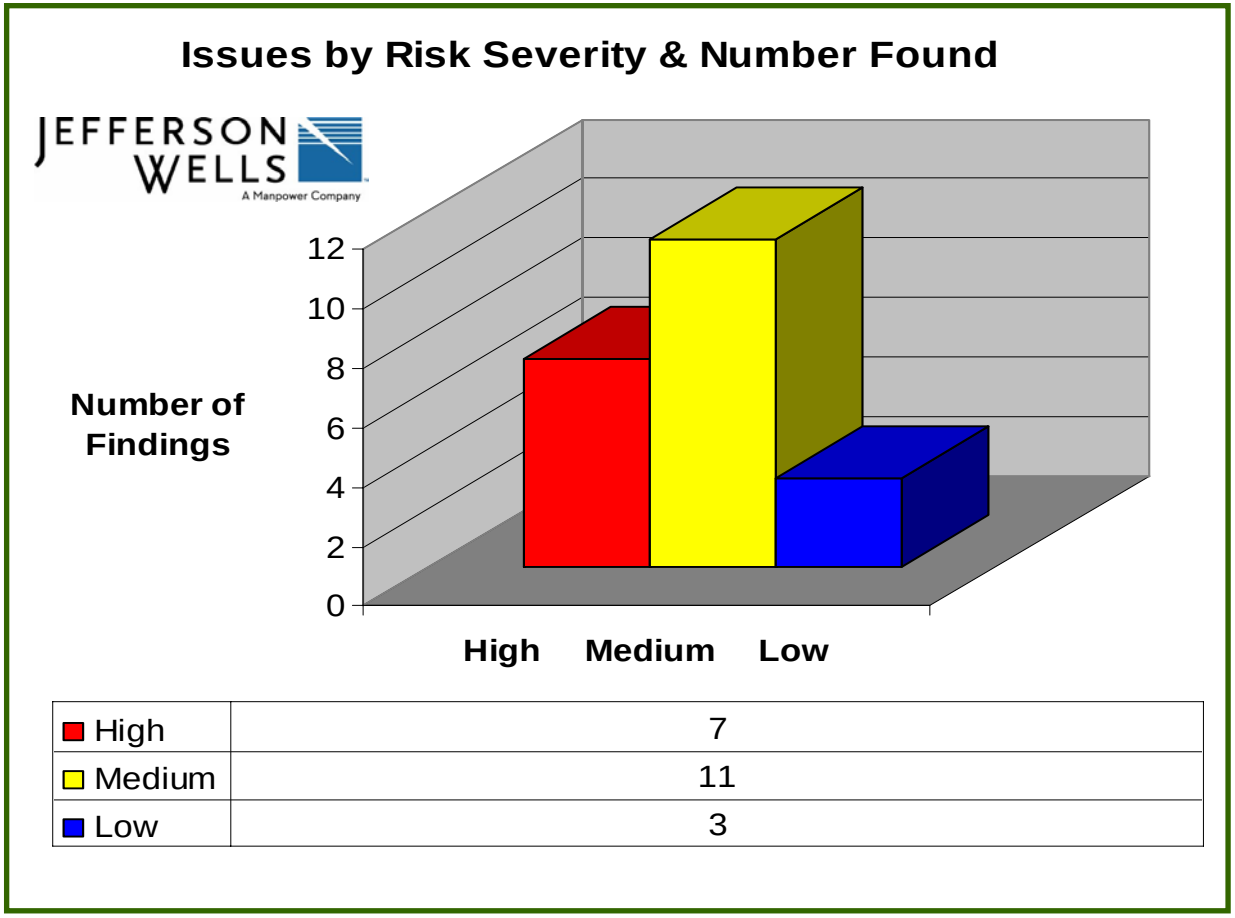
From your JWI IT Risk Assessment Team !!

JEFFERSON WELLS
A Manpower Company

Plans for Risk Assessment Results

Interim Results

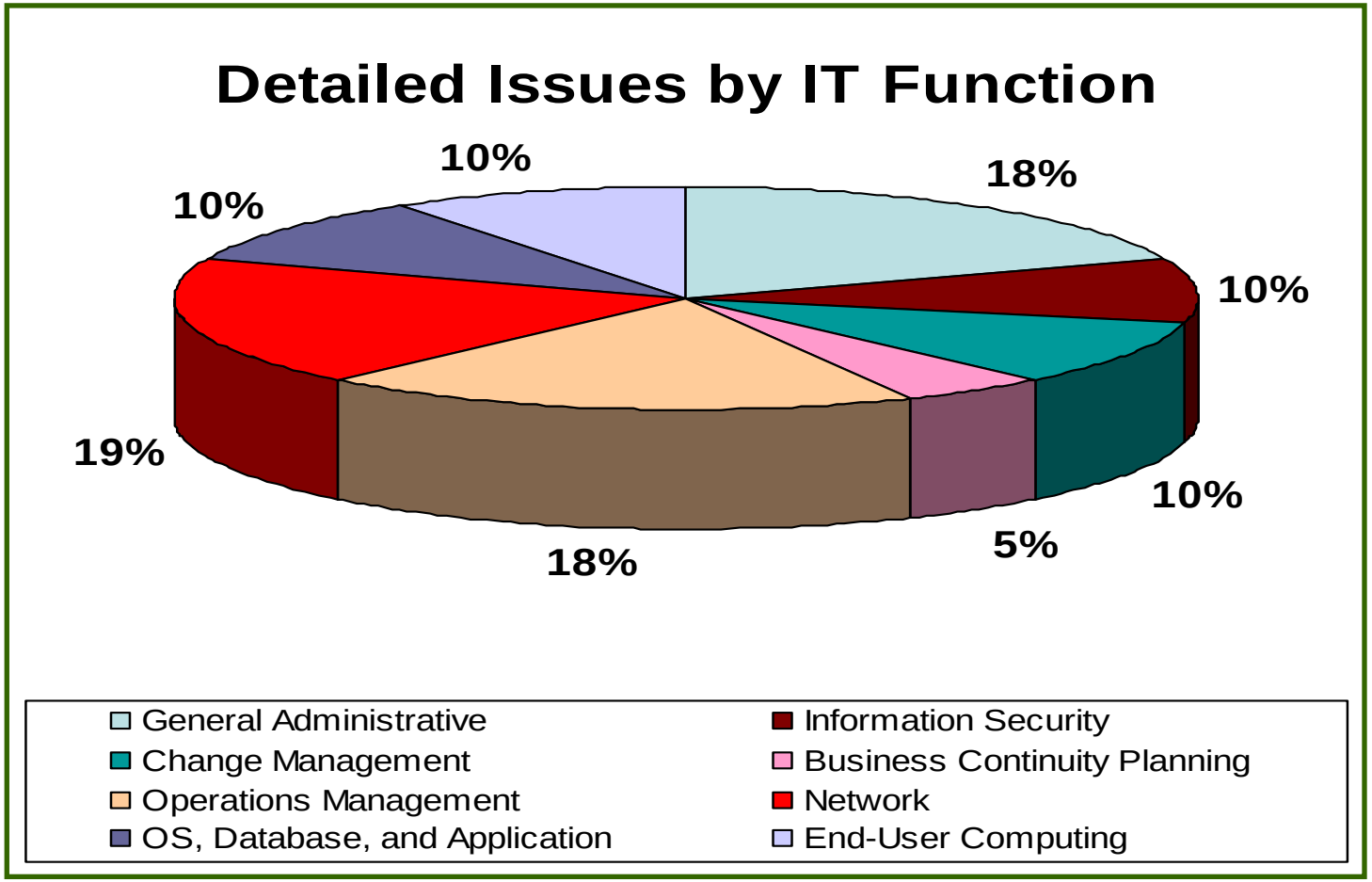
Current level of overall risk exposure for State Information Systems and Technology is too high.



High	7
Medium	11
Low	3

Interim Results

JWI identified 21 issues involving 8 different IT functions.



OPEGA's Plan for RA Results

- Identify root causes for Risk Assessment results
- Develop Findings and Recommendations that incorporate Risk Assessment results **and** root causes
- Present Final Report in January

OIT's Plan for RA Results

- Many issues raised in this assessment had already been identified and remedies for them were already in OIT's Strategic plan.
- Actions to address the remaining issues within OIT's area of responsibility will also be integrated into the Strategic Plan.
- OIT senior managers will provide OPEGA detailed action plans for addressing issues within their area of responsibility in first quarter of 2006.
- Implementation of actions subject to priorities and contingent on resource availability.
- Some issues are more systemic in nature and require inter-agency or high level policy and oversight decisions.

Questions?