Audit Challenges and Best Practices

in a Research University Environment

NSAA Annual Conference

Jeffrey Huskamp
Vice President and CIO

University of Maryland, College Park

- Carnegie Doctoral/Research University – Extensive
- 18th ranked public university (US News)
- Celebrated 150th anniversary in 2006
- Total budget $1.4B
- Enrollment
  - Undergraduate – 25,857
  - Graduate – 10,157

UNIVERSITY OF MARYLAND

University of Maryland, College Park (cont'd)

- Employees
  - Faculty – 3,752 (full-time and part-time)
  - Staff – 4,829
  - Graduate assistants – 3,873

- University structure and degrees
  - 1250 acres
  - Land grant institution for the State of Maryland
  - 13 colleges/schools (no medical school)
  - 127 undergraduate majors
  - 112 graduate degrees
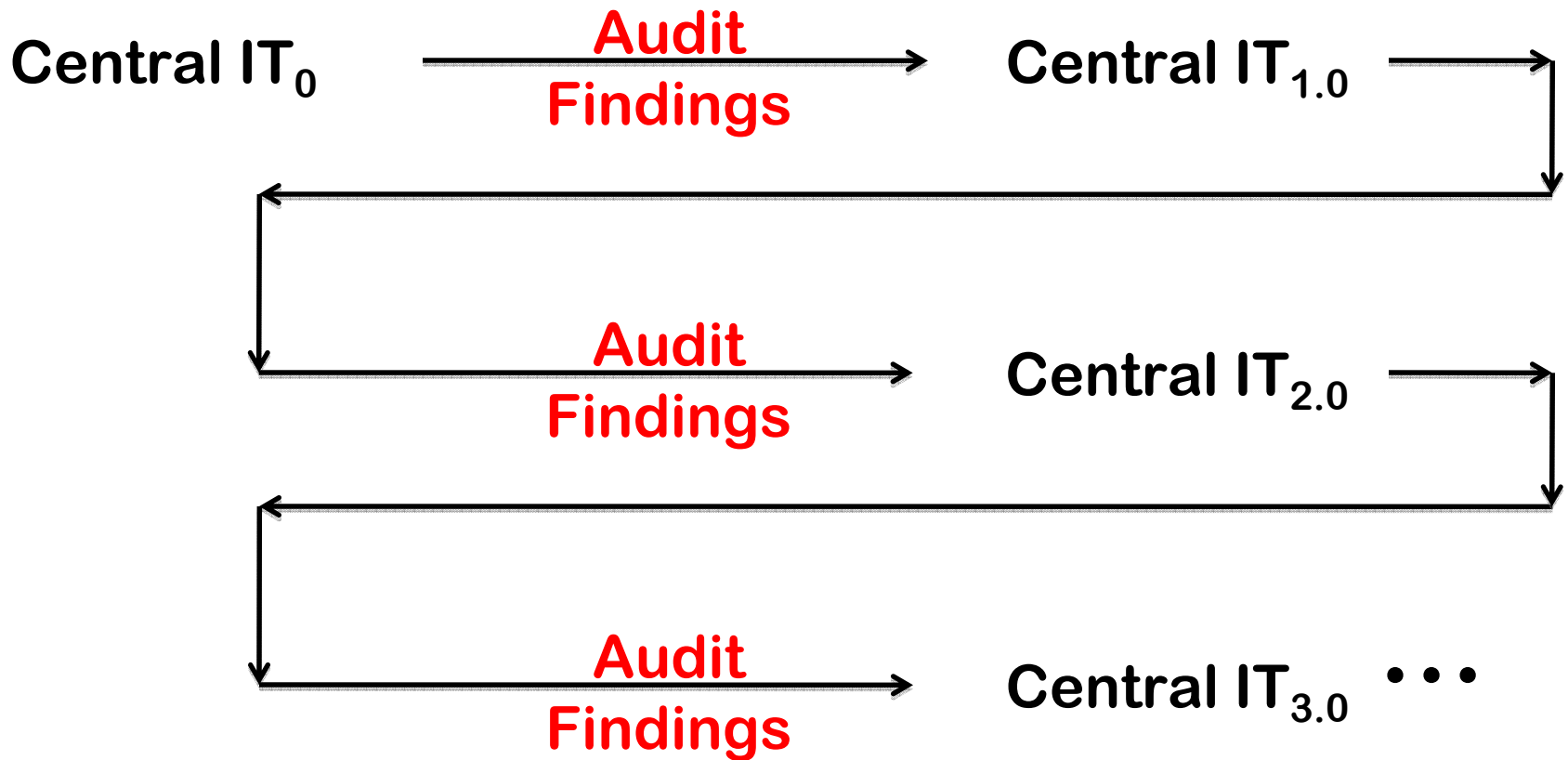
The Research University Environment

- Academic ingenuity reigns (universities understand and teach chaos theory)
- Decentralized information technology environment for education and research
  - >130 email systems, separate IT groups in every large unit
- Loose federation for IT direction
- Strict accountability for central IT
- Complex, multivendor environment not conforming to one grand plan
- Stovepipes are woven into the history

Campus Systems and Facilities

- Administrative system environment
  - Locally written administrative systems
  - Mostly mainframe based
  - Vendor solutions around the edges (e.g. student recruitment)

- Networking
  - 3500 wireless access points
  - Host institution for the Mid-Atlantic Crossroads
  - Member of Internet2

- Data centers
  - Two main central IT data centers
  - Contracted mainframe disaster recovery site

Old School Method of Audit Performance Improvement

$Central\ IT_0$ $\xrightarrow{\text{Audit Findings}}$ $Central\ IT_{1.0}$

$\xrightarrow{\text{Audit Findings}}$ $Central\ IT_{2.0}$

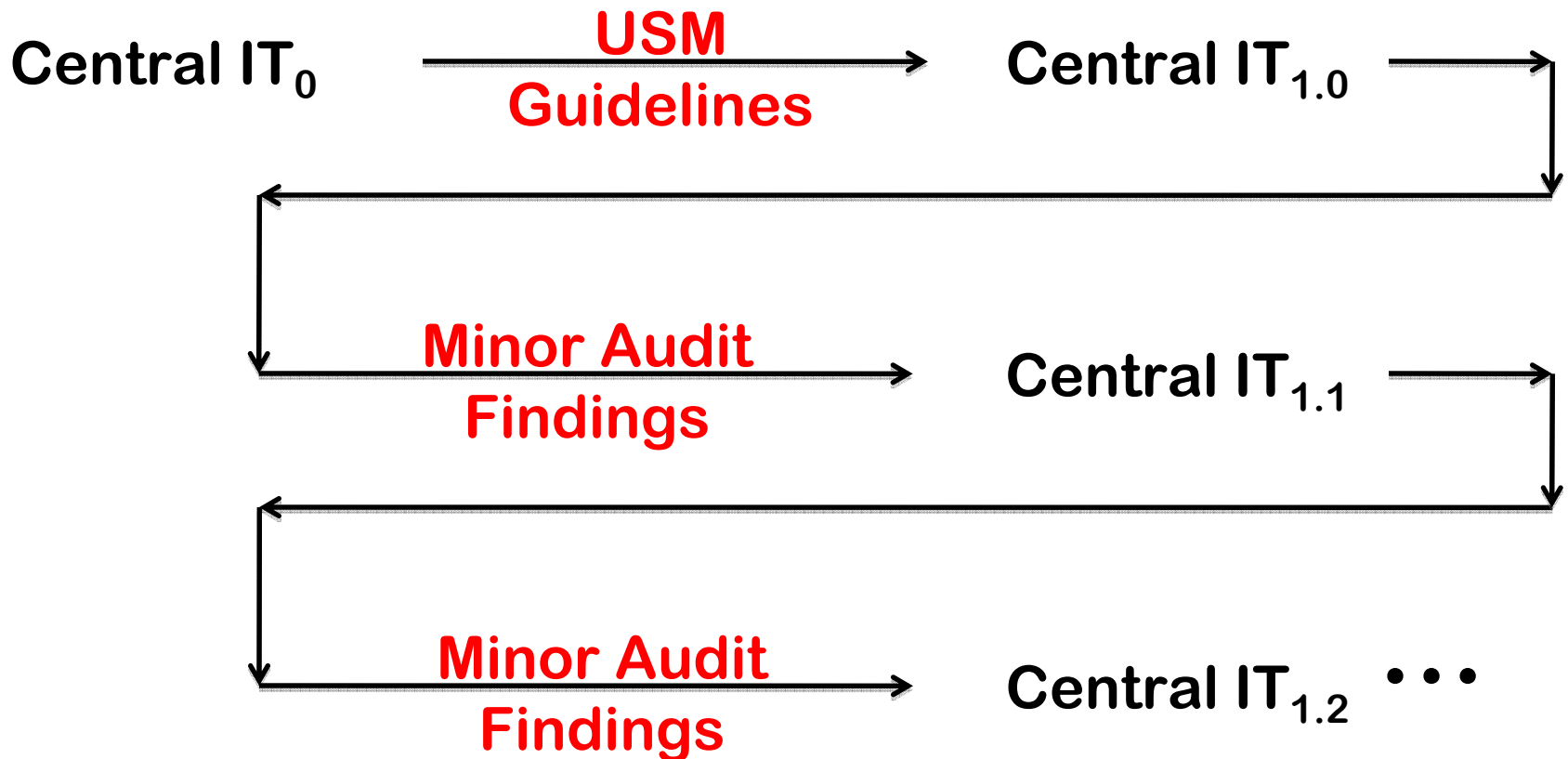$\xrightarrow{\text{Audit Findings}}$ $Central\ IT_{3.0}$ • • •

Case Study

- ## State audit report published in September 2003
  - 10 Findings including 3 repeated findings
- ## State audit began in October 2004
- ## State audit report published in January 2006
  - 7 Findings including 6 repeated findings
- ## Obviously moving in the wrong direction

Motivation for Change

- Auditors are a "free" consulting service
- Expect decreased number of security incidents
- Expect decreased risk
- External perception of institution
- Professional pride
  - Points of light in every organization
- Long term payoffs (with short term pain)

New School Method of Audit Performance Improvement

Central IT$_0$ $\xrightarrow{\text{USM Guidelines}}$ **Central IT$_{1.0}$**

Central IT$_{1.1}$

Minor Audit Findings

Central IT$_{1.2}$ • • •

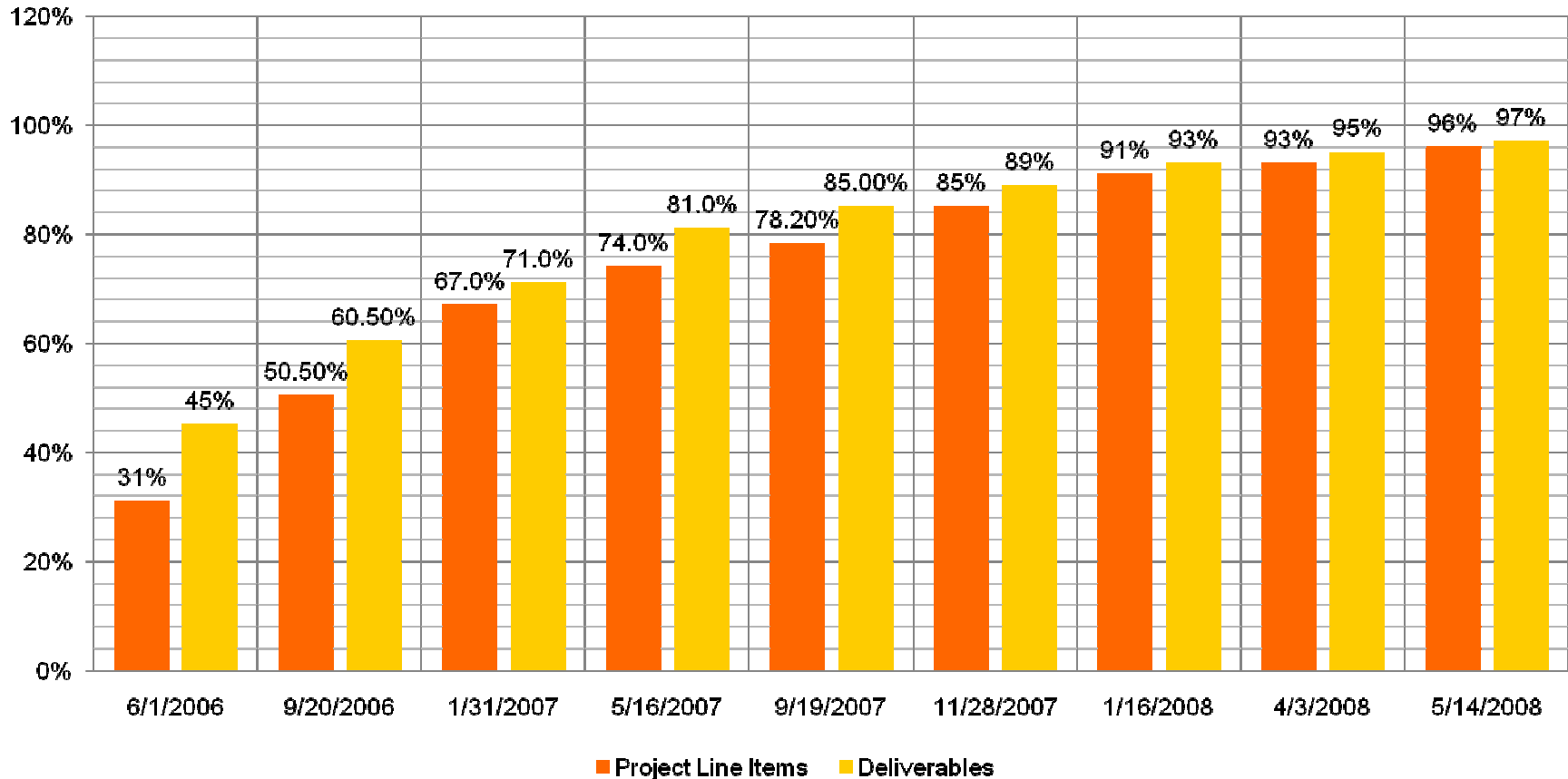Minor Audit Findings

UNIVERSITY OF
MARYLAND

Do The Hard Work

- <u>Step 1</u>: Start with the goal of conforming to all aspects of the USM guidelines

- <u>Step 2</u>: Create a set of deliverables that will accomplish the goal

- <u>Step 3</u>: Create a project plan that results in accomplishing all deliverables and assigns responsibility (98 deliverables, 503 line items)

- <u>Step 4</u>: Track progress

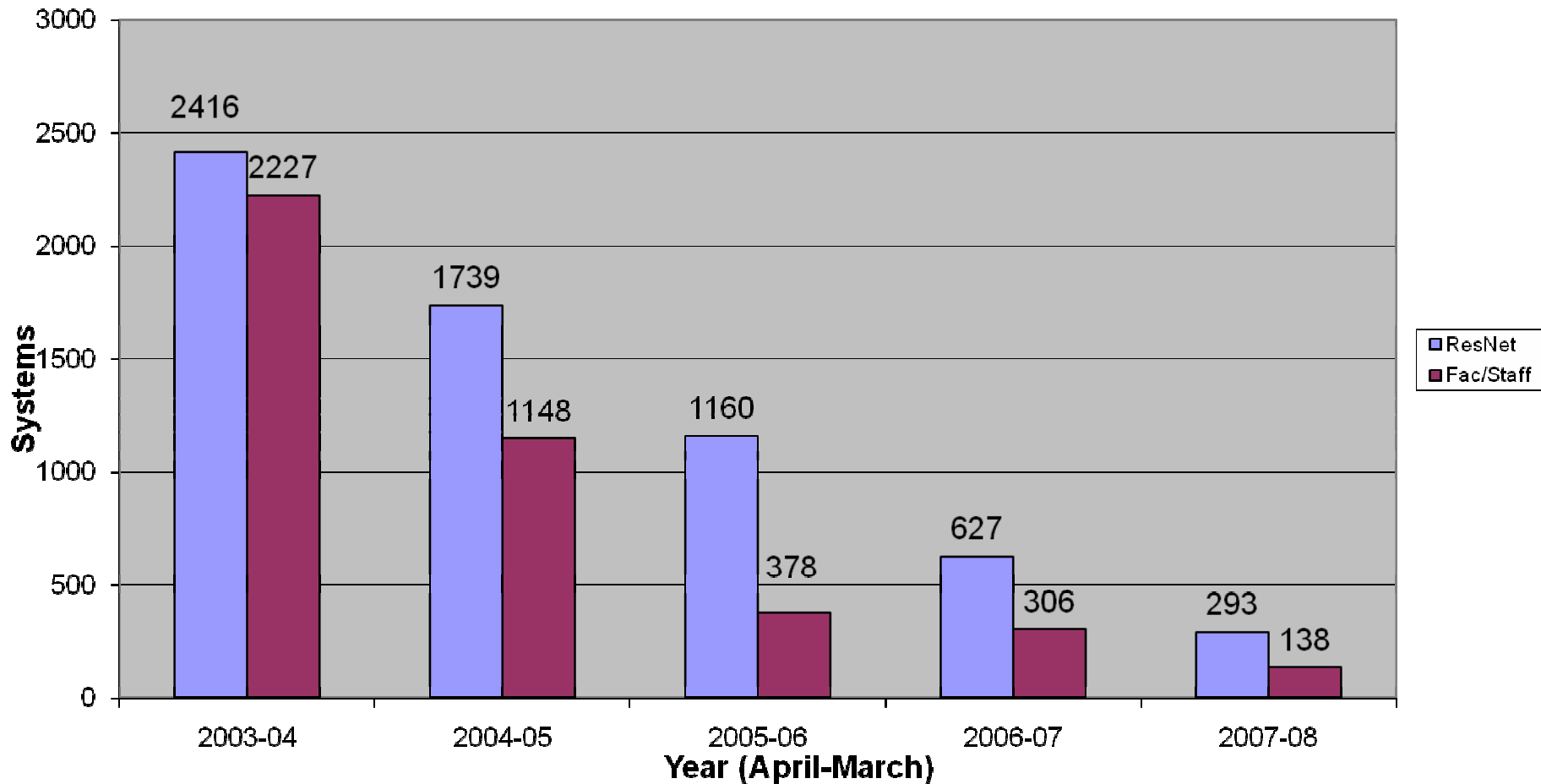- <u>Step 5</u>: Make mid-course corrections as needed

Track Progress

IT Security Project Progress

Date	Project Line Items	Deliverables
6/1/2006	31%	45%
9/20/2006	50.50%	60.50%
1/31/2007	67.0%	71.0%
5/16/2007	74.0%	81.0%
9/19/2007	78.20%	85.00%
11/28/2007	85%	89%
1/16/2008	91%	93%
4/3/2008	93%	95%
5/14/2008	96%	97%

Legend: ■ Project Line Items ■ Deliverables

Does it work?????

Security Incidents

Chart showing Security Incidents by Year (April-March), with Systems on the vertical axis ranging from 0 to 3000. Legend: ResNet, Fac/Staff.

Year (April-March)	ResNet	Fac/Staff
2003-04	2416	2227
2004-05	1739	1148
2005-06	1160	378
2006-07	627	306
2007-08	293	138

OIT Office of Information Technology

UNIVERSITY OF MARYLAND

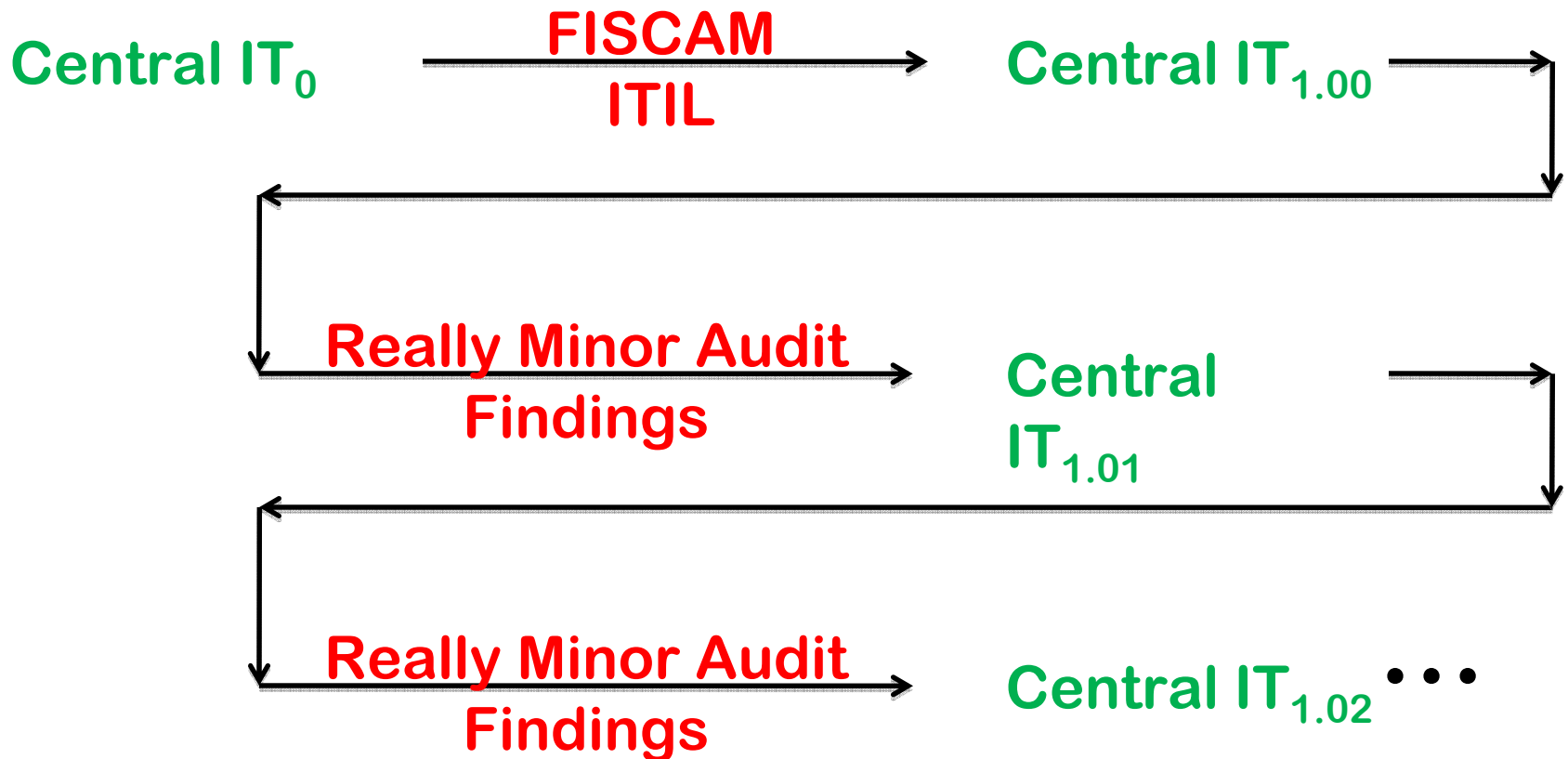# Does it work – part 2

The jury is out – the auditors are on campus and not finished

Future Method of Audit Performance Improvement

$$\text{Central IT}_0 \xrightarrow{\text{FISCAM}\ \text{ITIL}} \text{Central IT}_{1.00}$$

$$\xrightarrow{\text{Really Minor Audit Findings}} \text{Central IT}_{1.01}$$

$$\xrightarrow{\text{Really Minor Audit Findings}} \text{Central IT}_{1.02} \bullet \bullet \bullet$$

OIT Office of Information Technology

UNIVERSITY OF
MARYLAND

Pursue a Comprehensive Approach

- Get the institution involved
  - NSA Academic Center of Excellence in Information Assurance
  - Create the next generation of audit analysts for the institution

- Make it easy for units to reduce risk
  - Look for software that can be campus site licensed
  - Whole disk encryption to be available campus-wide

- Put campus policies in place that give responsibility for critical systems (e.g. networks, administrative systems) squarely on central IT

- Provide audit consulting to other units throughout the year

If A Research University Wants To Be Better…

- Create an infrastructure for success
  - Hire an internal IT auditor to be part of the central IT security staff, the point of contact for external auditors and consultant for all university units
  - Create an ethics organization
  - Establish a solid working relationship with the external auditors

- Raise awareness on campus

- Conduct formal audits of campus units with their cooperation

- Set a goal, develop a plan, recognize the implementation will take years, and there will be a budget impact

If A Research University Wants To Be WAAAY Better…

- ## Information Technology Infrastructure Library
  - Applications management
  - Change management
  - Asset and configuration management
  - Incident management
  - Operations management
  - Problem management
  - Release and deployment management
  - Service continuity management
  - …

Project NEThics
Internet + Ethics = NEThics

- Mission: to promote responsible use of information technology through user education and policy enforcement

- Web site: www.nethics.umd.edu

I'm Here To Help…

- Proactive "best practices" pointers
- High level analysis of the public audits from other agencies/units
- Prioritization of audit areas to address
- Citing the good things, even informally

Future Technology Challenges

- WiMAX high speed connectivity
- Mobile devices containing sensitive data
- Grid/distributed computing
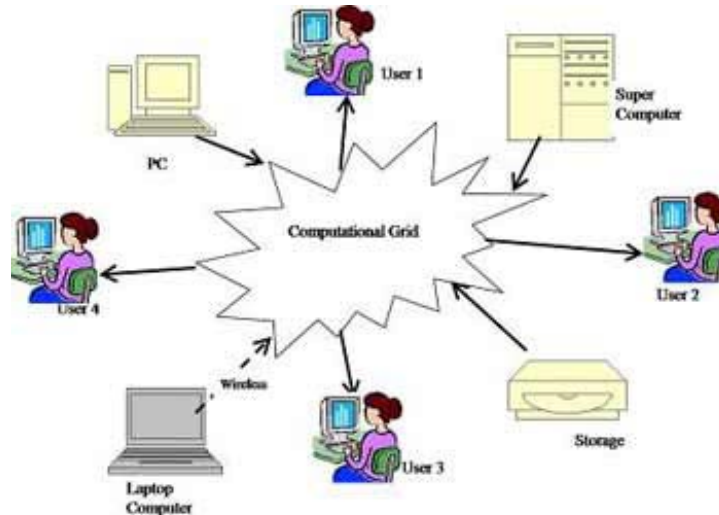
Future Software Challenges

- ## Open source
  - Kuali Foundation
  - Source code modifications by other institutions
  - Service Oriented Architecture for distributed computing
  - The rise of open systems
  - The fall of the mainframe

- ## Virtual teams
  - Beyond the firewall

- ## Log overload
  - Too many systems generating too many logs that need expensive log analysis tools to make any sense of the data

OIT Office of Information Technology

UNIVERSITY OF
MARYLAND

Contact Information

**Dr. Jeff Huskamp
Vice President and CIO
University of Maryland
1122 Patuxent Building
College Park, MD 20742**

Email: jhuskamp@umd.edu

UNIVERSITY OF
MARYLAND