

# LECTURE 1

## FUNDAMENTAL OF COMPUTER AUDIT

*Do not figure on opponents not attacking;  
worry about your own lack of preparation....*

*You can have all the protection mechanisms in  
place and still have security problems....*

*Need systematic preparation..*

***Technology is not enough....to be secure totally..thus?***

***Even the best security technology solution can protect everything  
100%....thus?***

***Computing Audit & Risk Management is required!***

Which Includes essential governance and operational processes such as:

- ✓ Incident management response process
- ✓ Classifying business value of data
- ✓ Risk assessments on internal systems
- ✓ Security Audits
- ✓ Governance, risk and compliance

***Technology is not enough....to be secure totally..thus?***

***Even the best security technology solution can protect everything  
100%....thus?***

***Computing Audit & Risk Management is required!***

Which Includes essential governance and operational processes such as:

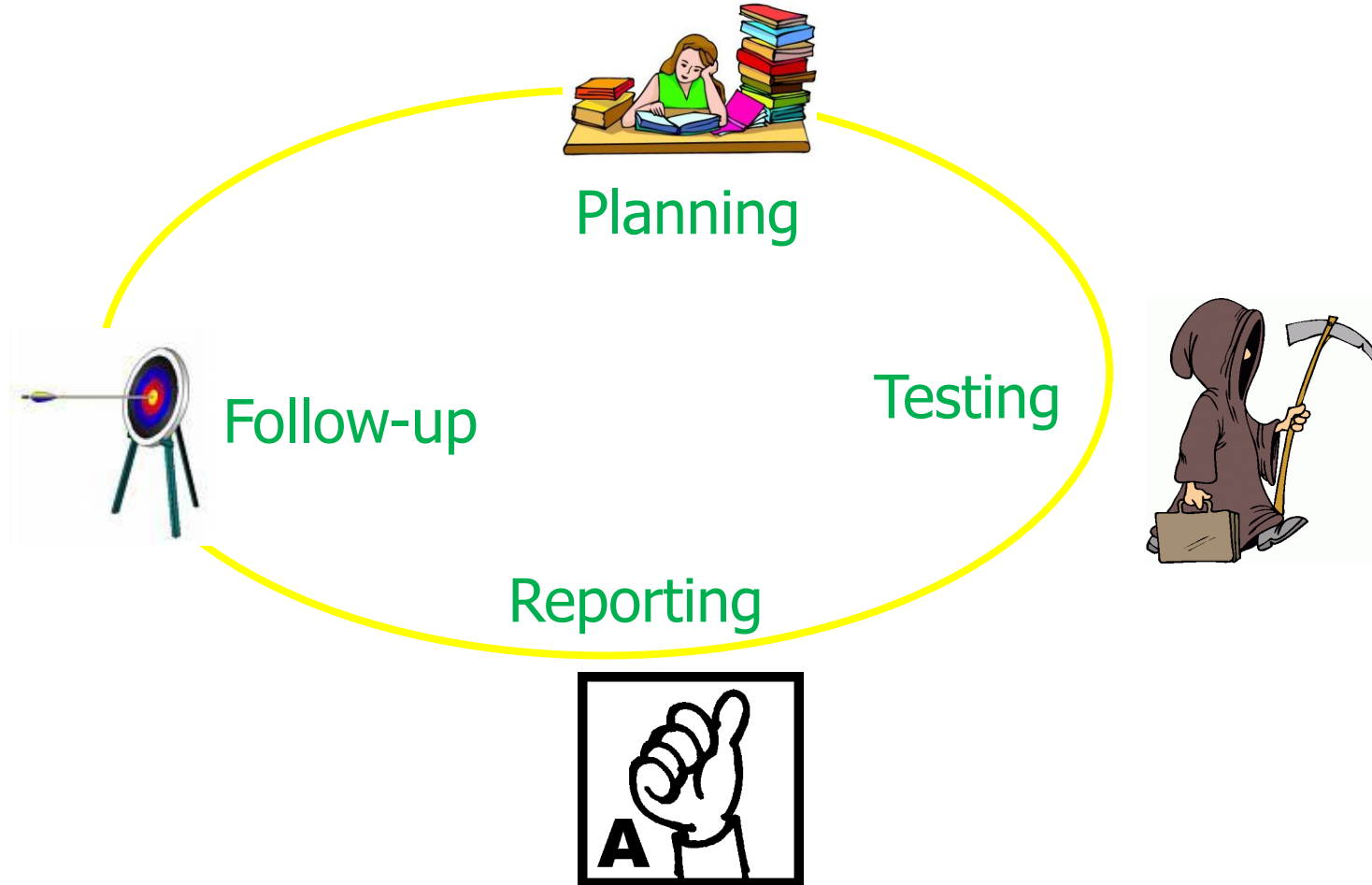
- ✓ Incident management response process
- ✓ Classifying business value of data
- ✓ Risk assessments on internal systems
- ✓ Security Audits
- ✓ Governance, risk and compliance

# What is Internal Audit?

Internal auditing is an independent, objective assurance and advisory activity designed to add value and improve an organization's operations.

Internal Audit helps organizations accomplish their objectives by evaluating business risk and controls and where appropriate, offer recommendations to improve risk management and governance processes.

# Audit Process



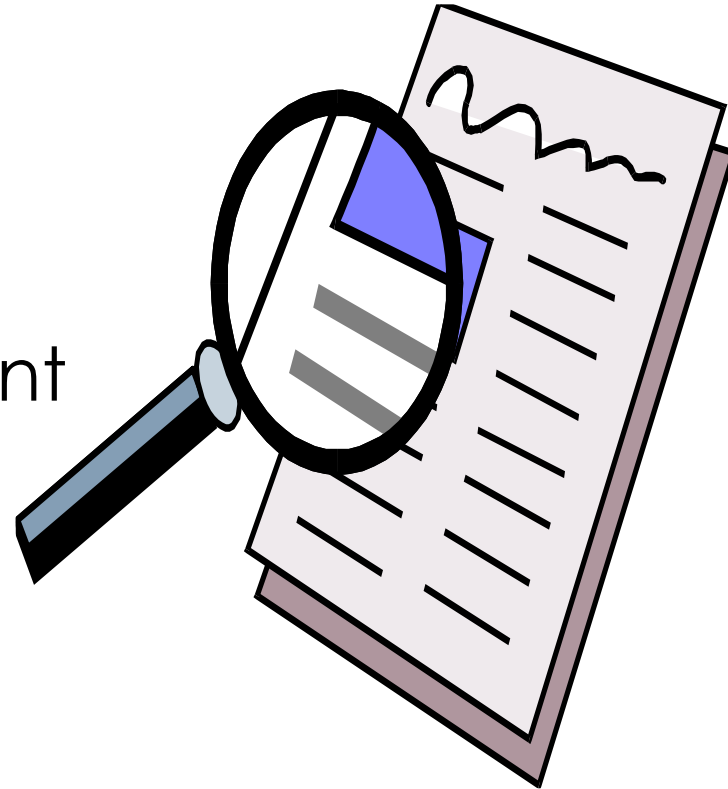
# Planning

- ✓ Annual Risk Assessment
- ✓ Preliminary Audit Plan
- ✓ Board of Visitors Approval
- ✓ Notification and Request for Information
- ✓ Understand Your Risks and Controls



# Testing

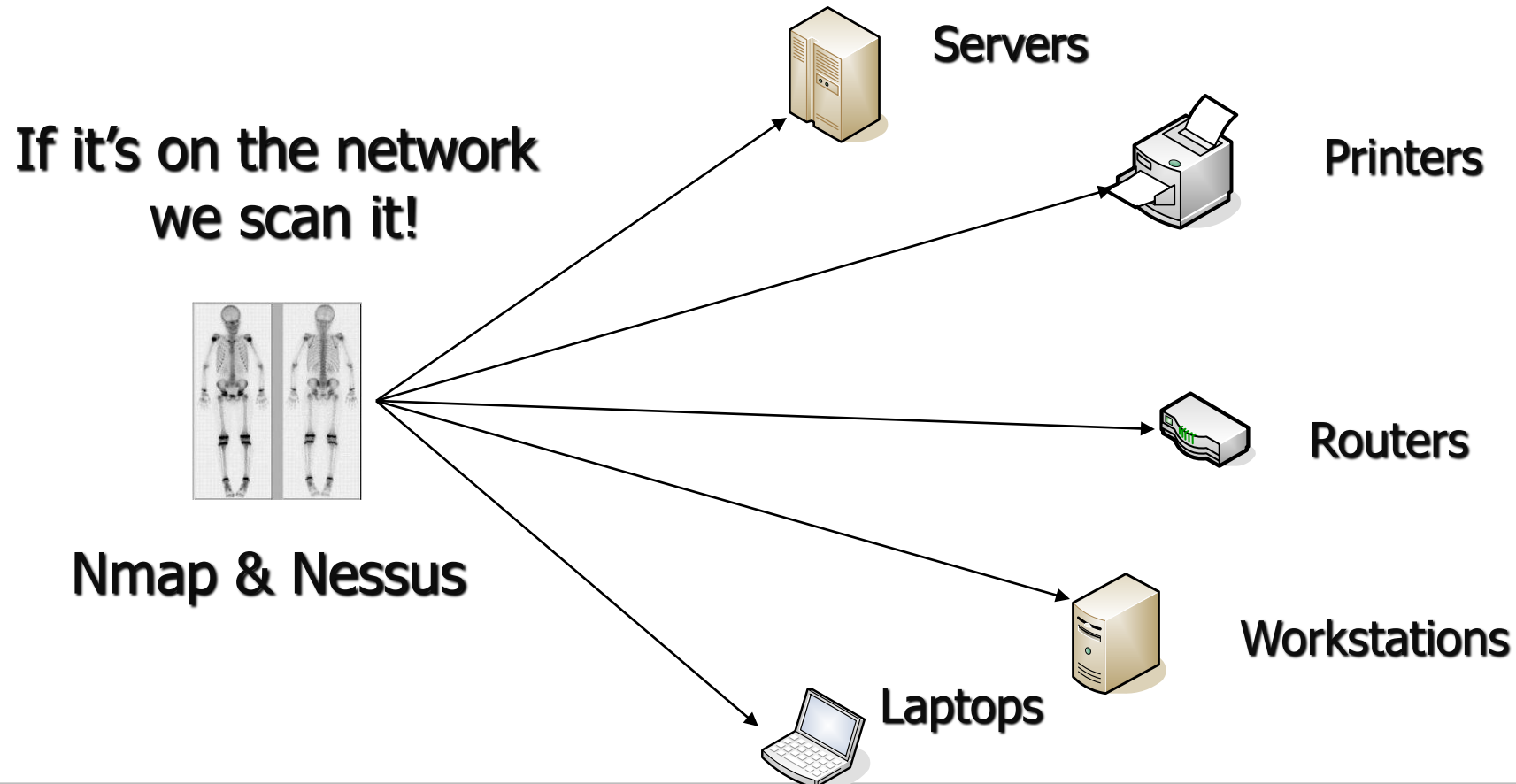
- ✓ Security
- ✓ Backup & Recovery
- ✓ Resource Management
- ✓ Web Site





# Security Testing

## Remote Vulnerability Scans

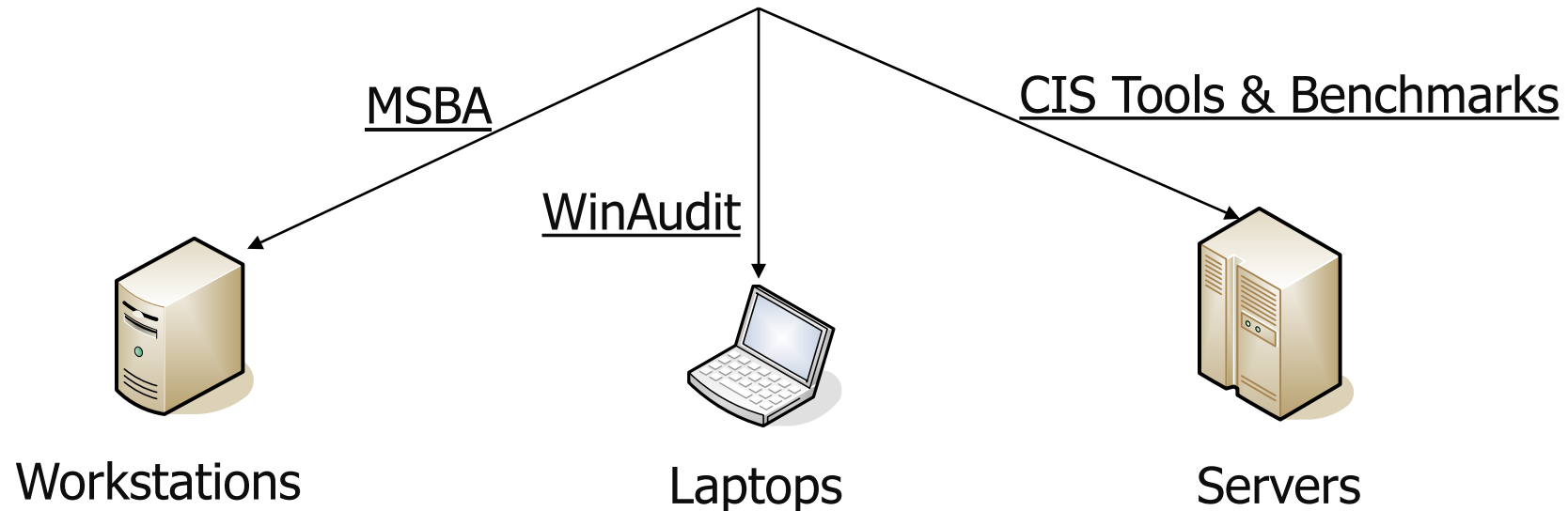


# Security Testing

On-Site, Follow-up Vulnerability Tests



**We Test Computers That May Have Security Vulnerabilities!**



# Backup & Recovery Testing

You Must Have Effective Controls to Backup & Recover



**“Critical Data”**

# Resource Management Testing

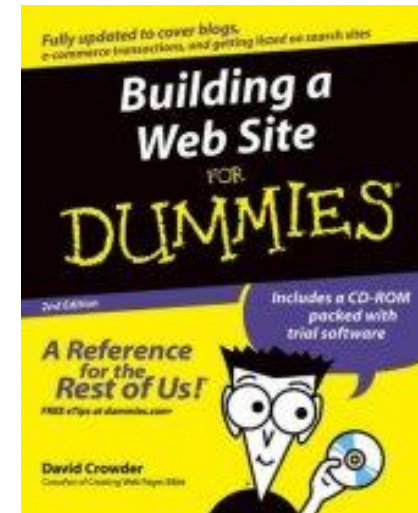
Computer Hardware & Software



Procurement through Surplus

# Web Site Testing

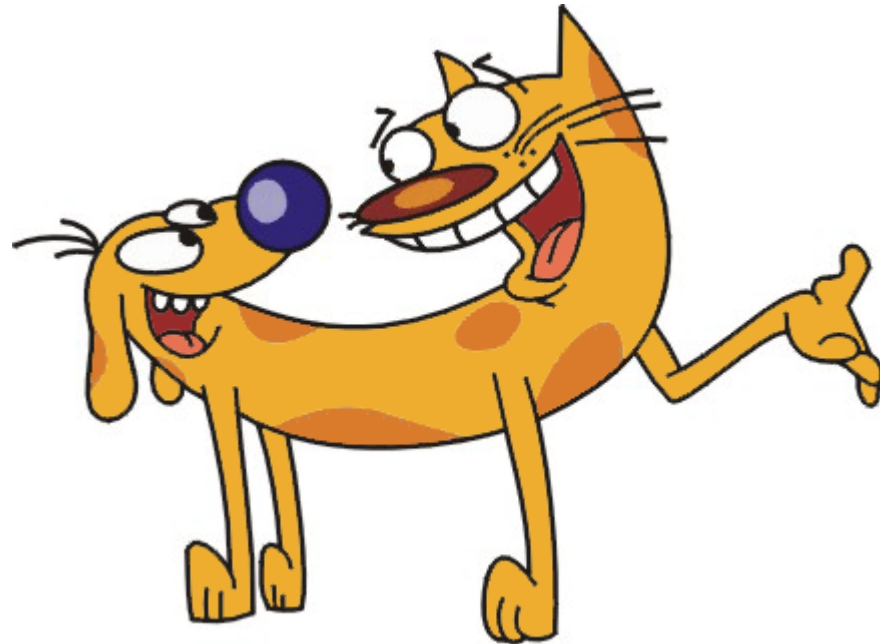
- ✓ University Relations Web Guidelines & Procedures
  - Web Development Best Practices
  - Content Recommendations
  - Templates
- ✓ Privacy Statement (Policy)
- ✓ Web Server & Application Security



# Reporting

**observations**

When Unexpected Results are Noted



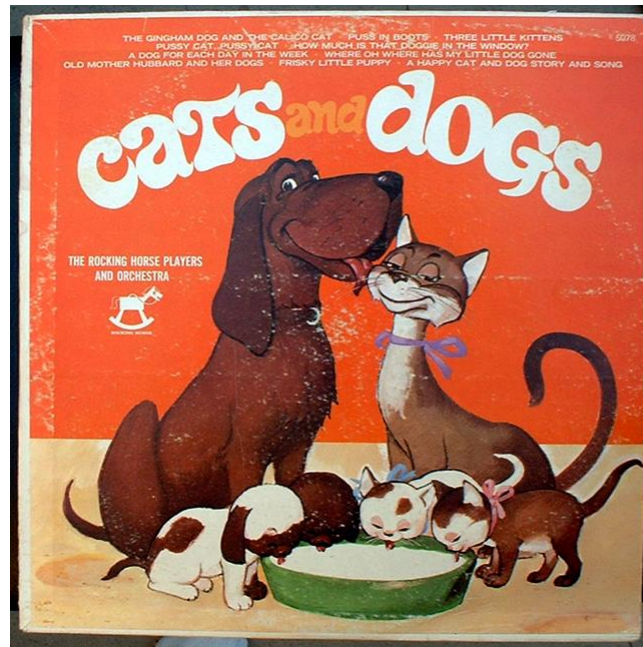
We Solicit Your Comments



# Reporting

recommendations

We May Recommend Opportunities

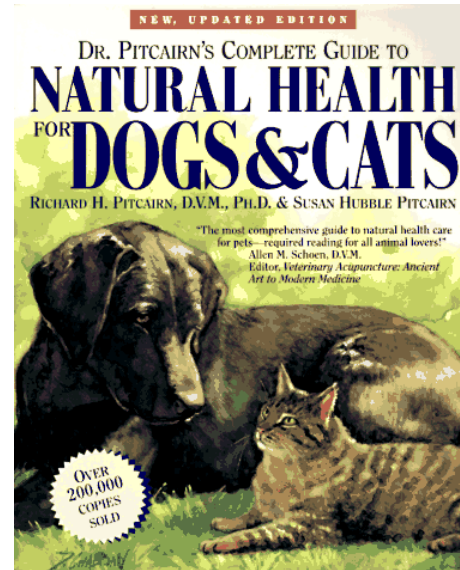


To Improve Your Controls

# Reporting

## management action plans

You Develop Plans, Schedules, and Priorities



To Implement Solutions



# Reporting

**findings**

A Final Report is Sent  
to  
The Board



# Reporting

**findings**

A Final Report is Sent  
to  
The Board



# Follow-up

- ✓ Follow-Up Actions are Based on Your “Management Action Plan”
- ✓ Progress is Monitored
- ✓ Some Re-Testing May be Necessary
- ✓ Board of Visitors is Updated
- ✓ Audit is closed

# Common Audit Observations

Weak Security Settings



Windows Operating System

# Common Audit Observations

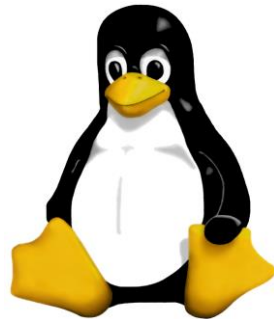
Missing Security Patches



Operating Systems

Applications

Databases



# Common Audit Observations

Misconfigured Anti-Malware Tools



Out-of-Date Threat Signatures  
Scans Not Scheduled

# Common Audit Observations

Inadequate Access Controls



Weak Passwords & File Permissions



# Common Audit Observations

Open Communication Ports

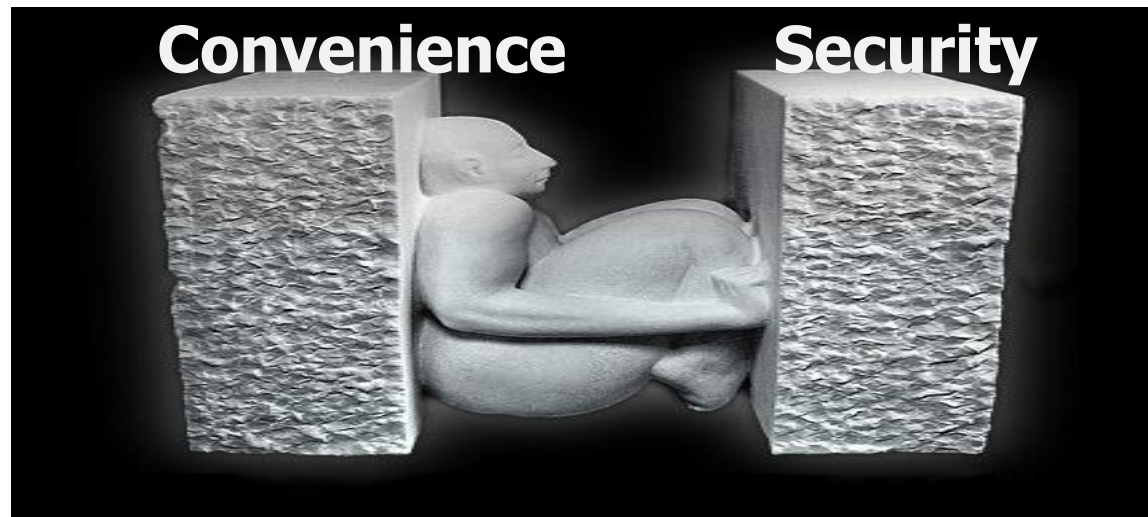


The Hacker's Point of Entry



# Common Audit Observations

“The System Administrator’s Dilemma”



How Much Risk is Senior Management Willing to Accept?

# So What Should We DO?

- ✓ Harden Security Settings
- ✓ Keep Everything Patched
- ✓ Install and Use Anti-Malware Tools
- ✓ Enforce Strong Passwords
- ✓ Close or Filter Communication Ports
- ✓ Test Your Systems
- ✓ Support Your System Administrator!

# YOUR OPINION?



# Quiz (15 min)