CONTINUUM WORLDWIDE℠

Benchmarking Information Security

Bill Dixon

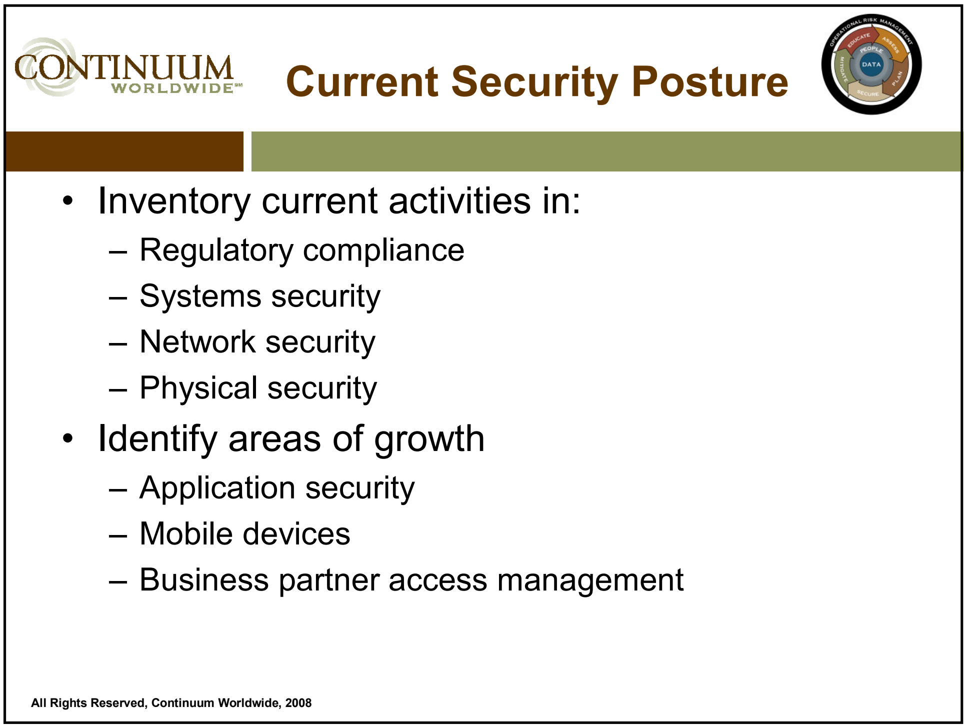
Nebraska CERT Conference

August 22, 2008

CONTINUUM WORLDWIDE℠

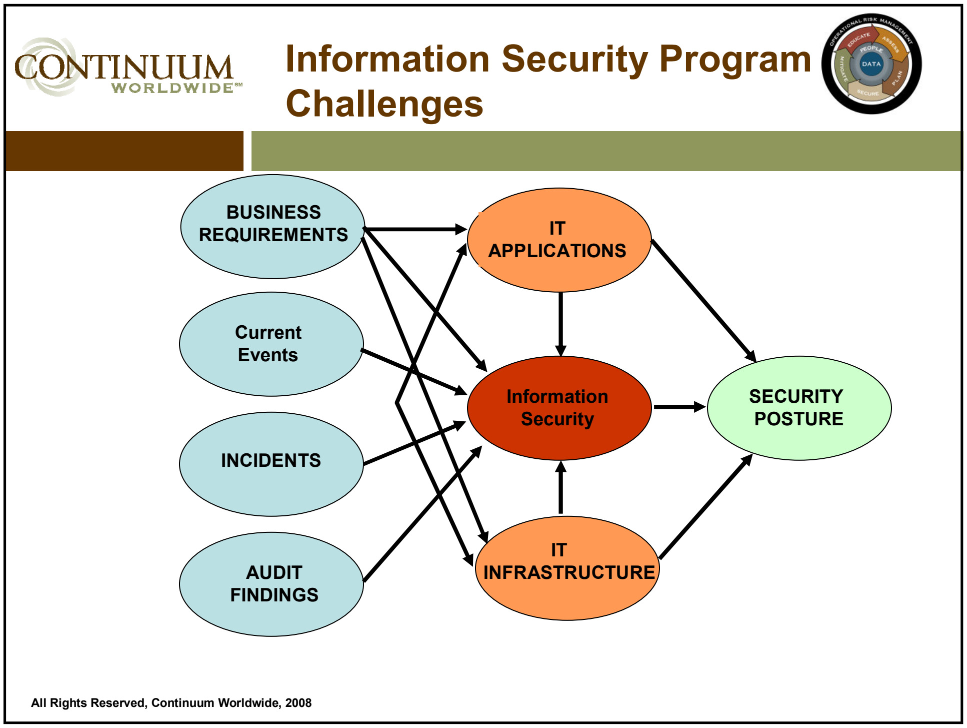
Agenda

- Information Security Management Challenges
- Establishing Frameworks
- Metrics
- Benchmarking
- Benchmark Scenario
- Discussion
- Questions



Current Security Posture

- Inventory current activities in:
  - Regulatory compliance
  - Systems security
  - Network security
  - Physical security
- Identify areas of growth
  - Application security
  - Mobile devices
  - Business partner access management



Information Security Program Challenges

BUSINESS REQUIREMENTS

Current Events

INCIDENTS

AUDIT FINDINGS

IT APPLICATIONS

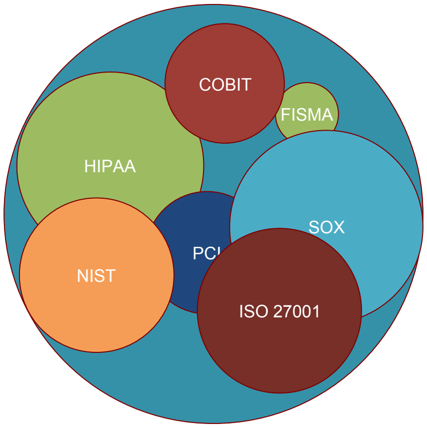
Information Security

IT INFRASTRUCTURE

SECURITY POSTURE

Information Security Program Framework

- The element(s) that guide the Information Security Program
- Framework examples
  - COSO
    - **COBIT**
  - ISO Standards
    - **ISO 17799, 27001**
  - NIST Standards
  - Industry Specific
    - **HIPAA, FISMA, PCI**



All Rights Reserved, Continuum Worldwide, 2008

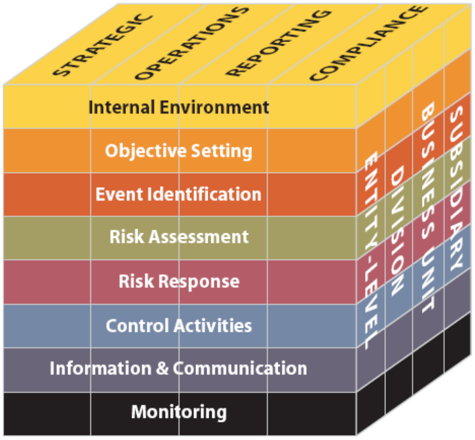
Example Information Security Framework

•Cross-Functional

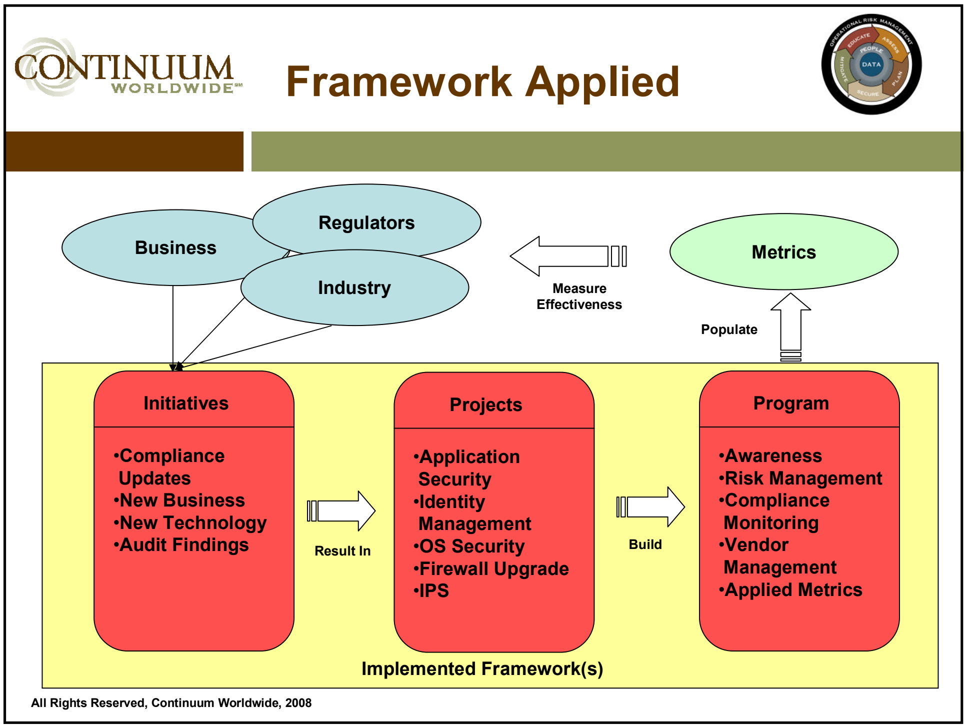
•Understandable

•Extensible

Multiple frameworks may apply



All Rights Reserved, Continuum Worldwide, 2008



CONTINUUM WORLDWIDE℠

Framework Applied

Business

Regulators

Industry

Measure Effectiveness

Metrics

Populate

Initiatives

- Compliance Updates
- New Business
- New Technology
- Audit Findings

Result In

Projects

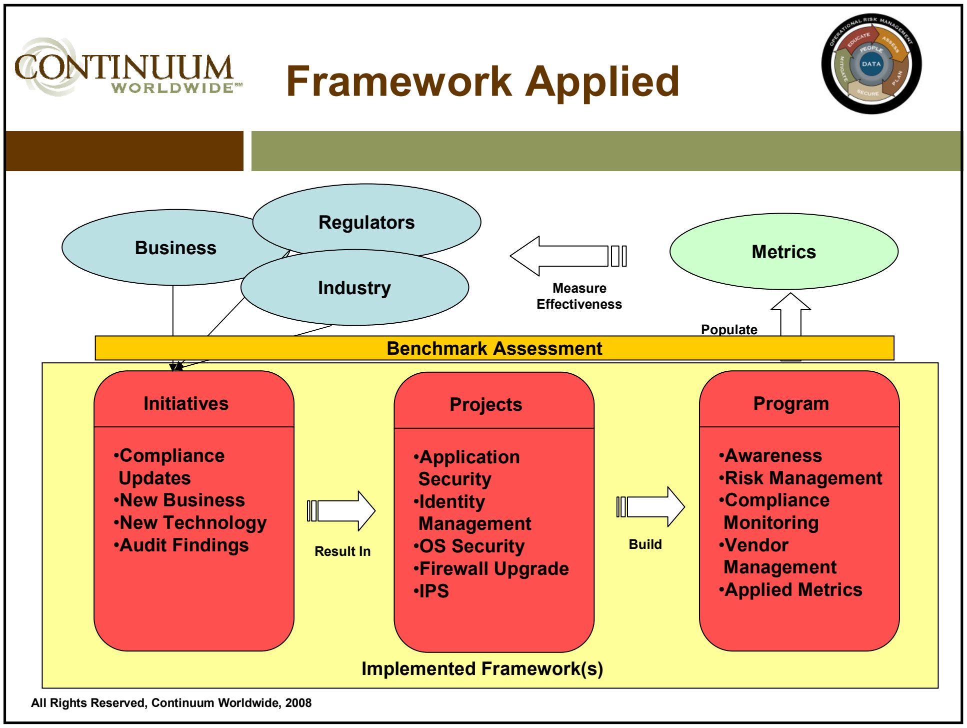
- Application Security
- Identity Management
- OS Security
- Firewall Upgrade
- IPS

Build

Program

- Awareness
- Risk Management
- Compliance Monitoring
- Vendor Management
- Applied Metrics

Implemented Framework(s)



CONTINUUM WORLDWIDE℠

Framework Applied

Business

Regulators

Industry

Measure Effectiveness

Metrics

Populate

Benchmark Assessment

Initiatives

- Compliance Updates
- New Business
- New Technology
- Audit Findings

Result In

Projects

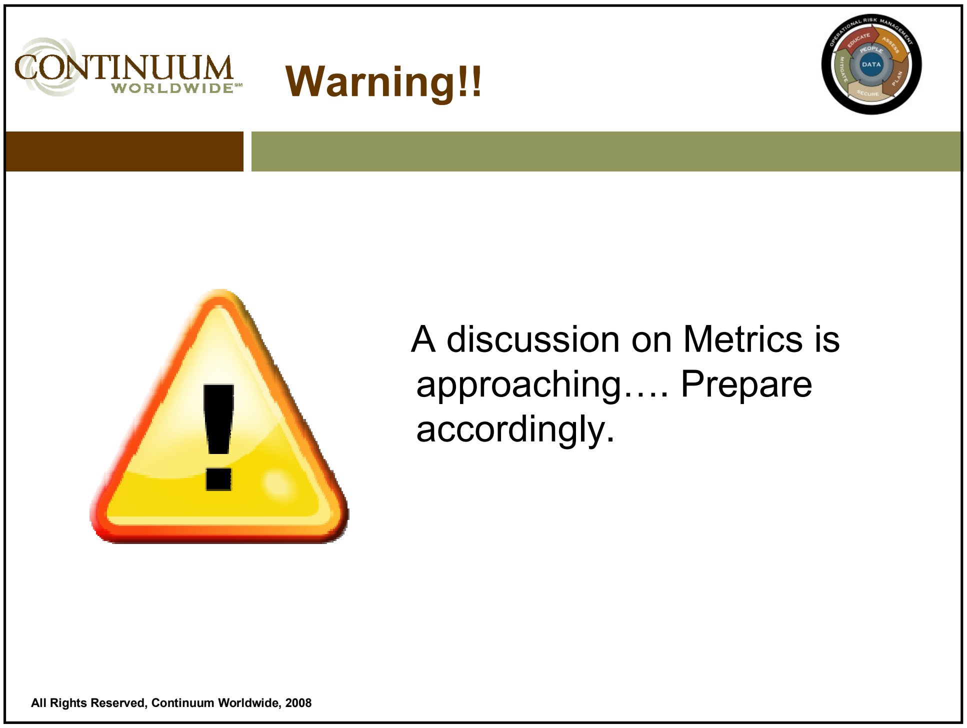
- Application Security
- Identity Management
- OS Security
- Firewall Upgrade
- IPS

Build

Program

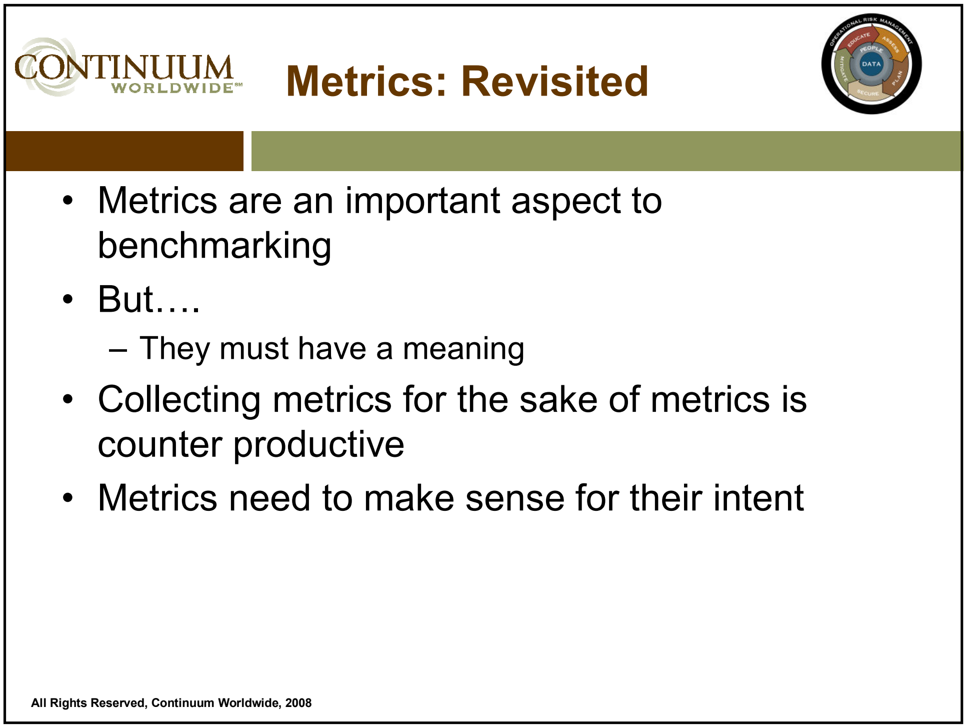
- Awareness
- Risk Management
- Compliance Monitoring
- Vendor Management
- Applied Metrics

Implemented Framework(s)



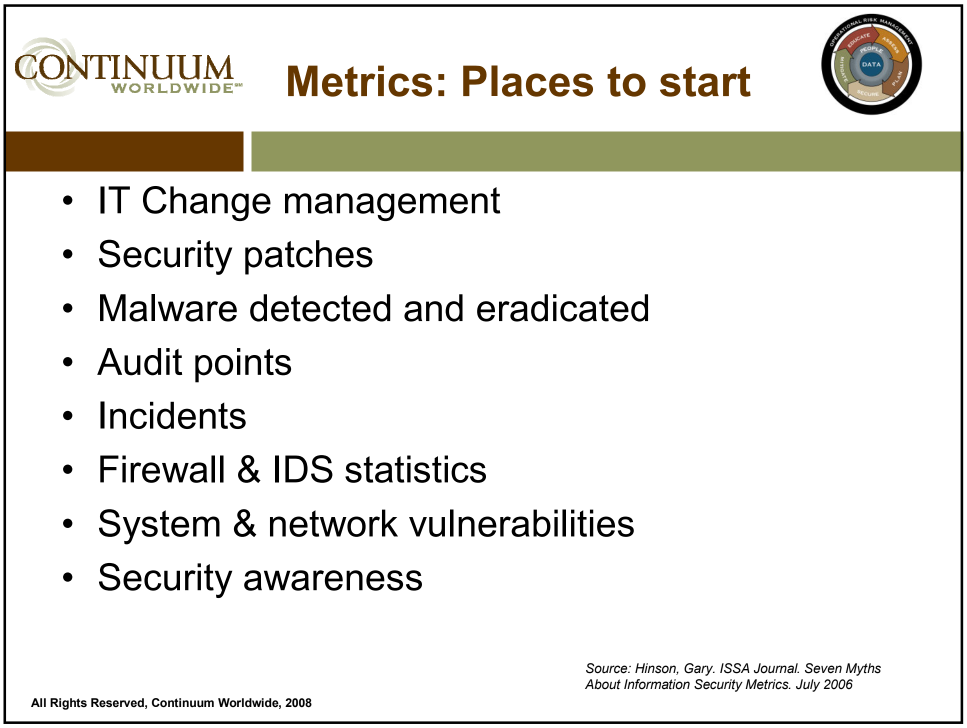
Warning!!

A discussion on Metrics is approaching…. Prepare accordingly.



Metrics: Revisited

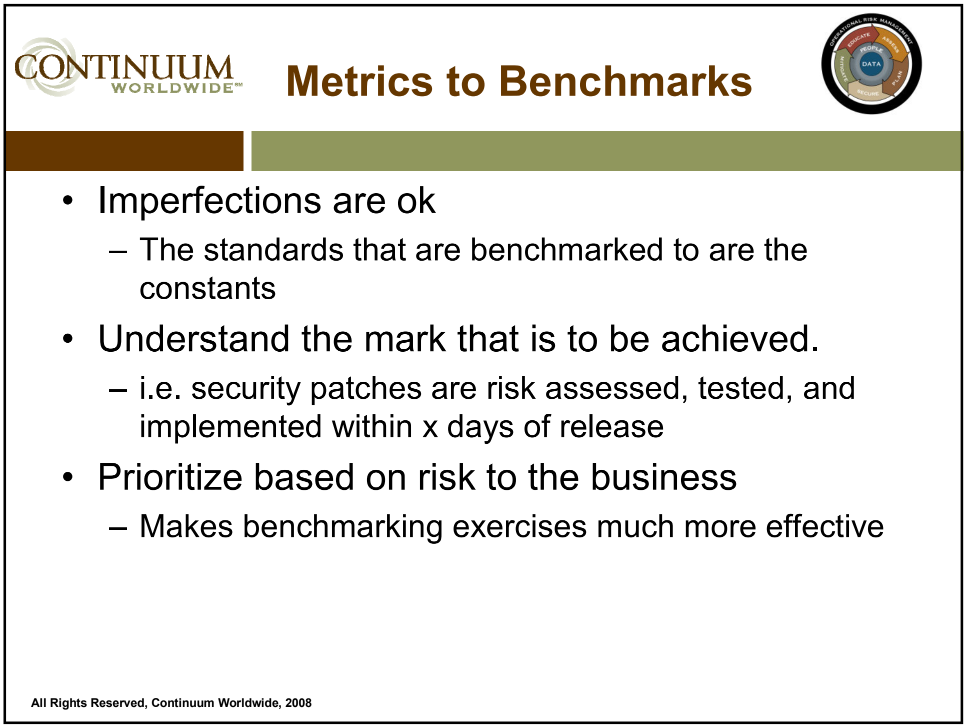
- Metrics are an important aspect to benchmarking
- But….
  - They must have a meaning
- Collecting metrics for the sake of metrics is counter productive
- Metrics need to make sense for their intent



Metrics: Places to start

- IT Change management
- Security patches
- Malware detected and eradicated
- Audit points
- Incidents
- Firewall & IDS statistics
- System & network vulnerabilities
- Security awareness

Source: Hinson, Gary. ISSA Journal. Seven Myths About Information Security Metrics. July 2006



Metrics to Benchmarks

- Imperfections are ok
  - The standards that are benchmarked to are the constants
- Understand the mark that is to be achieved.
  - i.e. security patches are risk assessed, tested, and implemented within x days of release
- Prioritize based on risk to the business
  - Makes benchmarking exercises much more effective

Benchmarking

- Benchmarking an Information Security Program enables:
  - The prioritization of initiatives
  - Realization of budget requirements based on industry
  - Establish metrics for success

Management Controls

- Infosec Program
- Infosec Organization
- Infosec Planning
- Policy Management
- Risk Management
- Monitoring the Program
- Review of Security Controls

Operational Controls

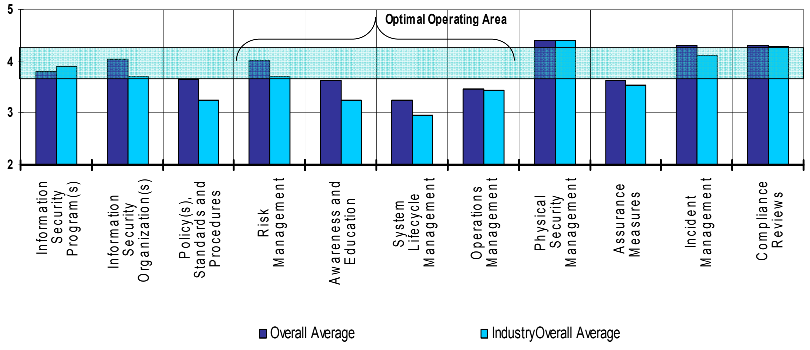
- Lifecycle Management
- HW/SW Maintenance
- Personnel Security
- Physical & Environmental Protection
- Production Input/Output Controls
- Data Classification
- Awareness & Training
- Incident Response

Technical Controls

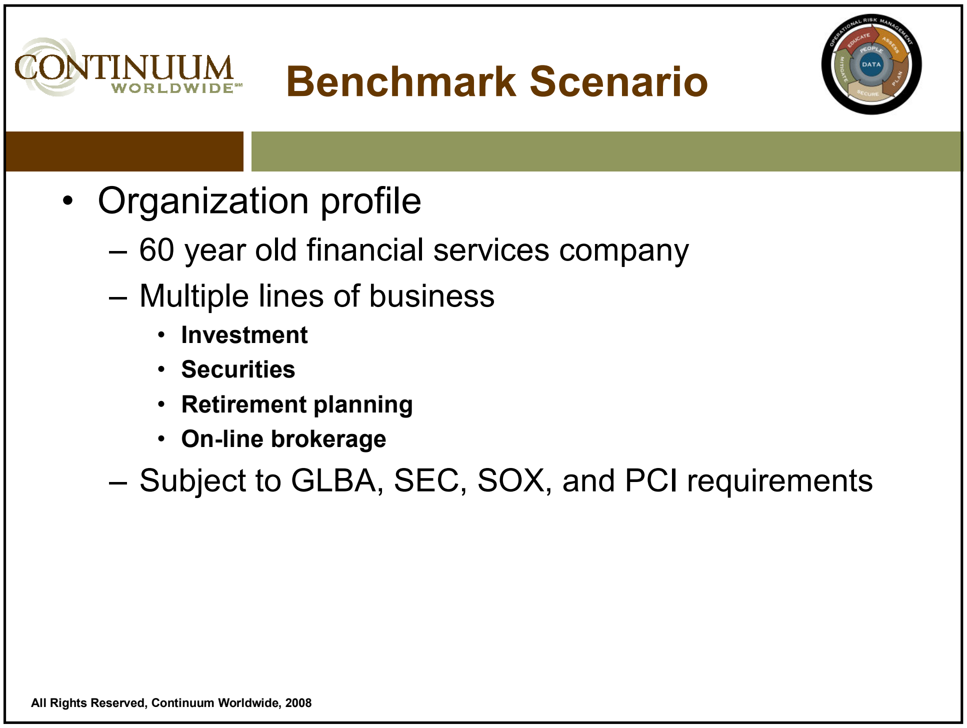
- Identification, Authentication, & Access Control
- Network Security Architecture
- Technical Vulnerability Management

All Rights Reserved, Continuum Worldwide, 2008

Sample Benchmarking Results



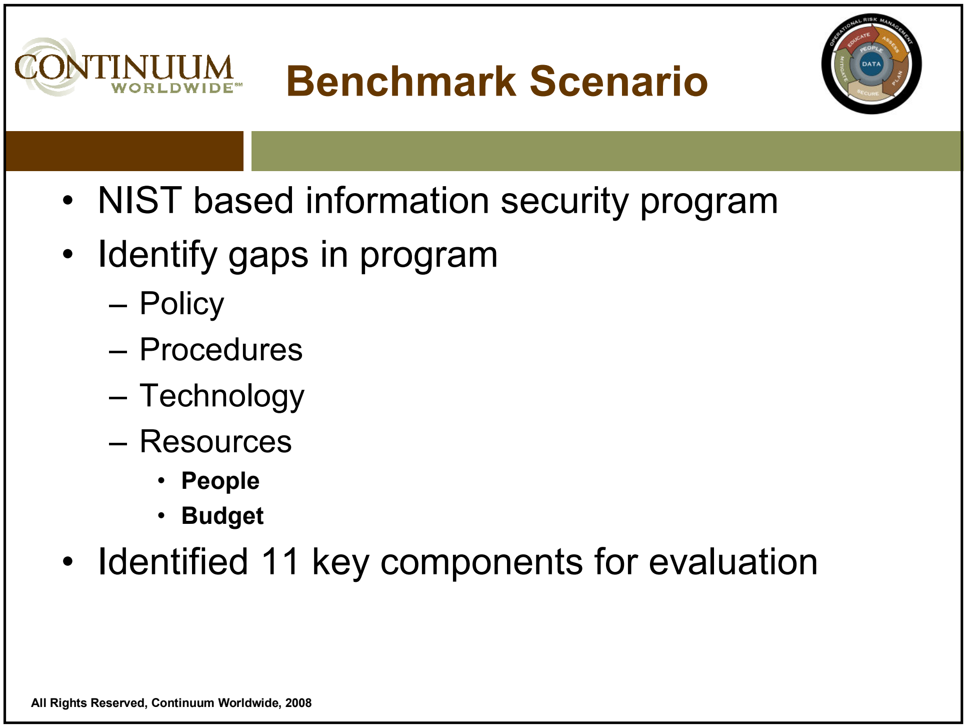
All Rights Reserved, Continuum Worldwide, 2008



CONTINUUM WORLDWIDE℠

Benchmark Scenario

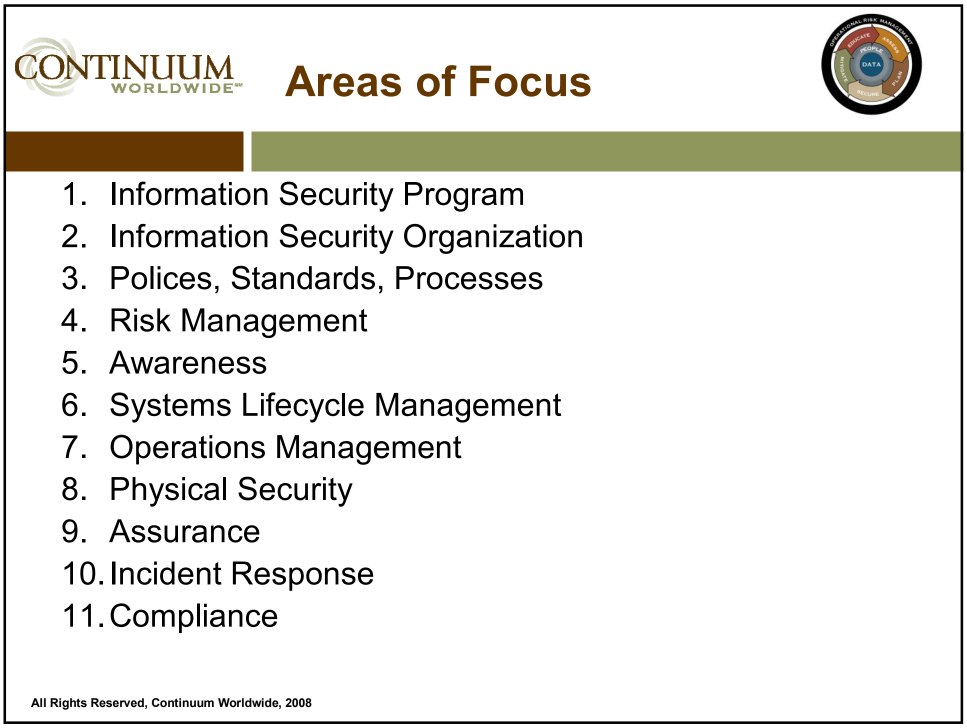
- Organization profile
  - 60 year old financial services company
  - Multiple lines of business
    - **Investment**
    - **Securities**
    - **Retirement planning**
    - **On-line brokerage**
  - Subject to GLBA, SEC, SOX, and PCI requirements



CONTINUUM WORLDWIDE℠

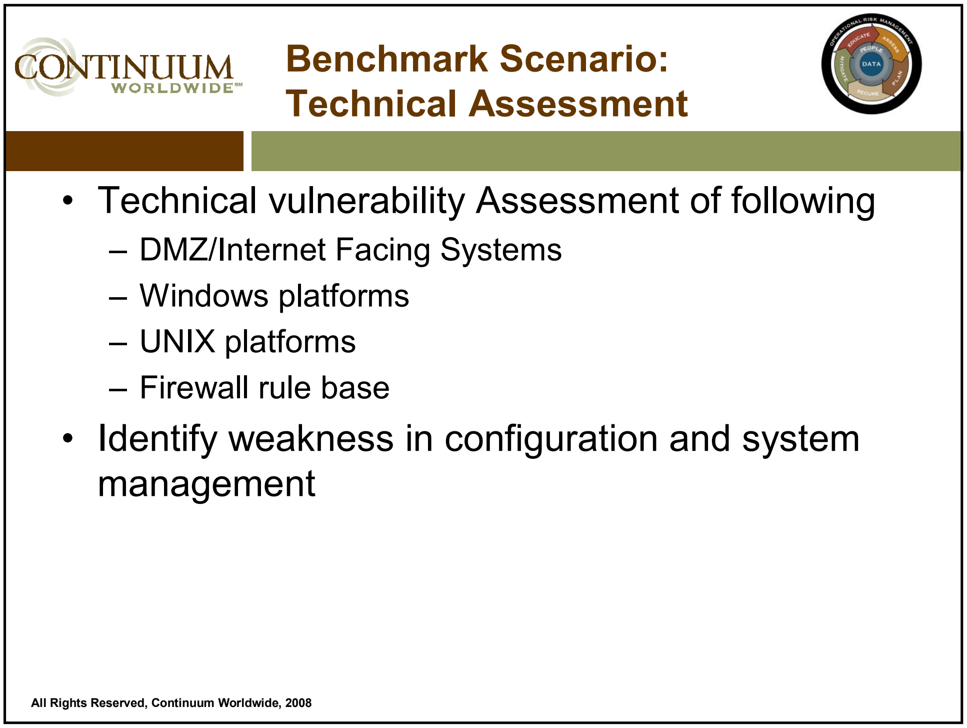
Benchmark Scenario

- NIST based information security program
- Identify gaps in program
  - Policy
  - Procedures
  - Technology
  - Resources
    - **People**
    - **Budget**
- Identified 11 key components for evaluation



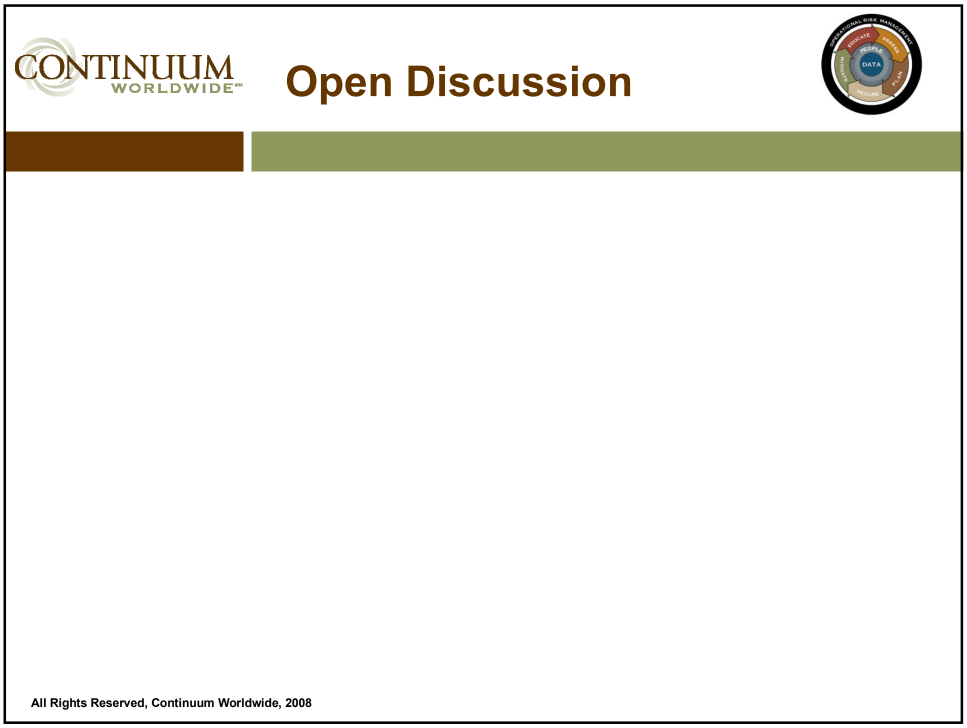
Areas of Focus

1. Information Security Program
2. Information Security Organization
3. Polices, Standards, Processes
4. Risk Management
5. Awareness
6. Systems Lifecycle Management
7. Operations Management
8. Physical Security
9. Assurance
10. Incident Response
11. Compliance

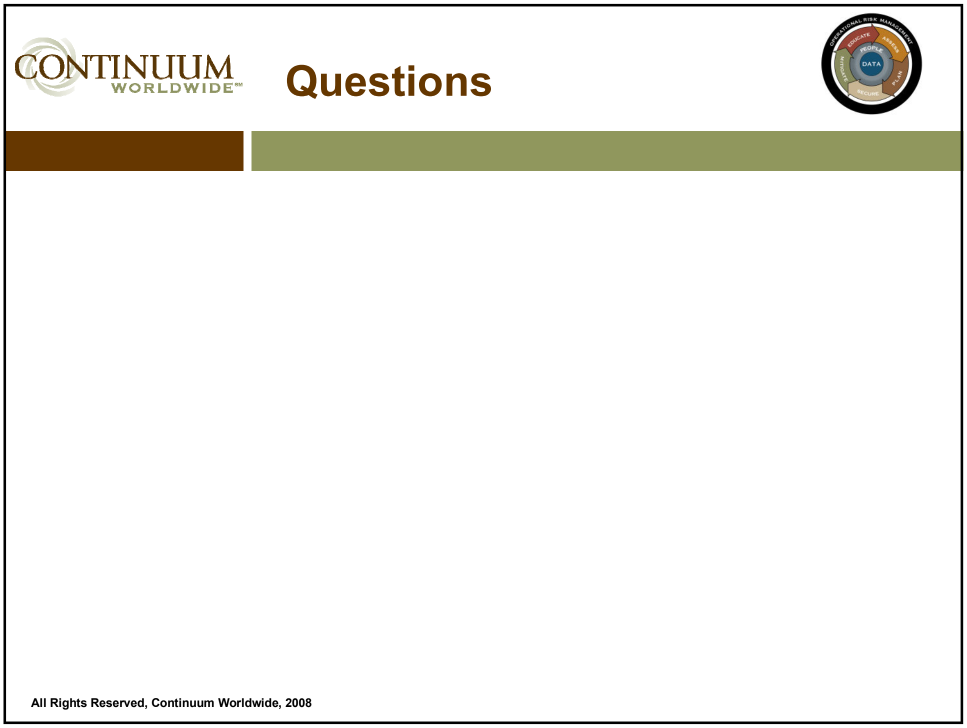


Benchmark Scenario: Technical Assessment

- Technical vulnerability Assessment of following
  - DMZ/Internet Facing Systems
  - Windows platforms
  - UNIX platforms
  - Firewall rule base
- Identify weakness in configuration and system management



Open Discussion



Questions

CONTINUUM WORLDWIDE℠