



Improving Your Internal Assessment Program



The world is your workplace
connect with **Getronics**.



September 20, 2006



Jean Silbaugh, CISSP

- You know you're from Pittsburgh when:
 - "Hey Yens" is your traditional greeting.
 - You own more Terrible Towels than bath towels.
 - Where Opening day of Deer Season is an unofficial state holiday.



Russ Hailey, CISSP

You know you're from Kansas when:

- Your closest neighbor is more than a mile away, and you can still see him from your front porch.
- Traffic congestion is ten cars waiting to pass a combine on the highway.
- A shotgun is your idea of instant messaging.



Goals

- Be more effective
- Become more efficient

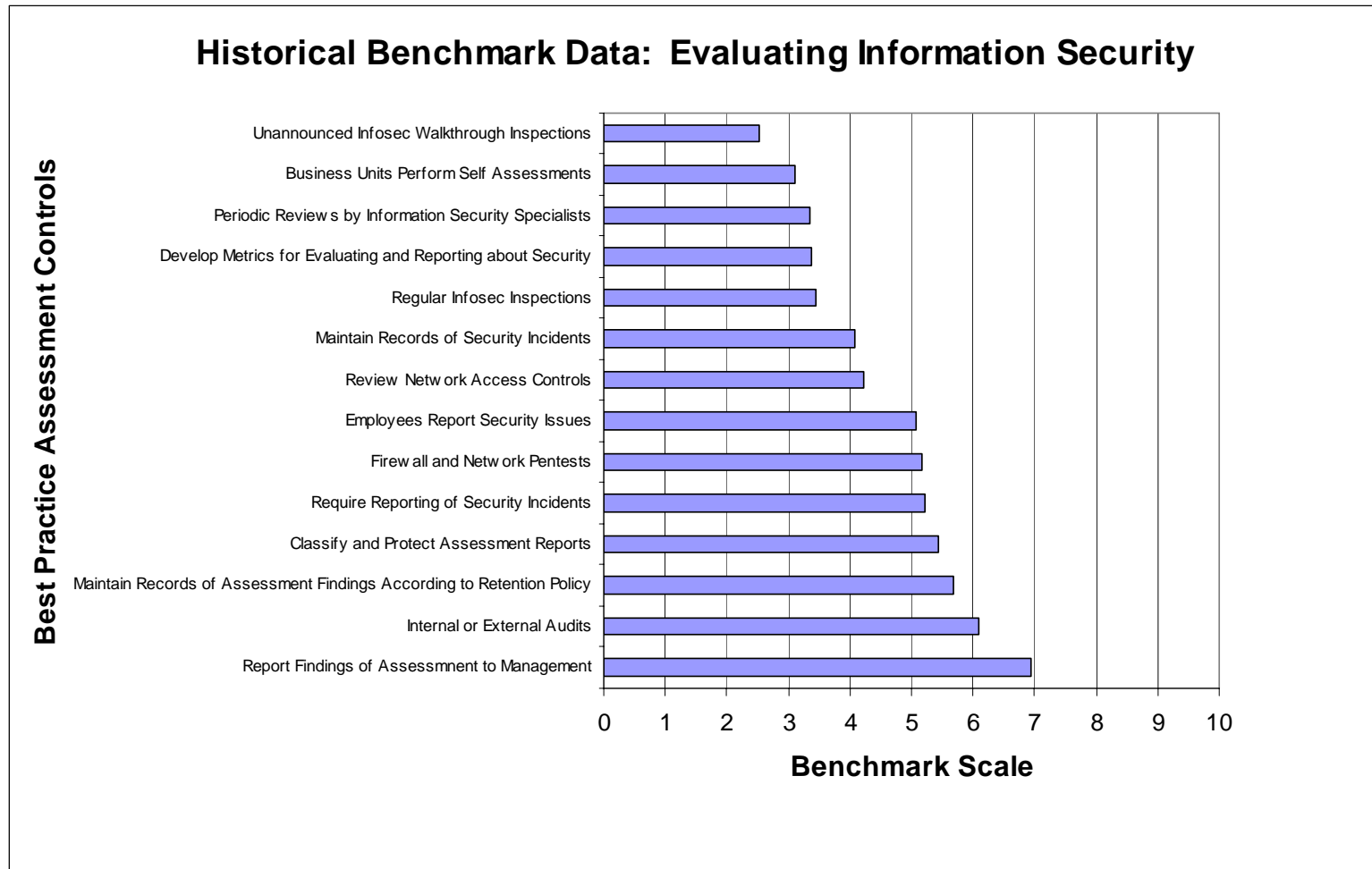
What are the Challenges for Internal Assessments

- Personnel
 - Bandwidth
 - Expertise
 - Experience
- Tools
 - Budget
 - Complexity
- Politics
- Compliance

What's the Problem? (Opinion)

- Organizations are increasingly dependent on external evaluations
- Internal evaluations lack some of the (perceived) sophistication of external evaluations
- Internal assessments are less likely to be grounded in consistent metrics
- Internal efforts are not as likely to employ rigorous methodologies

What's the Problem?





Five steps to effective and efficient internal assessments

1. Adopt a Process Maturity Framework
2. Select an Appropriate Assessment Strategy
3. Document a Security Control Catalog
4. Combine the Control Catalog and the PMF
5. Map Security Controls to Standards and Compliance Frameworks

Adopt a Process Maturity Framework

Framework Types

- ITIL
- Gartner
- NIST
- Getronics

Adopt a Process Maturity Framework

Process Maturity Frameworks - Summary

Level	ITIL	Gartner	Getronics (due care)
5	Optimized	Optimal	Audited by highly trained professionals Int. and ext. assessments as needed Audit and assessments are acted upon
4	Predictable	Managed	Audit/compliance process in place Management responds to reg. reports
3	Standardized	Proactive	Documented security control catalog Assessment personnel trained
2	Repeatable	Reactive	Unofficial processes and procedures Occasional assessments will occur
1	Initial	Chaotic	Few assessments, if any Security program undocumented Security dependent on a few individuals

Select an Appropriate Assessment Strategy

Standard Assessments

- Technical Audience
 - Network Penetration Testing
 - Application Security Assessment
 - Vulnerability Assessment
 - Wireless Security Assessment
- IT or Business Unit Audience
 - Risk Assessment
 - IT Security Scorecard
 - Personnel Security Review
- Corporate/Executive Audience
 - Benchmark
 - Gap Analysis
 - Executive Dashboard
 - Compliance Assessment

Select an Appropriate Assessment Strategy

Maturity Level	ITIL Description	Typical Focus	Assessment Type
5	Optimized	Corporate Strategy	Benchmark, Gap Analysis
4	Predictable	Aligning Business/IT	Scorecard, Dashboard
3	Standardized	Customer, Service Level	Risk, Personnel, Application
2	Repeatable	Products and Services	Pentest, VA, Wireless,
1	Initial	Technology	None

Document a Security Control Catalog

- NIST 800-53
- ISO 17799
- Add as needed
- Organize in a meaningful way
- Assign a unique ID number to each control

Document a Security Control Catalog

Example of Control Catalog Table of Contents

- Security Policy
- Organization of Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition, Development and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

Combine the Control Catalog and the PMF

Control Catalog	ITIL Process Maturity Framework				
	1	2	3	4	5
Security Policy					
Organization of Information Security					
Asset Management					
Human Resources Security					
Physical and Environmental Security					
Communications and Operations Management					
Access Control					
Information Systems Acquisition, Development and Maintenance					
Information Security Incident Management					
Business Continuity Management					
Compliance					

Combine the Control Catalog and PMF

- Creates outline for summary data
- Surveys are simple format for data collection
- Average the data across each control family
- Illustrate high level graph or scorecard to managers
- Illustrate more detailed charts to those responsible for the controls

Map Standards/Compliance to Controls

- Each control has a number (M.1.1.2)
- In database or other tool, cross-reference each control with appropriate standard or regulation that is satisfied
- Do so by giving each control additional reference numbers:
 - MyOrganization M.1.1.2
 - ISO 17799 I.1.1.2
 - Sarbox S.1.1.1
 - HIPAA H.2.1.2
- Net effect is that you can answer the question, "How compliant are we?"



Map Standards/Compliance to Controls

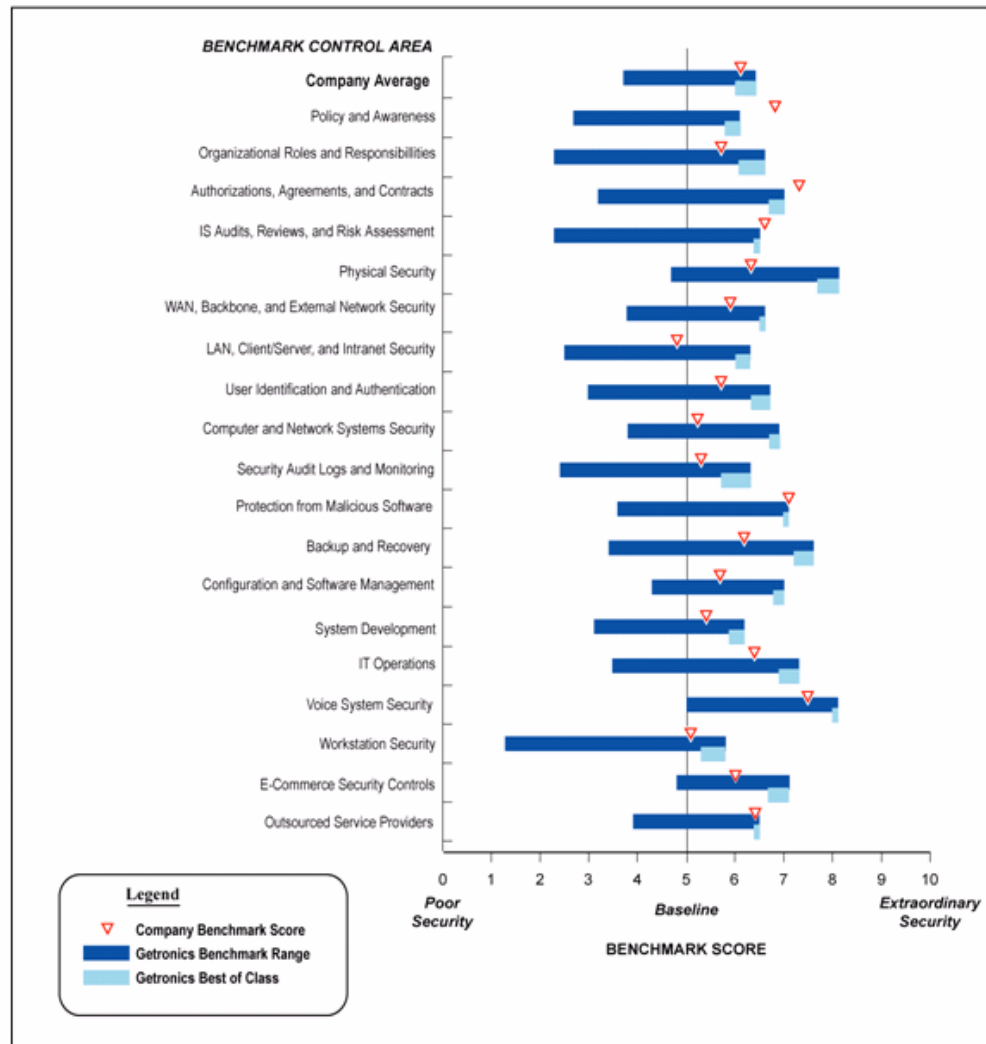
Mapping Produces Efficiency

- Each assessment has the potential for multiple reports
- One report (or appendix) for each compliance requirement and/or standard that is tracked within the organization
- Reduces the human effort and increases the efficiency of internal assessments

Map Standards/Compliance to Controls Example

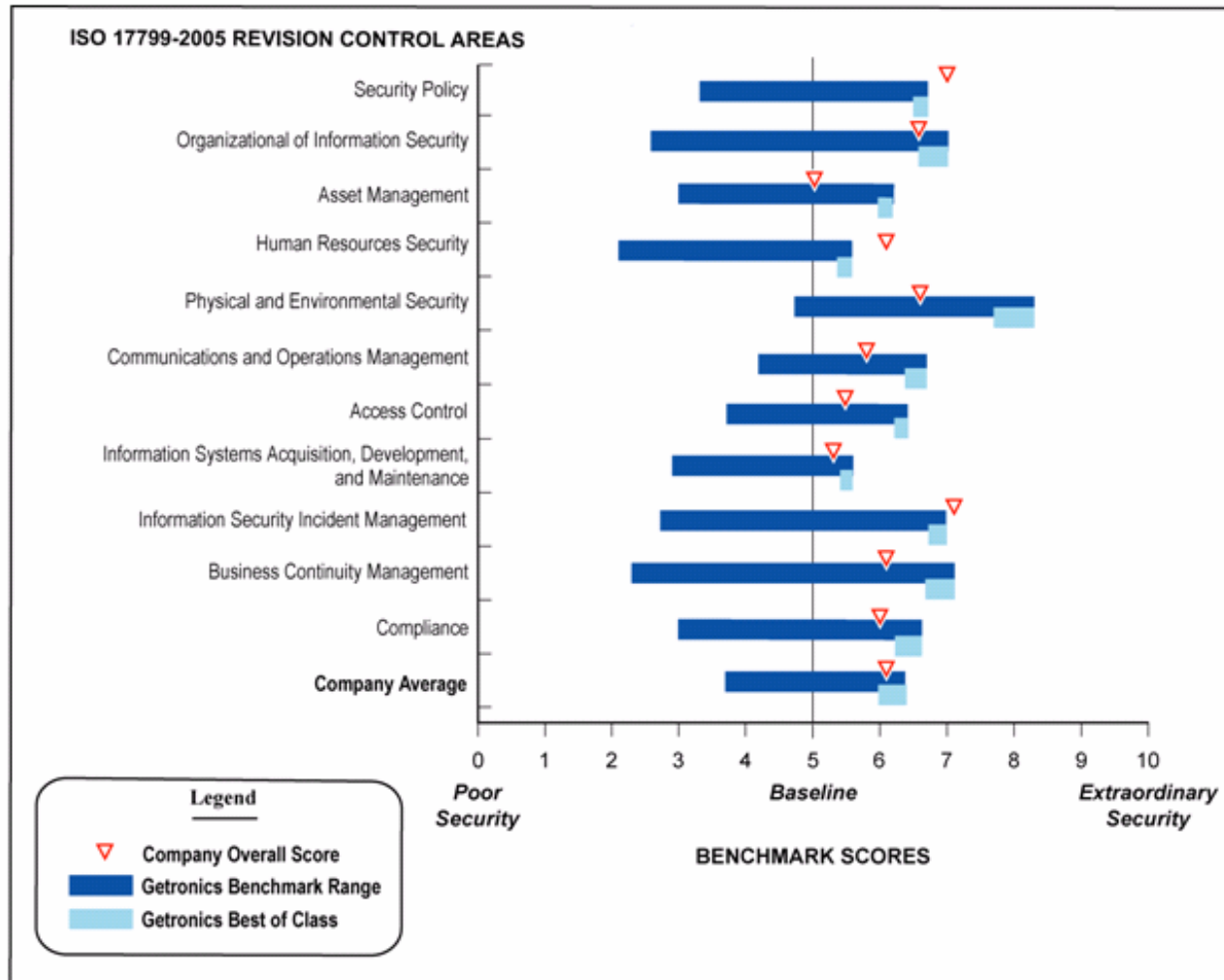
- An organization is ready to evaluate its security controls
- Uses ISO 17799 as its standard
- Required to comply with HIPAA
- Desires comparison to peer organizations
- Being efficient, this calls for a single benchmark

Map Standards/Compliance to Controls Information Security Program Benchmark



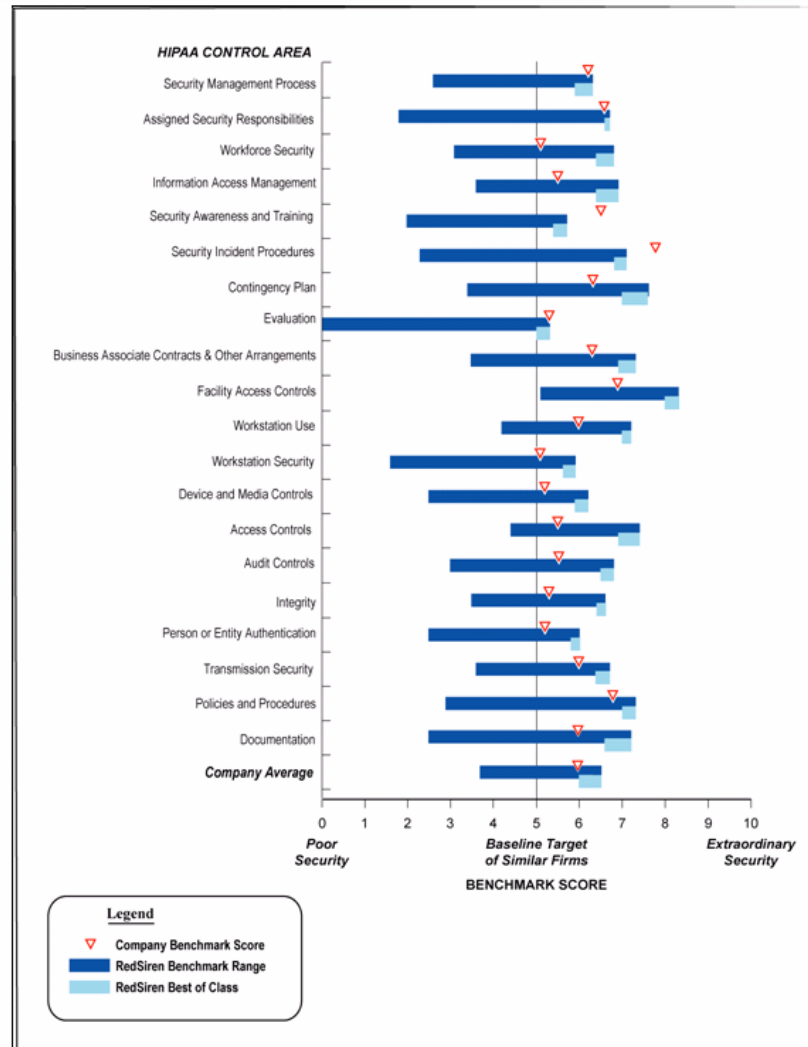
Map Standards/Compliance to Controls

ISO 17799 Benchmark



Map Standards/Compliance to Controls

HIPAA Information Security Benchmark



Thank you

▶ The world is **your** workplace.
Connect with **Getronics**.

Getronics
ICT SOLUTIONS AND SERVICES
www.getronics.com