

Implications of Recent Legal Changes on System Management and Information Assurance

Thursday, September 29, 2005

Robert Gezelter Software Consultant
35 – 20 167th Street, Suite 215
Flushing, New York 11358 – 1731
United States of America

+1 (718) 463 1079
gezelter@rlgsc.com
<http://www.rlgsc.com>

Pre-History

- Real Records did not reside on computers

1985

- NCSC “Orange Book”
- Military/Defense Orientation
- Perceived as irrelevant in the commercial world

2005 – Access Controls get serious

- Health Insurance Portability and Accountability Act of 1996
- Sarbenes-Oxley Act of 2002
- various SEC regulations
- miscellaneous other federal, state, and foreign regulations

The Trend is Toward Accountability & Integrity

- privacy
- disclosure controls
- auditability
- process, not detailed specifics of each law

What is the cumulative result?

- the civilian, non-defense world is now has its own requirements for “Orange Book” security
 - credentials
 - access control
 - auditing and alarms
 - clearance processes

Why process. not details?

- Details will inevitably change
- Processes must conform to detailed requirements, but are expensive to change when details change

What is the change from an IT perspective?

- Computerized records ARE the records
- Unaccounted for changes to data is forgery
- Change in cultural mindset
- Limitations on privilege/access
- the realities of audit controls
- “two-person rule”
- “Trusted Computing Base”

Management Challenges

- Limiting privileged access
- Users restricted to authorized applications
- Application-based controls do not meet the test
- Use of host system authorization controls

The IT System as Citadel

- must be a secure platform
- host authenticated credentials
- host controlled data access
- audited access to data

Ethics

- Curiosity
- Alteration
- “Rules of Engagement” (ROE)
- legal processes
 - internal – disciplinary
 - regulatory
 - civil
 - criminal

Legal Responsibilities

- Forgery
- Theft
- Evidence tampering
- Obstruction of justice
- Filing a false declaration
- other crimes

Questions?

Robert Gezelter Software Consultant
35 – 20 167th Street, Suite 215
Flushing, New York 11358 – 1731
United States of America

Session Notes & Materials:

<http://www.rlgsc.com/ieee/vermont/2005-09/index.html>

+1 (718) 463 1079
gezelter@rlgsc.com
<http://www.rlgsc.com>