

The Technical Aspects of Auditing

The value proposition of advancing the auditors technical knowledge

Who am I?

- Michigan State University – 9 years
 - System Engineering
 - Network Engineering
 - Security Engineering
 - Payment Card / ACH Processing
 - Information Assurance
- Perrigo Company – 1 ½ Years
 - Information Security Manager
- SANS Institute – 2 years
 - Local Mentor

Alphabet Soup

- Certified Information Systems Auditor (CISA)
- . . . Placeholder . . .
- Certified Information Systems Security Professional (CISSP)
- GIAC Systems and Network Auditor (GSNA)
- GIAC Certified Incident Handler (GCIH)
- Microsoft Certified Systems Engineer (MCSE)

Agenda

- Information Security functions and responsibility alignment
- Changing traditional views of audit
- Learning a new Skill
- War stories

Information Security Functions (Traditional)

Governance
Administration
Operations
Assurance

Information Technology	HR	Legal	Compliance	Internal Audit	External Audit
------------------------	----	-------	------------	----------------	----------------

A	I	I	I	I	
A	I		I	I	
A			I	I	
I			I	A	I

Finding Value - Governance

- Policies are the foundation of governance
- Top-down support is a pre-requisite.
- Internal Audit should be a key player in the policy development process.
 - Objectivity isn't spoiled, rather it's enhanced.
 - Creates first-hand intimate knowledge of the policy structure that results in a effective audit.

Finding Value - Governance

- There must be a collaborative effort for creating / maintaining policies.
- Board of Directors own governance of the organization.
- Governance is implemented by HR & Legal.

Finding Value - Administration

- Role-based access control can drive most administration tasks.
- Administration of Security is a partnership between Information Technology and Human Resources.

Finding Value - Operations

- Clearly defined as an Information Technology Function.
- Organizational maturity defines where operations are aligned.
- Organizational alignment of Information Security function can be a key indicator of maturity.

Finding Value - Assurance

- Traditionally the realm of auditors and auditors only.
- Assurance performed by multiple areas of the organization promotes overall security.
- Assurance within and Information Security group can extend the auditors function to achieve higher results.

Information Security Functions (The Value)

	Information Security	Information Technology	HR	Legal	Compliance	Internal Audit	External Audit
Governance	A	C	R	R		C	I
Administration	I	A	C			I	I
Operations	I	A				I	I
Assurance	R	C			R	A	I

The Traditional IT View of Audit

- Looking for problems.
- Promoting themselves by making us look bad.
- Always “ratting” us out to management.
- Unknowledgeable.
- We can always baffle them with BS.
- They don’t understand what its like.

Altering the Traditional View

- Increase technical knowledge of auditors.
- Increase organizational understanding of audit function.
- Utilize audit programs as “the bad guy.”
- Promote assurance roles within areas other than audit.

War Stories

- VPN to nowhere
- The little green man under my desk
- Tracing malicious email
- It's raining auditors!

SANS Institute

- SANS + Training Program for the CISSP® Certification Exam
 - April 1 to May 1, Tuesday & Thursday Evenings
- 50% discount on all @Home courses for ISACA members / colleagues
 - Includes CISA Prep