ISACA
Serving IT Governance Professionals
San Francisco Chapter

IT Audit Vs IT Security

Harshul Joshi
CISSP, CISA, CISM
Director, Information Technology Services
hjoshi@cbiz.com
408-795-3597

Audit

- Criticize
- Jack of all master of none
- Prior careers out of IT audit
- Never seen a TCP packet in their career
- Bible – Audit program

Security

- Complain
- Master of one
- Geeks
- Business ROI – what is that?
- My way or highway

No Seriously

- Audit
  - More breadth
  - Cross functional
- Security
  - Depth
  - IT focused

IT Audit

- Security
- Operations
- Change Management
- SDLC
- Policies and Procedures
- HR Aspect
- Compliance (PCI, SOX, GLBA)

IT Security

- Network layer (Firewalls, IDS, IPS)
- Application layer
- Web based (OWASP)
- Database
- Extensive use of Tools and Scripts
- Product specific (Cisco, Symantec, Checkpoint, Juniper)

So

- Security can be a subset of audit but with much less depth
- Both IT audit and security converge to provide overall IT governance
- Audit knows what to do and security know how to do
- Audit helps security gets budget

Let's take an example

- PCI – Flavor of the day
  - Requires security as well as process discipline to comply
  - Requires both auditors and security personal to be compliant

Where do we falter?

- Here is how an auditor will talk to a firewall specialist ---
  - Checklist based auditing
  - Lack of bigger picture from both sides
  - Same goal yet huge difference in opinion

Looking ahead – for Auditors

- Auditors will need to develop more depth in technology
- Cannot be just check list auditors
- Fundamentals are important
- Understand IT and Security team's limitation
- Realistic report writing

Looking ahead – for security

- Will be forced to be compliant with minimal jump in budget
- Can look to IT audit as a career switch
- Will need to self-discipline in terms of soft processes and procedures