



The Chartered Institute of
Public Finance & Accountancy

Key Information Security Issues for Internal Auditors

David Horn – 13th March 2011

What this presentation isn't.....



What this presentation is.....

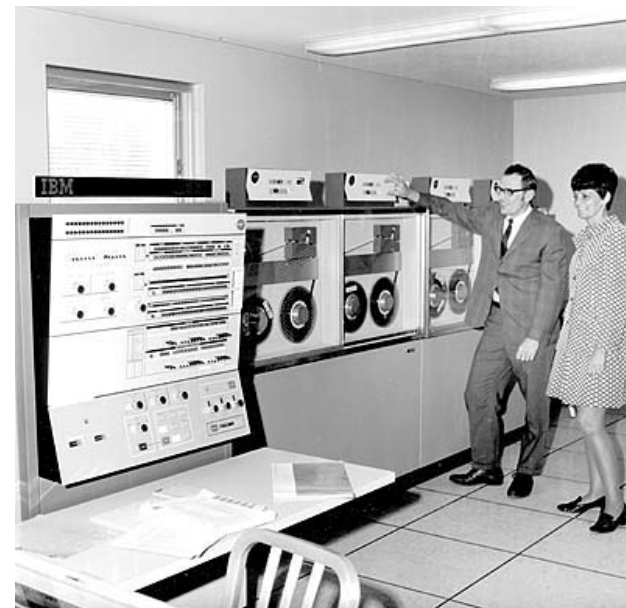




History:

The concept of I.T audits started back in the mid 1960's.

Since that time, IT auditing has gone through numerous changes, largely due to advances in technology and the incorporation of technology into business.



A Qualified Auditor

Only a qualified person/firm should be able to act as an auditor. Ideally a member (individual or a firm) of a recognised supervisory body e.g.CIPFA, IIA or ACCA etc and allowed by the rules of that body to be an auditor.

The Auditor's Main Objective

An information security audit is a systematic, measurable technical assessment of how the organisation's security policy is employed at a specific site.

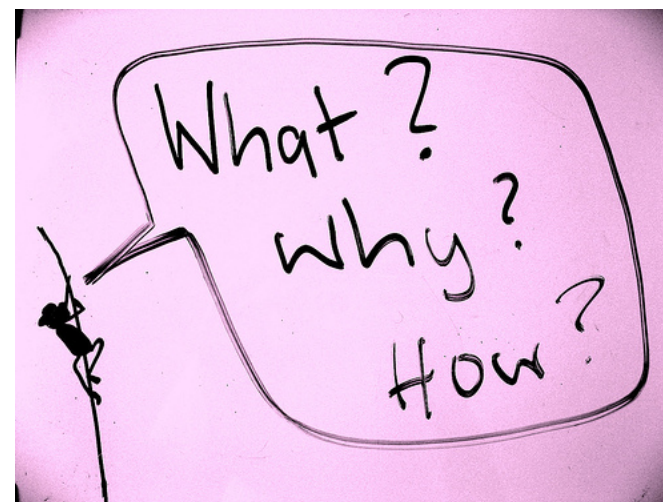
Unqualified Audit opinion

An auditor needs to be qualified to carry out an audit in order to give an unqualified opinion



What?

Physical security, logical security



Why?

Best practice, regulation, legal.

How?

Study & evaluate, test & evaluate

What?

Interview, vulnerability assessments, examination of O/S settings, analysis of network shares and historical data.

How security policies are used.



Audit logs for data

Encryption

Patching

Password strength

Configuration

Change Control

Asset register and control

Regular review of logs

Backup – stored, access, restored

Unnecessary applications removed

DR/BCP Plan - tested

Define the Scope

Who should carry out the audit?

Qualifications – ongoing?

CISA*, CIA, CAP, CCP, CISSP, CISM, CPA, CCA,
GSNA*, CITP,

* Only two that sufficiently demonstrate competencies regarding both IT and audit.



Guidelines / Best Practice.

Your own Security policies

ISO27001

Codes of connection

CJSM

DPA



So, what are the key issues ?



Lifestyle Devices



Exponential growth as job cuts loom

- Staff screening
- Audit list of removable devices
- Physical security of server rooms
- Monitor email and usage policies



Worryingly the key threats have not changed in the last decade

- Weak passwords
- Poor patch management
- Badly configured software

Migrating systems to the Cloud

- Key Concerns Now
 - Security – access control
 - Uptime
 - Tie in
 - Audit

- Compare the *Cloud.Com* is here!





<http://comparetheclouds.com/>

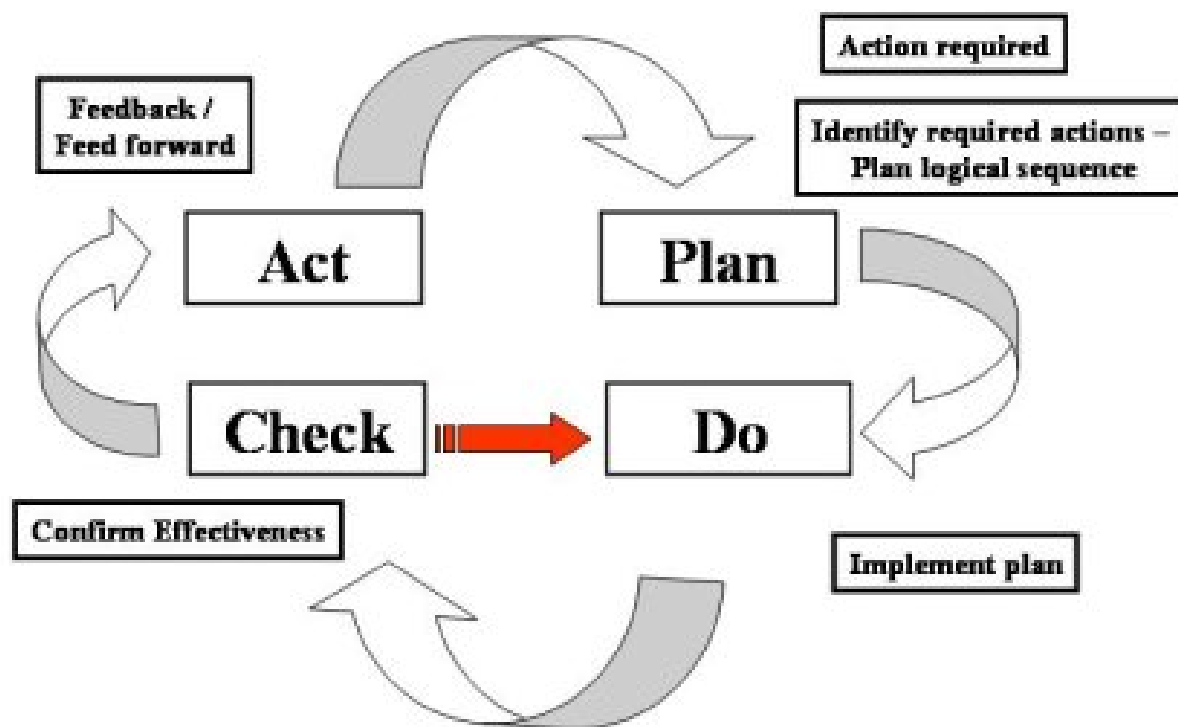


Microsoft[®]

amazon[®]

Google[™]

Problem Solving Cycle



Get your nose off the check list and sniff the air!

Auditing is not an event, it's a process.

Responsibility for informing and educating lies with you!



proactive

THANK YOU!



David Horn

Sapphire

North

*Globe House
Station Street
Stockton on Tees
TS20 2AB*

0845 58 27001

London

*Hamilton House
Mabledon Place
Bloomsbury
London
WC1H 9BB*

0845 58 27002

Scotland

*Suite 3
Commercial Centre
Kerse Road
Stirling Enterprise Park
Stirling
FK7 7RP*

0845 58 27003

E-mail – info@sapphire.net