Position Paper

IT Audit in a De-perimeterised Environment

Problem

IT audit is about the formal verification and validation of the quality and effectiveness of IT controls to support the overall business control objectives. From a security control perspective the residual IT security risks are relatively well understood in a network perimeter protected environment. This perimeter-based protection model has led to an IT audit practice that has matured into given sets of frameworks, methodologies, approaches, and models with certain sets of assumptions. CobiT (Control Objectives for Information and Related Technology) represents such maturity in IT control frameworks and is commonly referenced among IT auditors.

It is believed that there is no strategic impact to the underlying IT audit control framework(s) that have been serving as the foundation for the number of prevalent methodologies and approaches fundamentals of IT audit as a result of the implementation of the Jericho Forum Commandments.

However, a valid question to ask is whether the tactical/operational aspects of IT audit can scale to meet the challenges in a deperimeterised operational environment.

While IT security controls are important aspects of regulatory compliance, the intention of this paper is not to explore the consequences in this area. Instead the impact due to the Jericho Forum vision to the area of regulatory compliance is left to another paper titled “Regulation, Compliance & Certification” published by the Jericho Forum.

Why Should I Care?

- Without an appropriate IT audit scope, important IT controls within an organisation may not be fully tested – thus leading to higher levels of risk including regulatory compliance risks, if these controls are ineffective.
- IT audit is a measurement of IT risk management, which translates into business risk management.
- Improper management of IT risks is expensive, in particular in light of compliance to the US Sarbanes-Oxley Act (SOX).
- The fundamentals of IT audit require the ability to demonstrate the same risk-based control quality in a deperimeterization computing environment. The quality of Test of Design (TOD) and Test of Effectiveness (TOE) in such a deperimeterization computing environment with an arbitrary context should be maintained at a level no lesser than as in a perimeterization computing environment.
- Without the proper communication and appropriate appreciation of the major changes taking place, an organisation may fail to meet their auditor’s expectations.
**Recommended Solution/Response**

The Jericho Forum believes that there is no strategic impact to the fundamentals of IT audit described in the prevalent IT control frameworks such as CobiT, and a supplemental paper will be produced to justify this statement. However, there are significant impacts to the tactical IT controls in terms of scalability and operational complexity for the IT audit community which may impact on the cost/effort involved in audit. The impacts are major enough that advanced strategic planning and architecture upgrades are strongly recommended for highly regulated companies. Product vendors should also be part of the advanced planning to provide cost effective solutions.

Some of these tactical impacts can be linked to future control practices described by a number of Jericho Forum position papers such as Internet Filtering & Reporting, End Point Security, and Enterprise Information Protection & Control.

In the end the IT audit community within the Jericho Forum encourages the IT community to establish needed standards, guidelines, and solutions that are clearly linked to the management of business risks when embarking on a journey towards business agility in a deperimeterization computing environment.

However, as organisations move towards a de-perimeterised computing environment, several changes need to be considered from an IT audit tactical perspective:

- Control points that were centralised and external to applications and systems will change (end points have shifted). The shift in control points will create new scenarios of controls that are more application centric and data protection centric.
- Reliance and assumptions of controls over traditional internal components, such as a WAN or LAN, may no longer be relevant or appropriate (audit scope changes).
- A sampled assessment of decentralised components may not give a clear picture of the overall IT control environment (partners spread spyware, business boundary and IT boundary).
- The focus and importance of core IT systems may need to change – for example, increased reliance on Data Centre, client and application controls.
- Additional foundation services (Identity, Audit, Monitoring) may need to be included in the scope of future audits.

As such, IT auditors need to understand the potential changes in their client’s IT environment in order to appreciate how the goal of maintaining internal control has shifted. This is crucial to the success of an effective and relevant audit.

**Background & Rationale**

The IT audit services at major auditing firms are based on and structured around industry recognized control frameworks such as CobiT. A logical question to ask is whether the Jericho Forum vision has a significant impact on these IT audit services as well as the IT audit practice at any publicly registered companies. The impact can be further examined from a strategic and tactical perspective.

Extensive research has been conducted in the IT governance community and in the Jericho Forum community on prevalent control frameworks and taxonomy. The research has led to the conclusion that the strategic impact analysis of the Jericho Forum vision to IT audit can be achieved through the impact analysis against CobiT. However, the tactical impact analysis must be derived from the prevalent IT audit practice including feedback from the IT audit community.

The CobiT control objectives/framework that governs the IT processes is defined within four domains following the PDCA model (Plan-Do-Check-Act): Planning & Organisation; Acquisition & Implementation; Delivery & Support; and Monitoring.
Further, the principles or qualities of the control objectives are defined by seven categories as follows: Effectiveness; Efficiency; Confidentiality; Integrity; Availability; Compliance; and Reliability of Information.

Comparing each and every one of the Jericho Forum Commandments against the CobiT high level control objectives, we conclude that there is no strategic impact on the CobiT framework by the Jericho Forum vision. For instance, “The scope and level of protection must be specific & appropriate to the asset at risk” is covered by “PO9 Assess and Manage IT Risks” in CobiT 4.0; and “Authentication, authorization and accountability must interoperate/exchange outside of your locus / area of control” is covered by “DS5.3 Identity management”.

In other words the CobiT framework is sufficient in generality to provide the IT governance as well as strategic guidance on IT audits during the migration towards the Jericho Forum vision of a deperimeterized computing environment.

**Key Challenges and Next Steps**

Typical organisations moving towards a deperimeterised environment need to take on board the following challenges:

- Expanding the corporate boundary of the network.
- Thinking of the internal network as a semi public or public network.
- Pushing more applications and systems into data centers that are Internet accessible.
- Developing applications that are Internet enabled and take advantage of security controls such as transport layer security, authentication and authorisation controls.
- Relying more on endpoints in the network to protect themselves using patching, firewalling, anti-virus technologies.
- Identifying users and devices that connect to business systems and applications.
- Patching and managing devices that connect to corporate systems from remote and often untrusted Internet sources.
- Providing users who may be employees, customers, business partners, 3rd party suppliers with access to business applications.
- Providing a bridge between legacy systems and Internet accessible services.
- Supporting a variety of remote access methods through wireless, dial-up, VPN, 3G etc.

The following sections discuss some of the key challenges in detail that face IT auditors and their auditees when looking at an organisation who either has moved to or plans to adopt Jericho principles. Areas covered in these sections include:

- Audit planning
- Audit scope
- Review of audit assumptions
- Performing the audit.

**Audit Planning**

Before starting the audit of an organisation that is moving towards using Jericho principles, the auditor needs to understand the strategy that the organisation is following and where the organisation is along its roadmap. Planning the audit of a deperimeterised environment is just as important as conducting the audit itself. Because of its decentralised nature, auditors choosing inappropriate systems and controls may miss core foundation systems or waste time with inappropriate systems.

**Audit Scope**

When scoping a client’s IT environment, care needs to be taken to ensure that appropriate systems, environments and applications are covered to meet business and audit objectives.
Additional services may be developed to provide foundation services within a deperimeterised environment. These services may need to be added into the scope of an audit.

Traditional centralised services may not be appropriate, if decentralised controls have been adopted. In addition, the following core foundation capabilities will need to be covered in the scope of an audit in the future:

- Authentication and authorisation services.
- Time stamping.
- Monitoring and auditing.
- Encryption in transit and storage including data fields.
- End point security policy - firewalls, anti-virus, anti-spyware etc.
- Application security controls such as transaction and workflow related.
- Security at entry points such asvpn's, remote users, wireless users.
- Third party communications.
- Trust relationships with external parties - business partners, suppliers, customers.
- Data centre controls / SAS 70.
- Management of outsourced providers.

**Review of Audit Assumptions**

A deperimeterized environment may lead to audit assumptions being revisited, for instance:

- **Old audit assumption:** “We can rely on centralised controls and just audit these”.
  **Revised audit assumption:** “Several centralised foundation services may exist to support the deperimeterized environment and they need to be included in the scope of the audit. Additionally, decentralised controls, such as those at endpoints (clients and/or applications) may need to be looked at on an individual basis”.
  **Shift in thinking:** IT controls will have to be moved towards end points such as Data centres, applications, and clients.

- **Old audit assumption:** “The internal network is secure and out of scope from application audits”. Revised audit assumption: ”The internal network is or could be semi-public or public and as such all applications need to assume that the internal network cannot be fully trusted”.
  **Shift in thinking:** The organisation’s internal network may no longer be truly internal – several business partners, 3rd party suppliers and other users may have access to the network.

- **Old audit assumption:** “Taking a sample of systems and applications is representative of the IT environment”.
  **Revised audit assumption:** “The scope and scale of audits may need to expand to factor in centralised and decentralised points of control”.
  **Shift in thinking:** Each system and application will have a combination of centralised and decentralised IT controls. Controls will be built closer to the applications and users themselves.

**Performing the Audit**

When conducting the audit, the auditor will need to identify where controls can be relied upon from a centralised and decentralised perspective.

Checklists for effective IT audits are to be developed that will take into account of balancing the business context served by the IT environment and associated IT controls for proper value and assurance.