



IT Audit and Compliance

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.

Our assessment is that there is no strategic impact on the underlying IT audit control framework(s) that have been serving as the foundation for IT audit, arising from the impact 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 de-perimeterised operational environment. This paper addresses this question.

IT security controls are important aspects of regulatory compliance, so the impact on the area of regulatory compliance is also addressed briefly in this paper.

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 carries severe business impacts if regulatory non-compliance is revealed. The US Sarbanes-Oxley Act (SOX) represents an example.
- The fundamentals of IT audit require the ability to demonstrate the same risk-based control quality in a de-perimeterised environment as in a bounded environment. The quality of Test of Design (TOD) and Test of Effectiveness (TOE) in a de-perimeterised environment is required to be no less than as in a perimeterised environment.
- Without the proper understanding and appreciation of the major changes taking place as de-perimeterisation steadily increases, an organisation may fail to meet their auditor's expectations, unless the audited organisation promotes good communication of the impact that de-perimeterisation has on how effective audit of their organisation needs to be conducted.

- Against a landscape of increasing threats, vulnerabilities and regulatory compliance demands, the need will similarly increase for evidence that adequate and appropriate governance of Information Security has been implemented and continues to operate effectively across the scope of the organisation and its IT infrastructure.

Recommendations/response

Audit

While 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, there are significant impacts to the tactical IT controls in terms of scalability and operational complexity for the IT audit community which impact the cost/effort involved in audit. The impacts are sufficient to require strategic planning and architecture upgrades 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, Endpoint Security, and Enterprise Information Protection & Control¹. As organisations become increasingly de-perimeterised, 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 de-centralised components may not give a clear picture of the overall IT control environment (partners spread spyware, business boundary vs. 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 effective internal controls has shifted. This is crucial to the success of an effective and relevant audit.

Compliance

There is a need to build a body of best practice from both the audited and the auditor communities. Key components include the following:

- A Code of Practice and assurance process for Information Security Governance across the scope of the shared organisation/infrastructure. (The ISO 17799 standard and certification process meets this need.)
- Approved security implementation guidelines for supporting infrastructure - either generic for a platform type (e.g. desktop, server, firewall, etc.). Many individual

¹ Jericho Forum position papers are all available from www.jerichoforum.org/publications

organisations have developed their own or allowed limited sharing of them within selected security circles. The industry will benefit significantly from establishing a generic set of industry-recognised profiles.

- Assurance guidelines for technology components, critical to the security of the supported information systems. (The Common Criteria meet this need.)
- Real-time monitoring processes that can detect and report potential security vulnerabilities or breaches of security.

Background & Rationale

Audit

IT audit services at major auditing organisations are based on and structured around industry-recognized control frameworks such as CobiT. The impact of de-perimeterisation on the IT infrastructure and protection measures that are effective in de-perimeterised environments are significantly different to those in perimeterised ones – particularly with regard to perimeter firewalls and data-centric security. The auditors need to understand this, and the organisations being audited need to appreciate their responsibilities to partner with their auditors to explain how their systems meet the fundamental requirements underlying the audit objectives.

The Jericho Forum concluded from an extensive study on prevalent control frameworks and taxonomy that from the strategic impact viewpoint, the CobiT high level control objectives:

- processes – as defined within four domains following the PDCA model (Plan-Do-Check-Act): Planning & Organisation; Acquisition & Implementation; Delivery & Support; and Monitoring
- principles or qualities of the control objectives – as defined by seven categories: Effectiveness; Efficiency; Confidentiality; Integrity; Availability; Compliance; and Reliability of Information

that there is no strategic impact of the Jericho Forum Commandments on the CobiT framework.

However, the tactical impact analysis must be derived from the prevalent IT audit practice including feedback from the IT audit community.

Compliance

In organisations where the traditional “hard” network perimeter no longer exists, a new governance model is required that ensures that each node/endpoint is fit for purpose.

The Common Criteria - an ISO standard (ISO15408) for specifying security requirements for products and systems - allow us to specify the security features of a system and how it has been developed and tested, including independent third-party checking of claims. They are organised as a set of building blocks from which a range of complete standards can be built. The building blocks specify components of security solutions or development/test approaches in a technology-independent way. Some components can be customised to particular requirements, and it is also possible to develop new components. There is a common misconception that the Common Criteria are bureaucratic and costly to follow. This is certainly true of some existing standards and evaluation methods but the Common Criteria also allow for low-cost, non-bureaucratic standards to be built if that is desired.

Within the Jericho Forum sphere, the Common Criteria can be exploited to identify common component types and then develop a standard security functionality standard for each component. Components would include the following:

- The access device - the equipment a person uses to access a computer system.
- The server device - the equipment an automated service executes upon.
- The authentication service - to authenticate users, organisations, devices or services.
- The authorisation service - to authorise users, organisations, devices or services.
- The audit service - to maintain and query a record of events.

Key Challenges and Next Steps

Typical organisations moving towards a de-perimeterised 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 that face IT auditors and those being audited when looking at a de-perimeterised organisation.

Audit Planning

Before starting the audit, 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 de-perimeterised environment is just as important as conducting the audit itself. Because of its de-centralised 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 de-perimeterised environment. These services may need to be added into the scope of an audit.

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

- 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 as VPN'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 de-perimeterized 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 de-perimeterized environment and they need to be included in the scope of the audit. Additionally, de-centralised 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 de-centralised 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 de-centralised 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.
