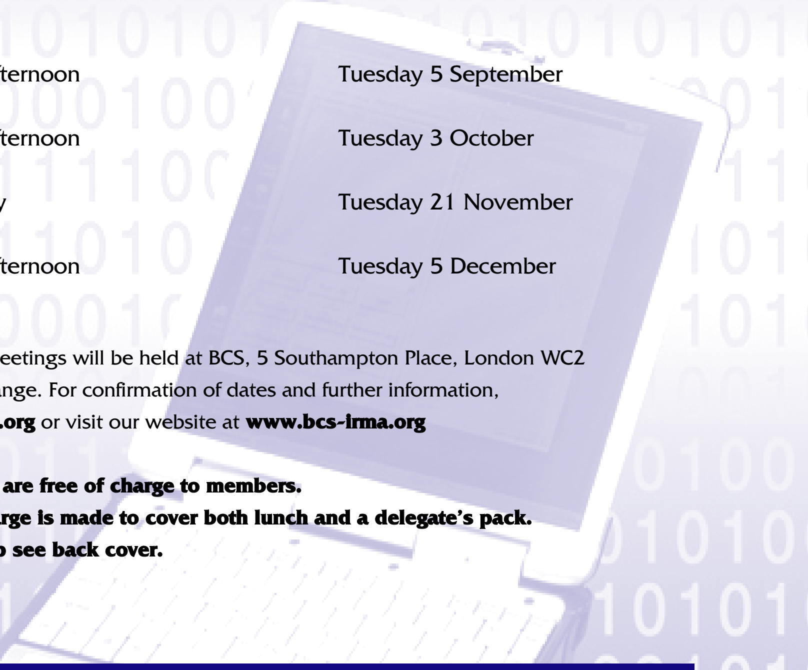
IRMA
INFORMATION RISK MANAGEMENT & AUDIT
◆ A SPECIALIST GROUP OF THE BCS ◆

JOURNAL

volume 16 number 1 spring 2006 ISSN 1741-4229

Programme of Briefings & Meetings 2006

Title	Meeting type	Date
Computer Audit Basics 4: Application Controls	Late afternoon meeting	Tuesday 24 January
Control Aspects of ITIL (Service Delivery) / Cobit	Late afternoon meeting	Tuesday 07 February
Wireless Technology	Late afternoon meeting	Tuesday 07 March
Latest Developments in IT Law	Late afternoon meeting combined with IRMA AGM	Tuesday 02 May
Project Control – The Auditor's Role in IS Projects/Systems Development	Full day briefing	Tuesday 06 June
Spreadsheet Risks: Ubiquity, Severity & Legality?	Late Afternoon	Tuesday 5 September
TBA	Late Afternoon	Tuesday 3 October
TBA	Full Day	Tuesday 21 November
TBA	Late Afternoon	Tuesday 5 December



Apart from any joint meetings with other organizations all meetings will be held at BCS, 5 Southampton Place, London WC2
This is a draft programme only and is subject to change. For confirmation of dates and further information,
watch the **Journal**, email **admin@bcs-irma.org** or visit our website at **www.bcs-irma.org**

The late afternoon meetings are free of charge to members.
For full day briefings a modest, very competitive charge is made to cover both lunch and a delegate's pack.
For venue map see back cover.

Email distribution is here . . .

Beginning from this issue, IRMA is moving from paper to electronic distribution of the Journal, so we need your email address! If you have not already supplied it, please can you send your email address to our admin office at admin@bcs-irma.org with your membership renewal or to the chair at brewer.alex@gmail.com (preferably with the subject "IRMA contact details"). Many thanks.

Contents of the Journal

GUIDELINES FOR POTENTIAL AUTHORS

The *Journal* publishes various types of article.

Refereed articles are academic in nature and reflect the Group's links with the BCS, which is a learned institute governed by the rules of the Privy Council. Articles of this nature will be reviewed by our academic editor prior to publication and may undergo several iterations before publication. Lengthy dissertations may be serialised.

Technical articles on any IS audit, security, or control issue are welcome. Articles of this nature will be reviewed by the editor and will usually receive minimal suggestions for change prior to publication. News and comment articles, dealing with areas of topical interest, will generally be accepted as provided, with the proviso of being edited for brevity. Book and product reviews should be discussed with the appropriate member of the editorial panel prior to submission. All submissions should be by e-mail and in Microsoft Word, Word-Pro, or ASCII format. Electronic submission is preferred.

Submissions should be accompanied by a short biography of the author(s) and a good quality electronic digital image.

Submission Deadlines

Spring Edition	7th February	Autumn Edition	7th August
Summer Edition	7th May	Winter Edition	7th November

PLEASE NOTE THE EMAIL ADDRESS FOR

IRMA ADMIN

IS:

admin@bcs-irma.org

The views expressed in the Journal are not necessarily shared by IRMA.
Articles are published without responsibility on the part of the publishers or authors for loss occasioned
in any person acting, or refraining from acting as a result of any view expressed therein.

The ***Journal*** is the official publication of the Information Risk Management & Audit Specialist Group of the British Computer Society. It is published quarterly and is free to members.

Letters to the editor are welcome as are any other contributions. Please contact the appropriate person on the editorial panel.

Editorial address:
47 Grangewood,
Potters Bar
Herts, EN6 1SL
Email: john@lhscontrol.com

Produced by Carliam Artwork,
Potters Bar, Herts

Editorial

John Mitchell

This is the first edition of the Journal to be issued solely in electronic format. Although you have been able to access the Journal on-line for some years now we have persisted in sending out a hard copy version as many of us prefer the ability to browse off-line, away from our desks. Alas, the expense of hard-copy production has now become unsustainable so we will only be publishing future copies as an Adobe PDF file on our web page. From there you can either browse on-line, as you may well be doing now, or download it to your personal device for off-line viewing, or actually printing it on your local printer. The access password will be changed every six months, but you will be informed of this via our regular email communication with you, so it is essential that our administrator has your latest email address (admin@bcs-irma.org).

One of the things that I advise companies on is business continuity planning (BCP) and there is always a spurt of activity after a disaster; viz 9/11, 7/7 and Hemel Hempstead. One of my regular findings is that very few firms seem to have their change programmes linked to their business continuity planning; this assumes that they are managing change in the first instance. Few companies consider BCP when they re-structure and even less when they outsource a process and yet these often have a greater impact on the BCP than a change to a computer system. Business continuity planning is a key component of disaster recovery planning (DRP), in that DRP is the later aspect of BCP. That is, your business continuity has failed and you now need to recover the situation. It's amazing how many auditors do not see the entire continuum, but BCP is about keeping the show on the road while DRP means that you have crashed. Reviewing your BCP and eliminating, so far a is possible, the single points of failure is usually far cheaper and less disruptive than having to invoke the DRP. Also, DRP testing is often very expensive, if you can do it at all. I am much in favour of desk-top walk through tests on a regular basis, as being a reasonable alternative to a proper test. They can be done frequently, with different staff and reflecting different scenarios. Audit can umpire these tests by determining the scenario at the last moment and 'killing off' some of the participants to see how well their deputies can manage without having to make the actual funeral arrangements. It's great fun too!

For good BCP/DRP you need a configuration management database (CMDB). In simplistic terms this is a superior asset register, usually with a relational database so that you can predict the impact of removing, adding or changing one of the assets. The CMDB is useful for establishing the minimum configuration needed to run a particular application and enables you to create what if type scenarios, such as the loss of a file, media, server or router. Very handy for identifying single points of failure without actually pulling the plug. Like all software tools however, it is only as good as its data and this is where the link to change management becomes important.

On a regular basis I receive emails warning me of some dire thing that is being perpetrated only to find out that it is actually a hoax. Invariably these start off with "a friend of mine ……", or more alarmingly "the police have warned …….". I immediately feed the lead words into my search engine to find the source of the warning and invariably find that the hoax is already well established. It's a bit like the urban myths of the 1990s, but the hoax hoax (that's my name for these) can now be spread so much faster. Some are not so harmless in that they persuade their victims to delete system files or to reveal credit card details, but the majority are just time wasters. What does amuse me is how defensive the relayers of these hoaxes become when I point out that they have been duped. I guess that it's a bit like being on the end of a less than favourable audit report.

The ID card bill progresses through Parliament with the likely cost varying widely depending on who is speaking. On the basis of past government system developments the centralised database, which is key to whole thing, has about as much chance of working as intended as the attempt to farm peanuts in Kenya in the middle of the last century. A more misguided solution to a non-problem is hard to imagine.

This edition concentrates on submissions from the antipodes. The major contribution is a paper defining a model to support information security governance from a combined team representing Queensland and Hong Kong universities, while our regular correspondent from that area, Bob Ashton, raises the problems associated with digital rights management. The chairman's column likens software infrastructure to archaeology and Mark Smith rakes up some great member benefits. The humour page is a great antidote to the SAD syndrome.

I hope to see some more of you at our future meetings. They provide good value CPE for many professional CPD programmes and you get decent food and drink too!

Chairman's corner

Alex Brewer

Happy New Year

We are now in the year of the dog, and well and truly into 2006. Those first quarter project deadline dates are now looming closer!

The other big change is that the IRMA journal will only to be published electronically, in keeping with many other organisations (my phone and gas bill are both available on line). So to anyone reading this, welcome to the online version of the journal! Our designer has been itching to lay out more than two colours, and with the move to the new format, now has his chance. Hopefully this column will still be published in black rather than yucky green!

As ever, if you have any thoughts on the new format or the content, or would like to submit a paper, please contact IRMA's administration at admin@bcs-irma.org.

With the AGM approaching in May, please do consider joining the committee. We meet at the BCS London HQ and expenses are available for attending committee meetings. Benefits include free attendance at all IRMA events, and participation in ongoing BCS activity (such as an earlier consultation on ID cards).

Last.minute.com

This year's Christmas shopping made the newspaper headlines because the volume of online shopping grew massively, while high street sales were similar to last year. In the online shopping a huge spike of demand appeared at the last moment, presenting significant logistical challenges to the businesses providing the service.

In IRMA we see similar challenges as our courses put on are only booked at the last minute - much later even than just two years ago. Our talk on Cobit and ITIL was very well attended, despite the very sparse attendance list available just a few days before.

Have we turned into a nation of last-minuters? I know from my time at an investment bank that the only reward for working overnight to get a project in on time will be the expectation that the same service will be forthcoming on the next project, only instead the planning will be based on this workload being the norm rather than a one-off burst of effort to complete the task.

I think there is a place for better planning at longer timescales, however this view appears at odds with where the world is going. The risks of this 'just-in-time' approach include project failure or late delivery, because less time is available to make things work when (inevitably) something goes wrong.

So this year, keep your project manager happy and buy your presents early!

Software Infrastructure is like archaeology

One thing I have noticed in my career is that software infrastructure is like archaeology: there is an analogy between the waves of computing introduced into organisations and the layers of rock that build up when looking at the earth's geology. The layers of software environments used changes every three years or so as a new style of computing is introduced. As time goes by, knowledge of the lower strata fades as people move on to new jobs or retire.

The geological strata of computing environments go something like this:

Business environment – people and processes

Mobile computing (Blackberry,
Wi-Fi, Windows Mobile)

.NET framework based computing

Web services computing (PHP, Perl, Java)

Object based computing (DCOM)

Windows based computing using
Microsoft's SQL Server databases

Windows based computing linked
to client server based computing

Object based computing (CORBA)

Middleware layers to link applications

Client server computing including SQL
databases which link to mainframe applications

Mainframe applications

Some of the layers are hard to place: middleware is pervasive in nature and turns up in different guises and different times. However, the basic message is that unless an organisation has a truly ruthless streak when it comes to stripping out old software, the chances are that the 'it ain't broke, don't fix it' dictum will mean that very reliable, but unnoticed and unmaintained code is probably supporting some key business functions.

Problems generally arise because no-one knows what occurs more than about three layers from the top. These layers are well known and probably reasonably documented, but the more layers down that you need to go to make changes, the more likely it is that only a few gurus will understand the systems beneath.

Some examples of this that I have heard about:

A key system was returned from its custom version to the vanilla product from the vendor after the last developer retired. Many functions were not available in the vanilla product, but at least it was supported.

Assembler programs were still used and maintained on a mainframe in the mid 1990s long after their sell by date, because of their mission critical nature.

A company's in house mainframe system was being systematically 'poked' by a developer to see what its response would be. There was no documentation for much of the functions added after the initial release, so this was the only way to find out how it worked.

While looking at a modern ERP system I was asking about the format of a table. I was told that a certain field couldn't be used because its format was 'packed'. When I queried the term (packed is a mainframe term, but the system was based on a SQL database), it seems that the vendor moved the product in the past, including the unmodified 'packed' format from the mainframe to the SQL database environment.

Passports now part of ID card scheme

Tony Blair got the ID card bill over a crucial vote this week: it now seems that in order to have a passport issued in future, you will require an ID card. As the cost of an ID card is anything from £30-£300, you might wish to renew your passport before 2008. Watch this space for developments.

IRMA MEMBERS' BENEFITS DISCOUNTS

Mark Smith

We have negotiated a range of discount for IRMA members, see below:

Don't miss our 20% discount for IACON 2006, which runs from 20th to 23rd March 2006, and our 15% discount for WEBSEC 2006, which runs from 28th to 31st March

Software

Product	Discount Negotiated	Supplier
Caseware Examiner for IDEA (mines security log files for Windows 2000, NT, XP)	15%	Auditware Systems (www.auditware.co.uk)
IDEA (Interactive Data Extraction and Analysis)	15%	Auditware Systems (www.auditware.co.uk)
Wizrule (data auditing and cleansing application)	20%	Wizsoft (www.wizsoft.com)
Wizwhy (data mining tool)	20%	Wizsoft (www.wizsoft.com)

Events

Event	Discount Negotiated	Contact
E-Tec courses (www.e-tecsecurity.com)	10%	Margaret Mason (info@e-tecsecurity.com)
IACON 2006 (www.iir-iacon.com)	20%	Jonathan Harvey (jharvey@iirltd.co.uk)
All Unicom events (www.unicom.co.uk)	20%	Julie Valentine (julie@unicom.co.uk)
Websec 2006 (www.mistieurope.com)	15%	Lisa Davies (LDavies@mistiemea.com)

We are constantly looking to extend this range of discounts to include additional events, training courses, computer software or other products that our members may find beneficial. If you have any suggestions for products we could add to the list, please contact Mark Smith (mark.smith@smhp.nhs.uk), our Members' Benefits Officer, and he will be happy to approach suppliers.

The Down Under Column

Bob Ashton – IRMA Oceania Correspondent

Rooted – Music While You Work or Another Way Around Your Firewall

Digital Rights Management

In many organizations today employees can be seen listening to music through headphones from their privately owned music CDs being played via the CD ROM drive of their employers' personal computers. Hitherto this behaviour has been tolerated or ignored by management as it has not presented any apparent risk to the employing organization. This scenario has radically changed because of a course of action taken by Sony BMG early in 2005.

Sony has included 3 different types of Digital Rights Management (DRM) software with its most recently released music CDs. One version of this software installs Sony's media player onto Windows based computers as the default media player, and at the same time limits the ability of the host computer to produce no more than 3 backup copies of the purchased music CD. These functions may be considered commercially justified, but the software also utilizes techniques borrowed from the criminal world of virus and spyware authorship to perform other functions, collectively known as a root kit. These undesirable functions are:

Phone Home Technology.

It has been established that the software secretly communicates with Sony over the Internet when listeners play the discs on computers that have an Internet connection. The software uses this connection to transmit the name of the CD being played to an office in Sony's music division in Cary, North Carolina. The software also transmits the IP address of the listener's computer.

Cloaking Technology.

The program copies itself to the Windows System Directory, hides itself and is designed to prevent any other process from accessing its processes, files, folders or registry sub keys.

Rootkit

A rootkit has been defined by Wired in the following way; "A rootkit is a particularly insidious type of Trojan horse that hides its existence from users and programs by tampering with the operating system at the most fundamental level. Where normal malicious code might be content to choose a deceptive file name, a rootkit 'hooks' operating system calls that might reveal its presence, and essentially reprograms them to lie – like bribing the coroner to conceal a murder."

Sony's software complies with this definition.

Risks

Music CDs carrying such software have become a new type of attack vector enabling malicious software to be installed unknown to the computer's owner, with all manner of consequences.

Malicious software designed to piggy back on Sony's already installed rootkit had been identified early in November 2005, and it is likely that many more attempts will be made to utilize this new vulnerability.

Sony's efforts in this regard will no doubt be regarded as well researched proof of concept case study by malware authors throughout the world, and now that this means of secretly inserting code onto a PC is publicly known, there is nothing to prevent other criminals from creating Trojan music CDs whose sole purpose is the transfer of malware, and distributing these CDs by any means available. This would be an easier task for malware authors than to keep devising new means of evading evolving firewall controls. Open season now exists for malware authors to apply their imaginations on how to best exploit this newly identified avenue into the heart of personal computers throughout the world.

It has been established that attempting to remove this software can completely disable a PC, requiring long hours of rectification.

Safeguards

This software can only be installed on a Windows PC by a user with Administrator rights. In a corporate environment end users should never have this access; however some users must have this privilege in any network. It will in future be prudent to prohibit the playing of any music CD or DVD through the CD ROM facility of a personal computer.

In the case of SOHO installations, Administrator is a common default. Home and small office users should no longer take the risk of playing music CDs on their PCs.

It is fortuitous that the use of newer music playing devices, such as the ipod, has become widespread as this new threat has emerged.

A Model to Support Information Security Governance

W. J. Caelli, Information Security Institute[1], Queensland University of Technology
G. Gaskell, Information Security Institute[1], Queensland University of Technology
Lam For Kwok, Department of Computer Science[2], City University of Hong Kong
D. Longley, Information Security Institute[1], Queensland University of Technology

[1] GPO Box 2434, Brisbane, Qld, 4001, Australia
{w.caelli | g.gaskell | d.longley | @qut.edu.au}

[2] Tat Chee Ave, Koowloon, Hong Kong
{cslfkwok@cityu.edu.hk}

ABSTRACT

Organisations are coming under increased pressure to demonstrate that their IT systems are protected according to best practices and published guidelines. Effective security documentation is required to support associated conformance audits and this paper describes a proposed database documentation approach for this purpose. The proposed model may moreover assist the audit beyond conformance at a process level, to a demonstration that the security rationale of guidelines and standards is implemented. As part of this approach to security audits the paper provides a detailed security rationale for the set of access controls contained in ISO 17799.

Keywords: Security Governance, ISO 17799, Security
Management, Compliance, Information Security Model

1 INTRODUCTION

1.1 INFORMATION SECURITY GOVERNANCE

Governments are placing increasing emphasis on the senior management and Board of Directors' responsibilities for corporate Governance, for example the Sarbanes Oxley Act in the United States and CLERP9 legislation in Australia. Information systems contain a large majority of the evidentiary records of corporate governance, and corporate management must therefore ensure that their information technology (IT) systems are implemented, maintained and operated to meet corporate and regulatory objectives. Hence information and communication technology (ICT) Governance is defined as: "*the system by which the use of ICT is controlled. It involves evaluating and directing the plans for the use of ICT to support the organization and monitoring this use to maintain the plan. It includes the strategy and policies for using ICT within an organization.*" [1]

ICT Governance in turn acknowledges the role of information security and includes recommendations such as:

- *Evaluate the risks to the integrity of ICT data holdings and the protection of resources from damage, abuse, or misuse;*
- *Direct arrangements for ensuring integrity, security and protection of key IT resources, ensuring the organization wide integration of physical and ICT related resources*;
- *Monitor the extent to which the required quality is provided* [1].

Similarly in the United States the Corporate Governance Task Force Report [2] defines Information Security Governance as: *a subset of organizations' overall governance program. Risk management, reporting, and accountability are central features of these policies and internal controls.*

Detailed recommendations on information security governance are also provided by the IT Governance Institute and in particular COBIT (Control Objectives for Information and Related Technology [3]) has been *"developed as a generally applicable and accepted standard for good IT security and control practices that provides a reference framework for management, users, and IS audit, control and security practitioners"* [4].

This task of information security governance is rendered more important by the ever-increasing reliance on ICT systems. Year by year manual checks and balances are replaced with automated information systems. Human participation in many business processes is being progressively removed and correspondingly we (as a society) require enhanced confidence in these key systems.

The information security governance task is also rendered more difficult by the rapid development of IT systems in the past decade. For example, these IT systems have greater inherent vulnerabilities, arising from their increased complexity and inter-networking; moreover system integration, designed to enhance efficiency and productivity, increases the potential business impact of IT system failures and misuse.

If IT security governance is to meet the objectives of corporate governance, i.e. protecting society against major disruption arising from corporate system failures, then the major task of implementing, monitoring and reporting corporate IT security must be fully addressed. The risks associated with corporate IT systems must be identified and information security management must be implemented and monitored.

1.2 IT SECURITY GOVERNANCE PROCEDURES

1.2.1 Risk Management

IT security governance guidelines have a consistent theme of senior management's responsibility in relation to risk management of information and IT assets, systems and networks. For example:

- *Evaluate the risks to the integrity of ICT data holdings and the protection of resources from damage, abuse, or misuse* [1];
- *Organizations should conduct periodic risk assessments of information assets as part of a risk management program* [1];

- *Is management confident that security is adequately addressed in the organisation? Has management set up an independent audit of information security? Does management track its own progress on recommendations?* [3].

It is perhaps surprising that none of the guidelines gives any indication of the magnitude or costs of these reporting tasks when undertaken in highly complex, tightly coupled IT systems. For example, the recommendation on periodic risk assessments is usually not accompanied with a reference to a recommended risk assessment methodology or software package, whilst the COBIT extract implies the use of external consultants for this task.

Drawing upon previous experience one might compare the current situation of complex, distributed corporate IT systems with those of US Federal Agencies in the early 1970's, when computing activities were often confined to mainframe computing centres. The managers of these Federal agency centres were required to conduct quantitative risk assessment audits. The response from managers was often negative, and the general reaction was the major effort of data collection was excessive in comparison to the benefits derived from the subjective risk estimations.

If organisations are now required to conduct, and report on, periodic risk assessments for large distributed systems, they will presumably need to:

1. Document in detail the security context of assets, IT systems and networks: including information on users, physical locations, third party accesses, outsourcing etc.
2. Determine the current level of risk.
3. Report risk levels and security recommendations to management.
4. Conscientiously update the information derived in (1) with changes in corporate IT systems and environments.
5. Periodically review the updated system data against the processes used in (2) and report any significant developments to management.

The emphasis on periodic risk assessment implies greater concentration on the recording and periodic updating of information security relevant data and hence comprehensive corporate security documentation. There appears to be no standards and limited guidance to security officers on the development of such comprehensive documentation to support regular risk assessments or security audits.

This paper builds upon earlier work [7,8] and the use of a database plus supporting software approach for such information security documentation as reported in two more recent papers [5, 6].

1.2.2 Information Security Management

Information security governance requires the top down implementation and monitoring of an information security management system. For example:

- *"Organizations should use security best practices guidance, such as ISO 17799, to measure information security performance"* [2].
- *"Direct arrangements for ensuring integrity, security and protection of key IT resources, ensuring the organization wide integration of physical and ICT related resources"* [1].
- COBIT makes extensive references to conformance with ISO 17799 [3].

BS/AS/NZS 7799 Part 2 describes procedures for conformance testing, e.g. ensuring that policies and procedures are implemented in accordance with the recommendations of the standard. At one level such conformance can be easily demonstrated by correspondence between documented corporate security policies and procedures and the corresponding set of standards recommendations. However, given the complexity of distributed corporate IT systems the degree of assurance associated with such audits is limited. In particular:

- ISO 17799 is directed to baseline security and the recommended controls must be enhanced for higher risk contexts as identified by risk assessment practices (See 1.2.1).
- BS/AS/NZS 7799.2 is a risk-based security standard. Organisations must assess their information security related business risks and select appropriate controls from both part 1 of the standard and from current industry security practices. As such, compliance to the standard is subjective depending on individual organisation's risk tolerance.
- The decision to implement the recommended controls depends upon the local context and the risk-based evaluations conducted by the management of each organisation.

The particular circumstances of a distributed, corporate IT system will dictate whether additional controls are required or indeed if all the recommended controls need to be implemented. This raises some problems from an IS governance viewpoint because the security officer will require some means of justifying decisions to deviate from the standard. Here the security documentation becomes a significant issue because the security officer will need such documentation to describe the corporate security scenario.

1.2.3 Demonstrating Conformance

The previous sections indicated that organisations need to develop comprehensive security documentation to demonstrate conformance with the two most significant requirements of IS Governance, i.e. risk management and information security management. There is, however, little guidance available on the implementation of such documentation. The next section outlines a proposed directory/ database approach to security documentation described in previous papers [5, 6] and this outline is followed by a detailed description of the use of this approach in demonstrating conformance to the ISO 17799 standard. A particular challenge for any security officer is to maintain the Statement of Applicability as required BS/AS/NZS 7799.2 (Section 4.3.1). As the control environment changes within an organisation, this document must be maintained. A software tool based on a dynamic information security model could greatly simplify this task.

2 INFORMATION SECURITY MODEL

2.1 OVERVIEW

Information Security Governance demands a rigorous reporting of corporate IT security but such reporting in turn demands a well-organized comprehensive security documentation set and there is little guidance available to security officers on the methodologies for such documentation. The Information Security Model (ISM) described in earlier papers [5, 6] was designed as a methodology to assist security officers in risk assessment and security design. This paper describes the use of the model to meet the demands of IS Governance and in particular to demonstrate conformance to ISO 17799.

2.2 DIRECTORY STRUCTURE

The essence of the model is a directory approach for the recording of the entities involved in the description of an information security context (See Figure 1). This directory structure enables each entity to be described with a unique ID, termed object identifier (OI) corresponding to its location in the directory tree. Each entity may be given arbitrary attributes in a <TAG VALUE FORMAT>, e.g. a network may include the attribute <COMMUNICATIONS PROTOCOL -TCP/IP>.

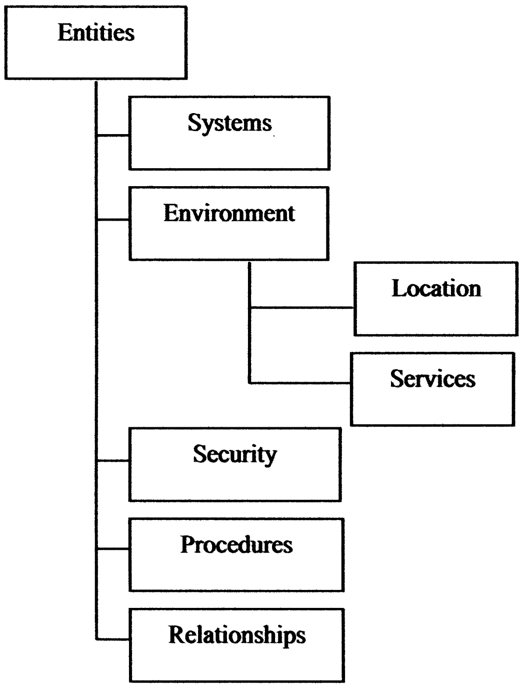


Figure 1 ISM Directory Structure

Links between entities can be described with a RELATIONSHIP ENTITY. Hence the RELATIONSHIP type CONNECTED_TO may be defined and the connection between Server (OI = S), and LAN (OI = L) may be recorded as a RELATIONSHIP entity of type CONNECTED_TO entity with attributes <INCIDENT_ENTITY - S> and <TARGET_ENTITY - L>.

The entity groupings in the model have been selected to reflect the security context of an organisation i.e.:

- Systems – platforms, hardware, software, networks, users, information assets;
- Environment – locations, services;
- Security – threats, countermeasures, threat trees etc. (See 2.3.2);
- Procedures – external (e.g. standards), internal (policies, security manuals etc);
- Relationships – relationships between the entities as described above.

The directory model provides a database structure for recording entities relevant to corporate security; the use of this structure in describing the corporate security context is described in the following section.

2.3 SECURITY CONTEXT

2.3.1 Overview

The prime purpose of the model is to develop and describe the information security context of the organisation by the use of interactive tools. These tools enable the security officer to explore and record the potential impact of unavoidable threats, and to explore of the effectiveness of various security systems. The two prime techniques used to this end are Threat Networks and Threat Countermeasure Diagrams.

The model deals with Threat Events (TE), i.e. a Threat impacts upon some model Entity, e.g. Fire in Main Building. External threats may result in the damage of information assets following a series of Threat Events: e.g.

- *Fire in Main Building causes Damage to Web Server;*
- *Damage to Web Server causes Loss of Availability of Internet Travel Booking System.*

Threat Propagations (TP) represent knowledge of the causal relationship between Threat Events; in general these causal relationships are conditional upon the various entities in the Threat Event. For example the damage to the Web Sever, in the above example, depends upon the fact that the server is located in the Main Building, and this fact must be recorded as a relationship in the model, describing the security context of the organization.

2.3.2 Threat Networks

The causal chain of Threat Events (TE) is represented by Threat Networks (TN) in the model; incident TEs representing the potential set, or some subset, of Threat Events to the organisation are the root set of TE nodes in the TN and the subsequent damage to information or business security assets are the leaves (See Figure 5). A database describing the organisation's security context, plus knowledge of the Threat Propagations, included as conditional relationships between TEs in the model, may be manipulated by model software to develop the Threat Networks. Threat propagations are not inevitable and there is a probability associated with such propagation; the probability that some incident threat will result in damage to an information asset depends upon the chain of TP probabilities in the Threat Network path, between the incident Threat and the subsequent damage. Countermeasures (See 2.3.3) or controls are employed to reduce the probability of Threat Propagations (See Figure 2).

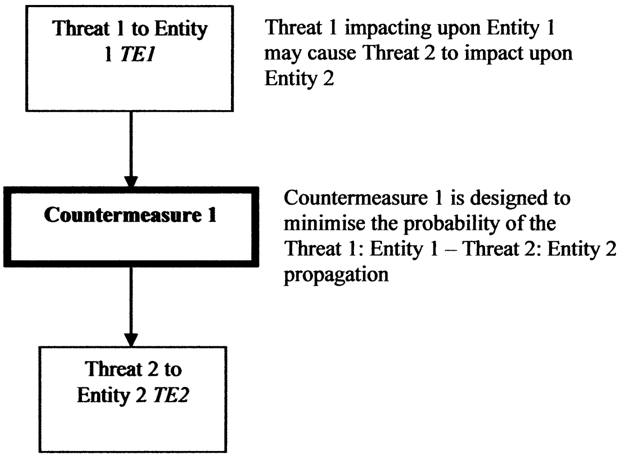

Threat 1 to Entity 1 *TE1*
Threat 1 impacting upon Entity 1 may cause Threat 2 to impact upon Entity 2
Countermeasure 1
Countermeasure 1 is designed to minimise the probability of the Threat 1: Entity 1 – Threat 2: Entity 2 propagation
Threat 2 to Entity 2 *TE2*

Figure 2 Elements of a Threat Network

2.3.3 Security Systems

2.3.3.1 Countermeasures

Countermeasures are deployed by organisations to inhibit unavoidable threats from damaging information assets. We may thus consider that the role of a countermeasure is to reduce the probability of some Threat Propagation located in the chain between an incident Threat Event and the subsequent asset damage. The role of the countermeasure depends upon its placement in the Threat Network; if it is required to protect a set of assets against a particular threat it will be located high in the network, close to the incident TE. A countermeasure to protect an asset against a variety of threats will, on the other hand, be located lower in the network and closer to the asset damage TE.

The effectiveness of a countermeasure is measured by the degree to which it reduces the probability of the propagation of the threat (i.e. TE1-TE2 in Figure 2). This countermeasure effectiveness depends, in turn, on its critical components, e.g. the firewall rules of a firewall. Such components may themselves be affected by deliberate attack, poor implementation or administration (See Figure 3). For example one of potential attacks on a firewall is that: *Attacker gains logical access to the firewall and modifies the firewall rules.*

Supplementary countermeasures or compensating controls (COBIT), e.g. access control on the firewall, are commonly provided to protect its components and hence increase the effectiveness of the countermeasure. It is shown later that many of the controls suggested in ISO 17799 represent such supplementary countermeasures.

2.3.3.2 Threat Countermeasure Diagrams

Supplementary countermeasures may themselves be protected by further supplementary countermeasures and the complete countermeasure structure can be represented by a Threat Countermeasure Diagram (TCD) which provides a rationale for the countermeasure and its defences (See Figure 3).

2.4 ISM SUMMARY

The ISM is a proposed model for information security documentation based upon an electronic database and supporting software for conformance checking (See 4.2.5), Threat Network and Threat Countermeasure Diagram construction. The ISM is designed to record the information security context of an organisation, and to provide interactive tools to assist the security officer in the design of security systems; it can also illustrate the rationale of the security measures adopted. The use of the ISM in demonstrating conformance to ISO 17799 recommendations is described in the next section. An early prototype of a tool implementing the ISM has been built. Initial evaluations of this tool by an external agency have shown the model is very useful in recording real-world security environments.

3 INTERPRETATION OF ISO 17799

3.1 INTRODUCTION

The Preface of Information technology-Code of practice for information security management AS/NZS ISO/IEC 17799:2001 [1] states that: *A comprehensive set of controls comprising the best information security practices currently in use is provided in this Standard. This guidance is intended to be as comprehensive as possible. It is intended to serve as a single reference point for identifying the range of controls needed for most situations where information systems are used in industry*

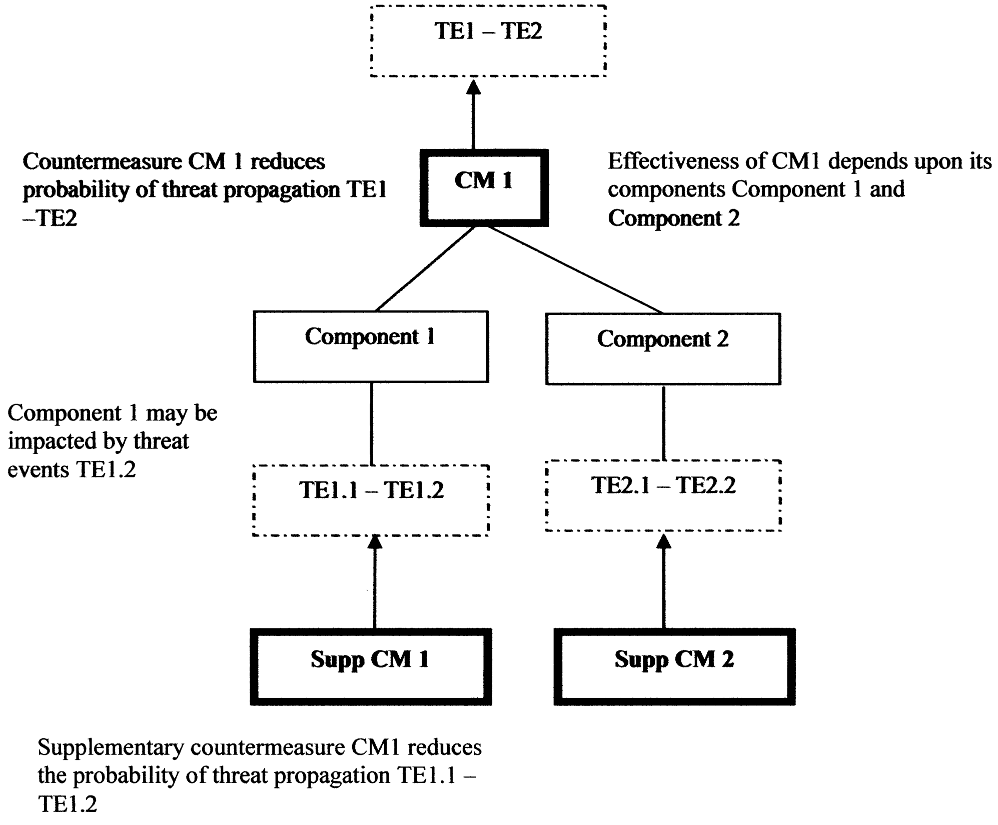

TE1 – TE2
Countermeasure CM 1 reduces probability of threat propagation TE1 –TE2
CM 1
Effectiveness of CM1 depends upon its components Component 1 and Component 2
Component 1
Component 2
Component 1 may be impacted by threat events TE1.2
TE1.1 – TE1.2
TE2.1 – TE2.2
Supp CM 1
Supp CM 2
Supplementary countermeasure CM1 reduces the probability of threat propagation TE1.1 – TE1.2

Figure 3 Threat Countermeasure Diagram

and commerce and can therefore be applied by large, medium and small organizations.

Security officers given the task of demonstrating conformance to the standard must consider these controls in the context of their organisations security stance, determine whether or not individual controls are required and the most effective means of implementing the requisite controls. Many conformance projects tend to seek a correlation between internal documentation and the standards recommendations. In this paper we consider the use of electronic documentation and information security models by the security officer and explore how the standards may be incorporated into such models. The purpose of the exercise is to demonstrate that this approach facilitates the task of setting up, developing, and maintaining organisational security systems and infrastructures. Moreover it enables the security officer to provide convincing evidence of conformance to both the content and the rationale of the standard.

The Access Control Section (Section 9) of the standard is analysed and discussed in detail below prior to a discussion on the integration of the subset of the standard into the Information Security Model. An analysis of Section 9 indicates that the purpose of various subsections may be classified as:

- Policy statements.
- Organisational Guidance Statements.
- Identification of Critical Entities.
- Countermeasures.
- Supplementary Countermeasures.

The *policy statements* provide the rationale for the controls. The *organisational guidance statements* assist the implementation of policies and are most likely to appear in some form of internal Manual of Procedures. *Critical entities* such at IT systems, networks, applications etc. essential for business operations are to be identified to assist in the prioritisation of security controls. The controls themselves are countermeasures, either procedural or hardware/ software, recommended for implementation and *supplementary countermeasures* serve to protect the operation of the main countermeasures. This classification actually reflects the structure of the standard itself, i.e.

- Section 3 – Security Policy.
- Section 4 – Organisational Security.
- Section 5 – Asset Classification and Control.
- Sections 6-11 – Detailed Controls.

The various policy statements, organisational guidance statements extracted from Section 9 of the standard are discussed below in the context of the ISM.

3.2 POLICY STATEMENTS

The general security policies described in Section 3 of the standards are complemented by more focussed access control policies. Hence:

- ***Section 9.1. Business Requirements for Access Control:*** *Access to information, and business processes should be controlled on the basis of business and security requirements.*
- ***Section 9.2 User Access Management:*** *Formal procedures should be in place to control the allocation of access rights to information systems and services.*
- ***Section 9.3 User Responsibilities:*** *Users should be made aware of their responsibilities for maintaining effective access controls.*
- ***Section 9.4 Network Access Control:*** *Access to both internal and external networked services should be controlled.*
- ***Section 9.5 Operating System Access Control:*** *Security facilities at the operating system level should be used to restrict access to computer resources.*
- ***Section 9.6 Application Access Control:*** *Security facilities should be used to restrict access within application systems.*
- ***Section 9.7 Monitoring System Access and Use:*** *Systems should be monitored to detect deviation from access control policy and record.*
- ***Section 9.8 Mobile Computing and Teleworking:*** *The protection required should be commensurate with the risks these specific ways of working cause. When using mobile computing the risks of working in an unprotected environment should be considered and appropriate protection applied. In the case of teleworking the organization should apply protection to the teleworking site and ensure that suitable arrangement are in place for this way of working.*

These policy statements are then expanded with a series of organizational guidance statements discussed in the next section.

3.3 ORGANISATIONAL GUIDANCE STATEMENTS

Security policies provided by the standards are intended to be interpreted in an organisational context, and then expanded in local documentation, e.g. Manuals of Procedures. An example of these clarification statements is:

Section 9.1. Business Requirements for Access Control: *The policy should take account of the following:*

a) security requirements of individual business applications;

b) identification of all information related to the business applications;

c) policies for information dissemination and authorization, e.g. the need to know principle and security levels and classification of information;

d) consistency between the access control and information classification policies of different systems and networks;

e) relevant legislation and any contractual obligations regarding protection of access to data or services;

f) standard user access profiles for common categories of job;

g) management of access rights in a distributed and networked environment which recognizes all types of connections available.

3.4 IDENTIFICATION OF CRITICAL ENTITIES

The standard recommends that critical entities be identified and be subject to additional security controls. ***Section 5.1.1 Inventory of Assets*** includes the statement: *An organization needs to be able to identify its assets and the relative value and importance of these assets.* Subsequent sections make reference the significance of other system entities related to such sensitive assets. For example:

- ***Section 7.1 Secure Areas:*** *Critical or sensitive business information processing facilities should be housed in secure areas, protected by a defined security perimeter,* *with appropriate security barriers and entry controls.*

- ***Section 7.2.1 Equipment Siting and Protection:*** *Information processing and storage facilities handling sensitive data should be positioned to reduce the risk of overlooking during their use.*
- ***Section 7.2.6 Secure Disposal or Re-use of Equipment:*** *Storage devices containing sensitive information should be physically destroyed or securely overwritten rather than using the standard delete function.*
- ***Section 9.4.1 Policy on Use of Network Services:*** *This control is particularly important for network connections to sensitive or critical business applications.*
- ***Section 9.5.8 Limitation of Connection Time:*** *Such a control should be considered for sensitive computer applications.*
- ***Section 9.6.2 Sensitive System Isolation:*** *Sensitive systems might require a dedicated (isolated) computing environment.*
- ***Section 9.8 Mobile Computing and Teleworking:*** *Equipment carrying important, sensitive and/or critical business information should not be left unattended.*

3.5 COUNTERMEASURES AND SUPPLEMENTARY COUNTERMEASURES

The standard contains an extensive list of controls, or countermeasures, and many of these controls serve as supplementary countermeasures, the list of controls contained in ***Section 9 Access Control*** are described in detail in this paper (See 4.2.4).

An example of countermeasures and supplementary countermeasures is given in ***Section 7 Physical and Environmental Security:***

- ***Section 7.1.1 Physical security perimeter supported by supplementary countermeasure;***
- ***Section 7.1.2 Physical entry controls;***
- ***Section 7.1.3 Securing offices, rooms and facilities.***

The next section describes the use of the ISM to record these interpretations of the standard and to demonstrate organizational conformance to it.

4 INCORPORATING STANDARDS INTO THE ORGANISATIONAL INFORMATION SECURITY MODEL

4.1 OVERVIEW

The Information Security Model [5, 6] contains detailed proposals for the development of a database plus supporting software to provide security officers with an interactive tool for security management. This section describes how this model can include details of standards such as AS /NZS ISO/IEC 17799:2001 and facilitate audits on conformance to the standards.

Conformance to the AS /NZS ISO/IEC 17799:2001 standard may be tested at a number of levels:

- Cross-reference between internal policies/ procedures and the corresponding standards subsections.
- Evidence of identification of critical assets, systems and networks as proposed by the standards.
- Evidence of implementation of recommended security measures for critical assets and systems.
- Evidence that the implementation of recommended controls conforms to the rationales of the standard.

Some level of conformance may be checked by manually viewing the ISM database information, but for complex systems it would be recommended that conformance software be developed to scan the database contents and report upon discrepancies. In the following sections the various levels of conformance are described. Whilst this section is described in the context of the ISM, the ideas presented are valid for a range of database security documentation approaches.

4.2 STANDARDS CONFORMANCE

4.2.1 Policies and Procedures

The AS/NZS ISO/IEC 17799:2001 Part 1 standard proposes a number of security policies (See 3.2) and also provides examples of procedures to implement those policies (See 3.3). Organisations normally reformulate such policies in a local context, recording them as organisational internal security policies. Organisational documents, e.g. Manuals of Procedures, then draw upon examples of procedures from the standard to advise on the implementation of these local policies. Part 2 of the standard describes various processes for checking that the internal policies and procedures conform to the standard.

The ISM directory provides for the storage of external and internal documentation (See Procedures in Figure 1), and such documentation can be categorised and cross referenced at any desired level of detail, e.g. down to individual subsections. Hence internal policies based upon similar policies recommended by the standard (See 3.2) may be cross-referenced with a Conformance Link (See Figure 4).

The implementation of such policies will depend upon internal procedures and these procedures can in turn be cross-referenced to the internal policies by Implementation Links (See Figure 4). Hence a security officer could easily demonstrate that the various policies and procedures recommended by the standard have been adopted by the organisation. The following sections discuss conformance checking at an implementation level.

4.2.2 Identification of Critical Assets and Systems

Information security management aims to protect organisational information assets against loss of confidentiality, integrity and availability, and the starting point for any viable risk management scheme lies with identification assets essential for the organisation's operation and survival. Hence ***Section 5.1.1 (Inventory of Assets)*** of the standard includes the statement: *An organization needs to be able to identify its assets and the relative value and importance of these assets.* This statement has a number of implications for the internal security procedures and documentation:

- Internal security policy statement on the requirement for the identification of sensitive assets.
- Allocation of responsibility for the identification of sensitive assets.
- Assignment of attributes, describing the relative asset value, to asset entities stored in the model.
- Links between high value assets and any internal policies and /or procedures dealing with the handling of such high value assets.

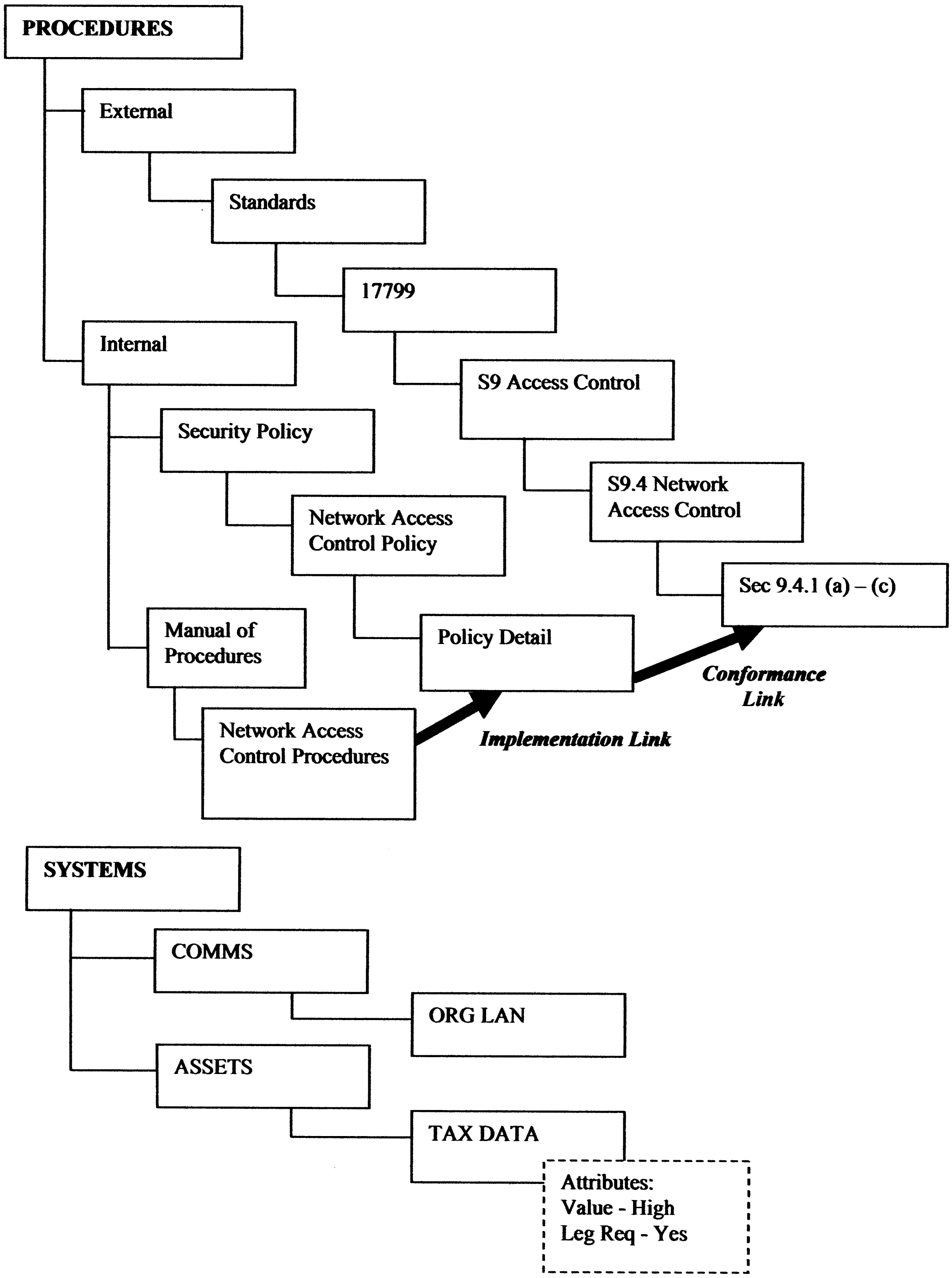


Figure 4 Diagram illustrating various conformance links in the model

- The asset attributes may also include information on regulatory or legislative implications (See Compliance with Legal Requirements Section 12.1 of the standard) e.g. tax data, personal data. Hence linkages should be established between assets with regulatory/ legislative implications and the internal policy/ procedures dealing with corresponding regulations etc.

High value assets may be identified in the model with an attribute <Value - High>; similarly any legislative requirements may be indicated with the attribute < Legislative Req - Yes>. Security Requirement Links may then be established between such assets and the corresponding Policy/ Procedures subsections in the internal documentation.

Sensitive assets are identified to ensure that they are processed, stored, transmitted etc. by systems and networks with the appropriate level of security. As mentioned above ***Section 4.1.3 (Allocation of Information Security Responsibilities)*** of the standard, specifies that: *The various assets and security processes associated with each individual system should be identified and clearly defined.* Thus the model should also incorporate appropriate links between identified high value assets and the systems/ networks that store, process, output and transmit such assets.

4.2.3 Security Measures for High Value Assets and Systems

Systems hosting high value assets should be subject to specific security policies and details of these measures should be included in the security database. For example, *Section 7.1 (Secure Assets)* includes the policy: *Critical or sensitive business information processing facilities should be housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls.* The sensitive systems, identified by their links with high value assets, might in turn be required to include Location links leading to the Environment (Physical Location) entities – describing the rooms or buildings hosting the systems. Buildings or rooms identified as hosting sensitive systems would in turn have links to subsections of internal documentation, specifying the physical security measures to be applied.

This and previous sections have demonstrated that the ISM can relate individual assets, systems, networks and physical locations to the security policies and procedures required by the standard. The next level of conformance checking involves auditing the security controls and countermeasures implemented, against those proposed by the standard.

4.2.4 Security Controls and Their Rationale

The standard states: *"A comprehensive set of controls comprising the best information security practices currently in use is provided in this Standard"*. Organisations must decide if and how these controls and security practices should be deployed locally, and their security documentation should contain sufficient information on the controls and rationale to ensure that they are implemented, operated, maintained and updated as the local context develops.

The documentation of security control rationale assists security officers in determining if and how the controls proposed by the standard should be implemented locally and in addition it informs:

- security auditors on the reason for any deviation between the local controls and those recommended by the standard;
- system developers of the implications of any proposed modifications to the implemented controls.

The ISM employs threat networks and threat countermeasure diagrams to illustrate the rationale of countermeasures, and supplementary countermeasures. A threat network (See Figure 5) illustrates the potential propagation of threats throughout the organization; commencing at the top with nodes representing incident threat events beyond the control of the organization, and terminating with nodes displaying business impacts arising from damage to information assets. Countermeasures are included in the threat networks and are associated with threat propagations, i.e. the role of the countermeasure is to minimize the probability of threat event *TE2* by addressing the threat propagation *TE1-TE2* (See Figure 3).

- Threat countermeasure diagrams (TCD) (See security auditors on the reason for any deviation between the local controls and those recommended by the standard;
- system developers of the implications of any proposed modifications to the implemented controls.

Threat countermeasure diagrams (TCD) (See Figure 3) illustrate potential attacks on the countermeasures themselves and the deployment of supplementary countermeasures. Countermeasure CM1, implemented to reduce the threat propagation TE1-TE2, depends upon its components (Components 1 & 2). If either component is adversely affected by a threat then the effectiveness of CM1 is reduced. Component 1 may be affected by threat event TE1.2 caused by TE1.1. A supplementary countermeasure (Supp CM1) is used to defend against this threat propagation.

Significant manual effort is involved in the production of threat networks and TCDs. The ISM therefore includes interactive software to facilitate the development and display of these diagrams. The next section (See 4.3) provides a detailed description of threat networks and TCDs corresponding to the controls described in ***Section 9 Access Control*** of the standard. These diagrams illustrate the ISM approach and to suggest how organizational security documentation may demonstrate conformance to the standard at this detailed level.

4.2.5 Conformance Checking

The model implementation as described above provides for various links between entities corresponding to the local policies and procedures, and the use of threat networks / TCDs to document controls and countermeasures. The database implementation of the security documentation facilitates ad hoc updating and hence assists in maintaining the currency of the security information, but such ad hoc updating can easily lead to inconsistencies in the stored data. Consider the following scenario. A change in organizational regulations now requires that a certain class of information be archived for five years. The nominated manager with responsibility for asset valuation requests that the value attribute for that asset be upgraded to high, and the asset legal attribute be added. This change, as seen above, has implications for other entities stored in the model, and there is no guarantee that these changes, or their security implications, will be immediately implemented by the person upgrading the asset value. Hence updating the asset value may result in the:

- absence of link from the high value asset to the corresponding internal policy;
- absence of link from the asset to the systems processing , transmitting or storing the asset;
- absence of link from the above systems to their locations;
- absence of link from the above locations to the procedures specifying required physical security.

In other words merely updating the asset value gives no assurance that the requisite security measures will be in place for this high value asset. Conformance checking software can, however, highlight such situations and report them to security management. For example, the updating process may indicate that the asset now requires a higher level of security.

The conformance software will be designed in the light of the local security policy and procedures, checking asset attributes, and links between entities, to ensure that conformance of local policies/ procedures with the standard, and conformance of system security etc. to the local policies. To this extent the conformance software is auditing conformance to internal security policies, at least to the extent that the policy or security procedure requirements for security entities such as assets, systems, locations etc are explicitly linked to those entities.

Such conformance software can embed local knowledge of polices and procedures and thus highlight apparent non-

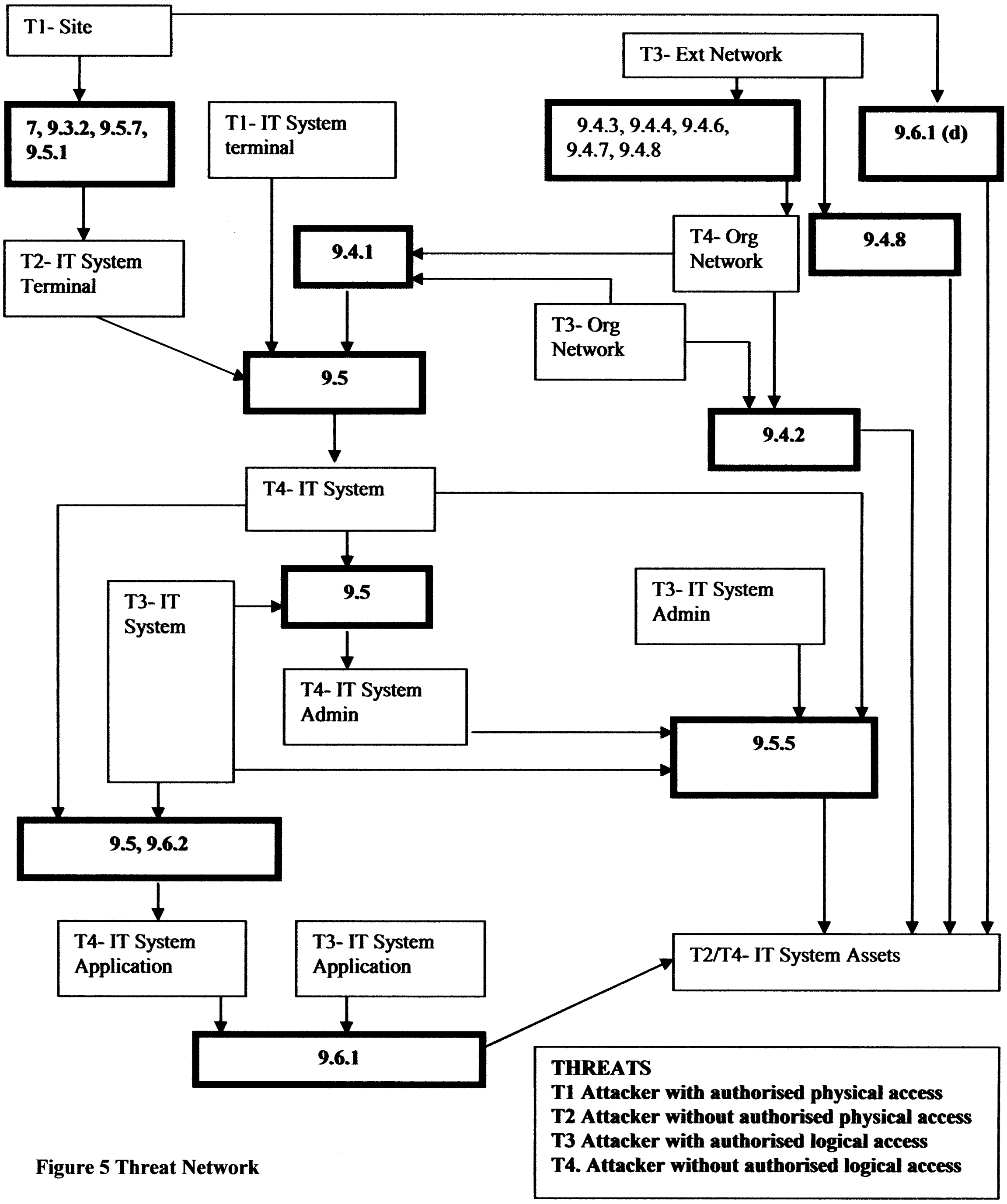


Figure 5 Threat Network

conformance when the database information is set up or modified. However it cannot determine if the requisite level of security is actually implemented. Security officers need to interpret threat networks/TCDs to check at this level of conformance. Conformance software can however report changes to stored information that could have implications for such threat networks/ TCDs.

The threat networks/ TCDs illustrating security controls will refer to assets, systems, networks etc. and may be influenced by changes to entity attributes. For example, a threat network may indicate that the risk of loss of availability of a network, due to severe weather events, is low partly because the routers are located in a well-constructed building. If the location is changed to a more vulnerable building then the probability of certain threat propagations will rise. Conformance software can at least detect changes to ISM database entities, referenced by nodes in threat networks / TCDs and thus report those modifications with potential implications for such threat networks/ TCDs.

4.3 INTERPRETATION OF ISO/IEC 17799 ACCESS CONTROLS

4.3.1 Overview

The previous section discussed the use of the ISM to check the conformance, consistency and effectiveness of organisational security management in relation to the ISO/IEC 17799 standard. The ISM employs threat networks and threat countermeasure diagrams (TCDs) to record the rationale and effectiveness of information security controls. In this section the approach is employed on the controls described in ***Section 9 Access Control*** of the standard. This discussion will thus describe the procedures suggested above (See 4.2.4) for checking the conformance and effectiveness of organisational controls against the standard.

4.3.2 An Access Control Threat Network

4.3.2.1 Overview

This section places the controls suggested by the standard in the context of typical organisational security scenario. As a first step a Threat Network (See Figure 5) was developed in accordance with the proposals of the ISM, concentrating on the access controls discussed in the ***Section 9 Access Control*** of the standard. The Threat Network assumes threats arising from attackers with

- authorised physical access to a site;
- authorised logical access to an external network;
- various levels of access rights.

It traces the potential threat paths down from illicit access to a sensitive information asset.

Hence the incident threats, illustrated as Threat Events with no incident threat, considered were (See Figure 5):

- attacker has authorised physical access to the organisation site;
- attacker has authorised logical access to an external network;
- attacker has authorised logical access to an internal network;
- attacker has authorised physical access to an IT terminal;
- attacker has authorised logical access to the IT system;
- attacker has authorised logical access to the IT system administration facilities;
- attacker has authorised logical access to the IT system application.

The end node of the threat network is a successful attack on information system assets processed by the IT system application i.e.

- attacker has unauthorised logical access to the IT system information asset.

The controls are indicated by boxes with thick borders and by the subsection reference of the standard. For example consider the path extracted from the threat network illustrated in Figure 6 representing an attacker:

- with authorised physical access to the organisation site, gaining access to a printer or terminal displaying confidential information, i.e. gaining unauthorised access to a printed version of the IT system information asset data.

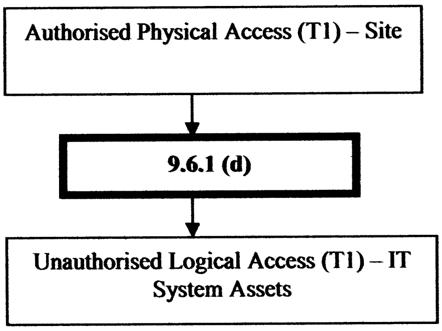

Authorised Physical Access (T1) – Site
9.6.1 (d)
Unauthorised Logical Access (T1) – IT System Assets

Figure 6 Path of Threat Network

This attack is countered by Section 9.6.1(d) which recommends – ensuring that outputs from application systems handling sensitive information contain only the information that are relevant to the use of the output and are sent only to authorized terminals and locations.

The countermeasures and supplementary countermeasures from the standard (See 3.5) were then examined and mapped to the threat propagation links in the diagram (See Figure 5). These controls are shown in outlined boxes with the relevant standard paragraph number (e.g. 9.5.7). The development of this threat network process proved to be quite instructive; in many cases the role of the control is not explicitly stated in the standard and controls which at first sight appeared to address on part of the threat network were found on closer inspection to be more appropriately placed elsewhere. In other cases it led to the refinement of the threat network with some propagation links expanded to include additional nodes.

The threat network indicates the threat propagations and countermeasures designed to inhibit such threat propagations. However, these countermeasure themselves may be subject to attack and hence require supplementary countermeasures to ensure their effectiveness. Threat Countermeasure Diagrams (TCDs) (See 2.3.3.2) are used to demonstrate the role of such supplementary countermeasures and are discussed below in relation to the various component parts of the overall threat network.

The following section presents a more detailed discussion of one small subset of the controls, proposed by the standard, in the context of the threat network and associated TCDs, hence providing an insight into the context and rationale of the controls. A comprehensive discussion of the threat network and associated TCDs is given in the Appendix (See 8).

4.3.2.2 Description of a Threat Network

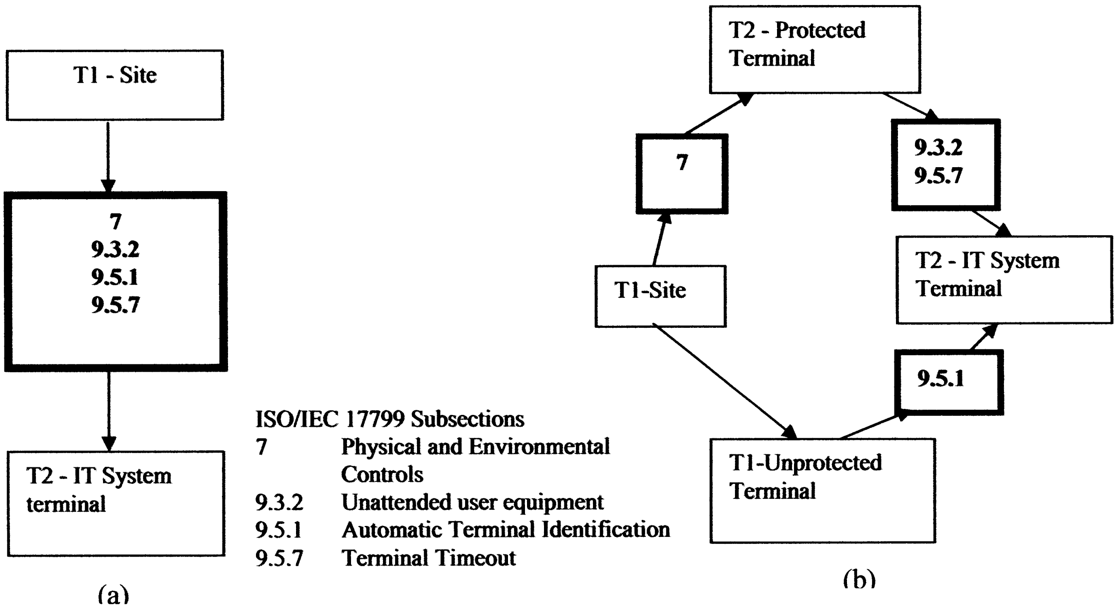
One section of the Threat Network is concerned with the situation in which someone allowed physical access to a public area can gain logical access to a terminal or workstation, with potential links to the identified sensitive information asset (See Figure 7 (a)). The controls actually address a refinement of this threat propagation i.e.

- physical access to a terminal in a protected area;
- physical access to a terminal in an unprotected area.

This expanded diagram is illustrated in Figure 7(b). ***Section 7 Physical and Environmental Protection*** of the standards contains physical access controls designed to reduce the threat propagation: *Authorised physical access to site leads to unauthorised physical access to protected terminal.* The threat propagation: *physical access to the protected terminal may result in logical access to the IT system terminal* is countered by the controls:

- ***9.3.2 – Unattended User Equipment,*** e.g. use of password protected screen savers
- ***9.5.7 – Terminal Timeout,*** i.e. ensuring that unattended terminals are automatically logged out after a specified period.

Terminals in an unprotected area should not allow access to an IT system with access to sensitive assets. This may be achieved by use of ***Automatic Terminal Identification (9.5.1)*** which ensures that only specifically authenticated terminals are allowed access to the IT System, terminals in unprotected areas would thus be identified as unauthorised terminals for this purpose.



ISO/IEC 17799 Subsections

7	Physical and Environmental Controls
9.3.2	Unattended user equipment
9.5.1	Automatic Terminal Identification
9.5.7	Terminal Timeout

Figure 7 Threat Paths Leading to Unauthorised Logical Access to IT System

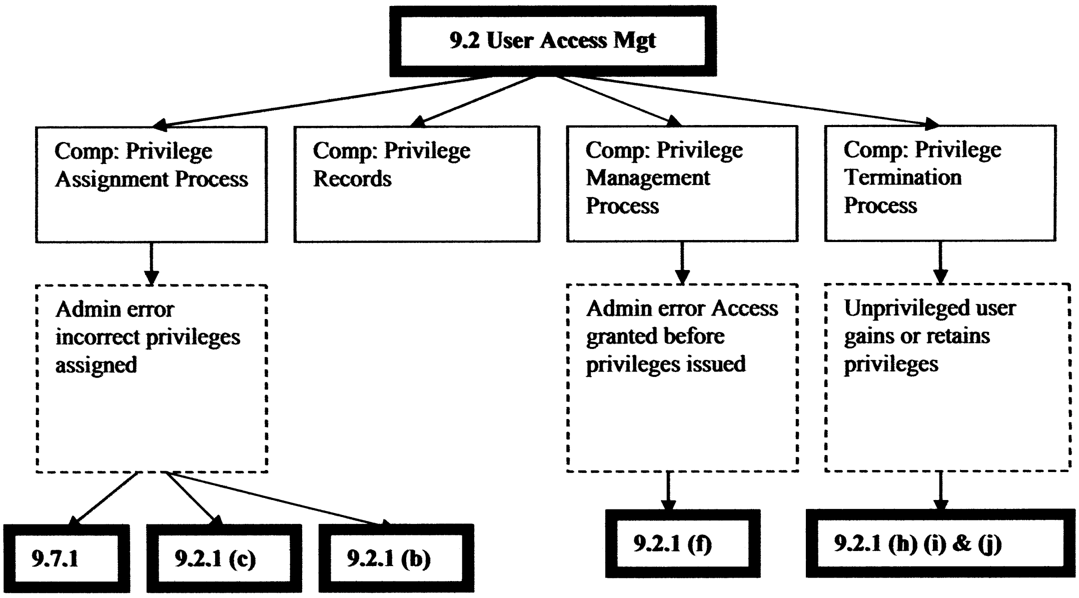

9.2 User Access Mgt
Comp: Privilege Assignment Process
Comp: Privilege Records
Comp: Privilege Management Process
Comp: Privilege Termination Process
Admin error incorrect privileges assigned
Admin error Access granted before privileges issued
Unprivileged user gains or retains privileges
9.7.1
9.2.1 (c)
9.2.1 (b)
9.2.1 (f)
9.2.1 (h) (i) & (j)

Figure 8 User Rights Management TCD

9.2.1 (c) Checks of privileges against policy
9.2.1 (b) Check privileges with owner
9.2.1 (f) Ensure privileges not granted before authorization process comp.
9.2.1 (h), (i) & (j) Termination procedures etc.
9.7.1 Event Logging

Section 9.5 of the standard describes Operating System Access Control discussed in detail below (See Appendix). ***Section 9.2 User Access Management*** provides supplementary countermeasures to support Operating System Access Control and is discussed in this section as an example of a TCD (See Figure 8). This section does not, however, include all the supplementary controls described in Appendix.

Access control systems do not guarantee to denial of access to attackers, they merely promise that access will be restricted to subjects with the appropriate access rights. An attacker could well attempt to gain the necessary rights in a fraudulent manner and ***Section 9.2 User Access Management*** introduces the policy that *formal procedures should be in place to control the allocation of access rights to information systems and services.* Hence Section 9.2 represents a supplementary control to Section 9.5 (See Figure 10).

The access rights assignment process itself has a number of components that may be subject to attack:

- rights assignment process,
- rights records,
- rights management process,
- rights termination process.

Each of these components is associated with supplementary controls to counter potential attacks, for example:

- Rights Assignment Process
  - Attacker may seek to gain an excess level of – standard proposed supplementary control is 9.2.1(c) checking that the level of access granted is appropriate to the business purpose...
  - Attacker may seek an unauthorised access right – standard proposed supplementary control is 9.2.1 (b) *checking that the user has authorization from the system owner for the use of the information system or service...*
- Rights Management Process
  - Access granted before rights management assignment completed – standard proposed supplementary control is 9.2.1(f) *ensuring service providers do not provide access until authorization procedures have been completed.*
- Termination Process
  - User continues to access system after need to know condition expires – standard proposed supplementary control is 9.2.1 (h) *immediately removing access rights of users who have changed jobs or left the organization.*
  - User incorrectly granted rights of previous user – standard proposed supplementary control is 9.2.1 (j) *ensuring that redundant user IDs are not issued to other users.*
  - Access rights retained in spite of 9.2.1 (h) – 9.2.1 (i) is actually a supplementary control to 9.2.1(h) i.e. *periodically checking for, and removing, redundant user IDs and accounts.*

5 CONCLUSIONS

IS Governance aims to protect society by encouraging organisations to implement a level of information security consistent with the risk of their IT system failures causing societal damage. The measures taken by organisational management to meet IS Governance requirements should encompass the spirit as well as the word of the legislation; in particular conformance to Information Security Management standards, e.g. ISO 17799, should be aimed at capturing the rationale of the recommendations.

The distributed complex IT systems currently deployed by many organisations renders such rigorous conformance testing difficult and time consuming, particularly when involve it involves cross checking internal documentation against the standards. This paper has sought to demonstrate the application of an electronic form of security documentation to such conformance testing employing the Information Security Model approach described in an earlier paper. The graphical representation of Threat Networks and Threat Countermeasure Diagrams facilitate the interpretation of the various controls described in the ISO 17799 standard. The recording of organisation security systems according to a proposed directory of security entities, combined with conformance software, can assist organisations to implement and maintain security regimes as recommended by the standards.

6 ACKNOWLDGEMENT

This paper was conducted under the auspices of the Australian Research Council funded project: Mapping Trusted Systems Technologies to E-security Requirements (Project ID: DP0449644).

7 REFERENCES

[1] Standards Australia (2004), *DR 04198: Corporate governance of information and communication technology*. http://www.standards.org.au/

[2] The Corporate Governance Task Force – National Cyber Security Partnership (2004), *Corporate Governance Task Force Report*, http://www.entrust.com/news/2004/corporategovernancetaskforce.pdf?entsrc=isgfullreport

[3] IT Governance Institute (2005), *Control Objectives for Information and Related Technology* (3e), http://www.itgi.org/

[4] Information Systems Audit and Control Association (2005), *Overview of COBiT*, http://www.isaca.org/

[5] Kwok LF and Longley D. "Security Modelling for Risk Analysis" *Proc. 18th IFIP World Computer Congress, IFIP 2004, 22-27 August 2004*, Toulouse, France, pp29-45

[6] Fung P, Kwok L F, and Longley D. "Electronic Information Security Documentation" in (Eds. Johnson C, Montague P, Steketee C) *ACSW Frontiers 2003*, Australasian Information Security Workshop (AISW2003), February 2003, Adelaide, Australia, pp25-31.

[7] Kwok L F and Longley D, "Information Security Management and Modelling", *Information Management and Computer Security*, Vol. 7, No. 1, 1999, pp.30-39

[8] Kwok L F and Longley D, "A Security Officers' Workbench", *Computers and Security*, Vol.15, No. 8, 1996, pp. 695-705.

8 APPENDICES

8.1 DETAILED DESCRIPTION OF CONTROLS

8.1.1 Authorised or Unauthorised Physical Access IT System Terminal – Unauthorised Logical Access to IT System

This section of the Threat Network is concerned with a situation in which an attacker with authorised or unauthorised physical access to a terminal connected to the IT System attempts to gain unauthorised logical access to the IT System itself (See Figure 9). The control described in ***Section 9.5 Operating System Access Control*** actually comprises a countermeasure supported by a number of supplementary countermeasures as illustrated by the Threat Countermeasure Diagram (TCD) (See Figure 10)

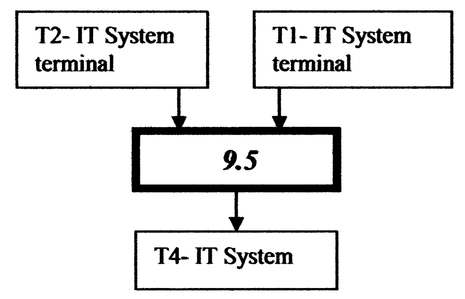
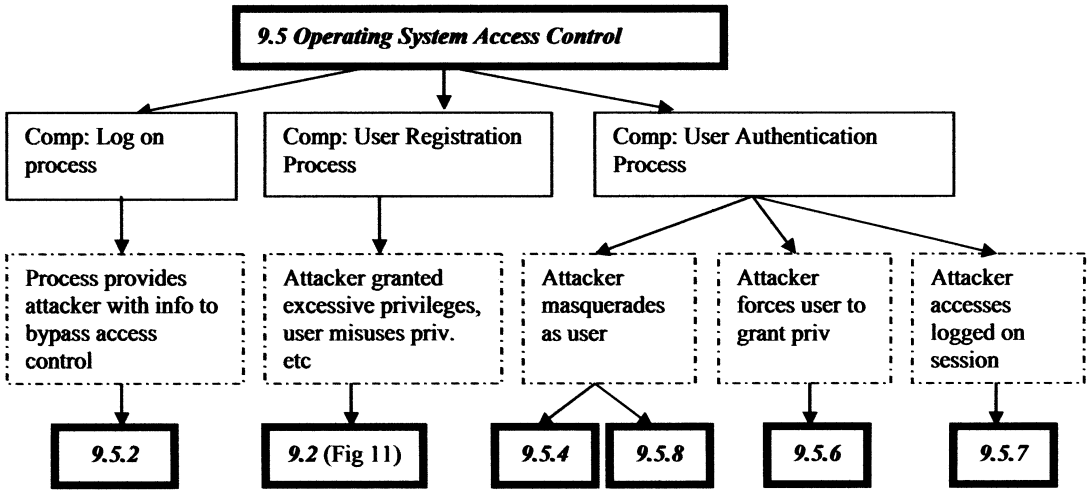


Figure 9 OS Access Control Component of Threat Network


9.5 Operating System Access Control
Comp: Log on process
Comp: User Registration Process
Comp: User Authentication Process
Process provides attacker with info to bypass access control
Attacker granted excessive privileges, user misuses priv. etc
Attacker masquerades as user
Attacker forces user to grant priv
Attacker accesses logged on session
9.5.2
9.2 (Fig 11)
9.5.4
9.5.8
9.5.6
9.5.7

9.2. User Access Mgt 9.5 Operating System Access Control
9.5.2 Terminal Log On Procedures 9.5.4 Password Management System
9.5.6 Duress Alarm 9.5.7 Terminal Timeout

Figure 10 OS Access`Control Threat Countermeasure Diagram

The effectiveness of the Operating System Access Control depends upon certain components of its operation, i.e.

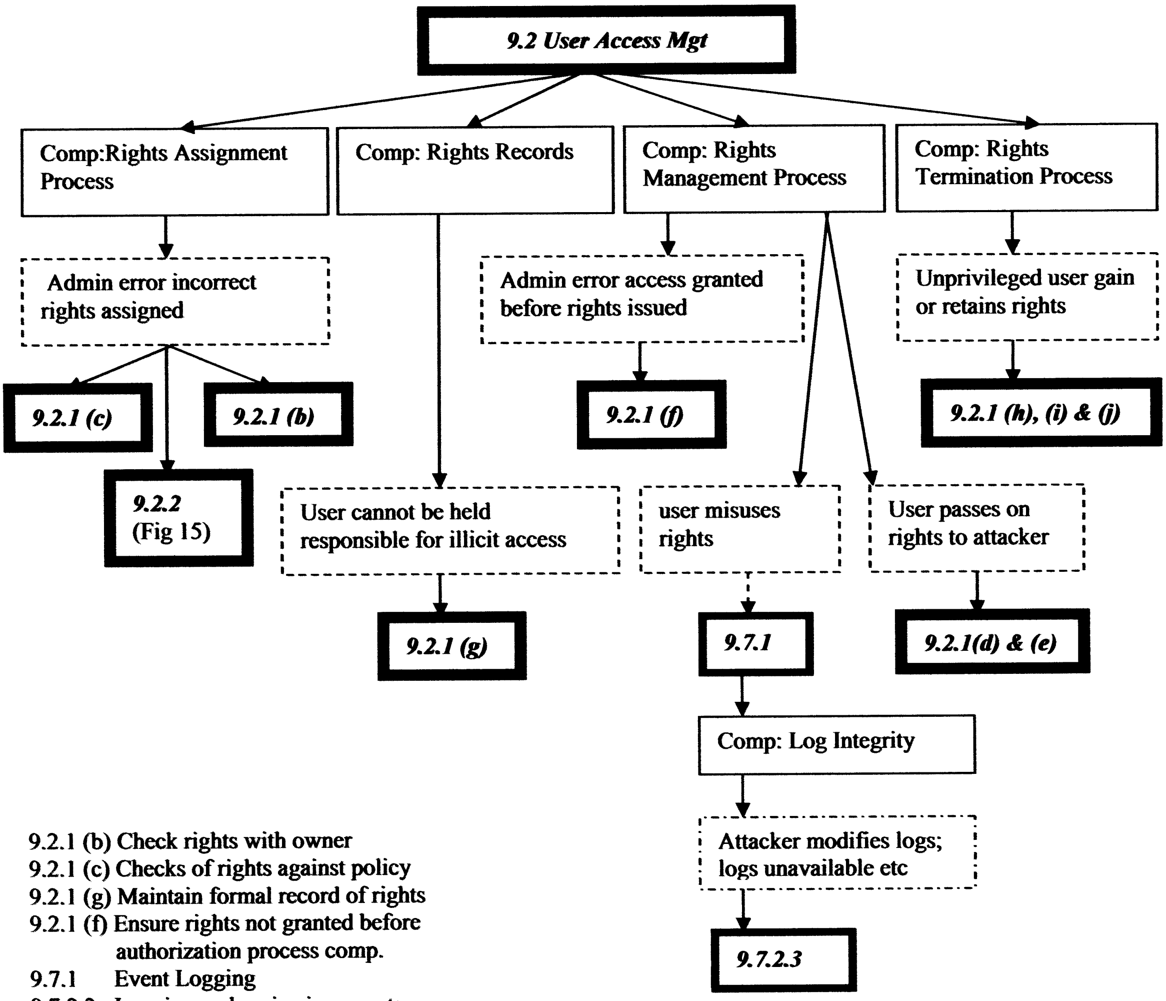
- Logon Process – the attacker may gain sufficient information from the logon screens and processes to facilitate an attack.
- User Authentication Process – an attacker may gain the rights of a registered user by misuse of this process.
- User Registration Process – the user may be granted excessive rights etc.

The standard provides additional controls, acting as supplementary countermeasures, to counter the potential attacks to these components, i.e.

- Logon Process – ***9.5.2 Terminal Log-on Procedures –*** advising on the minimisation of system information displayed, ensuring that the log on process does not provide useful information to the attacker etc.
- User authentication process:
  - Masquerade attacks – ***9.5.4 Password Management System*** providing advice on the selection of passwords etc 9.5.8 Limitation of Connection Time – minimising the periods during which the terminal may log onto the system.
  - Duress attacks – ***9.5.6 Duress Alarm to Safeguard Users*** hence allowing user to silently warn the system that the logged on user is acting under threat of physical attack.
  - Accessing a logged on terminal ***9.5.7 Terminal Timeout –*** minimising the period that the terminal is logged on after the operator ceases operations.
- The ***User Registration Process (9.2)*** is a component of the Operating System Access Control countermeasure that itself has a number of components impacting upon its effectiveness:
  - Rights Assignment Process – a user may be assigned excessive rights.
  - Rights Records – it may not be possible to make a user accountable for their actions.
  - Rights Management Process – users may misuse their rights.
  - Rights Termination Process – users may retain their rights after the "need to know" conditions expire.

The standard provides controls that may act as supplementary countermeasures to counter these potential security vulnerabilities (See Figure 11):

- Rights Assignment Process
  - ***Excessive rights assignment*** – ***9.2.1 (c)*** check proposed rights against policy
  - ***Incorrect rights assignment – 9.2.1 (b)*** check proposed rights with system owner
- ***Rights Records –*** user denies responsibility – ***9.2.1 (g)*** maintain formal record of rights
- Rights Management Process
  - Access granted before right management assignment completed – ***9.2.1(f)*** instruction to service providers not to provide premature access
  - User misuse rights – ***9.7.1*** event logging procedures to detect access misuse
    - Event logs not reviewed or illicitly modified – ***9.7.2.3*** procedures for logging and reviewing events
  - User passes on rights to attacker
    - ***9.2.1 (d)*** user given a statement of access responsibilities
    - ***9.2.1(e)*** user required to sign statement acknowledging access responsibilities
- Rights Termination Process
  - User continues to access system after need to know condition expires – ***9.2.1 (h)*** process for withdrawing rights as soon as user resigns, changes post etc
  - Access rights retained in spite of ***9.2.1(h) – 9.2.1(i)*** process for periodically checking and removing redundant accounts


9.2 User Access Mgt
Comp:Rights Assignment Process
Comp: Rights Records
Comp: Rights Management Process
Comp: Rights Termination Process
Admin error incorrect rights assigned
Admin error access granted before rights issued
Unprivileged user gain or retains rights
9.2.1 (c)
9.2.1 (b)
9.2.1 (f)
9.2.1 (h), (i) & (j)
9.2.2 (Fig 15)
User cannot be held responsible for illicit access
user misuses rights
User passes on rights to attacker
9.2.1 (g)
9.7.1
9.2.1(d) & (e)
Comp: Log Integrity
Attacker modifies logs; logs unavailable etc
9.7.2.3

9.2.1 (b) Check rights with owner
9.2.1 (c) Checks of rights against policy
9.2.1 (g) Maintain formal record of rights
9.2.1 (f) Ensure rights not granted before
authorization process comp.
9.7.1 Event Logging
9.7.2.3 Logging and reviewing events
9.2.1
(d) & (e) Written statement of conditions of access
(h), (i) & (j) Termination procedures etc.

Figure 11 User Access Management Threat Countermeasure Diagram

User incorrectly granted rights of previous user – ***9.2.1 (j)*** process for ensuring that redundant IDs are not reissued.

8.1.2 Authorised or Unauthorised Logical Access to IT System – Unauthorised Logical Access to IT System Applications

This section is concerned with a situation in which a user has successfully accessed the IT system and now attempts an unauthorised access to the applications linked to the sensitive system assets. The countermeasures provided are, ***Section 9.5 Operating System Access Control and Section 9.6.2 Sensitive System Isolation,*** e.g. running sensitive applications on dedicated computers (See Figure 12).

8.1.3 Authorised or Unauthorised Access to IT System Applications – Unauthorised Access to IT System Assets

This section is concerned with restricting the application user's ability to access the underlying information assets (See Figure 13). The controls proposed by the standards for this purpose are ***Section 9.6.1 Information Access Restriction:***

- ***9.6.1 (a)*** – use of menus etc to restrict user's freedom to navigate the assets;
- ***9.6.1(b)*** – restricting the user's knowledge of the application by editing the system documentation;
- ***9.6.1 (c)*** – controlling the user's access rights to the information – read, write etc.

8.1.4 Authorised and Unauthorised Access to IT System – Unauthorised Access to IT System Administration

This section is concerned with the situation in which an attacker seeks to gain administrative privileges in order to attack system assets. The control is illustrated in Figure 14 and expanded in Figure 15.

In effect the control is based upon ***Section 9.5 Operating System Access Control*** and addresses particularly the ***Privilege Assignment Process*** Component of that countermeasure using ***Section 9.2.2 Privilege Management***. This control has three components:

- System Privilege Assignment Process
- Privilege Records
- System Privilege Management Process

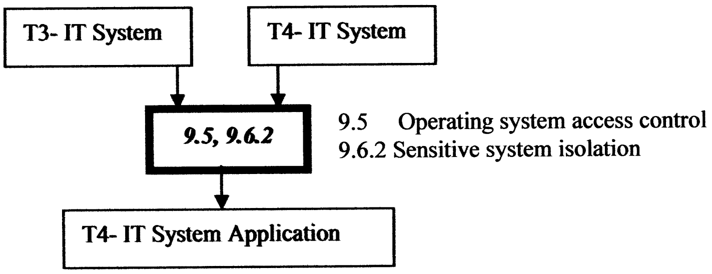

T3- IT System
T4- IT System
9.5, 9.6.2
9.5 Operating system access control
9.6.2 Sensitive system isolation
T4- IT System Application

Figure 12 Unauthorised Access to Application Component of Threat Network

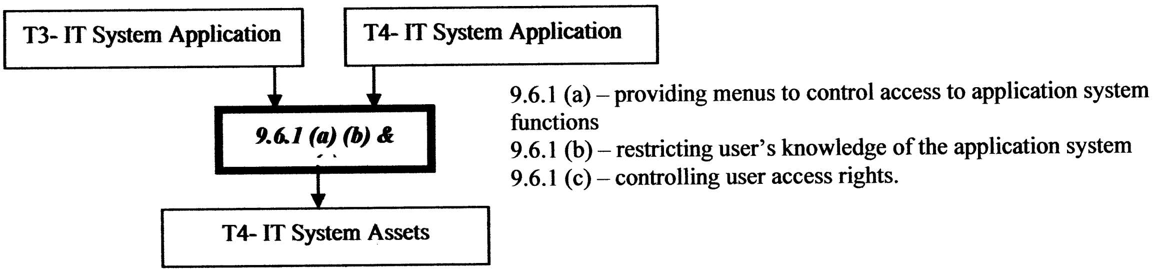

T3- IT System Application
T4- IT System Application
9.6.1 (a) (b) &
9.6.1 (a) – providing menus to control access to application system functions
9.6.1 (b) – restricting user's knowledge of the application system
9.6.1 (c) – controlling user access rights.
T4- IT System Assets

Figure 13 Application Access Control Component of Threat Network

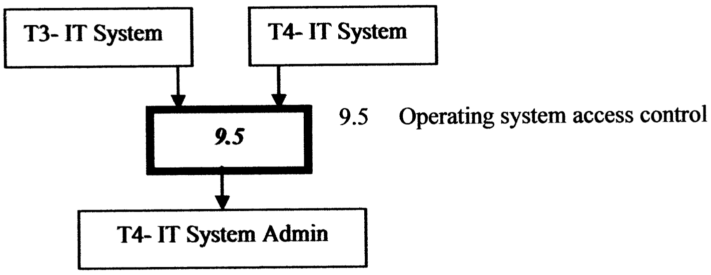


Figure 14 Access Control of System Privileges Component of Threat Network

The controls effective provide supplementary countermeasures to these components:

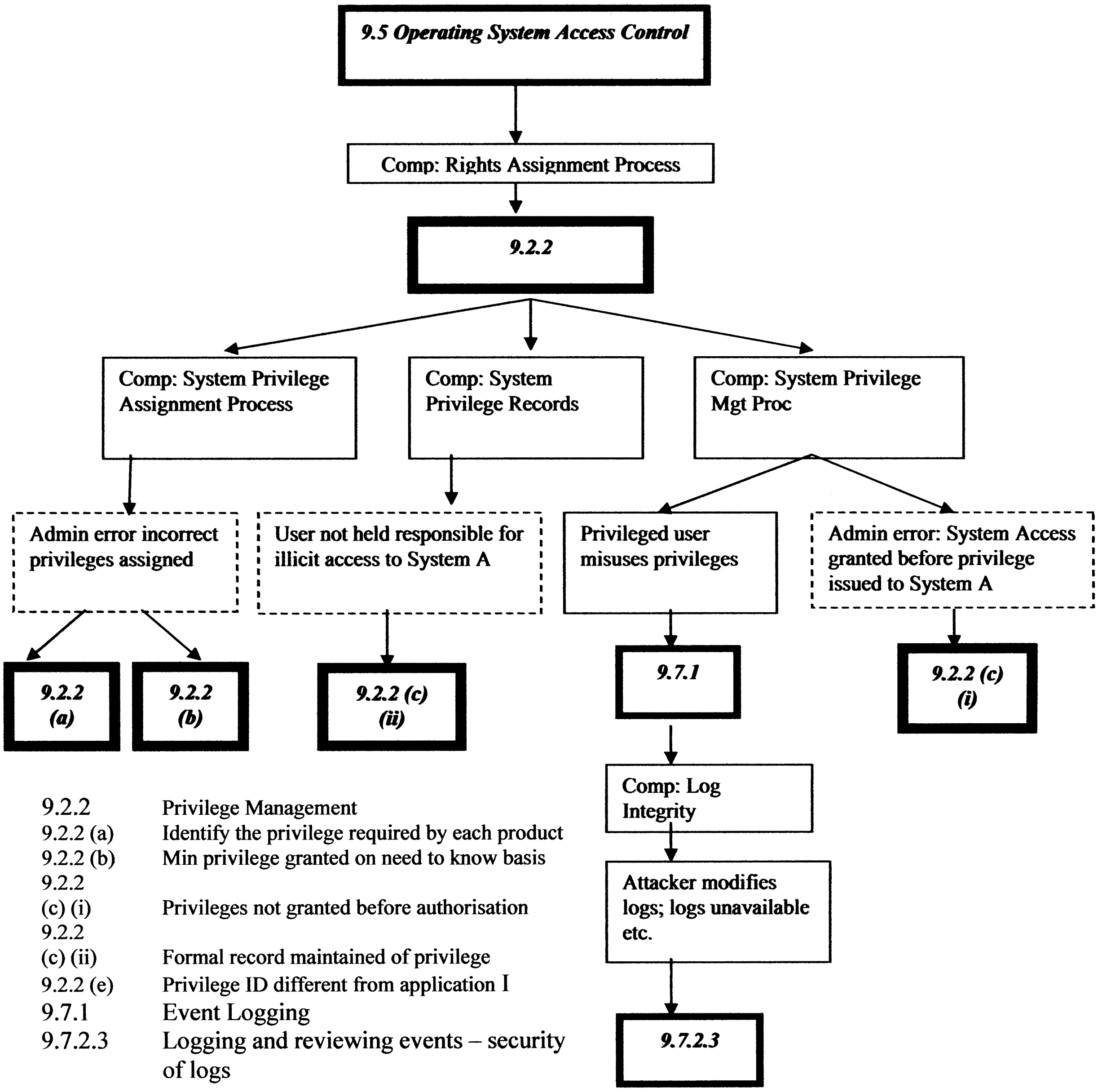
- System Privilege Assignment Process
  - Administration error excessive privileges assigned
    - ***9.2.2 (a) –*** identify the privileges associated with each product and staff category
    - ***9.2.2 (b)*** – allocate privileges on a need-to-know basis
- Privilege Records
  - User denies privileges were granted – ***9.2.2.(c)*** maintain a record of all privileges granted
- System Privilege Management Process
  - User misuses privileges – ***9.7.1 Event Logging –*** maintain logs of user activities
    - User tampers with logs – ***9.7.2.3 Logging and Reviewing Events*** – ensure security of logs.
  - Privileges granted before authorisation process completed – ***9.2.2 (c)*** privileges not granted before authorisation process completed.

8.1.5 Authorised or Unauthorised Logical Access to IT System or IT System Administration – Unauthorised Logical Access to System Assets

These controls are concerned with attacks that bypass the application software and attempt direct logical access to the sensitive assets; this will normally be attempted by the use of software utilities designed to read database files etc (See Figure 16). ***Section 9.5.5 Use of System Utilities*** provides a series of control to counteract this form of attack e.g. removing unnecessary utilities, requiring authentication for access to utilities etc.

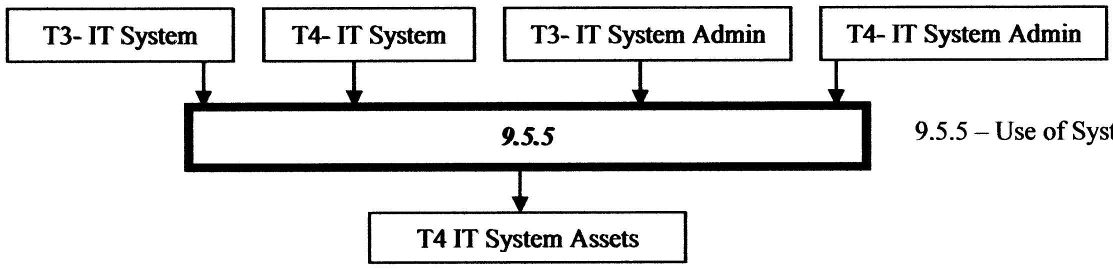
8.1.6 Authorised Physical Access to Site – Unauthorised Physical Access IT Assets

This section is concerned with direct physical access to sensitive information gained by an attacker with authorised physical access to the site. ***Section 9.6.1 (d)*** recommends that sensitive information only be transmitted to authorised terminals and printers, thus allowing for the prohibition of transmission to devices that may be accessed by unauthorised persons (See Figure 17).


9.5 Operating System Access Control
Comp: Rights Assignment Process
9.2.2
Comp: System Privilege Assignment Process
Comp: System Privilege Records
Comp: System Privilege Mgt Proc
Admin error incorrect privileges assigned
User not held responsible for illicit access to System A
Privileged user misuses privileges
Admin error: System Access granted before privilege issued to System A
9.2.2 (a)
9.2.2 (b)
9.2.2 (c) (ii)
9.7.1
9.2.2 (c) (i)
Comp: Log Integrity
Attacker modifies logs; logs unavailable etc.
9.7.2.3

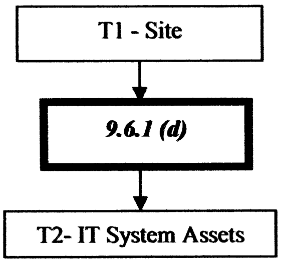
9.2.2	Privilege Management
9.2.2 (a)	Identify the privilege required by each product
9.2.2 (b)	Min privilege granted on need to know basis
9.2.2 (c) (i)	Privileges not granted before authorisation
9.2.2 (c) (ii)	Formal record maintained of privilege
9.2.2 (e)	Privilege ID different from application I
9.7.1	Event Logging
9.7.2.3	Logging and reviewing events – security of logs

Figure 15 Threat Countermeasure Diagram for Privilege Management



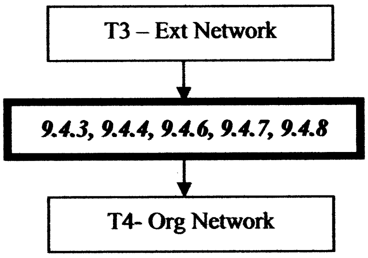
9.5.5 – Use of System Utilities

Figure 16 System Utilities Component of Threat Network



9.6.1 (d) Information Access Restriction –
send sensitive data only to
authorised terminals, printers etc.

Figure 17 Sensitive Peripherals Component of Threat Network



9.4.3	User Authentication for External Connections (Call Back)
9.4.4	Node Authentication
9.4.6	Segregation in Networks (Firewalls)
9.4.7	Network Connection Control (time of connection etc, effectively rules for firewalls))
9.4.8	Network Routing Control

Figure 18 Network Access Component of Threat Network

8.1.7 Authorised Logical Access External Network – Unauthorised Logical Access Organisational Network.

This section is concerned with attacks arising from external networks (See Figure 18). ***Section 9.4.6 Segregation in Networks*** recommends that organisation networks be segregated into domains to minimise the effort of securing networks carrying sensitive data. The controls are illustrated in Figure 19. The access from the external network may take the form of PSTN dialup or simple router connection. The controls comprise:

- ***Section 9.4.3 User Authentication for User Connections*** – e.g. the use of call back to authenticate external dial up connections;
- ***Section 9.4.4 Node Authentication*** – e.g. use of cryptographically based challenge response;
- ***Section 9.4.6 Segregation of Networks*** – e.g. firewalls.

- Firewall rules are important components of firewall countermeasures and this component may be subject to attack and require supplementary countermeasures.
  - The attacker may effectively seek to introduce malicious traffic that will bypass the rules – ***Section 9.4.7 Network Connection Control*** suggests measure such as restriction of time/ date of access to strengthen the defence.
  - The attacker may also seek to insert malicious traffic by disguising the source address to bypass the firewall rules – ***Section 9.4.8 Network Routing Control*** seeks to reduce the available paths to the protected network.

8.1.8 Authorised or Unauthorised Logical Access Organisational Network – Unauthorised Access IT System

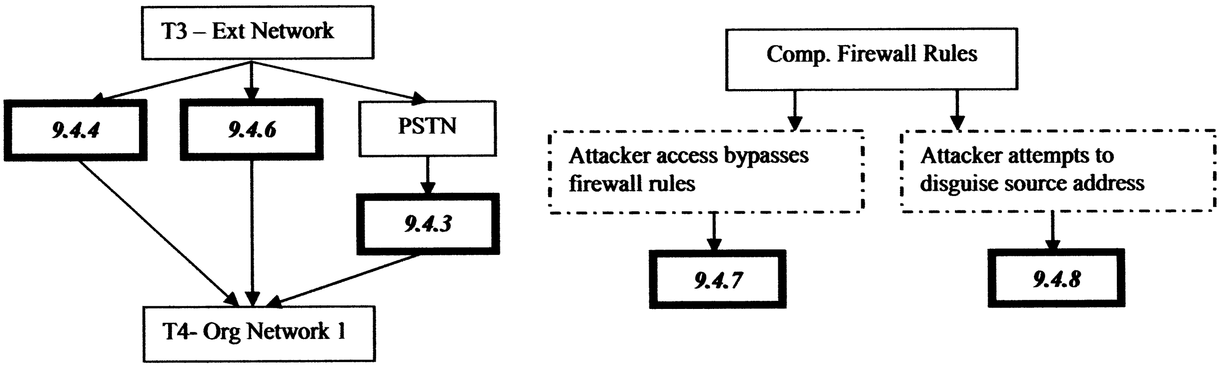

T3 – Ext Network
9.4.4
9.4.6
PSTN
9.4.3
T4- Org Network 1
Comp. Firewall Rules
Attacker access bypasses firewall rules
Attacker attempts to disguise source address
9.4.7
9.4.8

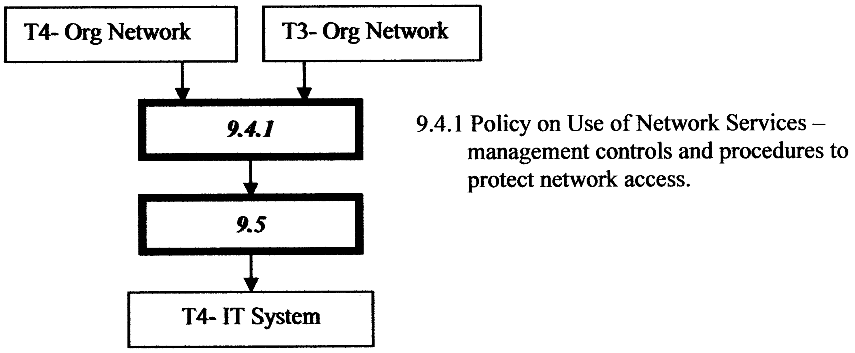
Figure 19 Expanded Components of Network Access Threat Network and Threat Countermeasure Diagram

Access from an organisation network to the IT System is subject to Section 9.4.1 – Policy on Use of Network Services and 9.5 Operating System Access Control (See Figure 20). Section 9.4.1 sets an overall policy on the use of networks and network services to provide a degree of control on the ability of an attacker to make illicit use of a network connection.

8.1.9 Authorised Logical Access External Network / Authorised and Unauthorised Logical Access Organisational Network- Unauthorised Access IT System Assets

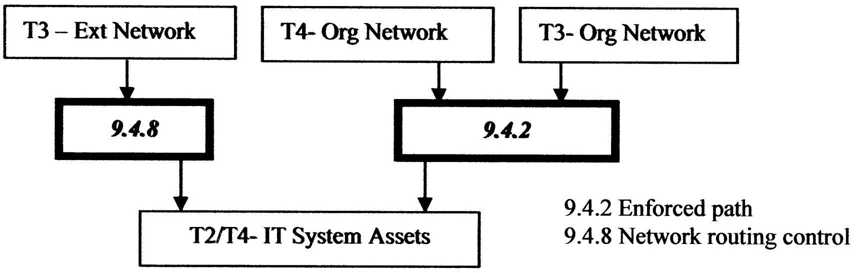
Information assets may be illicitly accessed by contravention of I.T. System access controls but they may also be accessed if they are transmitted over networks, hence the controls suggested in this section (See Figure 21) deal with network controls:

- Section 9.4.8 Network Routing Controls – ensure information flows do not breach access control policies
- Section 9.4.2 Enforced Path – use of Virtual Private Networks to protect the security of transmitted data.



9.4.1 Policy on Use of Network Services – management controls and procedures to protect network access.

Figure 20 Network to IT System Component of Threat Network



9.4.2 Enforced path
9.4.8 Network routing control

Figure 21 Network Security Component of Threat Network

Humour Pages

Call Centre Enquiries

British Rail Customer: "How much does it cost to Bath on the train?"

Operator: "If you can get your feet in the sink, then it's free"

Customer: "I've been ringing 0700 2300 for two days and can't get through to enquiries, can you help?".

Operator: "Where did you get that number from, sir?".

Customer: "It was on the door to the Travel Centre".

Operator: "Sir, they are our opening hours".

Samsung Electronics

Caller: "Can you give me the telephone number for Jack?".

Operator: "I'm sorry, sir, I don't understand who you are talking about".

Caller: "On page 1, section 5, of the user guide it clearly states that I need to unplug the fax machine from the AC wall socket and telephone jack before cleaning. Now, can you give me the number for Jack?"

Then there was the caller who asked for a knitwear company in Woven.

Operator: "Woven?. Are you sure?".

Caller: "Yes. That's what it says on the label – Woven in Scotland".

On another occasion, a man making heavy breathing sounds from a phone box told a worried operator: "I haven't got a pen, so I'm steaming up the window to write the number on".

Caller: "I'd like the RSPCA please".

Operator: "Where are you calling from?".

Caller: "The living room".

RAC Motoring Services

Caller: "Does your European Breakdown Policy cover me when I am traveling in Australia?".

Operator: Doesn't the product name give you a clue?

Computer Capers

Tech Support: "I need you to right-click on the Open Desktop"

Customer: "OK".

Tech Support: "Did you get a pop-up menu?".

Customer: "No".

Tech Support: "OK. Right-Click again. Do you see a pop-up menu?".

Customer: "No".

Tech Support: "OK, sir. Can you tell me what you have done up until this point?".

Customer: "Sure. You told me to write 'click' and I wrote 'click'".

Caller: "I deleted a file from my PC last week and I have just realized that I need it. If I turn my system clock back two weeks will I have my file back again?".

Welsh Directory Enquiries

Caller: "I'd like the number of the Argoed Fish Bar in Cardiff, please".

Operator: "I'm sorry, there's no listing. Is the spelling correct?".

Caller: "Well, it used to be called the Bargoed Fish Bar but the 'B' fell off".

Consultant/Senior Manager Speak

I can only please one person per day. Today is not your day. Tomorrow is not looking good either.

I love deadlines. I especially like the whooshing sound they make as they go flying by.

Tell me what you need, and I'll tell you how to get along without it.

Accept that some days you are the pigeon and some days the statue.

I don't have an attitude problem, you have a perception problem

On the keyboard of life, always keep one finger on the escape key.

I don't suffer from stress. I am a carrier.

You are slower than a herd of turtles stampeding through peanut butter.

Do not meddle in the affairs of dragons, because you are crunchy and taste

good with ketchup.

Everybody is somebody else's weirdo.

Never argue with idiots. They drag you down to their level, then beat you with experience.

A pat on the back is only a few inches from a kick in the butt.

Don't be irreplaceable. If you can't be replaced, you can't be promoted.

After any salary raise, you will have less money at the end of the month than you did before.

The more crap you put up with, the more crap you are going to get.

You can go anywhere you want if you look serious and carry a clipboard.

If it wasn't for the last minute, nothing would get done.

When you don't know what to do, walk fast and look worried.

Following the rules will not get the job done.

When confronted by a difficult problem, you can solve it more easily by reducing it to the question, "How would

the Lone Ranger handle this?"

Only the mediocre are at their best all the time.

There's a fine line between genius and insanity. I have erased the line.

Bring ideas in and entertain them royally, for one of them may be the king.

If at first you don't succeed......skydiving isn't for you.

Life is a waste of time; time is a waste of life, so get wasted all of the time and have the time of your life.

When everything is coming your way......you're in the wrong lane.

Talk is cheap because supply exceeds demand.

Even if you are on the right track, you'll get run over if you just sit

there.

Politicians and nappies have one thing in common; they should both be changed regularly for the same reason.

An optimist thinks that this is the best possible world. A pessimist fears that this is true.

There will always be death and taxes; however, death doesn't get worse every year.

In just one day, tomorrow will be yesterday.

I am a nutritional over-achiever.

I am having an out of money experience.

I plan on living forever. So far, so good.

Practice safe eating; always use condiments.

It's frustrating when you know all the answers but nobody bothers to ask you the questions.

The real art of conversation is not only to say the right thing at the

right time, but also to leave unsaid the wrong thing at the tempting moment.

Brain cells come and brain cells go, but fat cells live forever.

Age doesn't always bring wisdom. Sometimes age comes alone.

Put about 100 bricks in some particular order in a closed room with an open window.

Then send 2 or 3 candidates in the room and close the door.

Leave them alone and come back after 6 hours and then analyse the situation.

If they are counting the bricks...
Put them in the accounts department.

If they are recounting them...
Put them in auditing.

If they have messed up the whole place with the bricks...
Put them in engineering.

If they are arranging the bricks in some strange order...
Put them in planning.

If they are throwing the bricks at each other...
Put them in operations.

If they are sleeping...
Put them in security.

If they have broken the bricks into pieces...
Put them in information technology.

If they are sitting idle...
Put them in human resources.

If they say they have tried different combinations, yet not a brick has been moved...
Put them in sales.

If they have already left for the day...
Put them in marketing.

If they are staring out of the window...
Put them on strategic planning.

And then last but not least.

If they are talking to each other and not a single brick has been moved...
Congratulate them and put them in top management.

Haiku alerts

In Japan they have replaced the impersonal and unhelpful Microsoft 'error messages' with their own haiku poetry, each only 17 syllables:

five in the first line, seven in the second and five in the third:

Your file was so big
It might be very useful
but now it is gone

The Web site you seek
Cannot be located
But countless more exist

Chaos reigns within
Reflect, repent and reboot
Order shall return

Aborted effort:
Close all that you have worked on
You ask far too much

Windows NT crashed
I am the Blue Screen of Death
No one hears your screams

Yesterday it worked
Today it is not working
Windows is like that

First snow, then silence
Thhis thousand-dollar screen dies
So beautifully

With searching comes loss
and the presence of absence
'My Novel' not found

The Tao that is seen
Is not the true Tao - until
You bring fresh toner

Stay the patient course
Of little worth is your ire
The network is down

A crash reduces
Your expensive computer
To a simple stone

Three things are certain
Death, taxes and lost data
Guess which has occurred

You step in the stream
But the water has moved on
The page is not here

Out of memory
We wish to hold the whole sky
But we never will

Having been erased
The document you're seeking
Must now be retyped

Serious error
All shortcuts have disappeared
Screen. Mind. Both are blank

Corporate Lesson 1:

A man is getting into the shower just as his wife is finishing up her shower, when the doorbell rings.

The wife quickly wraps herself in a towel and runs downstairs. When she opens the door, there stands Bob, the next door neighbour. Before she says a word, Bob says, “I’ll give you $800 to drop that towel,”

After thinking for a moment, the woman drops her towel and stands naked in front of Bob. After a few seconds, Bob hands her $800 dollars and leaves. The woman wraps back up in the towel and goes back upstairs. When she gets to the bathroom, her husband asks, “Who was that?” “It was Bob the next door neighbour,” she replies. “Great!” the husband says, “did he say anything about the $800 he owes me?”

Moral of the story: If you share critical information pertaining to credit and risk with your shareholders in time, you may be in a position to prevent avoidable exposure.

Corporate Lesson 2:

A priest offered a lift to a Nun. She got in and crossed her legs, forcing her gown to reveal a leg. The priest nearly had an accident. After controlling the car, he stealthily slid his hand up her leg. The nun said, “Father, remember Psalm 129?” The priest removed his hand. But, changing gears, he let his hand slide up her leg again. The nun once again said, “Father, remember Psalm 129?” The priest apologized “Sorry sister but the flesh is weak.” Arriving at the convent, the nun went on her way. On his arrival at the church, the priest rushed to look up Psalm 129. It said, “Go forth and seek, further up, you will find glory.”

Moral of the story: If you are not well informed in your job, you might miss a great opportunity.

Corporate Lesson 3:

A sales rep, an administration clerk, and the manager are walking to lunch when they find an antique oil lamp. They rub it and a Genie comes out. The Genie says, “I’ll give each of you just one wish.” “Me first! Me first!” says the admin. clerk. “I want to be in the Bahamas, driving a speedboat, without a care in the world.” Poof! She’s gone. “Me next! Me next!” says the sales rep. “I want to be in Hawaii, relaxing on the beach with my personal masseuse, an endless supply of Pina Coladas and the love of my life.” Poof! He’s gone. “OK, you’re up,” the Genie says to the manager. The manager says, “I want those two back in the office after lunch.”

Moral of the story: Always let your boss have the first say.

Corporate Lesson 4 :

A crow was sitting on a tree, doing nothing all day. A rabbit asked him, “Can I also sit like you and do nothing all day long?” The crow answered: “Sure, why not.” So, the rabbit sat on the ground below the crow, and rested. A fox jumped on the rabbit and ate it.

Moral of the story: To be sitting and doing nothing, you must be sitting very high up.

Corporate Lesson 5:

A turkey was chatting with a bull. “I would love to be able to Get to the top of that tree,” sighed the turkey, but I haven’t got the energy.” “Well, why don’t you nibble on my droppings?” replied the bull. “They’re packed with nutrients.” The turkey pecked at a lump of dung and found that it gave him enough strength to reach the lowest branch of the tree. The next day, after eating some more dung, he reached the second branch. Finally after a fourth night, there he was proudly perched at the top of the tree. Soon he was spotted by a farmer, who shot the turkey out of the tree.

Moral of the story: Bullshï¿? t might get you to the top, but it won’t keep you there.

IRMA

INFORMATION RISK MANAGEMENT & AUDIT

◆ A SPECIALIST GROUP OF THE BCS ◆

BCS

THE BRITISH COMPUTER SOCIETY

Membership Application

(Membership runs from July to the following June)

I wish to APPLY FOR membership of the Group in the following category and enclose the appropriate subscription.

INDIVIDUAL MEMBERSHIP *(NOT a member of the BCS)*	£25
INDIVIDUAL MEMBERSHIP *(A members of the BCS)* BCS membership number: ___________________________	£15
STUDENT MEMBERSHIP – Full-time only and must be supported by a letter from the educational establishment. *(An annual quota is in operation, so IRMA retains the right to close this level of membership at any time).* Educational Establishment: ___________________________	£FREE

Please circle the appropriate subscription amount and complete the details below.

All communications from the Group are likely to be electronic.
Please tick this box to indicate you agree to be contacted this way. □

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE:
(STD Code/Number/Extension)

E-mail:

PROFESSIONAL CATEGORY: (Please circle)

1 = Internal Audit
2 = External Audit
3 = Data Processor
4 = Academic
5 = Full-Time Student
6 = Other (please specify)

SIGNATURE: DATE:

PLEASE MAKE CHEQUES PAYABLE TO "BCS IRMA"AND RETURN WITH THIS FORM TO

Janet Cardell-Williams, IRMA Administrator, 49 Grangewood, Potters Bar, Herts EN6 1SL. Fax: 01707 646275

Management Committee

CHAIRMAN	Alex Brewer	brewera@ebrd.com
SECRETARY	Siobhan Tracey	siobhantracey@aol.com
TREASURER	Jean Morgan	jean@wilhen.co.uk
MEMBERSHIP	Ross Palmer	ross.palmer@hrplc.co.uk
JOURNAL EDITOR	John Mitchell	john@lhscontrol.com
WEBMASTER	Allan Boardman	allan@internetworking4u.co.uk
EVENTS PROGRAMME CONSULTANT	Raghu Iyer	raguriyer@aol.com
LIAISON – IIA & NHS	Mark Smith	mark.smith@lhp.nhs.uk
LIAISON – ISACA	Ross Palmer	ross.palmer@hrplc.co.uk
MARKETING	Wal Robertson	williamr@bdq.com
ACADEMIC RELATIONS	Vacant	

SUPPORT SERVICES

ADMINISTRATION	Janet Cardell-Williams t: 01707 852384 f: 01707 646275	admin@bcs-irma.org

OR VISIT OUR WEBSITE AT	**www.bcs-irma.org**	Members' area
		Userid = irmalondon
		Password = 4members06

BCS IRMA SPECIALIST GROUP ADVERTISING RATES

Reach the top professionals in the field of Information Risk Management and Audit by advertising in the BCS IRMA SG Journal. Our advertising policy allows advertising for any security and control related products, service or jobs.

For more information, contact John Mitchell on 01707 851454, fax 01707 851455 email john@lhscontrol.com.

There are three ways of advertising with the BCS IRMA Specialist Group:

The Journal is the Group's award winning quarterly magazine with a very defined target audience of 350 information systems audit, risk management and security professionals.

Display Advertisements Rates:

- Inside Front Cover £400
- Inside Back Cover £400
- Full Page £350 (£375 for right facing page)
- Half page £200 (£225 for right facing page)
- Quarter Page £125 (£150 for right facing page)
- Layout & artwork charged @ £30 per hour

Advertising Flyers can be distributed with either the Journal or our regular Newsletter for varying advertising purposes, for example: job vacancies, new products, software. Please contact the editor for details.

Discounts:

Orders for insert distribution in four or more consecutive editions of the Journal, if accompanied by advance payment, will attract a 25% discount on quoted prices.

Direct electronic mailing

We can undertake direct mailing to our members on your behalf at any time outside our normal distribution timetable as a 'special mailing'. Items for distribution MUST be received at the office at least 5 WORKING DAYS before the distribution is required. Prices are based upon an access charge to our members plus a handling charge.
Access Charge £350. Please note photocopies will be charged at 21p per A4 side.

Personalised electronic letters:

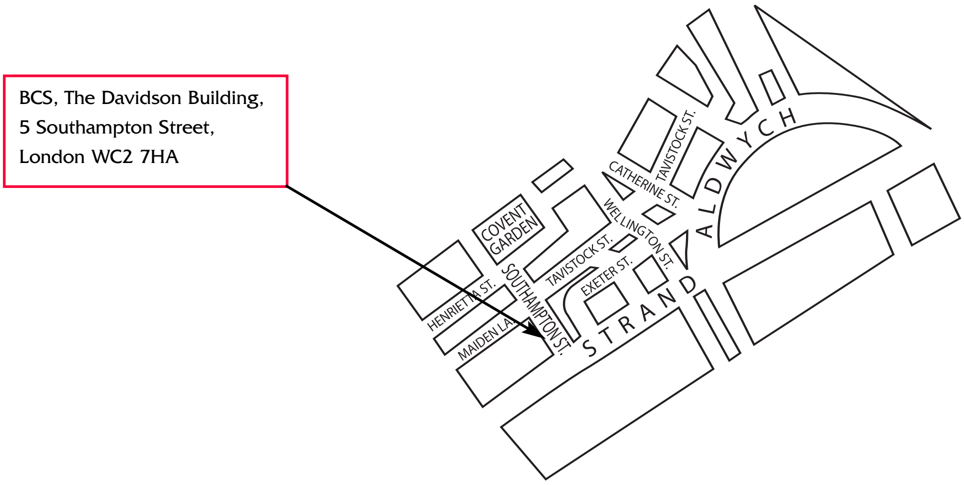
We can provide a service to personalise letters sent to our members on your behalf. This service can only be provided for standard A4 letters, (i.e. we cannot personalise calendars, pens etc.). If you require this service please add £315 to the Direct mailing rates quoted above.
Discounts: Orders for six or more direct mailings will attract a discount of 25% on the quoted rates if accompanied by advance payment

Contacts

Administration

Janet Cardell-Williams,
49 Grangewood, Potters Bar, Hertfordshire EN6 1SL
Email: admin@bcs-irma.org
Website : www.bcs-irma.org

Meeting Venue unless otherwise stated


BCS, The Davidson Building,
5 Southampton Street,
London WC2 7HA