Project Report for

ACE Information System Security

By Rajneesh Talwar

My Learning Institute

Project Report For ACE

[2009-2010]

ACKNOWLEDGEMENT

With immense please we are presenting "**ACE Information System Security**" Project report as a part of my ICT software designing. I wish to thank all the people who gave us unending support.

I express my profound thanks to my institute incharge Mukul Girdhar, Vice President Sedulity Solutions & Technologies, New Delhi. **(An ISO 9001:2008 Certified Organization)** 310 Suneja Tower-II, District Centre, Janak Puri, New Delhi-110058, Ph: 9811572430, 9312903095, Email: mukul@sedulitygroups.com, Website: www.sedulitygroups.com And Mr. Gopal Singh Rawat incharge IT in ACE and all those who have indirectly guided and helped me in preparation of this ACE project.

CERTIFICATE

This is to certify that the project

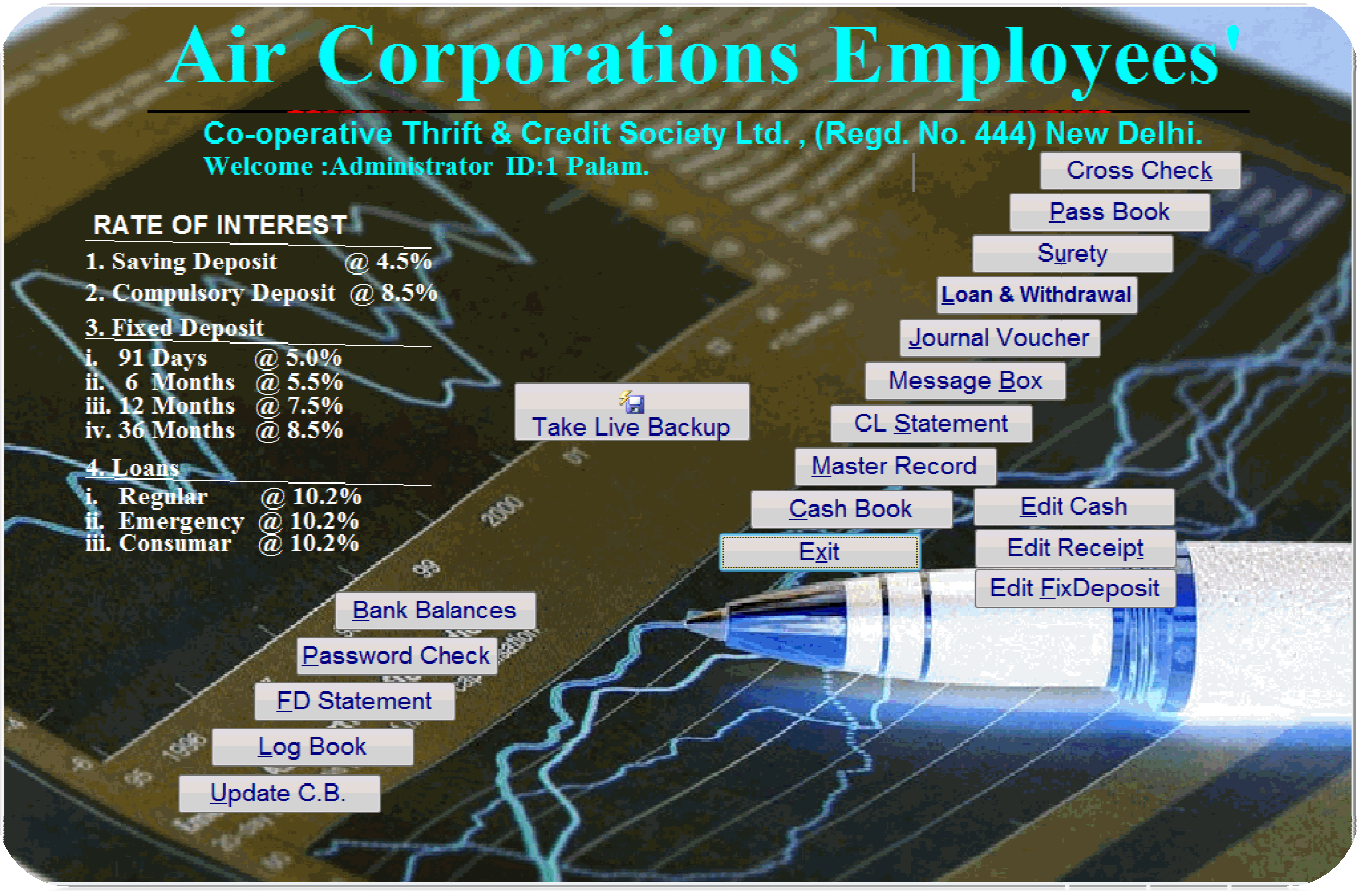
"**ACE Information System Security**"

Has been satisfactorily completed by
Rajneesh Talwar
Towards The Fulfillment of the ACE requirement and Goal Set
And it is approved by ACE

Project Guide ***Examiner*** ***Head of Department***

Air Corporations Employees

Co-operative
Thrift & Credit Society Ltd. ,
(Regd. No. 444) New Delhi.
ACE Information System Security



A Guide for Reviewing

ACE *Information System Security*

in

Air Corporations Employees

Issued by
EDP Audit Committee
ACE
Audited by Rajneesh Talwar April – 2010

A Guide for Reviewing

Information System Security in ACE

INTRODUCTION

Introduction

The ACE is a "Air Corporations Employees Co-operative Thrift & Credit Society Ltd." , its a type of banking SEWA for more than 6000 Indian Airlines employees member around the India are avail the facility of the same.

The software is made in VFP9.0 on .net platform which includes Forms, Reports, Queries, View, etc. etc. at the beginning they need to connect the 4 station to be connected to each other so that anyone can get their money from any station like, Delhi, Bombay, Calcutta, Madras A320 a Hanger, and Safderzung airport. Basically we connect all the station with the help of remote desktop, terminal services of Microsoft and for the security purpose we put some code and check other than inbuilt security. I describe the same further, that how it works and code of the same.

Mr. Gopal Rawat the Sr. Manager in IT is looking the transaction part of account vs software and handles it last 15 years. He help me to made this software live.

He face many problems in the existing work flow like person came to them and withdrawal the money but they cannot check there Signature ID and Photo ID because both are in the manual file system and take 15-20 minutes to find it out.

And we made software with the Scanned signature as well as photograph of the person who is having a account no. in the ACE and then link it to the transactions so whenever transaction is being done anyone can Tally the Picture of the person and Signature of the same person.

As far as connectivity is concern we have an issue with the security because we use a terminal services of Microsoft and user can be share the user ID and password and connect from any client from anywhere so, for that purpose we made some security code which checks every user ID Password and also check the Client machine ID and its MAC address and match with our database and then only allow to the specified users.

The main objective of this guide is to assist effective security programmes covering key information systems in their own office. This is not a detailed security audit guide: it is a description of a structured approach to assessing and managing risk in ACE information systems.

What Is ACE Information System Security

The objective of an ACE information system security programme is to protect an organisation's information by reducing the risk of loss of confidentiality, integrity and availability of that information to an acceptable level.

A good information security programme involves two major elements, risk analysis and risk management.

In the risk analysis phase, an inventory of all information systems is taken. For each system, its value to the organisation is established and the degree to which the organisation is exposed to risk is determined. Risk management, on the other hand, involves selecting the controls and security measures that reduce the organisation's exposure to risk to an acceptable level.

To be effective, efficient and reflect common sense, risk management must be done Risk management becomes a senior management issue. A balance has to be reached between the value of the information to the organisation on the one hand and the cost of the personnel, administrative and technological security measures on the other hand.

The security measures put in place need to be less expensive than the potential damage caused by the loss of confidentiality, integrity and availability of the information.

Many formal risk analysis methodologies on the market require technical expertise in the area of information technology and relevant controls and availability of precise threat frequencies that may be beyond the reach of many audit offices, at least initially.

The objective is to build up over time the necessary expertise and resources.

Information Security Framework

Information security is one element of a security infrastructure and, as such, should not be examined in a vacuum. There should be a framework of security policies dealing with all aspects of physical security, personnel security and information security. There should be clear roles and responsibilities for users, security officers and the Information Systems Steering Committee. An information security programme should include all aspects of the sensitivity of corporate information, including confidentiality, integrity and availability. A programme of security awareness should be in place reminding all staff of the possible risks and exposures and of their responsibilities as custodians of corporate information.

Referring to Table I, information security is a set of measures at the physical, personnel, administrative, computer and information system levels.

They must all work together. Information security is good management control and shortcomings at any level can threaten the security at other levels. If personnel security policies, for instance, are not well designed and implemented, information security could become very costly or almost impossible to support. On the other hand, minimal measures at all levels should ensure a minimum of protection to the information, provided the security risk is reasonable and accepted by management. There are also situations where security measures at one level may compensate for security weaknesses elsewhere. Encryption, for instance, adds an extra layer of protection for data confidentiality and integrity even in cases where physical, personnel or administrative security measures may be weak. Encryption remains one last defence to help prevent a breach of confidentiality or of integrity.

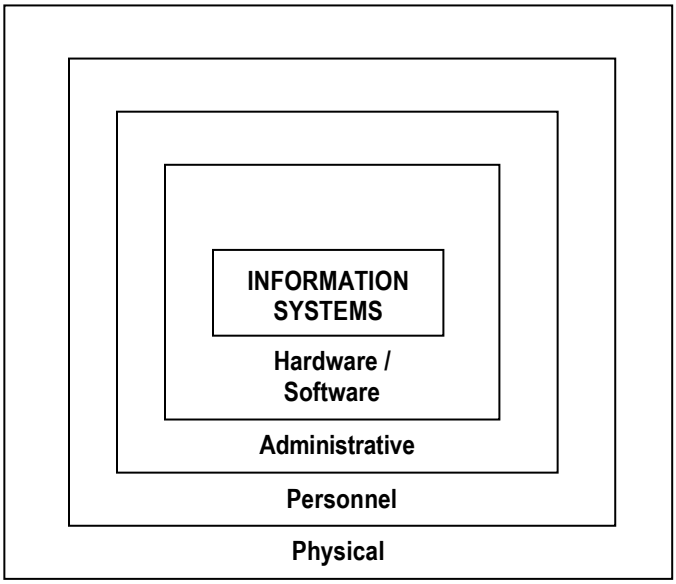


Table I Complementary Layers of Information Security

In planning for information security, the value of the information to management and the volume of that information relative to other types of information have to be balanced against the basic security limitations of the medium.

In many government departments, unless there are extreme requirements for carrying top secret information on a suitably protected laptop, the information should simply be created and carried otherwise.

For those departments, the cost and the constraints of the appropriate security controls and measures may just not be acceptable, given the small volume of information that needs such protection.

Two-Tier Approach to Information System Security Reviews

The guide introduces a two-tier approach to information system security reviews. The emphasis is on the use of common sense to always balance the cost of security to be built into a system to the value of the information carried by that system.

Given the limited resources of many Audit Institutions, it is proposed that we first use a top-down, manual, management view of information security. We should proceed to the second phase, a very detailed analysis aimed at a monetary valuation of information exposure to risk, only if management needs the monetary precision to support its decisions or if specific technical exposures are being examined.

Both methods incorporate the elements of risk analysis and risk management

The Top-down Information Security Review Approach

The top-down method is simple but complete and can help us and reach conclusions on the security exposures of the information system under review. It takes a top-down perspective of information security as it attempts to take a senior management perspective of what information is of value to the organization, what are the risks and the security exposures and what recommendations should be made.

This approach allows auditors to focus their attention on key information systems, especially those presenting special security concerns.

The top-down method relies on qualitative assessments of the risk for threats to occur and of the degree of their impact if they did occur. The focus is on assessing the value to management of the information or the data carried by the information systems, not so much the value of the technology itself [3].

For each information system, the value of the information to the organization, the threats and the possible impacts are evaluated first individually, then globally to determine a global degree of exposure to risk. These evaluations are subjective and usually expressed in terms of high, medium or low risk, impact and exposure.

Based on these evaluations, recommendations are made to management on the course of action to take or on the type of specific controls and security measures to put in place. These recommendations are part of risk management.

The top-down method has several advantages. It is easy and cheap to use. It is manual and can be used by anyone with staff knowledgeable in matters of management controls and of information and computer systems in general. Internal staff resources may be sufficient.

There is no need for sophisticated software packages to collect data about the information systems being reviewed, to obtain up-to-date and pertinent statistics and to produce very sophisticated analyses and reports. If a system is used, a word processing package is usually sufficient. Spreadsheets can help in producing summary tables.

The more adventurous may want to use packages that offer database functionality to collect information and later produce analysis reports.

[3] Contrary to the top-down method, the detailed methodologies used in the second tier of the Approach proposed by this Guide quantify in a very detailed manner the threats to the computer platforms on which information systems are running.

In the proposed Two-Tier Approach to Information System Security Review, the Top-Down Method is seen as a decision point in the overall method. Depending on the circumstances of the review, we may satisfy themselves with the results of the review or may decide to pursue the review with more sophisticated procedures in areas of special concern or where very technical or costly security measures may need to be justified to management.

Detailed Information System Security Method

The detailed methodologies used in the second tier of the approach proposed to Supreme Audit Institutions are a well known type of risk analysis and management based on a detailed and quantitative analysis of information system assets.

They attempt to measure the net monetary impact of security exposures and of the countermeasures put in place. Vendors around the world sell various security analysis packages that support such an approach.

Quantitative security analysis methods are usually made available with a computer software package for the benefit of the auditor as the task of entering data, calculating security exposures and reporting on the project may prove tedious and formidable. Such risk management packages come with expert help from the suppliers and training for the users of the method.

The objective is to provide an overview of a method which is best used with the support of an automated software package.

In contrast to the top-down approach, quantitative security analysis attempts to evaluate in monetary terms, in a very detailed and structured way, all the assets and all the possible threats and impacts to the information systems carried by an organization.

Through interviews and questionnaires, the possible impacts to the information are evaluated by the users and given a rank, from one to ten, depending on their seriousness. Annual loss expectancies are calculated next by combining asset replacement costs, threat probabilities and impact weighting factors.

Other differences may be the user friendliness of the method and the kind of support provided by the vendor. These are some of the concerns this two-tier approach attempts to address.

How To Use The Two-Tier Approach to ACE Information System Security

And

Remote Desktop A Server and Client Connections.

Planning.

Planning the security review is the key to success. It should cover the following main elements:

- Knowledge of the client and of the environment;
- Scope of the review: Which information systems, which logical, physical or geographical boundaries?
- Resources available: Qualified staff or consultants, budgets, timeframes;
- Availability of reliable threat statistics and cost figures, appropriate for the local conditions; adaptation of the default values, as necessary;
- Reporting requirements: Users of the report, context of the review (Annual Report, special report, internal, external, etc.), type of recommendations needed;
- Review method: Top-down approach, detailed analysis, or a combination of both.

With Remote Desktop, we can connect the Bombay, Calcutta , Madras, A320 Hanger and Safderzung Air port to our work Server at Delhi so they will access all of our programs, files, and network resources as though you were actually sitting in front of our computer at work.

We need the following instruction to be followed for the purpose of connection between client and server.

1.Microsoft Windows XP Professional must be installed on the computer containing the files and programs that you want to access from a remote computer. The computer must also be part of a corporate network in which Remote Desktop connections are permitted. This computer is known as the host.

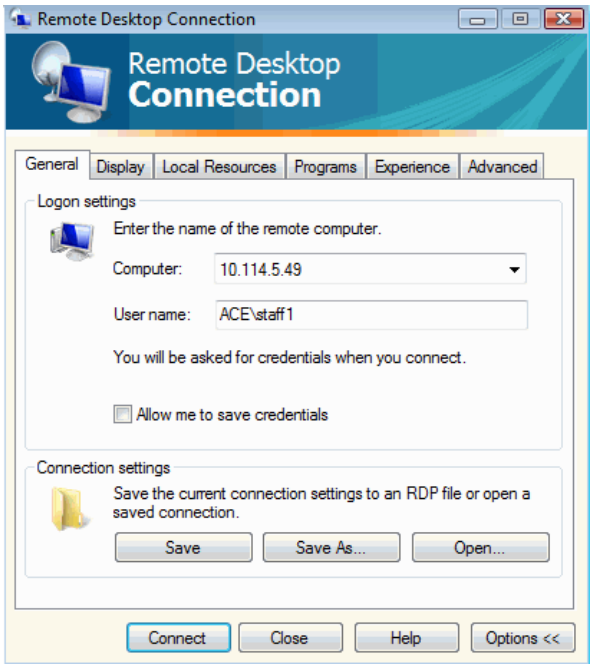
2.The remote computer must be running Windows 95 or later. This computer must also have the Remote Desktop Connection client software installed. The remote computer is known as the client.

3.Both computers must be connected to the Internet through a VPN connection.

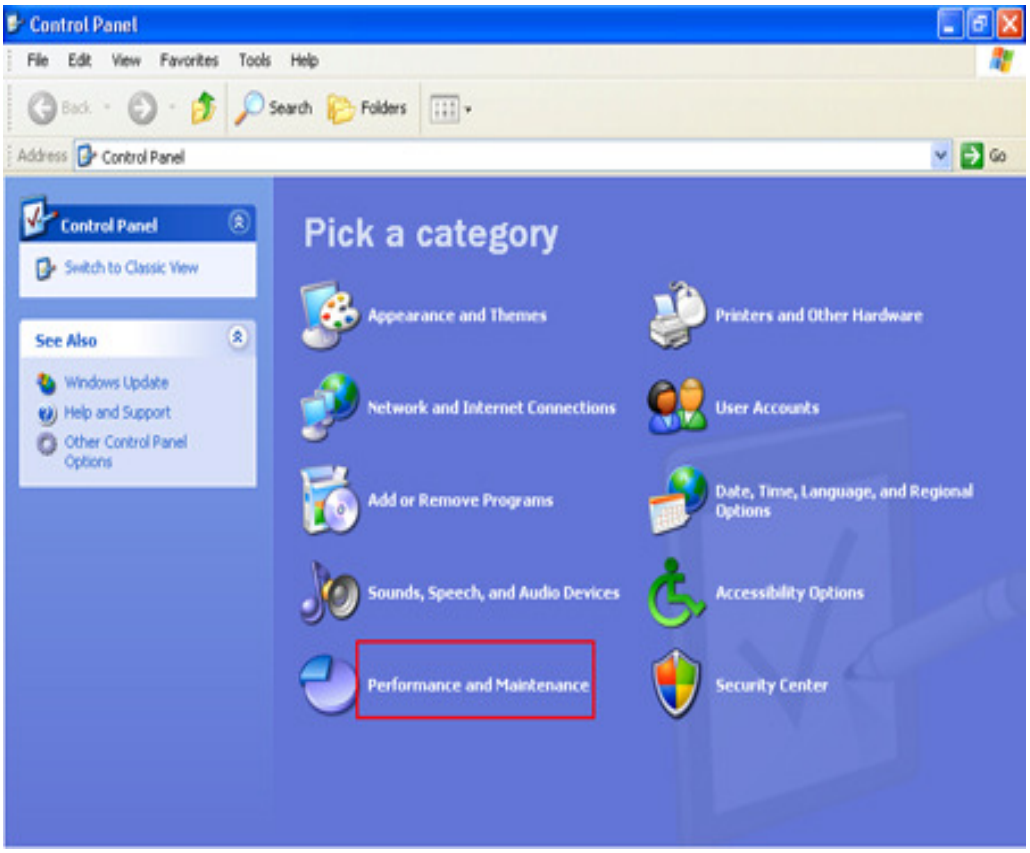
Note: If you're not connecting to the host computer through a VPN, you'll need to use the actual IP address of the host computer instead of the computer name.

- To set up the Remote Desktop, start with the host computer, which in this example is your work computer.

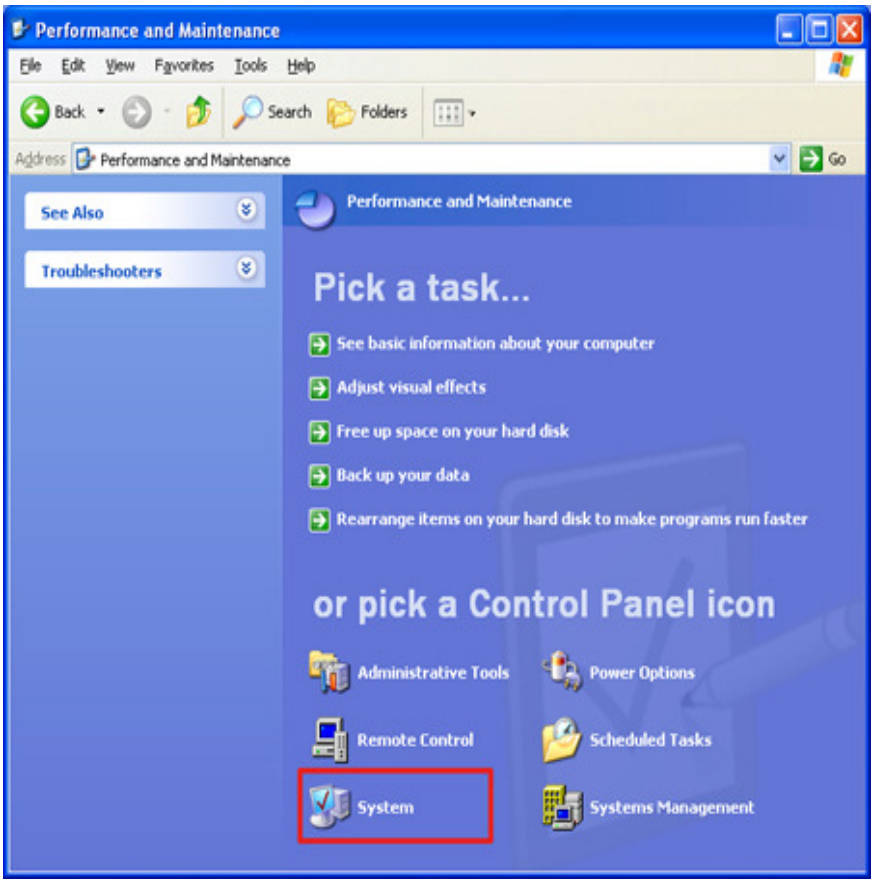
1.Verify that you are signed in as the administrator.



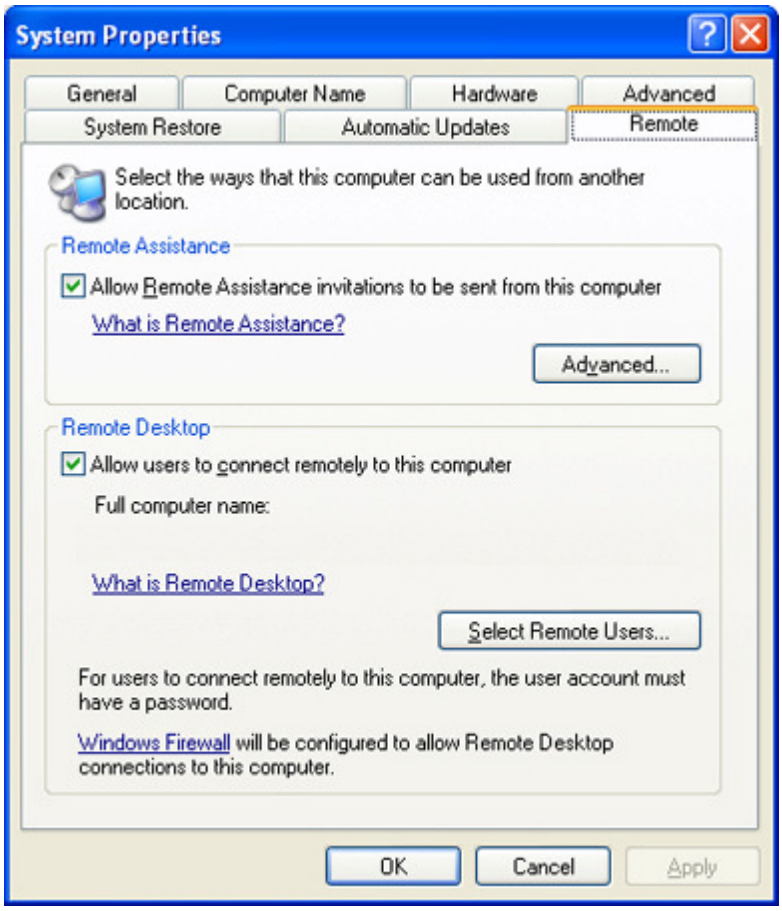
2.Click Start, click Control Panel, and then click Performance and Maintenance.



3. Click System.

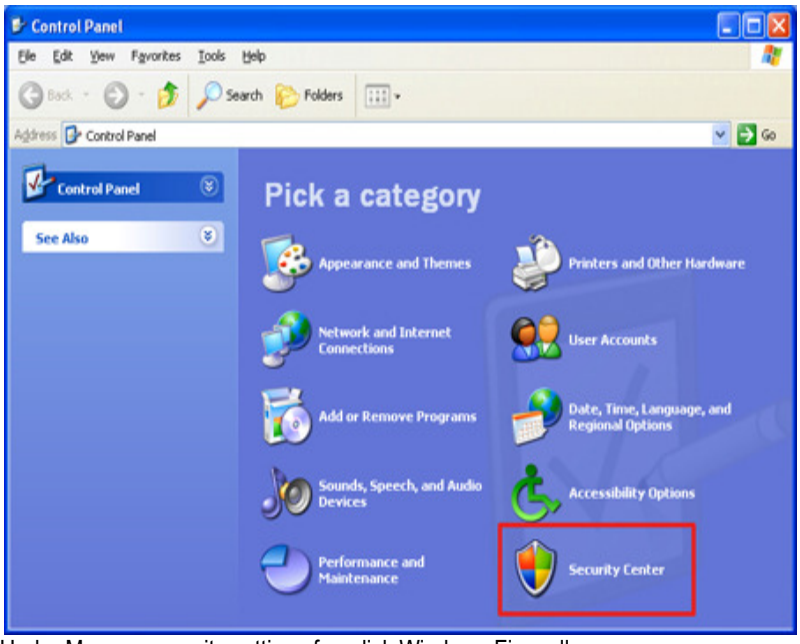


4. Click the Remote tab, select the Allow users to connect remotely to this computer check box, and then click OK.



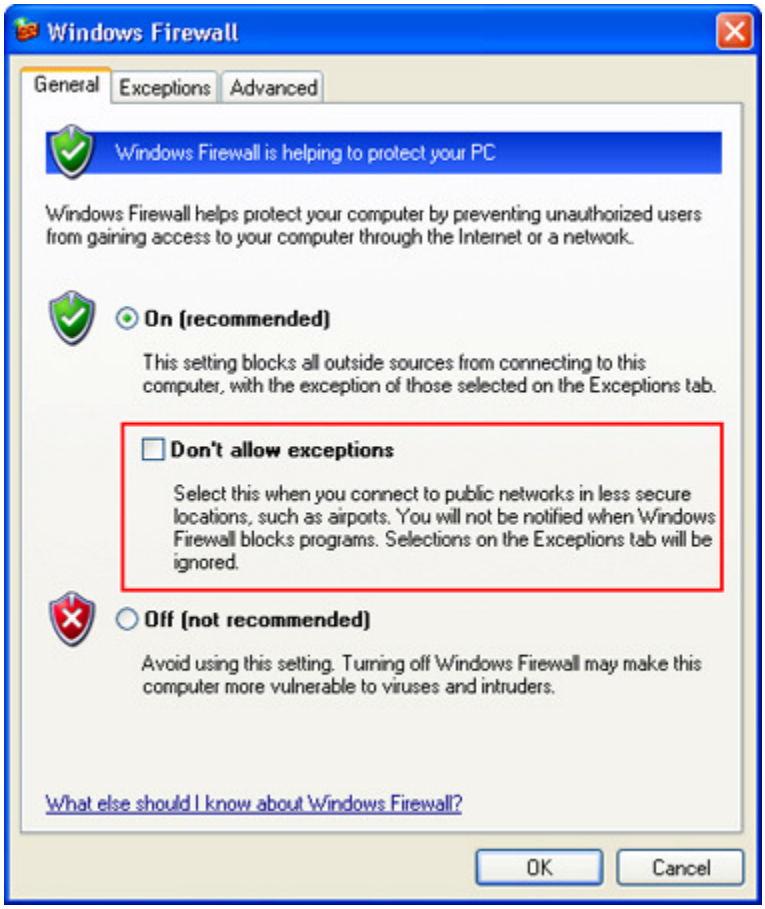
Next, make sure you have Windows Firewall set up to allow exceptions.

1.In the Control Panel, click Security Center.

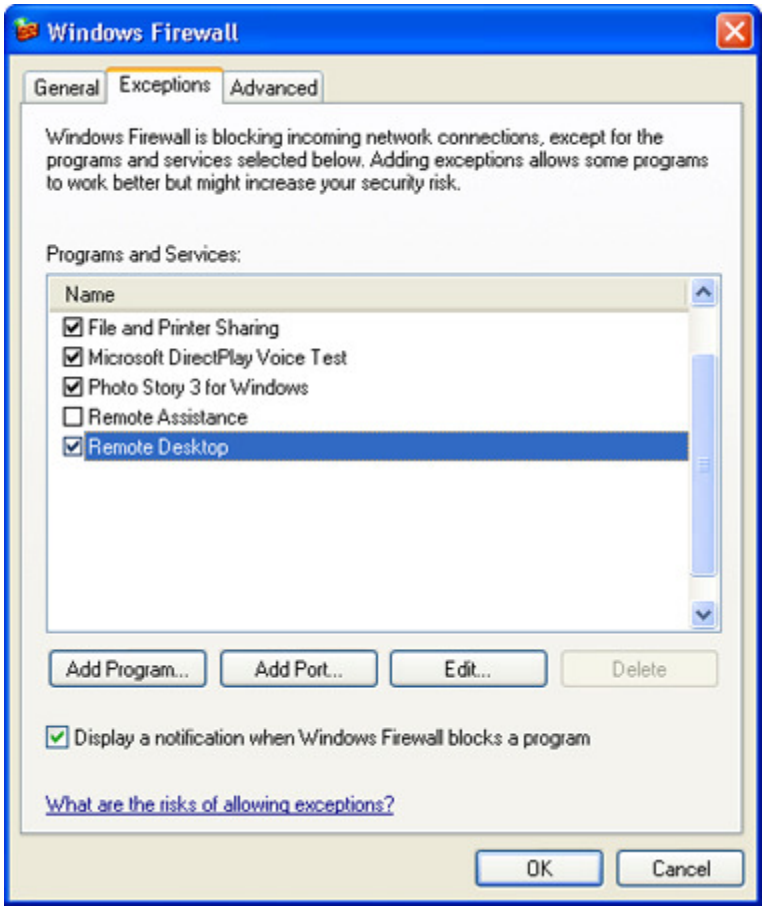


2.Under Manage security settings for, click Windows Firewall.

3.Make sure the Don't allow exceptions check box is not selected.



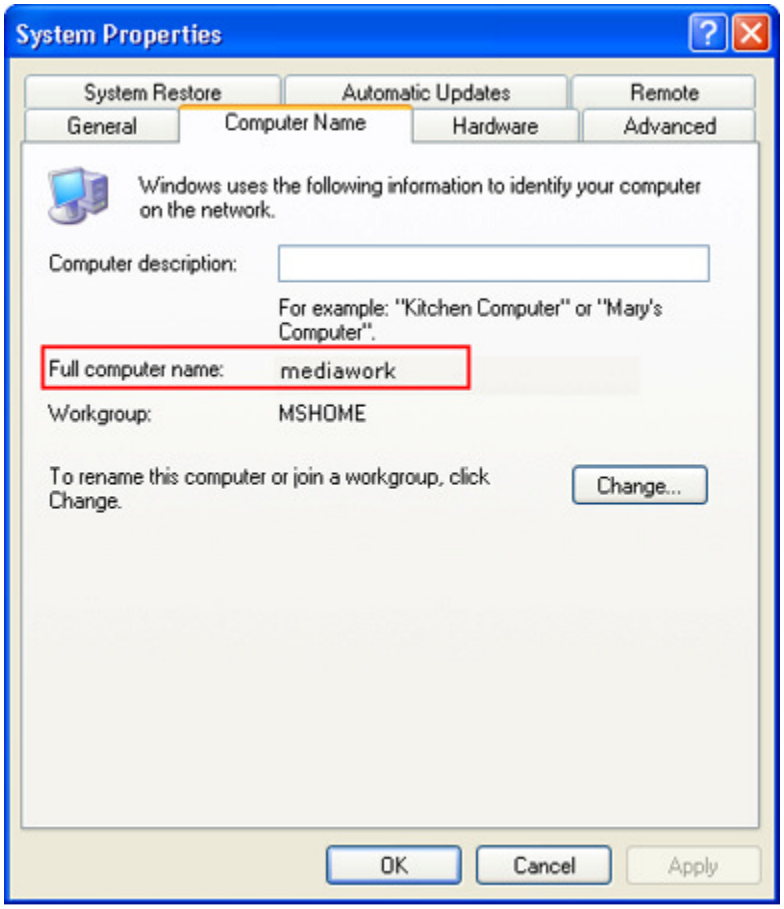
4.Click the Exceptions tab, and verify that the Remote Desktop check box is selected.



5.Click OK, and then close the Windows Security Center window.
Your host computer is now set up to allow remote access.

You will need the name of the host computer.

6.In Control Panel, click Performance and Maintenance, click System, and then click the Computer Name tab.



7.Write down the full computer name, and then click OK.

8.Close Control Panel.

.**In the Accessories menu, point to Communications, and then click Remote Desktop Connection.**
Note : Remember this host name is further used for security check

.In the Computer box, type the computer name of your host computer, which you wrote down earlier.

- T
o

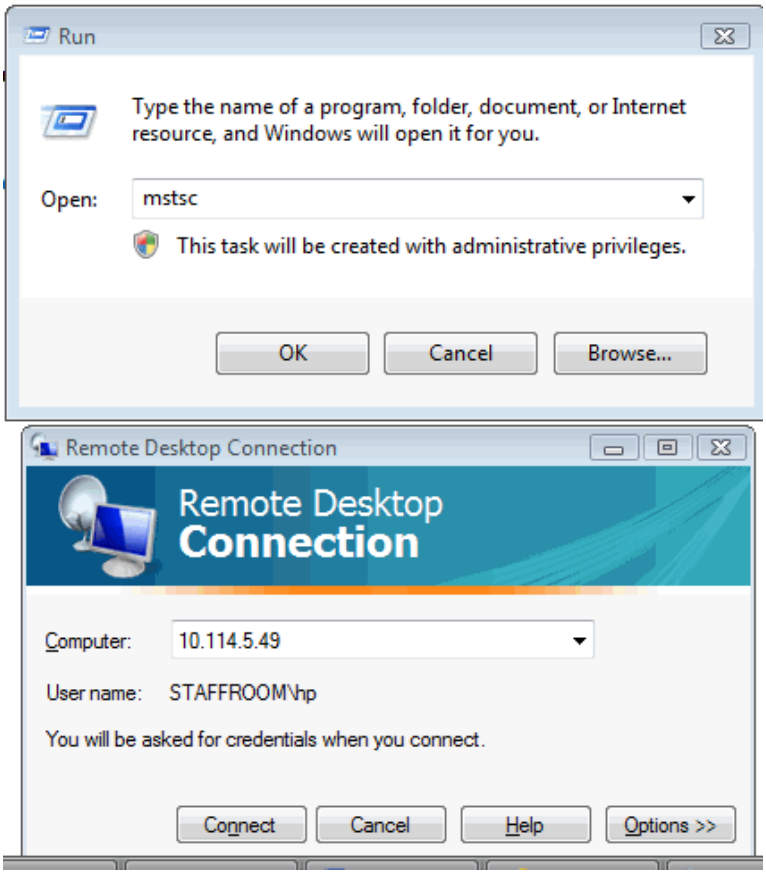
4.Click Connect.

When the Log On to Windows dialog box appears, type your user name, password, and domain (if required), and then click OK.

The Remote Desktop window opens, and you see the desktop settings, files, and programs that are on your host computer, which in this example is your work computer. Your host computer remains locked, and nobody can access it without a password. In addition, no one will be able to see the work you are doing remotely.

Now you may understand how we connect the our client machine to the server.

You may also type at the run command prompt MSTSC for as a shortcut of your remote desktop see the following picture.



You may collect the system MAC address for security check at command prompt type "ipconfig /all" and get the following picture, note down the Physical Address (MAC) of the client machine.

```
Tunnel adapter Local Area Connection* 11:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Teredo Tunneling Pseudo-Interface
   Physical Address. . . . . . . . . : 02-00-54-55-4E-01
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

Tunnel adapter Local Area Connection* 12:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : 6TO4 Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

C:\USERS\HP>ipconfig /all
```

When and How to Use Detailed Information Security Methods

There are circumstances where more detailed and quantified information security reviews will be the norm. This will be the case where we have the budgetary, technical and staff resources to conduct such detailed analyses or where reporting requirements dictate the approach to take.

Before attempting to use a detailed information security method, it is strongly recommended that we have to closer look at the following issues:

- availability or easy access to expertise in information technology and information security;
- availability of a suitable methodology;
- availability of a good software supporting package: Quantitative risk methods are very comprehensive and involve detailed methodologies that almost beg the use of a computer; on the other hand, the computer package usually introduces complexities of its own.
- budgets to adapt or customize the package to the environment under review: Several months of effort are not unheard of;
- training budgets, as the learning curve can be quite steep and costly, especially if consultants have to be used;
- time and financial resources: Detailed or quantitative security reviews tend to be lengthy and resource intensive; and,
- the need for such a detailed review: It has been argued that detailed, quantitative security reviews cannot be justified for commercial or ACE information systems which are neither complex nor highly sensitive.

Cost Effective Methodology

The purpose of this guide is to provide a cost effective methodology to assist in reviewing or establishing appropriate security policies and measures within an organization. Recognizing that security requirements need to be updated on a regular basis, the guide also provides for simple documentation, updating and reporting.

The guide describes computer security assessment from the perspective of management in a government organisation . Organisations can use this guide to assist in producing an "inventory" of computer applications used, assessing the sensitivity and security classification of the information, and completing a business impact threat risk security assessment. The person in charge of security utilises this work as a foundation for overall assessment of security policies and measures and for making recommendations.

we can use the guide in two ways: For internal purposes, to set up a security assessment process in their own organisation or, for external purposes, to help in reviewing the security assessment process in ACE.

This guide takes a top-down high level approach to information security. The emphasis is on the information carried on various electronic devices. In line with this high level approach, this guide categorises threats by general causes instead of their results, such as earthquakes instead of the destruction they may bring. A detailed bottom-up approach to information security, on the other hand, tends to examine every possible computer asset for weaknesses that may create loss exposures to the information generated or carried by those assets. The advantage of using the top-down approach is that it helps management to quickly target and focus on problem areas for further action. In some cases, this may point to the need for more detailed work to build a business case for extensive or costly security measures.

Because the method always takes a corporate or management view of information security, it remains flexible and can deal with issues of security policy as well as of security measures.

Evolution of Information Management

In managing information and applications, an organisation goes through four distinct stages, managing paper, managing automated technologies, managing corporate information resources, and finally, managing the strategic use of information. The technology and security challenges are to minimise the time and effort spent in each stage and to go through the stages as smoothly as possible.

At the managing automated technologies stage, the users are not significantly relying on computer applications but are achieving noticeable efficiencies. At the third stage, managing corporate information resources, computer security becomes a major concern due to significant reliance on computer based information and the exposures related to concentration of information at one place.

Security Management

One of the Organisation's key resources is its information. The first step to safe computing is adoption of information and administrative management policies and measures which embrace principles of good security management:

1. Security protection should be consistent with the value of the information being protected;
2. Security protection should remain with the information at all times as it is moved or processed; and
3. Security protection should be continuous in all situations. **The Security Team**

Under the leadership of the person in charge of computer security, a security team is selected. Full commitment by senior management is important if the team is to achieve its objectives. Its responsibility is to implement the security policy set out by senior management and to identify changes made necessary by developments in the organisation's information systems or the threats that face them.

The Process

Security policies are designed to protect information according to the exposures of the information. Security measures (standards, procedures, and tools) are the building blocks for protecting the information.

- **Sensitivity Statement:**

  Assessing the sensitivity of program and administrative applications (information systems) used in the Organisation, and determining the security classification.

  Confirming the Organisation's standard assessment of similar applications and, when appropriate, completing or updating an Information Sensitivity Statement & Security Classification form.

  Where desirable, rolling up individual sensitivity statements unto a Summary Description of Information Systems.

- **Business Impact Assessment:**

  Determining possible business impacts to the Organisation if the information were disclosed, integrity compromised or services disrupted.

- **Threat and Risk Assessment:**

  Determining the risk (the chance) that identified threats could occur.

- **Security Exposure Rating:**

  Evaluating the business impacts and the threats together to determine overall exposure to the Organisation.

  Confirming the Organisation's standard security assessment of similar applications and, when appropriate, confirming or updating a Business Impact and Threat Assessment form.

- **Security Decision and Recommended Actions:**

  Completing or updating a Summary of Security Assessments form.

  Making security decisions and recommending management actions to minimise identified exposures, and highlighting any serious security policy deficiency.

COMPLETION OF AN INFORMATION SENSITIVITY STATEMENT& SECURITY CLASSIFICATION FORM

Applications are owned by either a group or an individual. Where there is little interaction between applications, users of the output from the system can be readily identified. In highly integrated systems, an artificial boundary has to be agreed by all parties, including Senior Management.

A group may ask members to complete a User Information Sensitivity **when we work in a ACE they need to get an detail of each individual to be shown on screen so that they can handle it, and no one can get the money on behalf of others that could be done by shown there picture as well signature on screen. See image :**

SECURITY ASSESSMENTS & PROGRAMMING PATCH.

Set Default To \ace && set the default directory and some default settings to be done by the following commands.

```
*retu
Set Excl Off
Set Safe Off
Set Talk Off
Set Echo Off
Set Head Off
Set Mess To 27
Set Step Off
Set Scor Off
Set Conf On
Set Dele On
Set Cent On
Set Stat Off
Set Stat Bar Off
Set Procedure To toner
Set Sysmenu Off
Set Date brit
On Error
Public loconnectstring
Public gnhandle
Modify Window Screen Title 'ACE Information System Security' Icon File raj.ico Color Scheme 14
Noclose Nozoom Nofloat Nogrow
```

** Declare a WIN32 API Library command and get the remote session, Machine ID and Client Name from the WIN32API Lib.

```
Declare Long GetSystemMetrics In WIN32API Long SM_Item
#Define SM_REMOTESESSION 0x1000
xray=GetSystemMetrics(SM_REMOTESESSION) # 0
Select a
Use login
checkuser=.T.
Locate For Upper(Alltrim(a.username))==Upper(Getenv("USERNAME")) ;
        .And.  Upper(Alltrim(a.idname))==Upper(Getenv("CLIENTNAME"))
```

** Further check whether the above collected information from the Client machine with the help of WIN32 API is valid if it is then logbook entry is clean otherwise it may restrict the entry to the server.

```
If Found()
        Select a
        Use
        Do LOGBOOK
Else
        Do LOGBOOK
*Thisform.EMAILALERT("User:"+Upper(Getenv("SESSIONNAME"))+" Machine
ID:"+Upper(Getenv("CLIENTNAME")))
```

**** And the following message is given to the client machine.**

```
X=Messagebox("Because of a security error, the client could not connect to the terminal server.
"+Chr(13)+;
"After making sure that you are logged on to the network via correct terminal, try connecting to the
server again.",16,+0,"Microsoft Terminal Server Error")
        Select a
        Use
        Quit
Endif
*Transform(Getenv("SESSIONNAME"))+CHR(13)+TRANSFORM(GETENV("CLIENTNAME"))
Do Form toner

Procedure LOGBOOK
```

** Code to get the mac address and system ID from Client Machine when client try to connected to the server and check the same which already with us in the database.. **(See page 26)**

```
Local lcComputerName, loWMIService, loItems, loItem, lcMACAddress, xmac
Public xyz
xmac=''
lcComputerName = "."
loWMIService = Getobject("winmgmts:\\" + lcComputerName + "\root\cimv2")
loItems = loWMIService.ExecQuery("Select * from Win32_NetworkAdapter",,48)
For Each loItem In loItems
        lcMACAddress = loItem.MACAddress
        If !Isnull(lcMACAddress)
                xmac=Transform(lcMACAddress)+Space(5)+xmac
        Endif
Endfor
Declare Long GetSystemMetrics In WIN32API Long SM_Item
#Define SM_REMOTESESSION 0x1000
X=GetSystemMetrics(SM_REMOTESESSION) # 0
*       RETURN GetSystemMetrics(SM_REMOTESESSION) # 0
*ENDFUNC
```

**** Replace The entire information into a table called rdplog.dbf which is Useful to check time to time for security purpose.**

```
Select a
Use rdplog
Append Blank

xyz=Transform(Sys(0))+Space(5)+Transform(Getenv("SESSIONNAME"))+Space(5)+Transform(Date())+Space(5
)+Transform(Time())+Chr(13)+Transform(Getenv("CLIENTNAME"))

Replace rdptype With xyz,login With "IN at:"+Transform(Date())+Space(5)+Transform(Time())
Use
```

Following log book shows the (Macadd)MAC address and (Mid) Machine ID of the client machine

Name	User	Pass	Passdate	Passtime	Macadd	Mid
A.K.KHAZANCHI	ASHOK	ASHOK	12/31/08		01-23-45-67-89-ab	ASHOK
A.MAJUMDAR	AJITA	AM	12/31/08		00-13-11-86-80-cj	AJITA
AMAR NATH	AMAR	AMAR	12/31/08		00:A0:C9:14:C8:29	AMAR
ANITA SHARMA	ANITA	ANITA	12/31/08		08:00:69:02:01:FC	ANITA

rdplog.dbf

T-C - ACE Information & System Security Implementation

- **Threat (T):** Any potential event or act that is unwanted and can impact on an information system, such as a fire, natural disaster, unauthorised access, etc.
- **Countermeasure (C):** A control which is designed to enhance security by either reducing the threat, reducing the impact, detecting a security breach or recovering from a security incident.

Input / output ports

T Control over functions compromised by changing the port connections.

C Keep connection boxes in secure areas if you rely upon restricting functions to terminals connected to particular ports.

Modems

T Modems can be used to gain unauthorised access to the system.

C In general, do not attach modems to dial in lines. If there is a need for dial- in capability, provide access only to a central site that is protected with a bastion firewall. Restrict the caller to very specific applications within a bastion environment. Provide the caller with "terminal" sessions and not with "host" sessions or remote access sessions as these may provide open access to sensitive information on the microcomputer or on the network. Consider using encryption for the transfer and the storage of sensitive data.

Call-back features are usually too restrictive for auditors who are constantly moving in the field and may cause administrative headaches.

T Modems can be used for unauthorised transfer of information outside the organisation.

C Keep the number of modems to a minimum, monitor the usage of lines to which modems are attached, disable modem lines outside working hours.

Electronic mail

TElectronic mail can be used for the unauthorised transfer of information outside the organisation.

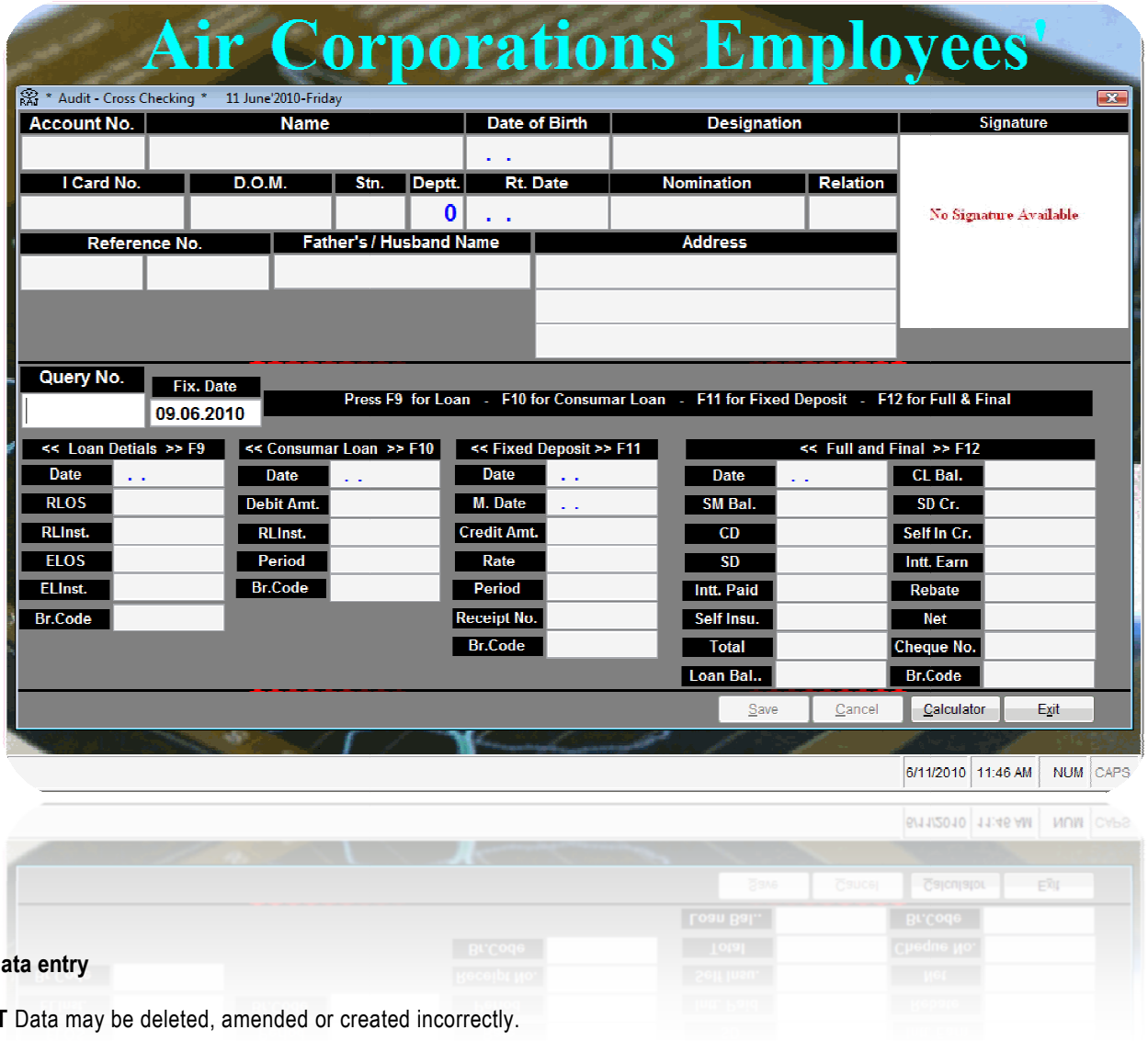
C Keep copies of all electronic mail sent out and keep records of sender and addressee.
Do spot checks on the contents of electronic mail.

Use searching programs to find key words in electronic mail.
Cross tabulate senders and addressees to establish any suspicious pattern.

Key personnel

T Key personnel who play an important role because of their duties or special skills may be absent for a long period of time.

C Consider alternative or backup personnel to replace key personnel should the need arise live backup can be taken see picture above.



Data entry

T Data may be deleted, amended or created incorrectly.

C Software should incorporate validation checks for all key fields, identification and authentication checks. Consider the introduction of authorisation and batching where possible the above picture shows audit – cross checking.

User	Datetime	Detail	Editdetail	Machine
			memo	
	28.09.2008@20:01:56	Exit From Main Login by: BranchID:	memo	RAJ # Rajneesh
A.MAJUMDAR	05.10.2008@12:41:41	Exit From Main Login by:A.MAJUMDAR BranchID:IGI	memo	RAJ # Rajneesh
ADMINISTRATOR	16.11.2008@11:47:05	Login Correct	memo	SERVER2003 # Administrator
AJITA	05.10.2008@12:40:38	Login Correct	memo	RAJ # Rajneesh
ARUN	27.01.2009@15:50:31	Login Correct	memo	ASMISERVER # Administrator
Administrator	28.09.2008@19:38:29	Login Correct	memo	RAJ # Rajneesh
GOPAL			memo	
GOPAL SINGH	27.01.2009@14:26:43	Entered into Main Programme	memo	ASMISERVER # Administrator
MITTAL	11.02.2009@09:55:31	Error in Login Try:1	memo	RAJSERVER # Administrator
MOHAN	05.10.2008@12:11:10	Error in Login Try:1	memo	RAJ # Rajneesh
MOHAN LAL	07.12.2008@23:14:27	Entered into Main Programme	memo	SERVER2003 # Administrator

The above picture shown the logbook maintained with date time and details on which forms user is work and from which machine the following is maintained under logbook.

Enquiries

T Anyone who gains enquiry rights within the system could become a source of unauthorised disclosure of information.

C Accountability and supervision are the main defence against unauthorised disclosure. The system can help by clearly marking printed output with appropriate privacy markings and ensuring that it is routed through an output control section who can log any sensitive output.

Individuals should have the minimum access rights consistent with their jobs.

Any failed access attempts should be logged and investigated by internal audit. Where 100% check is impracticable a statistical sample should be selected to ensure that testing is evenly spread over time. Internal audit or the systems audit team should undertake the checks.

Output handling

T There is a risk that output handling staff could copy output, lose it or route it to unauthorised staff / outsiders.

C All sensitive output should be routed through independent output handling sections but the staff in output handling should have no access to copiers and no rights to initiate output. Their sole role should be to record the production of sensitive output and route it to the correct recipient.

Programmers

T Programmers could compromise the controls of live information systems.

C Programmers should not have access to live information systems. Change control staff should be responsible for copying new software from the development environment to the live system.

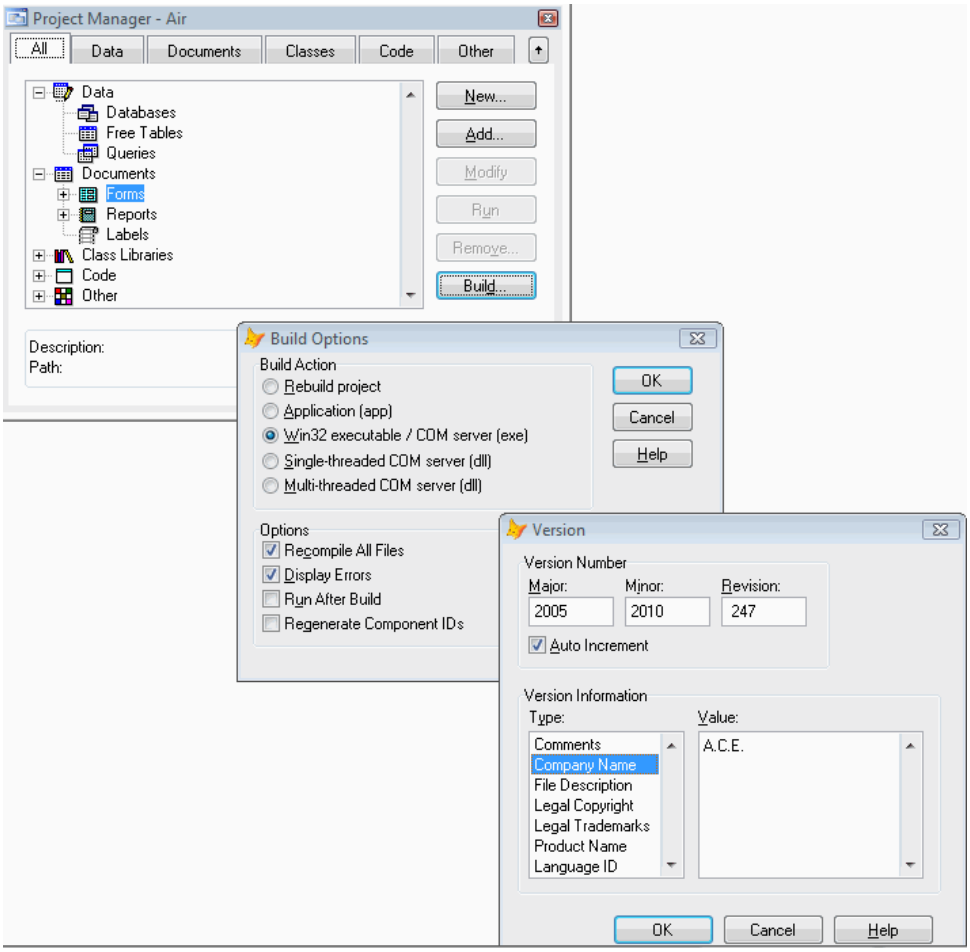
T Programmers could introduce covert functionality into their software such as time bombs or logic bombs.

C Programming should be modularised. Each unit should be subjected to peer review to guard against the introduction of unintended functions.

T Programs may compromise the integrity or availability of information systems if they are not thoroughly tested.

C All programs should be subjected to unit testing to ensure that expected outputs result from expected inputs. Testing should be undertaken by staff independent of the programmer and should be formally documented as part of the quality control procedures. Once a unit has been tested the programmer should have no further access to it.

Following picture shows how to compile and make version based exe for ACE



T Poorly documented programs can be difficult to maintain which may compromise the availability or integrity of dependent information systems.

C Documentation should be included in the quality control procedures. No unit should be passed to change control until the documentation is complete.

T Availability of information systems could be compromised if user instructions get out of step with the live information system programs.

C Completion of changes to user documentation should be a necessary prerequisite of a new unit being copied to the live system.

Analysts

T Availability and integrity may be compromised if analysts make design errors.

C Design documentation should include specifications that are intelligible to the clients. Clients should be required to sign off each stage in the design process. Prototypes may be a useful means of firming up client requirements before proceeding to a full functional design.

T Analysts have a broader perspective on the interaction of information systems than programmers. There is a risk that they might exploit their understanding to circumvent controls.

C Analysts should not have any write access to source code. They should not have access to compilers or assemblers that would enable them to develop their own applications.
Analysts should have no authority to initiate or authorise sensitive transactions.

System support

T Support staff act as custodians of information which belongs to others.
There is a risk that they could initiate changes to the information or programs or produce unauthorised output.

C Support staff should not have access to compilers or assemblers that would enable them to develop their own programs. They should have no access to the source code of the live information systems.

Powerful amendment facilities are often provided by operating system vendors to directly amend programs or data. Seek advice from the vendors about utilities that can be used to circumvent system controls and store them offline. Use of system amendment utilities should require the entry of a password known only to the shift leader. The media librarian should keep note of occasions when the restricted utilities are issued. All usage of restricted utilities should be logged and the internal / systems audit staff should review the logs kept by the operations supervisor and the media librarian.

If the operating system access control package is sophisticated enough to impose access, copy and execute controls over named utilities then this mechanism can be relied upon rather than keeping the utilities offline. If this course is adopted, the internal / systems audit staff should review access rights at regular intervals and insist that privileged users have their passwords changed frequently. Every time system amendment facilities are used the execute password should be changed.

Systems Programmers

T System programmers are responsible for maintaining the operating system environment. This will include the operating system and may additionally include network management software, database management systems, transaction processing software and storage management software. The work of systems programmers is often poorly understood which may lead to poor control over their activities. Systems programmers could accidentally or deliberately destroy the entire system.

C Systems programmers should not have access to the source code or data structures of any live information systems. They should not have access to compilers or assemblers in the live environment.

The access control software should restrict systems programmers to files which they have a legitimate reason to change. All activities by systems programmers should be logged.

Systems programmers should not have any access to the access control software or data files.

All changes to operating system software should be undertaken in a development environment and should be subjected to peer review

In the rare event that emergency changes have to be made without formal quality control the review process should take place after the event.

Change control

T Change control staff are responsible for copying programs and data from the development environment to the live environment. There is a risk that they could abuse their access to the live environment by altering live programs or data.

C Change control staff should not have access to program development tools that would enable them to compile their own programs.
Their activities should be carefully monitored by internal / systems audit staff.

Logical access control

T The access control staff are responsible for maintaining user profiles which
determine who has access to what. There is a risk that they will give themselves rights that are inconsistent with their functions.

C Changes to access profiles should be logged and the access control staff should be unable to switch the log off or to alter its contents.
Internal / systems audit staff should review access profiles paying particular attention to access rights of knowledgeable users and the users who have access to particularly sensitive programs / data.

Physical access control

T Security guards necessarily have access to secure areas during quiet hours. There is a risk that they will abuse the privilege.

C Security staff should have no access rights to information systems. Sensitive output should be locked away during quiet hours and all terminals logged out and switched off.

Auditors

T Auditors require extensive access to information systems and to logs. There is a danger that auditors could compromise system integrity either deliberately or accidentally.

C Auditors should not need write access to any areas other than their own. They should be given read only access to other areas on a need to know basis.

Data owners

T The owners of a set of information should be the staff who are responsible for maintaining it. Owners should be primarily responsible for the security of their own data. There is a risk that owners will abuse their privileges.

C Separation of duties within the staff comprising the owners should ensure that alteration, destruction, creation or output of sensitive information requires the co-operation of more than one person.

Following picture shows that Logbook database is updated with the name date time and details on which form the user is worked and machine id means from which machine he/she works.

User	Datetime	Detail	Editdetail	Machine
			memo	
	28.09.2008@20:01:56	Exit From Main Login by: BranchID:	memo	RAJ # Rajneesh
A.MAJUMDAR	05.10.2008@12:41:41	Exit From Main Login by:A.MAJUMDAR BranchID:IGI	memo	RAJ # Rajneesh
ADMINISTRATOR	16.11.2008@11:47:05	Login Correct	memo	SERVER2003 # Administrator
AJITA	05.10.2008@12:40:38	Login Correct	memo	RAJ # Rajneesh
ARUN	27.01.2009@15:50:31	Login Correct	memo	ASMISERVER # Administrator
Administrator	28.09.2008@19:38:29	Login Correct	memo	RAJ # Rajneesh
GOPAL			memo	
GOPAL SINGH	27.01.2009@14:26:43	Entered into Main Programme	memo	ASMISERVER # Administrator
MITTAL	11.02.2009@09:55:31	Error in Login Try:1	memo	RAJSERVER # Administrator
MOHAN	05.10.2008@12:11:10	Error in Login Try:1	memo	RAJ # Rajneesh
MOHAN LAL	07.12.2008@23:14:27	Entered into Main Programme	memo	SERVER2003 # Administrator

Data users

T Data users are given access rights to information by data owners. There is a risk that they will exceed the authority conferred on them by the owners.

C Data users should be given the minimum rights consistent with their legitimate need to access information. Access to sensitive information should be logged and any unusual patterns investigated.

Contractors Maintenance

T Maintenance engineers often have an intimate knowledge of the operating system as well as the hardware. This can enable then to exploit "trap doors" to compromise security.

C Maintenance engineers should not be left to work unattended and should not be allowed to take any files containing sensitive information off site.

The following picture shows that spice works software is running on the server side and check all the inventory or hardware with their respective department.

T Many systems have "maintenance users" with a default password. This can be used to gain unauthorised access to the system.

C Seek the vendor's advice on default users and passwords and change them regularly and, in particular, after every visit by an engineer ACE is using the SPICEWORKS for the inventory check on the network.

Visitors

T If visitors are allowed to see areas where sensitive information or processing takes place this may compromise security.

C Visitors should be required to wear identity badges and staff should be instructed to challenge anyone whom they do not recognise or who is not wearing a badge. In secure environments visitors should be escorted at all times.

Keep visitors away from sensitive areas. If they do need to see sensitive information then require them to sign non disclosure agreements and make sure that they do not see more than is necessary.

Intruders

T Intruders can compromise information system confidentiality, integrity and availability.

C Multiple layers of security offer the best protection. Avoid publicity. Make penetration of the perimeter difficult. Install intruder detection equipment. Lock rooms that give access to sensitive facilities. Use access control to make it difficult to make use of information systems even if an intruder gains access to a terminal.

Physical Buildings Site

T There is a risk that the site will be physically damaged. The specific risks that affect your site will depend upon local circumstances.

C Contingency plans should be developed, which include a plan for the continuation of critical functions in the event of damage to or destruction of the site. Contingency plans should be tested annually.

T Intruders may penetrate your site which could compromise availability, integrity or confidentiality of your information systems.

C Site level physical security should be consistent with the average value of your information systems. Particularly sensitive applications can be further secured by providing higher levels of security for the locations necessary to support them. Basic site security should include security guards who monitor people entering and leaving the site. Ground floor windows should be kept locked when rooms are unattended and fitted with intruder alarms.

Public parking should not be allowed in areas adjacent to critical facilities. Fire doors should open outward and be fitted with glass bolts and alarms linked to a central control panel in the security guards office.

T Sites which are used to support well publicised critical functions are particularly vulnerable.

C Keep the location of assets which support critical functions vague. Try to avoid unnecessary publicity. If the details of the site do become widely known then more extensive security measures will be required to compensate for the increased risks.

T Sites near to areas of dense population are more likely to suffer from the effects of civil disturbance.

C Key information system support sites should be situated away form conurbations if possible.

T Educational sites are particularly vulnerable to theft and attempted system penetration.

C Physical and logical access controls are often weak in educational sites. Ensure that areas which contain assets that are attractive and portable are secured to higher than base level. Accountability controls should be given a high priority for key systems accessible from educational sites.

Data entry / update

T Areas where information is entered or maintained are focal points for threats to the confidentiality and integrity of your information systems.

C Data entry areas should, where possible, be inaccessible to staff without a legitimate need to go there.
Terminals with access to facilities for updating critical information should not be visible from public areas. They should not be left logged in and unattended.

Applications which update key information should close down sessions where there has been no keyboard activity for more than a few minutes. Where the information has critical implications for key information systems the application should repeat identification and authentication checks at regular intervals and log all changes that are made. For particularly sensitive information, consider setting up applications so that changes cannot be finalised until confirmed by an authorising officer.

Processing

T Areas where information is processed may provide extensive opportunities to corrupt, disrupt or gain access to information systems.

C Restrict access to enforce separation of duties where possible.

T Mainframe computers often have exacting environmental requirements. This led to a natural isolation of key machines from staff who were not involved in operating them. As small machines have become more powerful so key applications have been moved onto them. Small machines can usually operate in a normal office environment. The use of distributed processing has in some cases led to information systems becoming reliant on a large number of geographically dispersed small machines. Downsizing has led to a neglect of the need to protect key machines leaving them vulnerable to physical abuse and environmental failure.

C Machines which support key functions should be physically isolated from the general office environment.
Consider the need to protect the power supply of any machines that play an essential part in critical information systems.

Printing

T Sensitive output should be routed through secure areas so that it can be monitored and possibly logged. In the case of financial stationery material loss could arise from theft of output. Where the value of the output lies in the need for confidentiality losses may be incurred by someone merely seeing the output without necessarily removing it.

C Access to rooms used for the output of valuable or sensitive information should be restricted to output handling staff. Physical and logical access control should enforce a separation of duties between those responsible for handling and registering output and those responsible for initiating or authorising it.

Storage

T Areas where information is stored may present an attractive target to someone trying to gain unauthorised access because a lot of information is gathered together.

C Sensitive information should be stored in secure archives / libraries.
Access should be restricted to librarians who should check the clearance of staff who request access and log information which is issued.

T Reliance upon unique archived copies of information renders you vulnerable to losses of the integrity and availability of your information.

C Adopt a backup policy which ensures that at least two copies of key information are held at geographically dispersed locations. The integrity of machine readable archives should be checked at regular intervals and any magnetic media archives should be copied at least every three years.

Communications

T Rooms which house network junction boxes, modem racks, telephone branch exchanges, or patch boxes provide an opportunity for unauthorised staff to identify equipment associated with sensitive facilities and disrupt the service or tap into it.

C Information systems cables and communications equipment should not be labelled in human readable form. Coded cable labels are preferable. The key to the cabling coding system should be locked away. If any cables are labelled they should all be labelled to make it more difficult to spot the route taken by key connections.

Junction boxes, modem racks and telephone exchanges should be secured. Access should be restricted to maintenance staff and network administrators.

Application development

T Applicationsoftware is potentially the most powerful means of compromising the integrity of information systems. Programmers or others with access to the development environment can introduce covert actions into the system.

C Programmers should be assigned work on a modular basis. Each module should have defined inputs and outputs. Peer review and unit testing should guard against the introduction of covert functionality. Change control staff should be separate from application programmers both physically and managerially.

Access to rooms which are used for application development of secure systems should be limited to the programmers. Analysts and change control staff should not be allowed access.

Strict accountability controls and a strong version control system should ensure that there is always a record of who did what and when. Development tools should be made unavailable during quiet hours.

Systems functions

T Systems diagnostics and management tools can be used to intercept network traffic and to circumvent controls.

C Access should be restricted to designated terminals and accountability controls used to monitor usage in much the same way as for application programmers. Physical access to systems terminals should be restricted to systems support staff and they should preferably work in pairs.

Plant

T Power supply is a key resource for information systems. Disruption to the power supply could destroy information and, in the case of power surges, the hardware that supports the system.

C All information system assets should have smoothed power supplies capable of eliminating harmful surges in the supply. Key machinery such as file servers will need an uninterruptible power supply unit to ensure that they can at least close down gracefully in the event of disruption of the supply. Access to plant rooms should be restricted to maintenance personnel.

Software

T Documentation is essential if software is to be maintained. There is a risk that it will be lost, destroyed or stolen. There may be a strong motivation for theft where the software performs functions which have a commercial value or disclose proprietary or sensitive information.

C Documentation should be examined as part of the quality control procedures. Once it has been approved registered copies should be filed by change control staff.

Backup copies of the documentation of the live system should be held at a remote site.

Documentation of sensitive systems should be treated like a registered file. Copies should be numbered, copying banned and issues should be on a need to know basis. Copies should be locked away when not in use.

Hardware

T Information systems assets are often both attractive, portable and easily damaged.

C A full inventory of all material information system assets should be kept, maintained and audited.

T Manuals for hardware are infrequently required but essential on the occasions that they are required. They are often difficult to replace and may contain information that would be of use to a system infiltrator.

C Keep hardware manuals in locked libraries or within secure areas. Issues of manuals should be registered especially where approval is granted to take the manual away from the room that houses the equipment. Keep copies of essential hardware manuals at a remote site.

Cabling diagrams

T Cabling diagrams are essential to the maintenance of networked systems. Loss could compromise the ability to maintain information systems or diagnose network faults. The diagrams are also very useful to anyone with an interest in infiltrating or disrupting the information services provided by the network.

C Network diagrams should be prepared and updated whenever a new routing or connection is introduced.
Copies of cabling diagrams should be kept at backup sites to facilitate recovery if the main site is damaged.
Access to cabling diagrams should be restricted to staff with a legitimate interest in cabling management / network administration.

Data dictionary

T The data dictionary should provide an index to the structure of all permanent information systems. It is an essential tool for the development of new information systems. It can be an invaluable aid to anyone wishing to infiltrate your information systems.

C Integrate the maintenance of the data dictionary with the change control procedures to ensure that it reflects the current structure of data held by your information systems.
Keep copies at remote sites.
Maintain a register of copies of documents which are derived from the data dictionary and treat sensitive extracts like registered files.

"Logical" Access Control and Accountability as part of a Security System

"Logical" access control using IDs and passwords enforces restricted access to **data** on an individual user basis. This is achieved through a security system which determines what the user can access and do, and maintains **accountability** through the creation of an **audit trail** which records the user's use of the computer.

Access control, as any other control, is not considered effective and reliable unless the control can be demonstrated to be working as intended and can be monitored.

An **audit trail** serves as evidence that the access control measure is working as intended and provides the means to investigate irregularities and to identify areas where controls could be improved. Within a computer security system, the **audit trail** is a history file created and protected by the system through password and encryption controls. The use of an **audit trail** is transparent to the user.

Under many security systems, the security administrator has access to all users' **audit trail** history files. Individual users have read access to their own **audit trail**.

Need to Know Principle

A fundamental principle of security policy is to restrict access to **data** and **assets** to those who need such access, which involves defining the specifications of sharing the data and assets. Within a computer environment this involves physically and/or logically (Security System) controlling access to **data** and **assets**.

For example, in an Audit Office, users protect client, audit and administrative **information** to keep others from accidentally reading, modifying or erasing the **information**.

Sensitivity of information:

Availability:the quality or condition of information, services, systems, and programs being available in a timely manner ("at the Organisation level").

Confidentiality: the quality or condition of being sensitive ("may cause injury if information is disclosed").

Integrity: the quality or condition of being accurate and complete ("may cause injury if information is modified, incorrect, or incomplete").

Security Exposure Assessment

A security exposure assessment is the result of combining a business impact assessment with a threat risk/probability assessment. A security exposure assessment is rated as:

> **High:** Dramatic impact - reasonable probability. Those events that have enough probability of occurrence and such strong business impact that it is prudent to take preventive and recovery steps. The expectation of damage is high enough that you don't have to agonise over precise predictions of probability.
>
> **Medium:** Significant impact - unknown probability. The business impact is such that steps should be taken. A review of the threats and their probability is required to reduce the threats to a manageable level.
>
> **Low:** Low impact - any probability. The so-what category. If it happens, it won't hurt that much. If you feel comfortable that the potential for damage is low, these are the threats you accept. There is no need to undertake detail probability analysis.

Security Infrastructure

Typically, in many At organisations, under similar or different titles, security administration is delegated in the following manner:

- **Chief Security Officer:** A Senior Executive, who has overall responsibility for security in the organisation. He is the liaison with all other government entities and is fully accountable for all matters of security within his own organisation.
- **Director of Security:** A senior manager, with delegated authority from the Chief Security Officer, who has the day to day responsibility for the administration of all security matters within the organisation.
- **Person in charge of computer security:** A senior manager, with delegated authority from the Chief Security Officer and reporting to the Director of Security, who has the day to day responsibility for the administration of computer and technology security matters within the organisation.

Finally. . .

Security Team: A team of individuals built from as wide a cross section of the organisation as possible. The team needs the full support and representative be an influential member of the user community and be the

- team leader. Users and senior management are more likely to accept security recommendations from the team as they are usually suspicious of reports produced by "technical specialists".

A corporate security policy, approved by senior management, is put in place to support the information system strategy which, itself, is based upon the mission and objectives identified in the statement of corporate policy.

Typically also, an **I**nformation **S**ystems **S**teering **C**ommittee (**ISSC**), chaired by a senior executive, plays an important role to ensure that all information systems in the organisation are developed and used in line with corporate objectives and strategies. ISSC oversees the implementation of the information systems policy and of the security policy.

Security Management Principles

1. Security protection should be consistent with the sensitivity of the **data** being protected;
2. Security protection should remain with the **data** at all times as it is moved or processed; and
3. Security protection should be continuous in all situations.

These principles are implemented by determining **data** sensitivity from the view of integrity, confidentiality & availability and the application of specific elements of a **Security Scheme** which includes people, physical, practice & procedures, hardware, software, applications, and back up elements of protection.

A Manual Quantitative Approach to ACE Information System Security

1. Overview

1.1 The objective of an information system security programme is to reduce the risk of loss of confidentiality, integrity and availability of information to an acceptable level.

1.2 The aim of an information system security method is to facilitate the establishment of a comprehensive, cost effective, security programme covering all key information systems. The method should assist users to establish a level of security commensurate with their requirements. Finding an appropriate level of security involves risk analysis and risk management.

1.3 **Risk analysis** is used to establish the degree to which information systems are exposed to risks. It entails examining the threats facing information systems, estimating the frequency with which they are expected to occur and then evaluating the impact that the organisation would suffer if threats do occur. "Exposure" is calculated by combining the valuation of impact and the estimated frequency of threats.

1.4 **Risk management** involves the choice of the cheapest countermeasures which reduce the organisation's exposure to risk to an acceptable level. Countermeasures are steps taken by the organisation to reduce the frequency of a threats or to reduce the impact when threats do occur.

1.5 Valuation is the key to establishing an appropriate level of security and users are the key to valuation. It follows that groups of users must be established at an early stage. Each system can be valued by reference to its users. A system with no users or one where the users place no value on the information received is worthless and should not be maintained let alone secured.

1.6 If systems faced no threats then security would not be required. The method should help identify threats to the confidentiality, integrity or availability of information systems. This involves identifying all of the components that must be in place if the users are to continue to receive a reliable service and then looking at events which would adversely affect each component. It also involves the identification of ways that information can leak from each component of the information system.

Once the value of a system and the threats that face it have been established a security requirement can be formulated. This will take the form of a list of measures that are necessary to reduce the risks faced by users to an acceptable level. Putting these measures in place and maintaining them is the job of the staff which make up the security infrastructure.

The security policy statement should provide a framework for the security programmes dealing with each major information system. Large organisations often produce security guidelines which set out security standards in great detail. The guidelines are intended to help staff translate the requirements of the security policy into a security programme for their systems.

information system security should be the establishment of an **I**nformation **S**ystem **S**ecurity **G**roup (**ISSG**). The security group should be responsible for the implementation of the security policy set out by senior management and identifying changes made necessary by developments in the organisation's

Computer Security specialists may not be required at all if the systems simple but for complex computerised systems their help will be required both in evaluating the threats to the system and formulating countermeasures.

2. Threats / Vulnerability

2.1 The first stage in assessing the threats facing a system is to establish the chain of assets which are involved in the supply of information to each major user. Remember the information security objectives of confidentiality, integrity and availability and think of all of the points in the system where any one of these objectives could be compromised. The list of assets will be longer for a networked application than for a manual or stand alone one. A stand alone word processor will be vulnerable through the screen, printer, keyboard and via any storage device such as floppy disks, paper or tapes. A networked system may be vulnerable at many other points including terminals, printers, telecommunications equipment linked to the network, the network cabling and both central and local disks.

2.2 Create a form for each asset or group of assets that you identify and then make a list of all of the events which could compromise integrity, availability or confidentiality of information systems that are connected to the asset. For each event you will have to make an estimate of the likelihood of the event occurring in any one year. This can be very difficult if there have been no occurrences of the event in the history

3. Threats / Vulnerability

3.1 The first stage in assessing the threats facing a system is to establish the chain of assets which are involved in the supply of information to each major user. Remember the information security objectives of confidentiality, integrity and availability and think of all of the points in the system where any one of these objectives could be compromised. The list of assets will be longer for a networked application than for a manual or stand alone one. A stand alone word processor will be vulnerable through the screen, printer, keyboard and via any storage device such as floppy disks, paper or tapes. A networked system may be vulnerable at many other points including terminals, printers, telecommunications equipment linked to the network, the network cabling and both central and local disks.

3.2 Create a form for each asset or group of assets that you identify and then make a list of all of the events which could compromise integrity, availability or confidentiality of information systems that are connected to the asset. For each event you will have to make an estimate of the likelihood of the event occurring in any one year. This can be very difficult if there have been no occurrences of the event in the history

of your information systems. Actuarial statistics from insurance companies may help you to make a realistic estimate of the frequency of unusual events. Whichever approach you adopt there will be an element of uncertainty. Records of past experience relate only to detected events; the security of the system may have been compromised but not detected. In addition there is no guarantee that events will occur with the same frequency that they have in the past.

3.3 The judgement of the expected frequency of events which could compromise security of your information systems plays an important part in the cost justification of measures to protect the system. If you do not gain senior management commitment to the strategy that you adopt for assessing the frequency of events you are unlikely to gain commitment to your recommendations.

34 If there are already measures in place to reduce the likelihood that the information system will be compromised you should note them and make an assessment of the annual cost of keeping them in place as well as the effect that they are judged to have on the frequency of events which could adversely affect the information systems. This information can be used later to decide whether the existing measures should be replaced with more effective ones.

4. Valuation

4.1 Analysis of the threats and vulnerabilities of the system results in a list of events that could adversely affect the information system. You should have agreed an expected frequency for each event. The next stage is to discuss the impact of each event with the users.

4.2 The values that users identify for the impact of each threat will be used as part of the cost justification for security measures. It is important that impacts can be expressed in monetary terms and that they are assessed on a consistent basis. Many impacts that can result from the compromise of an information system have no direct financial impact. In these cases it is necessary to construct scales which can be used to translate non financial impacts into monetary terms.

4.3 The key scale deals with financial loss and might look like the one shown below:

5. Security Administration

5.1 Once a list of **countermeasures** has been agreed these will have to be carried forward into the security programmes and the security operational procedures. The information system security group should be responsible for implementing the selected countermeasures.

5.2 Internal audit should review the risk assessment and risk management working papers and monitor the implementation and effectiveness of the countermeasures selected.

Short Glossary

Security Risk Terminology [11]

- **Countermeasure (C):** A control which is designed to enhance security by either reducing the threat, reducing the impact, detecting a security breach or recovering from a security incident.

  Synonyms: Cross check on every login

  Impact: The adverse effect or consequence of a threat occurring.

- **Probability:** The likelihood of a particular threat occurring.

- **Risk / Exposure:** A measure of the probability and magnitude of the impact of a particular threat on an information system. It is a function of a threat occurring and the possible loss that may result.

- **Risk Assessment:** A formal process to evaluate the chance of vulnerabilities being exploited, based on the effectiveness of existing or proposed security safeguards.

- **Threat (T):** Any potential event or act that is unwanted and can impact on an information system, such as a fire, natural disaster, unauthorised access, etc.

- **Vulnerability:** A measure of the likelihood of an asset succumbing to or being attacked by a particular threat.