TECHNICAL REPORT

ISO/IEC TR 13335-5

First edition
2001-11-01

Information technology — Guidelines for the management of IT Security —

Part 5: Management guidance on network security

Technologies de l'information — Lignes directrices pour la gestion de sécurité IT —

Partie 5: Guide pour la gestion de sécurité du réseau

Reference number
ISO/IEC TR 13335-5:2001(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.ch
Web www.iso.ch

Printed in Switzerland

TABLE OF CONTENTS

Foreword v

Introduction vi

1. SCOPE 1

2. REFERENCES 1

3. DEFINITIONS 2

4. ABBREVIATIONS 2

5. STRUCTURE 2

6. AIM 3

7. OVERVIEW 3

7.1 Background 3

7.2 Identification Process 3

8 REVIEW CORPORATE IT SECURITY POLICY REQUIREMENTS 6

9 REVIEW NETWORK ARCHITECTURES AND APPLICATIONS 6

9.1 Introduction 6

9.2 Types of Network 7

9.3 Network Protocols 8

9.4 Network Applications 8

9.5 Other Considerations 8

10 IDENTIFY TYPES OF NETWORK CONNECTION 8

11 REVIEW NETWORKING CHARACTERISTICS AND RELATED TRUST RELATIONSHIPS 11

11.1 Network Characteristics 11

11.2 Trust Relationships 12

12 DETERMINE THE TYPES OF SECURITY RISK 13

13 IDENTIFY APPROPRIATE POTENTIAL SAFEGUARD AREAS 17

13.1 Introduction 17

13.2 Secure Service Management 18
13.2.1 Introduction 18
13.2.2 Security Operating Procedures 19
13.2.3 Security Compliance Checking 19
13.2.4 Security Conditions For Connection 19
13.2.5 Documented Security Conditions for Users of Network Services 20
13.2.6 Incident Handling 20

13.3 Identification and Authentication 20
13.3.1 Introduction 20
13.3.2 Remote Log-in 20
13.3.3 Authentication Enhancements 21
13.3.4 Remote System Identification 21
13.3.5 Secure Single Sign-on 22

13.4 Audit Trails 22

13.5 Intrusion Detection 23

13.6 Protection Against Malicious Code 24

13.7 Network Security Management 24

13.8 Security Gateways 25

13.9 Data Confidentiality Over Networks 26

13.10 Data Integrity Over Networks 26

13.11 Non-Repudiation 27

13.12 Virtual Private Networks 28

13.13 Business Continuity/Disaster Recovery 28

14 DOCUMENT AND REVIEW SECURITY ARCHITECTURE OPTIONS 29

15 PREPARE FOR THE ALLOCATION OF SAFEGUARD SELECTION, DESIGN, IMPLEMENTATION AND MAINTENANCE 29

16 SUMMARY 29

Bibliography 31

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

In exceptional circumstances, the joint technical committee may propose the publication of a Technical Report of one of the following types:

— type 1, when the required support cannot be obtained for the publication of an International Standard, despite repeated efforts;

— type 2, when the subject is still under technical development or where for any other reason there is the future but not immediate possibility of an agreement on an International Standard;

— type 3, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example).

Technical Reports of types 1 and 2 are subject to review within three years of publication, to decide whether they can be transformed into International Standards. Technical Reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.

Attention is drawn to the possibility that some of the elements of this part of ISO/IEC TR 13335 may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC TR 13335-5, which is a Technical Report of type 3, was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques.*

ISO/IEC TR 13335 consists of the following parts, under the general title *Information technology — Guidelines for the management of IT Security*:

— *Part 1: Concepts and models for IT Security*

— *Part 2: Managing and planning IT Security*

— *Part 3: Techniques for the management of IT Security*

— *Part 4: Selection of safeguards*

— *Part 5: Management guidance on network security*

Introduction

The purpose of this Technical Report (ISO/IEC TR 13335) is to provide guidance, not solutions, on management aspects of IT security. Those individuals within an organization that are responsible for IT security should be able to adapt the material in this report to meet their specific needs. The main objectives of this Technical Report are:

- to define and describe the concepts associated with the management of IT security,
- to identify the relationships between the management of IT security and management of IT in general,
- to present several models which can be used to explain IT security, and
- to provide general guidance on the management of IT security.

ISO/IEC TR 13335 is organized into five parts. Part 1 provides an overview of the fundamental concepts and models used to describe the management of IT security. This material is suitable for managers responsible for IT security and for those who are responsible for an organization's overall security programme.

Part 2 describes management and planning aspects. It is relevant to managers with responsibilities relating to an organization’s IT systems. They may be:

- IT managers who are responsible for overseeing the design, implementation, testing, procurement, or operation of IT systems, or
- managers who are responsible for activities that make substantial use of IT systems.

Part 3 describes security techniques relevant to those involved with management activities during a project life cycle, such as planning, designing, implementing, testing, acquisition or operations.

Part 4 provides guidance for the selection of safeguards, and how this can be supported by the use of baseline models and controls. It also describes how this complements the security techniques described in Part 3, and how additional assessment methods can be used for the selection of safeguards.

Part 5 provides guidance with respect to networks and communications to those responsible for the management of IT security. This guidance supports the identification and analysis of the communications related factors that should be taken into account to establish network security requirements. It also contains a brief introduction to the possible safeguard areas.

Information technology — Guidelines for the management of IT Security —

Part 5:
Management guidance on network security

1. Scope

ISO/IEC TR 13335-5 provides guidance with respect to networks and communications to those responsible for the management of IT security. This guidance supports the identification and analysis of the communications related factors that should be taken into account to establish network security requirements.

This part of ISO/IEC TR 13335 builds upon Part 4 of this Technical Report by providing an introduction on how to identify appropriate safeguard areas with respect to security associated with connections to communications networks.

It is not within the scope of this TR to provide advice on the detailed design and implementation aspects of the technical safeguard areas. That advice will be dealt with in future ISO documents.

2. References

ISO/IEC TR 13335-1:1996, *Information technology — Guidelines for the management of IT Security — Part 1: Concepts and models for IT Security*

ISO/IEC TR 13335-2:1997, *Information technology — Guidelines for the management of IT Security — Part 2: Managing and planning IT Security*

ISO/IEC TR 13335-3:1998, *Information technology — Guidelines for the management of IT Security — Part 3: Techniques for the management of IT Security*

ISO/IEC TR 13335-4:2000, *Information technology — Guidelines for the management of IT Security — Part 4: Selection of safeguards*

ISO/IEC TR 14516:—[1)], *Information technology — Guidelines on the use and management of Trusted Third Party (TTP) services*

ISO/IEC 13888 (all parts), *Information technology — Security techniques — Non-repudiation*

ISO/IEC 15947:—[1)], *Information technology — Security techniques — IT intrusion detection framework*

ISO/IEC 7498-1:1994, *Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model*

ISO 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*

1) To be published.

ISO/IEC 7498-3:1997, *Information technology — Open Systems Interconnection — Basic Reference Model: Naming and addressing*

ISO/IEC 7498-4:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 4: Management framework*

(Other relevant, non ISO/IEC, references are given in the Bibliography.)

3. Definitions

For the purposes of this part of ISO/IEC TR 13335, the definitions given in Part 1 of ISO/IEC TR 13335 apply: accountability, asset, authenticity, availability, baseline controls, confidentiality, data integrity, impact, integrity, IT security, IT security policy, non-repudiation, reliability, risk, risk analysis, risk management, safeguard, threat, vulnerability.

4. Abbreviations

EDI	-	Electronic Data Interchange
IP	-	Internet Protocol
IT	-	Information Technology
PC	-	Personal Computer
PIN	-	Personal Identification Number
SecOPs	-	Security Operating Procedures
TR	-	Technical Report

5. Structure

The approach taken in TR 13335-5 is to first summarize the overall process for identification and analysis of the communications related factors that should be taken into account to establish network security requirements, and then provide an indication of the potential safeguard areas (in doing so indicating where relevant content of other parts of TR 13335 may be used).

This document describes three simple criteria to aid those persons responsible for IT security to identify potential safeguard areas. These criteria identify (1) the different types of network connections, (2) the different networking characteristics and related trust relationships, and (3) the potential types of security risk associated with network connections (and the use of services provided via those connections). The results of combining these criteria are then utilised to indicate potential safeguard areas. Subsequently, a brief introductory description is provided of the potential safeguard areas, with indications to sources of more detail.

6. Aim

The aim of this document is to provide guidance for the identification and analysis of the communications related factors that should be taken into account to establish network security requirements, and to provide an indication of the potential safeguard areas.

7. Overview

7.1 Background

Government and commercial organizations rely heavily on the use of information to conduct their business activities. Loss of confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability of information and services can have an adverse impact on an organization's business operations. Consequently, there is a critical need to protect information and to manage the security of IT systems within organizations.

This critical need to protect information is particularly important in today's environment because many organizations' IT systems are connected by networks. These network connections can be within the organization, between different organizations, and sometimes between the organization and the general public. Both governmental and commercial organizations conduct business globally. Therefore they depend on all kinds of communication from computerized to other 'classical' means. Their network needs have to be fulfilled, with network security playing an increasing significant role.

Clause 7.2 summarises the recommended process for the identification and analysis of the communications related factors that should be taken into account to establish network security requirements, and the provision of an indication of the potential safeguard areas. Subsequent clauses then provide further detail of this process.

7.2 Identification Process

When considering network connections, all those persons in the organization who have responsibilities associated with the connections should be clear about the business requirements and benefits. In addition, they and all other users of the connections should be aware of the security risks to, and related safeguard areas for, such network connections. The business requirements and benefits are likely to influence many decisions and actions taken in the process of considering network connections, identifying potential safeguard areas, and then eventually selecting, designing, implementing and maintaining security safeguards. Thus, these business requirements and benefits need to be kept in mind throughout the process. In order to identify the appropriate network related security requirements and safeguard areas, the following tasks will need to be completed:

- review the general security requirements for network connections as set out in the organization's corporate IT security policy (see clause 8),
- review the network architectures and applications that relate to the network connections, to provide the necessary background to conduct subsequent tasks (see clause 9),
- identify the type or types of network connection that should be considered (see clause 10),
- review the characteristics of the networking proposed (aided as necessary by the information available on network and application architectures), and the associated trust relationships (see clause 11),
- determine the related types of security risk, where possible with the help of risk analysis and management review results - including consideration of the value to business operations of the information to be transferred via the connections, and any other information potentially accessible in an unauthorized way through these connections (see clause 12),
- identify the references to the potential safeguard areas that may be appropriate, on the basis of the type(s) of network connection, the networking characteristics and associated trust relationships, and the types of security risk, determined (see clause 13),
- document and review security architecture options (see clause 14),
- prepare to allocate tasks for the detailed safeguard selection, design, implementation and maintenance, using the identified references to potential safeguard areas and the agreed security architecture (see clause 15).

It should be noted that general advice on the identification of safeguards is contained in Part 4 of TR 13335. This Part (5) of TR 13335 complements Part 4 and provides an introduction on how to identify appropriate safeguard areas with respect to security associated with connections to communications networks.

Figure 1 below explains the overall process of identification and analysis of the communications related factors that should be taken into account to establish network security requirements, and the provision of indications of potential safeguard areas. Each step of the process is described in further detail in the clauses following the figure.

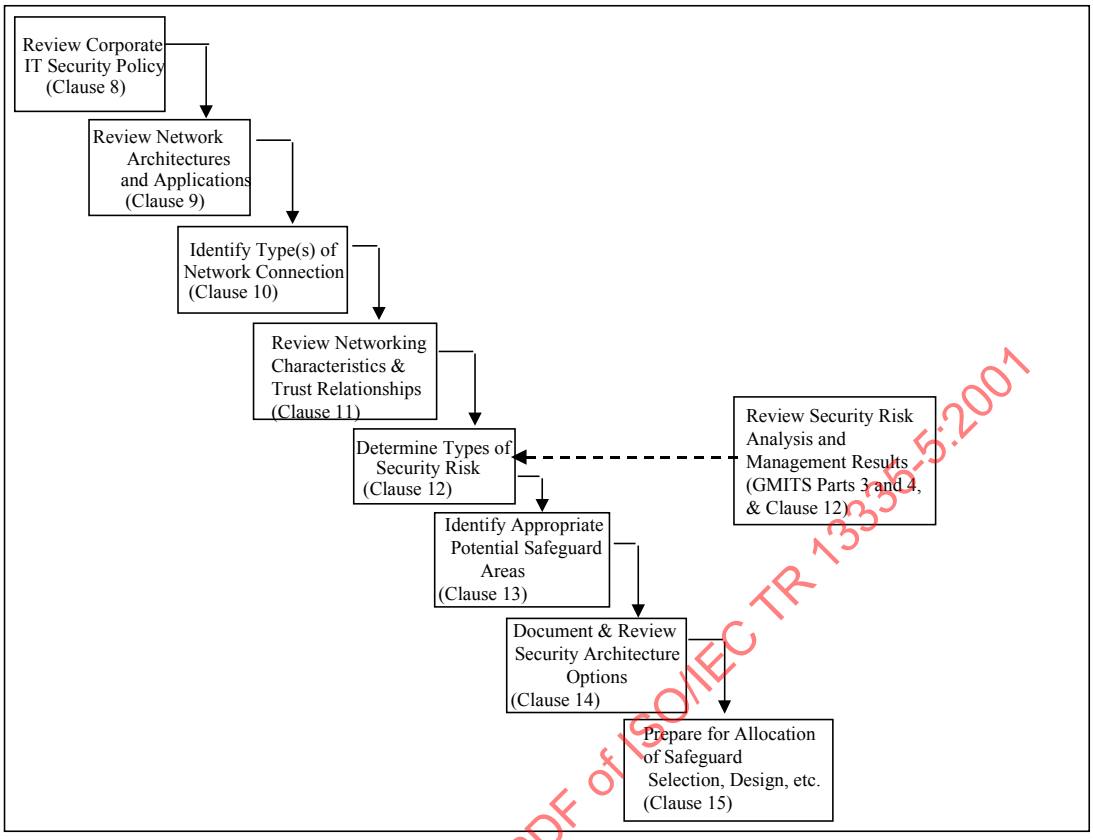

Figure 1: Process for the Identification and Analysis of Communications Related Factors Leading to the Establishment of Network Security Requirements

It should be noted that, in Figure 1, the solid lines represent the main path of the process, and the dotted line where the types of security risk may be determined with the aid of results from a security risk analysis and management review.

In addition to the main path of the process, in certain steps there will be a need to re-visit the results of earlier steps to ensure consistency, in particular the steps ”Review Corporate IT Security Policy” and ”Review Network Architectures and Applications”. For example,

- after types of security risk have been determined there may be a need to review corporate IT security policy because something has arisen that is in fact not covered at that policy level,

- in identifying potential safeguard areas, the corporate IT security policy should be taken into account, because it may, for example, specify that a particular safeguard has to be implemented across the organization regardless of the risks,

- in reviewing security architecture options, to ensure compatibility there will be a need to consider the network architectures and applications.

8 Review Corporate IT Security Policy Requirements

The organization's corporate IT security policy may include statements on the need for confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability, as well as views on types of threat, and safeguard requirements, that relate directly to network connections.

For example, such a policy could state that:

- availability of certain types of information or services is a major concern,
- no connections via dial-up lines are permitted,
- all connections to the Internet must be made through a security gateway,
- a particular type of security gateway must be used,
- no payment instruction is valid without a digital signature.

Such statements, views and requirements, being applicable organization-wide, must be accounted for in the determination of the types of security risk (see clause 12 below) and the identification of potential safeguard areas for network connections (see clause 13 below). If there are any such security requirements then these can be documented in the draft list of potential safeguard areas, and as necessary reflected in security architecture options. Guidance on the positioning of a corporate IT security policy document within an organization's approach to IT security, and on its content and relationships with other security documentation, is provided in Parts 2 and 3 of TR 13335.

9 Review Network Architectures and Applications

9.1 Introduction

Later steps in the process of moving towards the confirmation of potential safeguard areas, i.e. identification of the:

- type(s) of network connection that will be used,
- networking characteristics and associated trust relationships involved,
- types of security risk,

and indeed the development of the list of potential safeguard areas (and later the related designs for securing a particular connection), should always be done in the context of the network architecture and applications that already exist or are planned.

Thus detail should be obtained of the relevant network architecture and applications, and reviewed, to provide the necessary understanding and context for the process steps that follow.

By clarifying these aspects at the earliest possible stage, the process of identifying the relevant security requirement identification criteria, identifying potential safeguard areas, and refining the security architecture, will become more efficient and will eventually result in a more workable security solution (see clauses 9.2 to 9.5 below).

At the same time, consideration of network and application architectural aspects at an early stage allows time for those architectures to be reviewed and possibly revised if an acceptable security solution cannot be realistically achieved within the current architecture.

The different areas that need to be considered under network architectures and applications include:

- types of network,
- network protocols,
- network applications.

Some of the issues for review for each of these areas are discussed in clauses 9.2 to 9.4 below. Other considerations are introduced in clause 9.5.

(General guidance on network and application architectures can be found in ISO/IEC 7498.)

9.2 Types of Network

Depending on the area they cover, networks can be categorized as:

- Local Area Networks (LAN), which are used to interconnect systems locally,
- Metropolitan Area Networks (MAN), which are used to interconnect systems in a metropolitan range,
- Wide Area Networks (WAN), which are used to interconnect systems in wider areas than MANs, up to a world wide coverage.

9.3 Network Protocols

Different protocols have different security characteristics and need to be afforded special consideration. For example:

- shared media protocols are mainly used in LANs (and sometimes in MANs) and provide mechanisms to regulate the use of shared media among the systems connected. As a shared media is used, all information on the network is physically accessible by all connected systems,

- routing protocols are used to define the route through the different nodes on which information travels within MANs and WANs. Information is physically accessible for all systems along the route, and routing may be changed, either accidentally or intentionally.

The protocols may be used on different network topologies, for example bus, ring and star, whether implemented through wireless or non-wireless technologies, which may have further impact on security.

9.4 Network Applications

The type of applications used over a network need to be considered in the context of security. Types can include:

- terminal emulation based applications,

- store and forward or spooler based applications,

- client server applications.

9.5 Other Considerations

When reviewing the network architecture and applications, consideration should also be given to existing network connections within, to or from the organization, and to the network to which the connection is proposed. The organization's existing connections may restrict or prevent new connections, e.g. because of agreements or contracts. The existence of other connections to or from the network to which the connection is required could introduce additional vulnerabilities and thus higher risks, possibly warranting stronger and/or additional safeguards.

10 Identify Types of Network Connection

There are many generic types of network connection that an organization may wish to utilise. Some of these types of connection can be made through private networks (to which access is restricted to a known community), and some could be made through

public networks (to which access is potentially available to any organization or person). Further, these types of network connection could be used for a variety of services, e.g. electronic mail or Electronic Data Interchange (EDI), and could involve use of Internet, Intranet or Extranet facilities, each with differing security considerations. Each of the types of connection may have different vulnerabilities and thus associated security risks, and consequently eventually require a different set of safeguards.

Table 1 below shows one way of categorizing the generic types of network connection that may be required to conduct business, with a descriptive example shown for each type.

Taking due account of relevant network architectures and applications (see clause 9 above), one or more of the types shown in Table 1 should be selected as appropriate to the network connection(s) being considered.

It should be noted that the generic types of network connection described in this document are organized and categorized from a business perspective rather than a technical one. This means that two different types of network connection may sometimes be implemented by similar technical means, and that in some cases the safeguards may be similar, but there are other cases where they will be different.

Table 1: Types of Network Connection

Clause	Type of Network Connection	Descriptive Example
10.1	Connection within a single controlled location of an organization.	Interconnection between different parts of the same organization within the same controlled location, i.e. a single controlled building or site.
10.2	Connection between different geographically disparate parts of the same organization.	Interconnection between regional offices (and/or regional offices with a headquarters site) within a single organization across a wide area network. In this type of network connection, most if not all users are able to access the IT systems available via the network, but not all users within the organization would have authorisation for access to all applications or information (i.e. each user's access would only be in accordance with privileges granted). One type of access from another part of the organization could be for remote maintenance purposes. There might be more access privileges assigned to this type of user and connection.

Clause	Type of Network Connection	Descriptive Example
10.3	Connections between an organization site and personnel working in locations away from the organization.	Use of mobile data terminals by employees (e.g. a salesperson verifying stock availability from a customer site) or the establishment of remote links to an organization's computing systems by employees working from home or other remote sites not linked via a network maintained by the organization. In this type of network connection, the user is authorized as a system user on his local system.
10.4	Connections between different organizations within a closed community, e.g. because of contractual or other legally binding situations, or of similar business interests, e.g. banking or insurance.	Interconnection between two or more organizations where there is a business need to facilitate inter-organizational electronic transactions (e.g. electronic funds transfer in the banking industry). This type of network connection is similar to 10.2 above, except that the sites being interconnected belong to two or more organizations, and the connection is not intended to provide access to the full range of applications utilized by each of the participating organizations.
10.5	Connections with other organizations.	There could be access to remote databases held by other organizations (e.g. through service providers). In this type of network connection, all users, including those of the connecting organization, are individually pre-authorized by the external organization whose information is being accessed. However, although all users are pre-authorized, there may be no screening of potential users other than in relation to their ability to pay for the services being offered. There could also be access to applications on the organization's systems that store or process the organizational information that may be provided to users from external organizations. In this circumstance, the external users would be known and authorized. One type of access from another organization could be for remote maintenance purposes. There might be more access privileges assigned to this type of user and connection.

Clause	Type of Network Connection	Descriptive Example
10.6	Connections with the general public domain.	Access could be initiated by the organization's users to public access databases, Web sites, and/or electronic mail facilities (e.g. via the Internet), where the access is initiated for purposes such as the retrieval of information or the sending of information from/to persons and/or sites which have not been specifically pre-authorized by the organization. In this type of connection, the organization's users may be utilising this facility for organizational (possibly even private) purposes; however, the organization may have little, if any, control over the information being transmitted. Access could be initiated by external users to the organization's facilities (e.g. via the Internet). In this type of network connection, access by the individual external users has not been specifically pre-authorized by the organization.

11 Review Networking Characteristics and Related Trust Relationships

11.1 Network Characteristics

The characteristics of the existing or proposed network should be reviewed. It is particularly important to identify whether the network is:

- a public network - a network accessible by anyone, or
- a private network - a network consisting of owned or leased lines, therefore considered to be more secure than a public network.

It is also important to know the type of data transported by the network, for example:

- a data network - a network transferring primarily data and making use of data protocols,
- a voice network - a network intended for telephone but also usable for data, or
- a network encompassing both data and voice.

Other information, such as whether the network is a packet or switched network, is also germane.

Further, it should also be established whether a connection is permanent, or established at need.

11.2 Trust Relationships

Once the characteristics of the existing or proposed networking have been identified, and at minimum it has been established if the network is public or private (see clause 11.1 above), then the related trust relationships should be identified.

Firstly, the applicable trust environment(s) associated with the network connection(s) should be identified using the simple matrix shown at Table 2 below.

Table 2: Description of Trust Environments

Trust Environment	Description
Low	Network with an unknown community of users.
Medium	Network with a known community of users and within a closed business community (of more than one organization).
High	Network with a known community of users and solely within the organization.

Secondly, the relevant trust environment(s) (from Low, Medium and High) should be related to the applicable network characteristic (public or private) and the type(s) of network connection involved (from clauses 10.1 to 10.6), to establish the trust relationships. This can be accomplished using the matrix shown in Table 3 below.

Table 3: Identification of Trust Relationships

		TRUST ENVIRONMENTS		
		LOW	**MEDIUM**	**HIGH**
TYPES OF NETWORK CONNECTION (See Clause 10)	**PUBLIC**	**10.6**	**10.4** **10.5**	**10.2** **10.3**
	PRIVATE	**10.4** **10.5**	**10.4** **10.5**	**10.1** **10.2** **10.3**

From Table 3 the reference category for each relevant trust relationship can be determined. All of the possible categories are described in Table 4 below.

Table 4: Trust Relationship References

Trust Relationship Category	Description
LOW/PUBLIC	Low trust, and use of a public network.
MEDIUM/PUBLIC	Medium trust, and use of a public network.
HIGH/PUBLIC	High trust, and use of a public network.
LOW/PRIVATE	Low trust, and use of a private network.
MEDIUM/PRIVATE	Medium trust, and use of a private network.
HIGH/PRIVATE	High trust, and use of a private network.

These references will be used in clause 12 to confirm the types of security risk and identify potential safeguard areas.

This task can be aided as necessary by the information available on network architectures and applications (see clause 9).

12 Determine the Types of Security Risk

As reflected earlier, the majority of organizations today are dependent on the use of IT systems and networks to support their business operations. Further, in many cases there is a definite business requirement for the use of network connections between the IT systems at each organization's location, and to other locations both within and outside the organization. When a connection is made to another network, considerable care should be taken to ensure that the connecting organization is not exposed to additional risks. These risks could, for example, result from the connection itself or from network connections at the other end.

Whilst network connections are important for business reasons, it has to be recognized that the use of these connections could yield additional security risks - some possibly related to ensuring adherence to relevant legislation and regulation. The types of risk reflected in this clause relate to concerns about unauthorized access to information, unauthorized sending of information, the introduction of malicious code, denial of receipt or origin, and denial of service connection. Thus the types of security risk that an organization might face relate to loss of:

- confidentiality of information,

- integrity of information,
- availability of information and service,
- non-repudiation of commitments,
- accountability of transactions,
- authenticity of information,
- reliability of information.

Not all of the possible types of security risk will apply to every location, or to every organization. However, the relevant types of security risk need to be identified so that potential safeguards areas can be identified (and eventually safeguards selected, designed, implemented and maintained).

Information should be gathered on the implications to business operations related to the types of security risk referred to above (desirably from the results of a security risk analysis and management review [1]), with due consideration of the sensitivity or value of information involved (expressed as potential adverse business impacts) and related potential threats and vulnerabilities. Related to this, if there is likely to be more than a minor adverse impact on the business operations of the organization, then reference should be made to the matrix in Table 5 below.

It is emphasized that in completing this task, use should be made of the results from security risk analysis and management review(s) conducted with regard to the network connection(s). These results will enable a focus, to whatever level of detail the review(s) have been conducted, on the potential adverse business impacts associated with the types of security risk listed above, as well as the threat types, vulnerabilities and hence risks of concern.

The relevant trust relationship references determined from using clause 11 above should be identified along the top of the matrix in Table 5, and the impacts of concern on the left hand side of the matrix. The references at the pertinent intersections should then be noted – these are the references to the potential safeguard areas that are introduced in clause 13 below.

[1] Guidance on security risk analysis and management approaches is provided in Parts 3 and 4 of TR 13335.

Table 5: Types of Security Risk and References to Potential Safeguard Areas

Types of Risk		Trust Relationship References					
		LOW/ PUBLIC	MEDIUM/ PUBLIC	HIGH/ PUBLIC	LOW/ PRIVATE	MEDIUM/ PRIVATE	HIGH/ PRIVATE
	Loss of Confidentiality	13.2.2 13.2.3 13.2.6 13.4 13.5 13.7 13.8 13.9 13.12	13.2.2 13.2.3 13.2.4 13.2.6 13.3.2 13.3.3 13.3.4 13.4 13.5 13.7 13.8 13.9 13.12	13.2.2 13.2.3 13.2.5 13.2.6 13.3.2 13.3.3 13.3.4 13.3.5 13.4 13.5 13.7 13.8 13.9 13.12	13.2.2 13.2.3 13.2.4 13.2.6 13.3.2 13.3.4 13.4 13.5 13.7 13.8 13.9 13.12	13.2.2 13.2.3 13.2.4 13.2.6 13.3.2 13.3.3 13.3.4 13.4 13.7 13.8 13.9 13.12	13.2.2 13.2.3 13.2.5 13.2.6 13.3.2 13.3.5 13.4 13.7 13.9
	Loss of Integrity	13.2.2 13.2.3 13.2.6 13.4 13.5 13.6 13.7 13.8 13.10 13.12	13.2.2 13.2.3 13.2.4 13.2.6 13.3.2 13.3.3 13.3.4 13.4 13.5 13.6 13.7 13.8 13.10 13.12	13.2.2 13.2.3 13.2.5 13.2.6 13.3.2 13.3.3 13.3.4 13.3.5 13.4 13.5 13.6 13.7 13.8 13.10 13.12	13.2.2 13.2.3 13.2.4 13.2.6 13.3.2 13.3.4 13.4 13.5 13.6 13.7 13.8 13.10 13.12	13.2.2 13.2.3 13.2.4 13.2.6 13.3.2 13.3.3 13.3.4 13.4 13.6 13.7 13.8 13.10 13.12	13.2.2 13.2.3 13.2.5 13.2.6 13.3.2 13.3.5 13.4 13.6 13.7 13.10
	Loss of Availability	13.2.2 13.2.3 13.2.6 13.4 13.5 13.6 13.7 13.8 13.13	13.2.2 13.2.3 13.2.4 13.2.6 13.3.2 13.3.3 13.3.4 13.4 13.5 13.6 13.7 13.8 13.13	13.2.2 13.2.3 13.2.5 13.2.6 13.3.2 13.3.3 13.3.4 13.3.5 13.4 13.5 13.6 13.7 13.8 13.13	13.2.2 13.2.3 13.2.4 13.2.6 13.3.2 13.3.4 13.4 13.5 13.6 13.7 13.8 13.12 13.13	13.2.2 13.2.3 13.2.4 13.2.6 13.3.2 13.3.4 13.4 13.6 13.7 13.8 13.12 13.13	13.2.2 13.2.3 13.2.5 13.2.6 13.3.2 13.3.5 13.4 13.6 13.7 13.12 13.13

Types of Risk		Trust Relationship References					
		LOW/ PUBLIC	MEDIUM/ PUBLIC	HIGH/ PUBLIC	LOW/ PRIVATE	MEDIUM/ PRIVATE	HIGH/ PRIVATE
	Loss of Non-Repudiation	13.2.2 13.2.3 13.2.6 13.4 13.5 13.7 13.11 13.13	13.2.2 13.2.3 13.2.4 13.2.6 13.3.2 13.3.3 13.3.4 13.4 13.5 13.7 13.11 13.13	13.2.2 13.2.3 13.2.5 13.2.6 13.3.2 13.3.3 13.3.4 13.3.5 13.4 13.5 13.7 13.13	13.2.2 13.2.3 13.2.4 13.2.6 13.3.2 13.3.4 13.4 13.5 13.7 13.11 13.13	13.2.2 13.2.3 13.2.4 13.2.6 13.3.2 13.3.4 13.4 13.7 13.11 13.13	13.2.2 13.2.3 13.2.5 13.2.6 13.3.2 13.3.3 13.3.4 13.3.5 13.4 13.7 13.13
	Loss of Accountability	13.2.2 13.2.6 13.2.4 13.6 13.7 13.8 13.12	13.2.2 13.2.6 13.2.4 13.3.4 13.4 13.6 13.7 13.8 13.12	13.2.2 13.2.6 13.3.3 13.3.4 13.4 13.6 13.7 13.8 13.12	13.2.2 13.2.3 13.2.4 13.2.5 13.2.6 13.3.3 13.3.4 13.4 13.6 13.7 13.8 13.12	13.2.2 13.2.3 13.2.4 13.2.5 13.2.6 13.3.3 13.4 13.6 13.7 13.12	13.2.2 13.2.3 13.2.4 13.2.5 13.2.6 13.3.3 13.3.4 13.4 13.7
	Loss of Authenticity	13.2.2 13.2.6 13.2.4 13.3.3 13.5 13.6 13.8 13.10 13.12	13.2.2 13.2.6 13.2.4 13.3.3 13.3.4 13.4 13.5 13.6 13.8 13.10 13.12	13.2.2 13.2.6 13.3.2 13.3.3 13.3.4 13.4 13.5 13.6 13.7 13.8 13.10 13.12	13.2.2 13.2.3 13.2.4 13.2.5 13.2.6 13.4 13.5 13.6 13.8 13.10 13.12	13.2.2 13.2.3 13.2.4 13.2.5 13.2.6 13.3.2 13.4 13.5 13.6 13.10 13.12	13.2.2 13.2.3 13.2.5 13.2.6 13.3.2 13.3.4 13.4 13.5 13.6 13.7 13.10

Types of Risk		Trust Relationship References					
		LOW/ PUBLIC	MEDIUM/ PUBLIC	HIGH/ PUBLIC	LOW/ PRIVATE	MEDIUM/ PRIVATE	HIGH/ PRIVATE
	Loss of Reliability	13.2.2 13.2.6 13.2.4 13.3.3 13.5 13.6 13.8 13.12 13.13	13.2.2 13.2.6 13.2.4 13.3.3 13.4 13.5 13.6 13.7 13.8 13.12 13.13	13.2.2 13.2.6 13.3.2 13.3.3 13.3.4 13.4 13.5 13.6 13.7 13.8 13.12 13.13	13.2.2 13.2.3 13.2.4 13.2.5 13.2.6 13.4 13.5 13.6 13.8 13.12 13.13	13.2.2 13.2.3 13.2.4 13.2.5 13.2.6 13.3.2 13.5 13.6 13.7 13.12 13.13	13.2.2 13.2.3 13.2.5 13.2.6 13.3.2 13.3.4 13.5 13.6 13.7 13.12 13.13

It should be noted that the table appears to indicate that the more a user is trusted, the more safeguards are necessary. There are two reasons for this.

Firstly, there are a number of safeguards described in Part 4 of TR 13335 (and thus not repeated in this TR) that would be selected to protect the host IT facilities, including for identification and authentication, and logical access control. The configuration of the permissions (privileges) in the lower trust situations needs to ensure that access is only provided to resources that are consistent with the trust model and needs of the intended access. In low trust situations the strength of identification and authentication, and logical access control, safeguards (as described in Part 4 of TR 13335), needs to be higher than in high trust situations. If this cannot be assured, then relevant additional safeguards would need to be implemented.

Secondly, trusted users are usually given access to more important/critical information and/or functionality. This can mean a need for additional safeguards, as a reflection of the value of the resources accessed and not on the trust in the users.

13 Identify Appropriate Potential Safeguard Areas

13.1 Introduction

On the basis of the references identified from using clause 12, the potential safeguard areas should now be identifiable from clause 13. Clauses 13.2 to 13.13 introduce potential safeguard areas that should be selected as appropriate after use of clause 12 above. It should be noted that a particular security solution may in fact encompass a number of the potential safeguard areas introduced in clauses 13.2 to 13.13.

It should be noted that there are a number of safeguards that are relevant to IT systems whether or not they have any network connections. These safeguards should be selected

through the use of Part 4 of TR 13335. It should also be noted that this TR assumes that baseline safeguards as described in Part 4 of TR 13335 would be in place for an organization's systems from which network connections are made.

This list of potential safeguard areas will need to be thoroughly reviewed in the context of the relevant network architectures and applications. It will then be used as the basis to prepare for the later allocation of detailed security safeguards selection, design, implementation and maintenance (see clause 15 below).

13.2 Secure Service Management

13.2.1 Introduction

A key security requirement for any network is that it is supported by secure service management activities, which will initiate and control the implementation, and operation, of security. These activities should take place to ensure the security of all of an organization's IT. With regard to network connections, management activities should include:

- definition of all responsibilities related to the security of network connections, and designation of a security manager with overall responsibility,
- documented system security policy, and accompanying documented technical security architecture [2],
- documented security operating procedures (SecOPs),
- the conduct of security compliance checking, to ensure security is maintained at the required level,
- documented security conditions for connection to be adhered to before connection to an organization or community is permitted,
- documented security conditions for users of network services,
- a security incident handling scheme,
- documented and tested business continuity/disaster recovery plans.

It should be noted that this clause builds upon aspects described in Part 4 of TR 13335. Only those topics that are especially important with regard to the use of

[2] As part of the technical architecture design process, a Technical Security Architecture Design (Safeguard Specification) should be produced and documented (that is compatible with the Technical Architecture Design, and vice versa).

network connections are further described in this document. For topics not mentioned further here, the reader should thus consult Part 4 of TR 13335.

13.2.2 Security Operating Procedures

In support of the system security policy, security operating procedures (SecOPs) documents should be developed and maintained. They should contain details of the day-to-day operating procedures associated with security, and who is responsible for their use and management.

13.2.3 Security Compliance Checking

For network connections, security compliance checking should take place against a comprehensive checklist constructed from the safeguards specified in the:

- 'system' security policy
- related SecOPs,
- technical security architecture,
- security gateway service access (security) policy,
- business continuity plan(s),
- where relevant, security conditions for connection.

This should occur prior to live operation of any network connection, prior to a major new release (related to significant business or network related change), and otherwise annually.

13.2.4 Security Conditions For Connection

Unless security conditions for connection are in place and contractually agreed, an organization is in effect accepting the risks associated with the other end of a network connection.

As an example, organization A may require that before organization B can be connected to its systems via a network connection, B must maintain and demonstrate a specified level of security for its system involved in that connection. In this way A can be assured that B is managing its risks in a way that is acceptable. In such cases A should produce a security conditions for connection document that details the safeguards to be present at B's end. These should be implemented by B, followed by that organization signing a binding statement to that effect and that security will be maintained. A would reserve the right to commission or conduct a compliance check on B.

There will also be cases where organizations mutually agree a ‘security conditions for connection’ document which records obligations and responsibilities for all parties, including reciprocal compliance checking.

13.2.5 Documented Security Conditions for Users of Network Services

Users authorized to work remotely should be issued with a documented ‘security conditions for users of network services’ document. This should describe user responsibilities for the hardware, software and data in relation to the network, and its security.

13.2.6 Incident Handling

Unwanted incidents are more likely to occur, and more serious adverse business impact to result, where there are network connections (as opposed to where there are none). Further, with network connections to other organizations in particular there could well be significant legal implications connected with incidents.

Thus, an organization with network connections needs to have a well documented and implemented incident handling scheme and related infrastructure in place to be able to respond quickly as incidents are identified, minimise their impact and learn the lessons to attempt to prevent re-occurrence.

13.3 Identification and Authentication

13.3.1 Introduction

It is important to ensure that the security of network service and related information is preserved by restricting access through connections to authorized personnel (whether internal or external to the organization). Requirements for these are not exclusive to the use of network connections, and thus detail appropriate to the use of a network connection should be obtained by using Part 4 of TR 13335.

Four safeguard areas that could be relevant to the use of network connections, and the IT systems directly related to such connections, are introduced in clauses 13.3.2 to 13.3.5 below.

13.3.2 Remote Log-in

Remote log-ins, whether from authorized personnel working away from the organization, from remote maintenance engineers, or personnel from other organizations, are accomplished either via dial-ups to the organization, Internet connections, dedicated trunks from other organizations, or shared access through the Internet. They are connections established at need by either internal systems or contractual partners using public networks. Each type of remote log-in requires additional safeguards appropriate to the nature of the connection type. Safeguard examples are:

- not allowing direct access to system and network software from accounts used for remote access, except where additional authentication has been provided (see clause 13.3.3 below), and perhaps end-to-end encryption,

- protecting information associated with e-mail software and directory data stored on PCs and laptops used outside of an organization's offices by its personnel, from unauthorised access.

13.3.3 Authentication Enhancements

The use of user id/password pairs is a simple way to authenticate users, but they can be compromised or guessed. There are other more secure ways to authenticate users, particularly for remote users. Authentication enhancements are needed when there exists a high possibility that an unauthorized person may gain access to protected and important systems. This may be, for example, because the access may be initiated using public networks, or the accessing system may be out of the direct control of the organization (e.g. laptop).

Where authentication enhancements over network connections are required (for example, by contract) or justified by the risks, an organization should consider strengthening the person authentication process by implementing relevant safeguards. Examples are:

- using other means of identification to support the authentication of users, such as remotely verified tokens, smart cards and magnetic stripe cards (e.g. through readers attached to PCs), hand held one time pass key generation devices, dial-back modems, and biometric based facilities,

- ensuring that the token or card can only function in conjunction with the authorized user's authenticated account (and preferably, that user's PC and location/access point) and, for example, any related Personal Identification Number (PIN) or biometric profile,

- using caller line verification,

- using links via modems that are disconnected when not in use, and only connected after verification of the caller's identity.

13.3.4 Remote System Identification

As implied in clause 13.3.3 above, where relevant authentication should be enhanced by verification of the system (and its location/access point) from which external access is made.

It should be recognised that different network architectures can offer differing identification capabilities. Thus the organization may achieve enhanced identification by

choosing an appropriate network architecture. All security safeguard capabilities of the chosen network architecture should be considered.

13.3.5 Secure Single Sign-on

Where network connections are involved, users are likely to encounter multiple identification and authentication checks. In such circumstances users may be tempted to adopt insecure practices such as writing down passwords or re-using the same authentication data. Secure single sign-on can reduce the risks of such behaviour by reducing the number of passwords that users have to remember. As well as reducing risks, user productivity may be improved and help desk workloads associated with password resets may be reduced.

However, it should be noted that the consequences of failure of a secure single sign-on system could be severe because not one but many systems and applications would be at risk and open to compromise (sometimes termed the ”keys to the kingdom” risk).

Stronger than normal identification and authentication mechanisms may therefore be necessary, and it may be desirable to exclude identification and authentication to highly privileged (system level) functions from a secure single sign-on regime.

13.4 Audit Trails

It is important to ensure the effectiveness of network security through detection, investigation and reporting of security incidents. Sufficient audit trail information of error conditions and valid events should be recorded to enable thorough review for suspected, and of actual, incidents. However, recognising that recording huge amounts of audit related information can make analysis difficult to manage, and can affect performance, care has to be taken over time in what is actually recorded

Most audit safeguards required in relation to network connections and related IT systems can be determined by using Part 4 of TR 13335. For network connections, auditability of the following types of event is important:

- remote failed log-on attempts with dates and times,
- failed re-authentication (or token usage) events,
- security gateway traffic breaches,
- remote attempts to access audit trails,
- system management alarms with security implications (e.g. IP address duplication, bearer circuit disruptions),

Audit trails will contain sensitive information or information of use to those who may wish to attack the system through network connections. Further, possession of audit trails may provide proof of transfer over a network in the event of a dispute, and are therefore particularly necessary in the context of ensuring integrity and non-repudiation. Therefore all audit trails should be appropriately protected.

13.5 Intrusion Detection

As network connections increase, it will become easier for intruders to:

- find multiple ways to penetrate an organization's IT systems and networks,
- disguise their initial point of access, and
- access through networks and target internal IT systems.

Further, intruders are becoming more sophisticated, and more advanced methods of attack and tools are easily available on the Internet or in the open literature. Indeed, many of these tools are automated, can be very effective, and easy to use - including by persons with limited experience.

For most organizations it is economically impossible to prevent all potential penetrations. Consequently, some intrusions are likely to occur. The risks associated with most of these penetrations can be addressed through the implementation of good identification and authentication, logical access control and accounting and audit safeguards, together with an intrusion detection capability. Such a capability provides the means by which to predict intrusions, and identify intrusions in real-time and raise appropriate alarms. It also enables local collection of information on intrusions, and subsequent consolidation and analysis, as well as analysis of an organization's normal IT patterns of behaviour/usage.

In many situations it may be clear that some unauthorized or unwanted event is happening. It could be a slight degradation in services for apparently unknown reasons, or it could be an unexpected number of accesses at unusual times, or it could be the denial of specific services. In most situations it is important to know the cause, severity and scope of the intrusion as soon as possible.

It should be noted that this capability is more sophisticated than the audit trail analysis tools and methods that are implied in clause 13.4 above and the related clause of Part 4 of TR 13335. The more effective intrusion detection capabilities use special post-processors that are designed to use rules to automatically analyze past activities recorded in audit trails and other logs to predict intrusions, and to analyze audit trails for known patterns of malicious behaviour or behaviour which is not typical of normal usage.

For more detail the reader should refer to ISO/IEC 15947 - IT Intrusion Detection Framework.

13.6 Protection Against Malicious Code

Users need to be aware that malicious code may be introduced into their environment through network connections. Malicious code may not be detected before damage is done unless suitable safeguards are implemented. Malicious code may result in compromise of security safeguards (e.g. capture and disclosure of passwords), unintended disclosure of information, unintended changes to information, destruction of information, and/or unauthorized use of system resources.

Some forms of malicious code can be detected and removed by special scanning software. Scanners are available for firewalls, file servers, mail servers, and workstations for some types of malicious code. Further, to enable detection of new malicious code it is very important to ensure that the scanning software is always kept up to date, through at least weekly updates. However, users and administrators should be made aware that scanners cannot be relied upon to detect all malicious code (or even all malicious code of a particular type) because new forms of malicious code are continually arising. Typically, other forms of safeguard are required to augment the protection provided by scanners (where they exist).

Users and administrators of systems with network connections should be made aware that there are greater than normal risks associated with malicious software when dealing with external parties over external links. Guidelines for users and administrators should be developed outlining procedures and practices to minimise the possibility for introducing malicious code.

Users and administrators should take special care to configure systems and applications associated with network connections to disable functions that are not necessary in the circumstances. (For example, PC applications could be configured so that macros are disabled by default, or require user confirmation before execution of macros.)

Further detail on malicious code can be found in Part 4 of TR 13335.

13.7 Network Security Management

The management of any network should be undertaken in a secure manner, and indeed provide support for the management of network security. This should be accomplished with due consideration of the different network protocols available and related security services.

In furtherance of this, an organization should consider a number of safeguards, the majority of which can be identified through using Part 4 of TR 13335. In addition, remote diagnostic ports, whether virtual or physical, should all be protected from unauthorized access.