INTERNATIONAL STANDARD

ISO/IEC 27033-2

First edition
2012-08-01

Corrected version
2012-08-15

Information technology — Security techniques — Network security

Part 2: Guidelines for the design and implementation of network security

Technologies de l'information — Techniques de sécurité — Sécurité de réseau

Partie 2: Lignes directrices pour la conception et l'implémentation de la sécurité de réseau

Reference number
ISO/IEC 27033-2:2012(E)

COPYRIGHT PROTECTED DOCUMENT

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.org
Web www.iso.org

Published in Switzerland

Contents

Page

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 2. 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.

Attention is drawn to the possibility that some of the elements of this document 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 27033-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This first edition of ISO/IEC 27033-2 cancels and replaces ISO/IEC 18028-2:2006, which has been technically revised.

ISO/IEC 27033 consists of the following parts, under the general title *Information technology — Security techniques — Network security*:

— *Part 1: Overview and concepts*

— *Part 2: Guidelines for the design and implementation of network security*

— *Part 3: Reference networking scenarios – Threats, design techniques and control issues*

The following parts are under preparation:

— *Part 4: Securing communications between networks using security gateways*

— *Part 5: Securing communications across networks using Virtual Private Networks (VPNs)*

Securing IP network access using wireless will form the subject of a future Part 6.

Further parts may follow because of the ever-changing and evolving technology in the network security area.

This corrected version of ISO/IEC 27033-2:2012 corrects the title on the cover page and on page 1.

Information technology — Security techniques — Network security

Part 2: Guidelines for the design and implementation of network security

1 Scope

This part of ISO/IEC 27033 gives guidelines for organizations to plan, design, implement and document network security.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 7498 (all parts), *Information technology — Open Systems Interconnection — Basic Reference Model*

ISO/IEC 27000:2009, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management*

ISO/IEC 27005:2011, *Information technology — Security techniques — Information security risk management*

ISO/IEC 27033-1, *Information technology — Security techniques — Network security — Part 1: Overview and concepts*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 7498 (all parts), ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, and ISO/IEC 27033-1 apply.

4 Abbreviations

For the purposes of this document, the abbreviations used in ISO/IEC 27033-1 and the following are applicable.

IPS	Intrusion Prevention System
POC	Proof of Concept
RADIUS	Remote Authentication Dial-In User Service
RAS	Remote Access Service
SMS	Simple Message Service
SMTP	Simple Mail Transfer Protocol
TACACS	Terminal Access Controller Access-Control System
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security

5 Document structure

The structure of ISO/IEC 27033-2 comprises:

- Preparing for Design of Network Security
  - Introduction
  - Asset Identification
  - Requirements collection
  - Review of requirements
  - Review of existing designs and implementations
- Design of Network Security
  - Introduction
  - Design principles
  - Design Signoff
- Implementation
  - Introduction
  - Criteria for network component selection
  - Criteria for product or vendor selection

- Network management
- Logging, monitoring and incident response
- Documentation
- Test Plans and Conducting Testing
- Sign off

6 Preparing for design of network security

6.1 Introduction

The objectives of network security are to enable the information flows that enhance an organisation's business processes, and to prevent information flows that degrade an organisation's business processes. The preparation work for the design and the implementation of network security involves the following stages:

- Asset identification
- Requirements collection
- Review of requirements
- Evaluation of technical options and constraints
- Evaluation of existing designs and implementations

These stages should result in the early documentation consisting of all the inputs for following design and implementation steps.

6.2 Asset identification

Identification of assets is a critical first step in determining the information security risks to any network. The assets to be protected are those which would degrade the organization's business processes were they to be inappropriately disclosed, modified or unavailable. They include physical assets (servers, switches, routers, etc), and logical assets (configuration settings, executable code, data, etc). This register of assets should already exist as part of continutiy planning/Disaster recovery risk analysis. The questions that must be answered are:

- What are the distinct types of network equipment and facility groupings that need to be protected?
- What are the distinct types of network activities that need to be protected?
- What information assets and information processing capabilities need to be protected ?
- Where information assets reside in the information systems architecture?

Identifiable assets include those required to securely support management, control and user traffic and the features required for the functioning of the network infrastructure, services, and applications. These include devices such as hosts, routers, firewalls, etc, interfaces (internal and external), information stored/processed and protocols used. The protection of infrastructure assets is only part of the objective of the network security design. The principle objective is the protection of business assets such as information and business processes.

6.3 Requirements collection

6.3.1 Legal and regulatory requirements

The legal and regulatory requirements for the location and function of the network should be gathered and reviewed to ensure that the requirements are met in the design of the network. Particular care should be taken where information flows across jurisdictional or regulatory boundaries. In such cases, the requirements of both sides of the boundary must be recorded.

6.3.2 Business requirements

The organization's business processes and data classification types determine its access requirements. The network should be configured to enable this access, to and from its information assets, for suitably authorised users, and prevent all other access. Access to Information will often relate to services on open ports (for example HTTP on TCP port 80) specific hosts (such as www.example.org at IP address 10.11.12.13) particular groups of hosts (for example the 172.128.97.64/24 subnet) or particular network interface devices (such as the interface with MAC address 10:00:00:01:02:03). The organisation will need to identify those services that it provides to others, those services that it uses of others, and those services it provides internally.

6.3.3 Performance requirements

Traffic data is required to enable the configurations for the communication lines, servers and security gateways/firewalls to be documented such that on implementation a good level of service can be provided in accordance with user expectations – with no 'over-configuration' and related unnecessary costs. Information should be gathered on such as the speeds of any existing communication links, configuration/capacity of routers at any third party locations, the number of users that will be allowed access via each link (concurrent access and number of users with access), minimum, average and maximum user connect time required, identity of what authorized users will access over the link, number of web page hits required, database access hits required, growth expected over one year and three/five years, and whether a Windows log-on is required. Use could be made of telecommunications table (queuing) theory for sizing the number of ports, channels required, particularly over dial-up links. These performance requirements should be reviewed, queries resolved and the performance criteria required to be met by the technical architecture and related technical security architecture formally agreed.

6.4 Review requirements

A review of the current capabilities and any planned technical network architecture changes needs to be done and compared to the technical security architecture being developed to note any incompatibilities. Any incompatibilities need to then be reviewed and the appropriate architectures modified.

The information to be gathered during the review should include at a minimum the following:

- identification of the type(s) of network connection to be used,
- determination of the security risks,
- development of the list of required technical security architecture and security controls,
- network protocols to be used,
- network applications used on different aspects of the network

The information gathered should be in the context of the network capabilities. Detail should be obtained of the relevant network architecture and this shall be reviewed to provide the necessary understanding and context for process steps that follow. By clarifying these aspects at the earliest possible stage, the process of identifying the relevant security requirement identification criteria, identifying control areas, and reviewing the technical security architecture options and deciding which one shall be adopted, should become more efficient and eventually result in more workable security solution. For example it may be that because of the location there is only one conduit for all network connections to be established through, so even if a security control might be to have different conduits for redundant connections, that is not possible based on the location picked. Other controls may have to be determined then to find the best way to protect the network connections.

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

6.5 Review of existing designs and implementations

The review of the existing security controls must be conducted in the light of the results from a security risk assessment and management review (details on risk management can be found in ISO/IEC 27005). The results of the security risk assessment may indicate which security controls are required commensurate with the assessed threats. A gap analysis will need to be completed against the current network security architecture to determine what is not addressed in the existing network security architecture.

The network security architecture should encompass the existing security controls and any missing or new security controls.

7 Design of network security

7.1 Introduction

The network security architecture exists to restrict traffic flowing between different trust domains. The most obvious boundary between trust domains is the interface between an organization's internal network and the outside world. An organisation of any significant size will also have boundaries between internal trust domains which must be identified and controlled. The network security architecture includes a description of the interfaces between an organization's/community's internal network and the outside world. Reflecting the requirements mentioned in clause 6.4 above and addressing how to protect the organization from the common threats and vulnerabilities as described in ISO/IEC 27033-1.

Guidance on general best practice design is provided in clause 7.2 below, and guidance on the network security architecture aspects related to specific networking technologies to address the requirements of today and the near future is provided in ISO/IEC 27033-4 and onward. Guidance on specific scenarios that are possible for an organization are covered in ISO/IEC 27033-3.

Technical assumptions made during the requirements gathering should be documented, for example:

- only authorized IP communications should be allowed (firewalls normally only support IP communications, and if any other protocols were allowed then it could be difficult to manage them);
- if non-IP protocols are a requirement then they should be dealt with either outside the security architecture or by tunnelling the protocol.

A network security architecture would normally encompass services, such as the following but not limited to these:

- identification and authentication (passwords, tokens, smartcards, certificates, RAS/RADIUS/terminal access controller access control system plus (TACACS+), etc.);
- logical access controls (single sign on, role based access control, trusted databases, application controls, firewalls, proxy devices, etc.);
- security audit and accounting (audit logs, audit log analysis facilities, intrusion detection facilities, write once read many (WORM) devices, etc.);
- assured storage clearance/secure deletion (provable 'wipe' facilities);
- security testing (vulnerability scanning, network 'sniffing', penetration testing, etc.);
- secure development environment (separate development and test environments, no compilers, etc.);
- software change control (configuration management software, version control, etc.);
- secure software distribution (digital signing, SSL, transport Layer security (TLS) (RFC 5246), etc.);

- secure maintenance and availability (good back-up/restore facilities, resilience, clustering, data vaults, diverse communications, etc.);

- transmission security (use of transport encryption, spread spectrum technology, Wireless LANS (WLANs), VPNs/extranets.

7.2 Design principles

7.2.1 Introduction

Common risk areas associated with networking security architectures are design failures due to poor design and/or the lack of appropriate consideration of business continuity planning or the design does not correspond to the current or expected threat level. Fundamental elements are needed to develop network security architectures that encompass all the identified security controls and business requirements. Most of these elements can be covered by general network security design best practices. ISO/IEC 27033-4 and onward cover design and implementation in detail on some aspects of the network technical security architecture best practices. Additional detailed guidance on best practice implementations can be found in other publications.

The following sections provide general guidance on design best practices to be followed when considering a network security architecture.

7.2.2 Defence in depth

Organizations need to look at security not just from one perspective, but as a pervasive layered approach. Security must be comprehensive across all network layers. Adopting a layered approach is considered to be defence in depth. The components of security are a combination of policy, design, management and technology. Each organization needs to determine its needs and design a defence in depth based upon those needs.

Many mobile devices have USB and network connectivity, as well as wireless capability. These devices can be connected to the internal network or systems on it in an ad-hoc manner; should this be done with the device's wireless connectivity open and unsecured, these devices could act as a rogue wireless access point on the internal network, bypassing the perimeter controls. Strict policies should be in place to restrict the connection of unsecured mobile devices to the network, and routine scanning of the wireless channels should be done to detect any rogue access points.

Any wireless access points should be in a DMZ. Those that are in the internal network should have strict connections settings: the strongest security (WPA2 where possible), and MAC address filtering to restrict the devices that can connect to it to those that are authorised. ISO/IEC 27033-3 provides more details on the threats presented by mobile communications technology and the relevant controls.

The defense in depth principle represents the use of multiple security controls or security techniques to help mitigate the risk of one component of the defense being compromised or circumvented. An example could be anti-virus software installed on individual workstations when there is already virus protection on the firewalls and servers within the same environment. Different security products from multiple vendors may be deployed to defend different potential vectors within the network, helping prevent a shortfall in any one defence leading to a wider failure; also known as a "layered approach"

Figure 1 shows how there is perimeter security, with a more finer grain for infrastructure security, still more finer for the hosts, then applications and finally data. All of the layers are to protect the data.

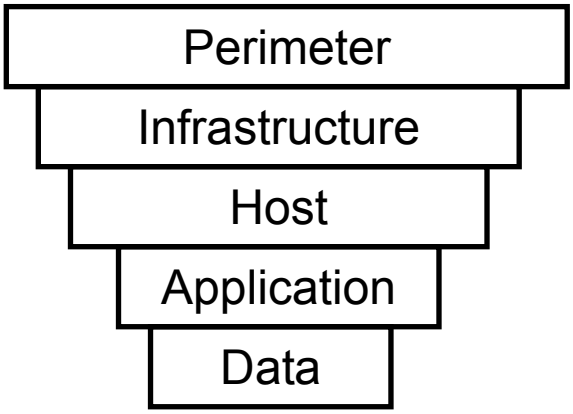

Figure 1 — Defence in Depth Approach

Security solutions based on the layered approach are flexible and scalable. The solution is adaptable to the security needs of the organization.

7.2.3 Network Zones

Network zoning using the concept that system resources of different sensitivity levels (i.e., different risk tolerance values and threat susceptibility) should be located in different security zones. This creates a way to have the systems make available only such data that is necessary for conducting the tasks (e.g., only servers providing services to the Internet are registered in public DNS) for that particular zone.

The basic means of keeping network traffic flowing where you want and restricting it where you do not is a security gateway: dedicated firewall devices, firewall functions in IPS devices, and access control lists in network routers and switches.

With proper placement and configuration, security gateways help create secure architectures, dividing the network infrastructure into security zones and controlling communication between them. Additional information of how to place and configure security gateways can be found in ISO/IEC 27033-4.

The compartmentalization principle describes the following network security design rules:

- Networks of different sensitivity levels should be located in different security zones:
  - Devices and computer systems providing services for external networks (e.g., the Internet) should be located in different zones (De-Militarized Zone – DMZ) than internal network devices and computer systems.
  - Strategic assets should be located in dedicated security zones.
  - Devices and computer systems of low trust level such as remote access servers and wireless network access points should be located in dedicated security zones
- Networks of different types should be located in separate security zones:
  - User workstations should be located in different security zones than servers
  - Network and security management systems should be located in dedicated security zones
  - Systems in development stage should be located in different zones than production systems

7.2.4 Design resilience

Network Security design should incorporate several layers of redundancy to eliminate single points of failure and to maximize the availability of the network infrastructure. This includes the use of redundant interfaces, backup modules, standby devices, and topologically redundant paths. In addition, the designs also use a wide set of features destined to make the network more resilient to attacks and network failures.

7.2.5 Scenarios

A network environment under review can often be characterized by particular network scenario(s) and 'technology' topic(s) that are associated with well defined threats, design considerations and control issues. Such information is very useful when reviewing technical security architecture/design options and selecting and documenting the preferred technical security architecture/design and related security controls.

ISO/IEC 27033-3 references such scenarios, and for each scenario provides detailed guidance on the security threats and the security design techniques and controls required to counter those threats.

7.2.6 Models and Frameworks

Historically a component of security system engineering includes selection, use or development of a security model or framework.

The security model is used to describe the entities (subjects governed by an organization's security policy) and define the access rules necessary to instantiate said policy. The security model typically focuses on either confidentiality via access controls or information integrity, where some are formally defined and others informally defined.

Security frameworks typically provide an organization a way to form a general outline of how to form a secure system. An example of a framework would be ITU-T X.805. This overarching framework for the ITU-T X.800 series of recommendations to fit into to provide end-to-end network security. To this end, X.805 defines the concept of security dimensions that are containers for tools, technologies, standards, regulations, procedures, etc. that span either aspects of security. X.805 recognizes that redundant security mechanisms are avoided by identifying security capabilities in one layer that protect another layer, (Layer here is used in the context of X.805) thus reducing the overall cost of a security solution. X.805 is a generic security framework and as such does not provide a specification for any particular information system or component. Rather it specifies security principles and target security capabilities facilitating end-to-end network security. An example of how ITU-T X.805 can be applied in support of ISO/IEC 27001 controls can be found in Annex C.

7.3 Design Sign off

Signoff of the completed Network Security design should be signed off by the appropriate levels of management.

8 Implementation

8.1 Introduction

The implementation of Network security should be based on the design of the Network security described in the clause 7.

The implementation of Network security consists of: Segmentation and compartmentalization

- Criteria for Network component selection;
- Criteria for product or vendor selection;
- Network management;
- Logging, monitoring and incident response;
- Documentation;
- Test plans and conducting testing;
- Sign off

8.2 Criteria for Network component selection

For any secure network design there is a combination of common components that can be used. These components are used in a combination that will create a technical network security design. The remainder of clause 8 and ISO/IEC 27033-3 and onward go into technical detail on some of the components listed below. These components will be used in some combination to secure the requirements reflected in clause 6.4. Some of these components may include:

- Segmentation and compartmentalization
- Security Management systems (e.g. monitoring and configuration management)
- Basic Security technologies, such as Identity management, cryptography, etc.
- Network admission control devices
- Threat mitigation techniques
- Perimeter devices
- Network filters such as firewalls and content inspection services Remote-access devices
- Intrusion detection systems/Intrusion prevention systems
- Endpoint protection
- Routers and switches
- Extranet connections

8.3 Criteria for product or vendor selection

Product selection should not be undertaken in isolation, but conducted as an iterative process associated with the design of the network security architecture.

Some examples of what product selection should be based on include:

– technical suitability and merit of the product;

– performance;

– protocol support;

– resilience;

– compatibility;

– extensibility;

– network management facilities;

– audit capability;

– compliance;

– technical documentation;

– maintenance;

- remote diagnostic facilities;
- logical security;
- assurance of security capabilities via schemes such as an ISO 15408 evaluation (or equivalent)
- vendor ‘characteristics’ (capability, track record, commitment to quality, market position, size, overall competence including for the products under consideration, organizational/financial stability, references, and training facilities);
- timescales for delivery;
- costs.

8.4 Network management

Network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance and provisioning of networked systems.

- Operation deals with keeping the network (and the services that the network provides) up and running smoothly. It includes monitoring the network to spot problems as soon as possible, ideally before users are affected.
- Administration deals with keeping track of resources in the network and how they are assigned. It includes all the "housekeeping" that is necessary to keep the network under control.
- Maintenance is concerned with performing repairs and upgrades - for example, when equipment must be replaced, when a router needs a patch for an operating system image, when a new switch is added to a network. Maintenance also involves corrective and preventive measures to make the managed network run "better", such as adjusting device configuration parameters.

Misconfiguration of network related components, either intentional or deliberate, impose significant risks, not only regarding availability, but often also regarding integrity and confidentiality.

Therefore controls to address these risks are necessary. Such controls can be categorized in organizational controls or technical controls.

Organizational controls can include proper entitlement of administrative personal, operational principles such as four eyes principle, appropriate separation of duties as wells as procedures and policies to avoid default or weak passwords. Operational controls can include configuration and version control to address potential misconfiguration or tracking changes in the configuration of devices.

Technical controls include the use of administration interfaces and tools which provide appropriate authentication and authorisation quality and confidentiality. Technical management is required for a number of networking related components. Security gateways could be managed locally or remotely, but remote management should use tools which ensure strong or two-factor authentication or at least technically avoid default or weak passwords and which provide adequate integrity and confidentiality functions would be used whenever possible. Examples are the use of encrypted VPN tunnels configured with appropriate levels of encryption or SSH terminal emulation. Servers could also be managed locally or remotely. Where the servers support sensitive information then again the remote management must use tools which ensure strong or two-factor authentication or at least technically avoid default or weak passwords and which provide adequate integrity and confidentiality functions would be used whenever possible.

Infrastructure components, such as switches and routers, could be managed locally from the console port, remotely from a central management station, using terminal emulation program to work online on a remote computer or from distributed management system. However, it is recognized that these protocols are not secure unless they can be configured with a method that can fully encrypt the connection. One example of secure remote connection which can fully encrypted and includes a secure file transfer facility is SSH. Further, access to infrastructure components should be controlled by an authentication server.

Networks that are outsourced to a provider normally have their own management systems. However, they should be managed from a central management station using secure remote management methods. Remote management methods should include encryption and authentication using public key cryptography. Examples of secured methods that could be used are, Telnet and TFTP via a VPN tunnel, or SSH, which is controlled by an authentication server.

Many organizations use simple network management protocol (SNMP) management traps to directly monitor such networks. There are significant risks with SNMP version 1 and version 2 that have weak or no security. Therefore if an organization decides to use SNMP the use should be using version 3 with full security controls.

8.5 Logging, monitoring and incident response

An audit server should be configured with all security gateway systems, located on a DMZ that is secure from both the outside and the inside networks as well as any other security relevant devices located inside or outside the DMZ. The audit server should not be part of the internal network domain and should only be directly accessible by an assigned security officer for the security gateway/firewall system. However, write access will be needed to allow audit logs to be uploaded by a secure protocol (for example Secure Copy Protocol (SCP)) from infrastructure components, servers and firewalls. All firewall and associated audit logs should be directed to this audit server for later examination by security staff, with audit analysis software provided to allow review of the audit log files.

Security information management includes the collection and standardization of information collected so that decisions can be made based on that information. Information collected may include syslogs, SNMP information, IDS/IPS alerts, and flow information.

Where possible, the audit server and or IDS/IPS systems should be configured to alert an assigned security officer by email, SMS, or both according to the priority level of any detected abnormal activity. Should any abnormal activity be detected that could constitute an attempted attack, the assigned security officer should implement incident response procedures according to the priority level of the alert. Information security incident management is covered in more detail in ISO/IEC 27035.

8.6 Documentation

The network security architecture document is one of the critical technical security document and, as stated earlier, should be compatible with the related security risk assessment and risk management review results, organization/community networking and information security policies, and other security policies as relevant. As with any critical documentation these documents should be kept under change control. An example template is given in Annex B.1. It should reference the related technical architecture documentation and other technical security documents. Key related documents include:

- Documentation on information security requirements for all managed network components (such as Gateways, Firewalls, Routers etc.). These requirements include also functional security requirements such as Firewall rule base requirements.– see Annex B.2 for an example template;
- audit log analysis software requirements documentation;
- product analysis reports.

8.7 Test plans and conducting testing

A security testing strategy document should be developed that describes the approach to be taken with testing to prove the networking technical security architecture. It should concentrate on how the key technical security controls should be tested to verify that the defined requirements are met, and that policies are implemented as designed. To verify these viewpoints, system test and checklist-based checking are conducted.

The testing strategy document should include areas such as:

– identification and authentication mechanisms

– resilience of design

– authorisation mechanisms

– implementation of policy controls

– verification of hardened operating systems

– verification of audit log solution

The testing strategy should also include unit and usability testing to ensure suitability of design.

Before conducting a system test, a testing plan should be prepared. The testing plan should include testing-data with testing-scenarios for its evidence. The testing plan should also include an appropriate testing term. The testing-data should be carefully prepared to be able to examine the functionality of the technical security controls.

8.8 Sign off

Signoff of the completed Network Security implementation should be signed off by the appropriate levels of management.

Annex A
(informative)

Cross-references between ISO/IEC 27001:2005/ISO/IEC 27002:2005 network security related controls and ISO/IEC 27033-2:2012 clauses

ISO/IEC 27001:2005/ ISO/IEC 27002:2005 clause		ISO/IEC 27033-2:2012 clause
10.6.1- Network Controls	Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.	See below against ISO/IEC 27001/27002 clauses 10.6.1 IG a) to e).
10.6.1 IG a)	Operational responsibility for networks should be separated from computer operations where appropriate.	8.3 Network management
10.6.1 IG d)	Appropriate logging and monitoring should be applied to enable recording of security relevant actions.	8.4 Logging and monitoring
10.6.1 IG e)	Management activities should be closely coordinated both to optimize the service to the organization and to ensure that controls are consistently applied across the information processing infrastructure.	8.3 Network management
10.6.2 – Security of Network Services	Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided in-house or outsourced.	6.3 Requirements collection 6.4 Review Requirements
10.8.1 Information exchange policies and procedures	Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities.	8.5 Documentation
11.4.1 Policy on use of network services	Users should only be provided with access to the services that they have been specifically authorized to use.	8.3 Network Management
11.4.2 User authentication for external connections	Appropriate authentication methods should be used to control access by remote users.	8.3 Network Management

Annex B
(informative)

Example documentation templates

B.1 An example network security architecture document template

B.1.1 Introduction

Including sections such as:

- purpose/objectives/scope,
- assumptions, both technical and otherwise,
- document status,
- document structure.

B.1.2 Business related requirements

Including sections such as:

- introduction,
- context,
- networking and other IT services.

B.1.3 Technical architecture

Including sections such as:

- introduction,
- technical overview,
  - summary,
  - major domain 1,
  - major domain 2,
  - major domain 3,
  - etc.,
  - servers,
  - workstations,
  - logging,

  - management,
  - authentication and access control,
  - service coverage and resilience,
- system locations,
- system components,
- interconnections,
- component 1,
  - overview,
  - configuration,
  - logging,
  - management,
- component 2,
  - overview,
  - configuration,
  - logging,
  - management,
- component 3,
  - overview,
  - configuration,
  - logging,
  - management,
- component ‘x’ etc.,
- server management,
  - introduction,
  - monitoring of services,
  - extended system administration (XSA),
  - enterprise security manager (ESM),
  - any other manager,

- firewalls,
  - introduction,
  - overview,
  - firewall configuration back-up,
  - design criteria and configuration,
  - rule bases,
- firewall management,
  - configuration,
  - firewall alerts,
  - remote access,
- logging,
- back-up system,
  - introduction,
  - firewalls,
  - servers,
  - applications,
- network communications,
  - local area networking, e.g. VLANs, WLANs,
  - routers,
  - switches,
  - IP addressing,
- management responsibilities,
  - servers,
  - firewalls,
  - infrastructure,
  - application management.

B.1.4 Network services

Including sections such as:

- introduction,
- services at location x,
- services at location y,

There should be a list of all network services by location, including such as:

- KiloStream services,
- MegaStream services,
- frame relay services,
- ATM,
- IP Clear/ MPLS,
- broadband services,
- Wi-Fi/WiMax,
- LAN connect services,
- GSM,
- primary rate ISDN (up to 30 of 64 Kbps channels delivered over a MegaStream),
- ISDN basic rate interface (BRI), (2 × 64 Kbps channels),
- analogue direct exchange lines (DELs),
- intranet/extranet services,
- ISPs,

with all lines and services included.

If the list is extensive then it should be included in an annex with references to it from the main body of the document.

B.1.5 Hardware/physical layout

Including sections such as:

- introduction,
- location.

There should be a list of all hardware, with floor plans and cabinet layouts – by location, including coverage of, for example, servers, routers, switches, firewalls and other communications equipment. As all hardware should be labelled, the labelling plan should be included or at least referenced.

Table B.1 shows an example hardware list table. There should be a table for each type of hardware – the example table covers server components.

Table B.1 — Example Hardware List Table

Server component	Hardware	Software	Comment
Name and manufacturer of server	Part number	Software and version	Specific comments as required, such as. scaled vertically, or clustered.

B.1.6 Software

Including sections such as:

- introduction,
- list of software,
  - software at location x,
  - software at location y,
  - etc.

The list of all software, including version numbers, should include such as:

- Windows software,
- firewalls,
- RAS/RADIUS,
- router software,
- switch software,
- proxy,
- audit management,
- mail servers,

- SMTP mail relay,
- content management,
- Java/ActiveX screening,
- web servers,
- FTP servers,
- domain controllers,
- back-up software,
- other software.

The list should be included in an annex with references to it from the main body of the document.

B.1.7 Performance

Expected performance details should be included, including for ‘subsystems’ such as:

- desktop,
- servers,
- LAN,
- WAN,
- gateways,
- external services.

B.1.8 Known issues

Details of known issues, including regarding areas of non-compliance, should be included under such headings as technical, physical and environmental, including sections such as:

- introduction,
- areas of non-compliance.

B.1.9 References

References should be included to all related documentation, including:

- security risk assessment and management review results,
- networking security policy,
- information security policy,
- other security policies as relevant,
- the technical architecture documentation,

- the service access (security) requirements documents for each firewall system (that include the firewall rule base(s)),
- (audit) log analysis software requirements documentation,
- product analysis reports,
- generic testing strategies and plans,
- the information security incident management scheme,
- SecOPs,
- conditions for secure connection for third parties,
- user guidelines for third party users.

B.1.10 Appendices

Include details of such as:

- hardware configuration,
- server/console configurations,
- firewall configurations,
- router configurations,
- software configuration,
- database configuration,
- IP addressing plan,
- SNMP configuration,
- system traps,
- application traps,
- standards.

B.1.11 Glossary

B.2 An example template for a Functional Security requirements document

NOTE One document should be produced for each firewall system.

B.2.1 Introduction

Including sections on such as:

- background/scope/objectives,
- firewall system name,

- firewall location,
- firewall role,
- name of person/group responsible for firewall operation,
- record of revisions to document content,
- references.

B.2.2 Firewall configuration

Including sections on such as:

- introduction,
- identity of links via firewall system,
- firewall architecture overview,
- firewall system details:
  - hardware,
  - software,
  - firewall architecture,
  - firewall service,
  - firewall management,
  - inner router,
  - outer router,
  - DMZ hub,
  - anti-malicious code server,
  - SMTP mail,
  - web pages,
  - SMTP mail server,
  - (audit) logging server,
  - UPS,
  - other components,
  - other controls required,
- description of links to, and of, other systems,
- information types involves and their sensitivity,
- user types and numbers etc.

B.2.3 Security risks

Including sections on such as:

- introduction,
- potential adverse business impacts (sometimes known as asset valuations),
- threat assessments,
- vulnerability assessments,
- risk assessments,

in the context of the firewall usage.

B.2.4 Security management

Including sections on the responsibilities of such as:

- security officer/group,
- network personnel,
- firewall support personnel,
- network management,
- other IT management,
- users.

B.2.5 Security administration

Including sections on such as:

- SecOPs,
- security compliance reviews,
- availability,
- maintenance,
- configuration control,
- capacity management,
- problem management,
- service level management,
- expiry of this document.

B.2.6 Authentication and access control

Including sections such as:

- introduction,
- logical access controls for such as firewall administrators, internal and remote users,
- external access control measures such as network to firewall rule base, secure platform and application proxy servers,
- network level protection.

B.2.7 (Audit) Logging

Including sections on such as log:

- information to be recorded,
- analysis to be conducted and with what tools,
- security.

B.2.8 Information Security incident management

Including sections on such as log related:

- introduction,
- incident reporting,
- incident handling,
- etc.

B.2.9 Physical security

Including sections on the responsibilities of such as control of access to the:

- firewall system,
- cabling.

B.2.10 Personnel security

Including sections applicable to firewall related personnel on such as:

- recruitment screening/checking,
- security awareness and training.

B.2.11 Appendices

Including on such as service and protocol details:

- access outwards and inwards,
- remote management,
- firewall management,
- DMZ server management,
- any other relevant service and protocol details.

B.2.12 Glossary

Annex C
(informative)

ITU-T X.805 framework and ISO/IEC 27001:2005 control mapping

ITU-T X.805 can also be used for technical augmentation of controls in the ISO/IEC 27001:2005 standard. In particular, as depicted in Figure C.1, ITU-T X.805 can augment four controls in ISO/IEC 27001:2005 security policy, asset management, access control, and information security incident management. The specific ITU-T X.805 layer, planes, dimensions applicable to each of these controls is depicted in the Figure. For example, for asset management, the infrastructure and service layers, and the control, and management planes are the most applicable, with the access control and availability dimensions being the most prominent concerns.

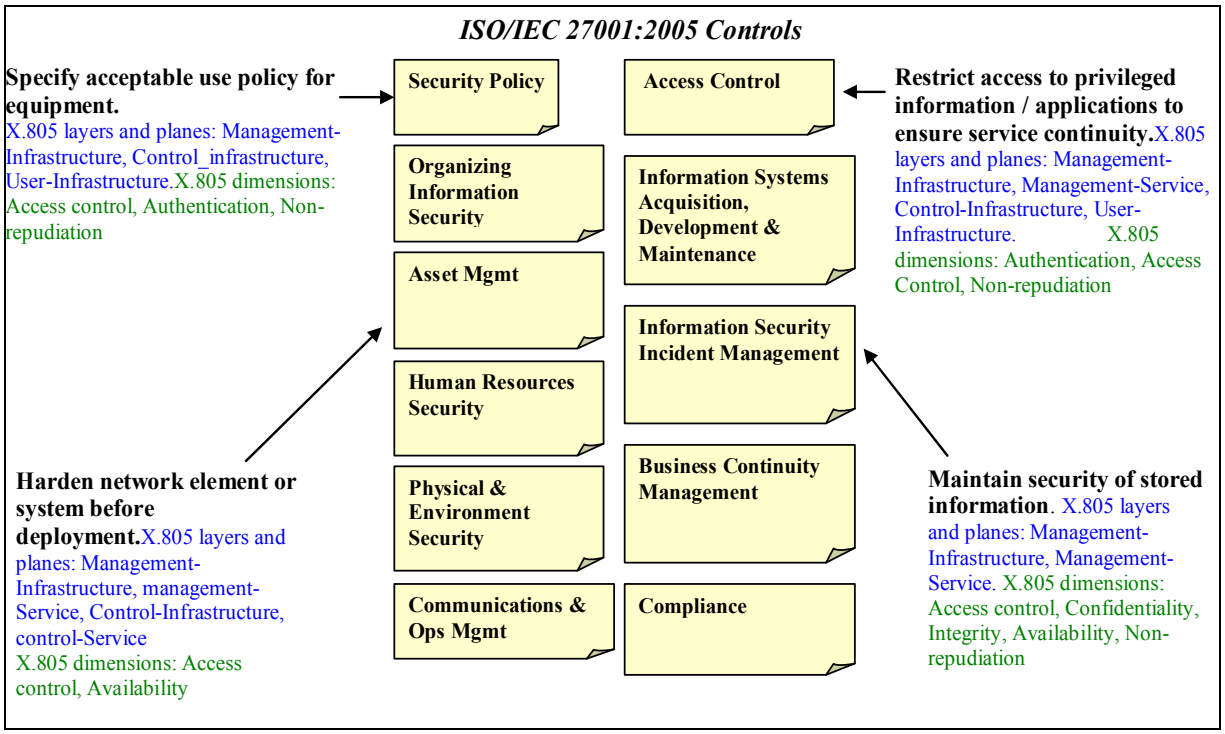

Figure C.1 — ITU-T X.805 Augmentation for ISO/IEC 27001 Controls

As an example, the augmentation can be used to systematically assess and design the security for an enterprise data center that stores its employee information, specifically personal information that should be restricted to authorized users only. The employee information is accessed by several support organizations employed by the enterprise, one of which is the help desk; in addition, the data center and systems contained therein are maintained by the corporate IT organization. As seen in Figure C.2, the Help Desk accesses the employee information for handling complaints, supporting orders for new IT services, resolving problems employees are having with IT services (e.g., remote access), etc. In addition, the Corporate IT organization accesses the employee information as part of its maintenance activities of file system maintenance, system updates, patch management etc.

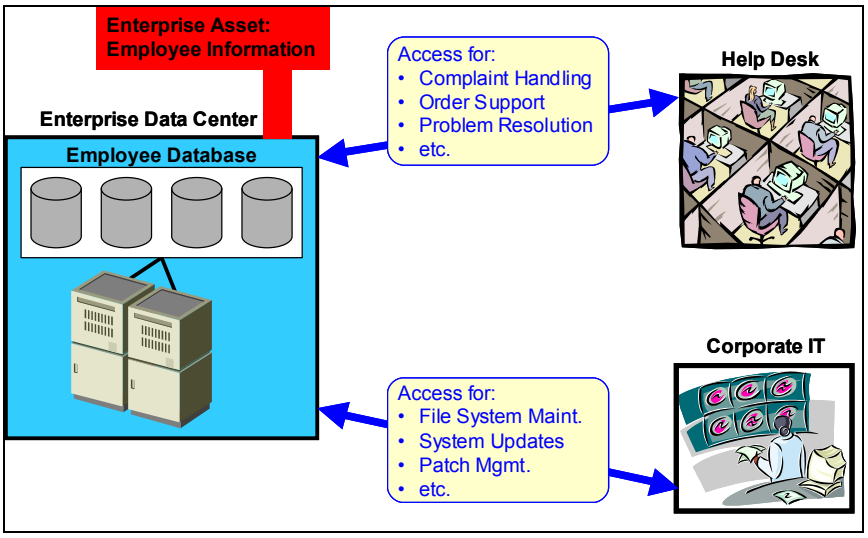

Figure C.2 — Access Scenario for Enterprise Asset

An ITU-T X.805 threat/vulnerability analysis reveals that members of the corporate IT organization can view and modify the employee information thereby making it vulnerable to disclosure and corruption in the infrastructure layer (see Figure C.3). In addition, as part of performing problem resolution, employee information is transmitted in the clear between the data center and the help desk; thereby making it vulnerable to disclosure, corruption and interception in the services layer. Thus, controls must be identified and selected to protect employee information against threats and vulnerabilities in the management plane of its infrastructure and services layers. It should be noted that a step-by-step ITU-T X.805 analysis is not presented in this paper. Only the result of such an analysis is assumed for brevity.

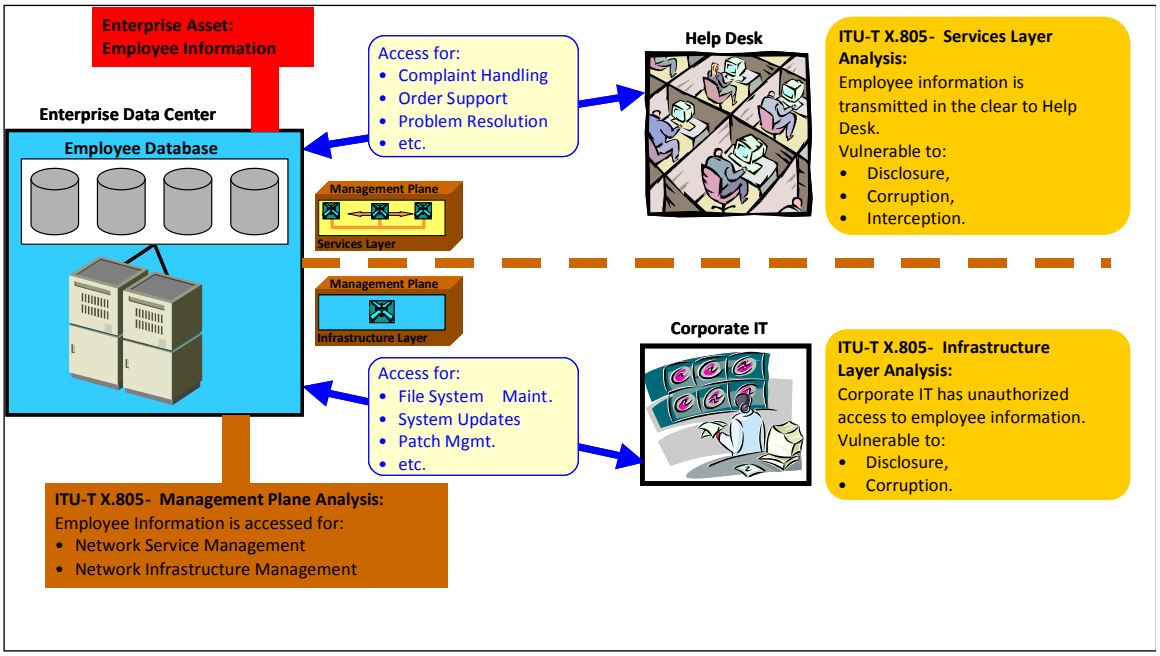

Figure C.3 — ITU-T X.805 Threat and Vulnerability Analysis Results for Enterprise Asset

ISO/IEC 27001:2005 Control A.10.9.2 is identified and selected as being required to protect the management of employee information in the services and infrastructure layers due to the vulnerabilities and threats identified there by the ITU-T X.805 analysis (Figure C.4). ISO/IEC 27001 Control A.10.9.2 states that information involved in on-line transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

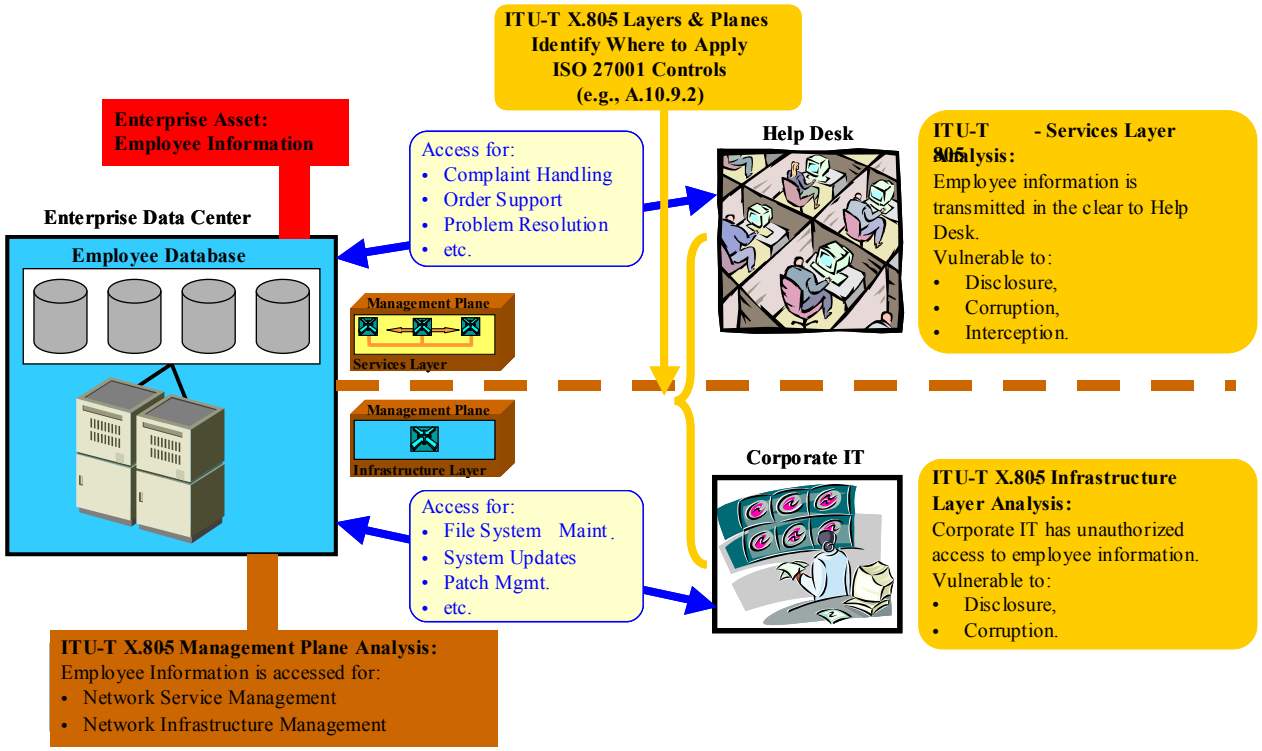

Figure C.4 — ISO/IEC 27001 Controls

The ITU-T X.805 dimensions provide implementation and operation details for Control A.10.9.2 in the services and infrastructure layers for the employee information asset. In the services layer, Communications Security dimension provides for the use of VPNs to prevent misrouting. The Data Integrity dimension provides for the use of IPSec AH to prevent incomplete transmission, unauthorized message alteration and duplication as well as prevent message replay. The Data Confidentiality dimension provides for the use of IPSec ESP to prevent unauthorized disclosure. In the infrastructure layer, the Data Integrity dimension provides for the use of file checksums to prevent unauthorized alteration, the Data Confidentiality dimension provides for file encryption to prevent unauthorized disclosure, and the Access Control dimension provides for the use of file system access control lists (ACLs) to prevent unauthorized duplication. Figure C.5 depicts how the ITU-T X.805 dimensions provide for the implementation and operation of control A.10.9.2 to protect the employee information asset.

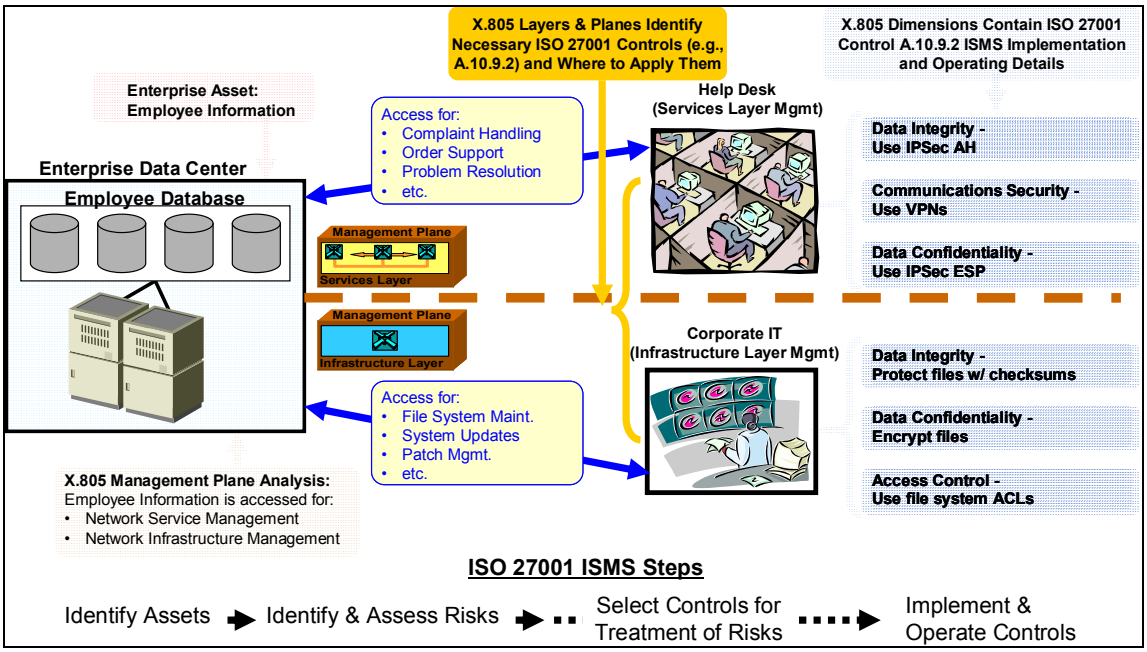

Figure C.5 — ITU-T X.805 for ISO/IEC 27001:2005 Implementation

Bibliography

[1] ITU-T X.805, *Security architecture for systems providing end-to-end communications*

[2] RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2*, IETF, August 2008

ICS 35.040

Price based on 28 pages