COMMUNICATION SECURITY ON INTERNET

An INTOSAI EDP Audit Committee Project

The Swedish National Audit Office

Dnr 25-2001-1059

ISBN 91 7498 466 7

The Swedish National Audit Office

To the members of the INTOSAI Standing Committee on EDP Audit

At the 8th meeting of the INTOSAI Standing Committee on EDP Audit in Harare in 1999, the Swedish National Audit Office (RRV) accepted to conduct a study concerning Communication Security on Internet. The RRV, in cooperation with Stockholm University, has carried out such a study during 2000-2001. A reference group with members from the SAIs of India, UK and Russia has been involved in the project.

The result of the study is a report and model for auditing communication security in the public sector. The model mainly consists of a question database containing 15 domains. The report and the question database are included in this document.

After having performed this study of communication security in the public sector and taken account of comments from Committee members on a draft report presented at the 10th meeting in Ljubljana this year, we are happy to present this report also including suggestions for further actions related to communication security.

Gert Jönsson
Assistant Auditor General, Head of the Financial Audit Department

2001-10-01

Summary

At the 8th meeting of the INTOSAI Standing Committee on EDP Audit in Harare in 1999, the Swedish National Audit Office (RRV) accepted an offer to conduct a study concerning Communication Security on Internet. One of the reasons for conducting a study in this area is that, to support the audit statements that SAIs have to issue, the need to audit the authorities' use of the Internet as a communication carrier of business information has increased of late. This is due to the fact that the Internet has become more and more common as a means of communication.

The aim of the work that formed the basis for this report has been to create an audit model for communication security in the public sector. This model, or "Best Practice", in the field has come to be represented by a question database containing 15 domains dealing with communication security. This database allows auditors to search for questions individually or by area in order to audit different aspects of communication security, independently of technical solution.

The communication security aspects in three existing information security standards – ISO / IEC 17799-1, FA22 and PD5000 – have been used to create this model.

The audit model has been tested on three authorities. The conclusions drawn from these audits have led to a certain amount of reworking of the model, as well as providing an insight into which questions are not applicable as things stand at present, and which questions may gain in importance in the near future.

Conclusions:

- Basic criteria for good communication security, such as a risk analysis and documents dealing with policy on information security and policy on e-mail, often do not exist or have no official status within the organisation.
- Information security issues have no obvious place with authority management.
- The opportunities for secure communication that meet demands concerning confidentiality, integrity and accessibility are currently limited, as few authorities have tools for authentication, encryption and signing. At present, the use of a Public Key Infrastructure (PKI) is the closest we can get to communication that meets the said demands.
- More and more authorities will probably choose the Internet as a means of communicating information, and this will increase the need for PKI tools. This is why the need is also increasing for audit programmes of the type that this project has attempted to describe.
- The Swedish Qualified Electronic Signatures Act, which came into force on 1 January 2001, will probably prepare the way for the Swedish authorities to create solutions for secure Internet communication.
- None of the three standards forming the basis for this work *alone* meets the overall needs in this area. In other words at least two different standards ought to be considered to cover all topics that are of interest when auditing this area.
- The most detailed standard is PD5000, although this standard primarily seems to apply to a future perspective in comparison with the situation with which RRV

came into contact in the case studies, on account of the fact that it assumes that the authorities are using tools which support authentication, encryption, etc.

- The modifications that had to be made to the model on the basis of the audits carried out meant that greater emphasis had to be placed on policy issues than had originally been planned due to the fact that the shortcomings in this area were greater than anticipated.
- Auditing of several of the technical aspects in the model was seen as somewhat pointless, as the technical applications commissioned had not been based on policies and active decisions on the part of the management. These policies and guidelines should constitute perhaps the most important foundation against which technical solutions are to be assessed. One of the foundations for a secure communication environment vanishes if these controlling documents do not exist.

As a result of discussions in connection with the 10th meeting of the INTOSAI Standing Committee on EDP Audit in Ljubljana, May 17th-18th 2001, RRV has tried to point out the way in which the model could be further developed. Mainly this consists of a stronger focus on risk analysis and risk assessment approached from two different angles. First, a connection has been made to the IT Service Management Model presented by SAI Norway at the Committee meeting in Ljubljana in May 2001. Secondly, a matrix of risks, potential impacts and suggestions for a risk management strategy have been added to each of the 15 domains of the question database annexed to this report. In the final chapter of the report, a number of suggestions for further studies in the area of communication security are included. These suggestions include evaluation of the model by other SAIs, developing the model so as to have an even stricter risk based approach and further exploration of areas outside the scope of this study.

1. Background

The use of public networks such as the Internet as a means of communication has become a common feature in the public sector. There is great variation in the use of these means of communication. Some government authorities and public enterprises use the Internet only for communication by e-mail, while others also have websites which contain information on the authority and via which, in some cases, visitors may submit and retrieve information of a more or less sensitive nature. Depending on how each authority is organised, communication between certain authorities' Local Area Networks (LANs) all over the country can take place via the Internet.

At the INTOSAI IT Committee meeting in Harare in 1999, the Swedish National Audit Office accepted an offer to conduct a study concerning Communication Security on Internet. The result of the study is presented in this report. The aim of our work, which formed the basis for the report, has been to create a model for auditing communication security in the public sector.

The work has been carried out by Riksrevisionsverket (RRV, the Swedish National Audit Office) in co-operation with Stockholm University. Theoretical studies, case studies etc presented in chapters 1-7, including the annexed question database, have been carried out by Ann-Mari Uddmäre (RRV) and also represents her graduate work at Stockholm University. Further development of the report after the 10th meeting of the INTOSAI Standing Committee on EDP Audit, has been carried out by Frank Lantz (RRV). Bengt E W Andersson (RRV) has contributed to the study throughout the project.

2. Scope

2.1 Aim and objective

The aim of the work was to create an audit model, “Best Practice”, relating to how SAIs can audit authorities in order to determine whether they have reliable control over their data communication via the Internet. Depending on the audit responsibilities of various SAIs this can be essential to determine if operations have been performed efficiently and in compliance with applicable laws and regulations; which in RRV:s case must be stated in the audit opinion for each client.

The model has been created without implementing an in-depth analysis of the technical aspects of data communication, but with a more fundamental starting point relating to which decisions and actions that need to be taken to manage the potential risks surrounding electronic communication; i.e. ensuring that communication is secure and reliable.

The model contains a series of questions which are applicable to the auditing of the control environment / system for data communication at various types of authorities. It will be possible to use this model as a tool to help create specially designed audit programmes depending on the type of authority to be audited.

The aspects of data communication of particular importance in the model are as follows:

1. The use of e-mail, both internal and external. This also includes e-mail attachments.
2. The retrieval / sending of information from / to internal networks by interested parties, such as distance workers or auditors. Is sufficient security maintained in the authorities’ internal networks, when it comes to external use from these parties?

The model has been created with the aid of the knowledge collated from various security standards and experiences from the audits of the Swedish National Audit Office and others.

The model has been developed under the conditions which prevail in Sweden. Although our aim was to produce a general model, some parts are affected more than others by conditions in Sweden. For this reason, it is important when applying the audit model, that it is to adapted to suit the regulations and conditions in force in the environment in which it is to be used.

2.2 Method

One condition needed to be able to fill the model (and a database) with relevant questions is knowledge of the areas of communication, communication protocols, encryption, firewalls, security standards, communications technology, operating systems and the criteria that apply to administration in the public sector. Knowledge has been collated by studying references and standards and by participating in conferences and courses. A reference group consisting of the research and development committee at ISACA and staff from RRV has also been linked with the project. In addition, the project plan has been discussed with SAI India and NAO/UK. This has led to the formulation of a large number of audit questions, which are part of the database/model.

The model was then tested on three authorities. This test looked at the current use of Internet communication, what levels of communication security the authorities had and how the authorities had established and decided their current security levels. Furthermore we studied how the authorities had ensured that the security level specified would be observed and whether the authorities had assessed their vulnerability by means of a risk analysis. The authorities were chosen on the basis that the selection should cover various types of organisations. Among the factors involved in the selection was to include organisations that are centralized vs. decentralized, organisations dealing with sensitive information and organisations of different sizes.

Certain changes were made to the audit model after the test. Above all, greater emphasis has been placed on questions dealing with the management's control of the security levels concerning communication within the organisation, in the form of internal control documents.

The model, and a preliminary version of this report was presented at the 10th Meeting of the INTOSAI Standing Committee on EDP Audit in Ljubljana, May 17th-18th 2001. Discussions during the meeting, as well as suggestions and material from NAO/UK and SAI Norway, have served as input for some further development of the model, the result of which is presented in chapter 8. The main focus of these additions is on the theme of risk assessment and risk management. It should be noted that information presented in chapter 8.1 was thus not part of the model that was tested during the three audits mentioned above.

As a last step in our work we present some suggestions for further development of the model in chapter 8.2.

2.3 Exclusions

The following exclusions applied to the work with the audit model:

- The work has not dealt with in-depth technical solutions regarding how communications equipment and security mechanisms are rigged, but with security and technical issues on a more fundamental level.

- The work has not gone into detail on matters relating to physical security and access- and control systems.

- The work has mainly focused on "ad-hoc like" information exchange of as part of the daily operations.

- The work has dealt with communication security, in the form of transport security and access security, over public networks using Internet technology. Thus communication by means of telephone and fax, for example, has not been taken into consideration.

- The work has dealt with data *integrity* when sending data; that is to say, ensuring that data sent is not distorted by the time it is received. The information *quality* of the data communicated has not been taken into account.

3. Communication and security – definition

Security of communication is of the utmost importance if the authorities are to be able to use the information that they access via the Internet.

Issues that must be taken into consideration in order to establish good communication security include the following:

- statutory and regulatory requirements for the activities of the authorities.
- various risks that can apply to the authority, depending on the nature of its operations and environment
- public access to official records and secrecy: depending on how the legislation is formulated, it is necessary to decide how the information to be communicated is to be dealt with in this respect.
- good manners, which for example includes appropriate ways of expressing oneself in e-mail messages.
- internal policy which regulates, for example, how various types of information are to be communicated, who has the right to submit certain types of information, etc.
- agreements/contracts on how communication is to take place between various parties.
- planning for continuity and breakdowns which take electronic communication into account.

It should be possible to make the following demands of communication, so that communication between two parties can be considered to be secure:

- Non repudiation (prevention of message / file rejection or denial of receipt); it must not be possible to subsequently deny the existence of a message.
- Confidentiality or secrecy: it must not be possible for unauthorised parties to read the message on its way between the sender and the recipient.
- Integrity: the message must not be distorted between sending and receipt.
- Accessibility: the message must be accessible to the right sender and the right recipient.
- Authenticity: the message must come from the right sender, who must be able to prove that he or she is the person he or she claims to be.
- Timeliness: the message should be delivered to the recipient within reasonable time after it has been sent

These demands must be met to varying degrees in the case of data communication.

Confidentiality, reliability and accessibility in communication are cornerstones which have to be in place if authorities are to be able to perform their operations securely. For a SAI to be able to submit an audit report, including management statements and auditor certificates, the SAI must also be able to audit whether the information administration processes within the authority function reliably. This is to ensure that the information on which the SAI issues its statement is essentially true. Reliable input to the information processes is achieved by means such as good access and transport security when communicating data.

4. Important standards in the field of communication security

Below is a description of the security standards that have been used as input for the building of the audit model. To begin with, it ought to be mentioned that some of the standards also cover areas that do not directly affect matters of communication security. The parts of the respective standards that do not deal with the subject matter referred to in this document have not been taken into account when producing the audit model.

It is important to note that the standards described relate in certain parts to Swedish and European conditions and may vary from what is applicable in other countries. It is assumed that the auditors using the audit model will have a detailed knowledge of any supplementary standards and regulations applicable in the environment in which the audit is to be carried out.

For more extensive information about general data communication theory, information is available in the training material published on the INTOSAI IT-Committee website (http://www.nao.gov.uk/intosai/edp/trainingindex.html), for example in the student notes to the modules IT-awareness (chapter 7), IT-controls (chapter 12) and IT-security (chapters 6 and 8).

4.1 ISO/IEC 17799 (SS627799)

ISO/IEC 17799-1 is an international standard for a management system for information security, which originates from the British standard BS7799. SS627799 is a Swedish version of this standard.

This standard consists of two parts. The first part contains guidelines for the management of information security. The second part is a specification for part 1, and it contains more detailed descriptions of what the guidelines involve.

4.2 FA22

FA22 is a standard prepared by Överstyrelsen för civil beredskap (ÖCB), the Swedish Agency for Civil Emergency Planning, on the basis of § 22a in the Standby Ordinance for Data Systems Important to Society. The general advice and regulations here are obligatory for the Swedish authorities affected by the relevant legislation, but they may also be applied to other authorities.

4.3 BSI-DISC PD 5000

BSI-DISC PD 5000 is a standard that covers a number of areas, including electronic storage, electronic communication, policy on e-mail, and so on. This also includes checklists for five different areas (BSI-DISC PD 5000-6:2000): electronic storage, electronic communication and policy on e-mail, identity, signature and copyright, the use of certification bodies, and the use of trusted third-party archives.

5. A model for auditing communication security

This section contains a background description of the audit model. To begin with, it should be observed that some parts of the audit model refer to Swedish legislation that regulates what authorities can do in respect of individual citizens. Therefore we would like to stress once again, the importance when using the model, of adapting it to suit the unique conditions in force in the environment in which it is to be used.

In our work with the audit model, two areas – policies and procedures and encryption – have stood out as being of particular importance. Therefore, we will look at these areas briefly below.

5.1 Policies and procedures

More or less all the questions included in the audit model are based on the fact that policies must exist, which regulate the use of various systems and applications in the operations of the authorities. It is important that these policies or guidelines be decided at management level within the organisation so that they are of sufficiently high status to be observed at all levels within the organisation. Established policies and procedures, based on a risk analysis, have been considered in this work to be a fundamental factor that must be in place in order to be able to carry out an assessment of the security level. From the auditor's point of view, the lack of controlling documents is in itself such a shortcoming in our assessment of the management's administration of the operations (which is one of the parts we mention in the audit statement), that the question could be raised of the relevance of continuing the audit.

In the audit model, we also find recurring the question of documented procedures for various processes and work operations in the case of electronic communication. Documented procedures serve to make things easier for the users of electronic communication systems. In this way, even people who do not use the system frequently can remain secure in the knowledge that they are handling the system in a reliable way.

Documented procedures also prevent the organisation from ending up reliant on key personnel, a situation which can cause disruption to operations if one or more people leave the organisation.

Finally, procedures have to be documented in order to serve as evidence that a message has actually been dealt with correctly, and that the identities of the sender and recipient and the integrity of the content have been established in a correct, complete manner. In this way, it is possible to link a message to a certain individual or organisation and to prove that this message is actually genuine. To be able to attain this aim in a secure manner, the organisation also has to have adequate physical security as well as a well-organised and satisfactory access control system. However, these issues do not lie within the scope of this report, but the line of reasoning put forward and the issues dealt with by the audit model assume that an acceptable level of security exists in respect of physical and logical access to systems and premises. If there is any uncertainty on these points, special audits of these should be implemented if so deemed necessary.

5.2 Encryption

Several sections in the audit model contain questions on encryption and the use of PKIs (Public Key Infrastructures). Encryption is used to conceal the content of a message so that no unauthorised person can read it during transport / transfer from one computer to another.

To encrypt a message, an encryption key is required which works together with a mathematical algorithm to replace each character in the message text with another as per the pattern in the algorithm. When the recipient wants to read the message, it has to be decrypted by running the algorithm backwards. The message then appears in clear language.

One method (Figure 1) is known as symmetrical encryption and is based on the concept of the encryption key being known only by the sender and the recipient. If the encryption key is revealed, unauthorised people can read the message. This encryption technology currently requires very long keys.

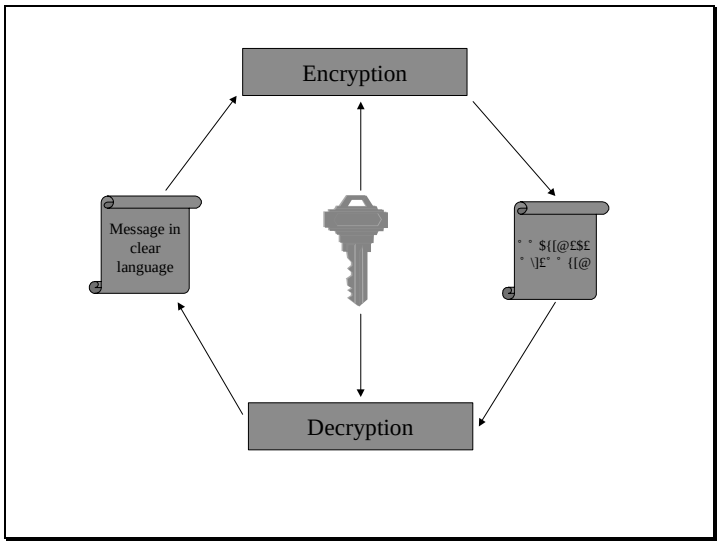

Figure 1 Symmetrical encryption (Norman 1998)

A more secure type of encryption is asymmetrical encryption, which is based on encryption and decryption by means of two different keys (Figure 2). The sender encrypts the message using a private, secret key, and the recipient decrypts the message using the sender's public key.

The public key may be available from a third party, looked up in a directory or sent to the recipient by the sender. Only this unique combination of keys can be used to decrypt the message.

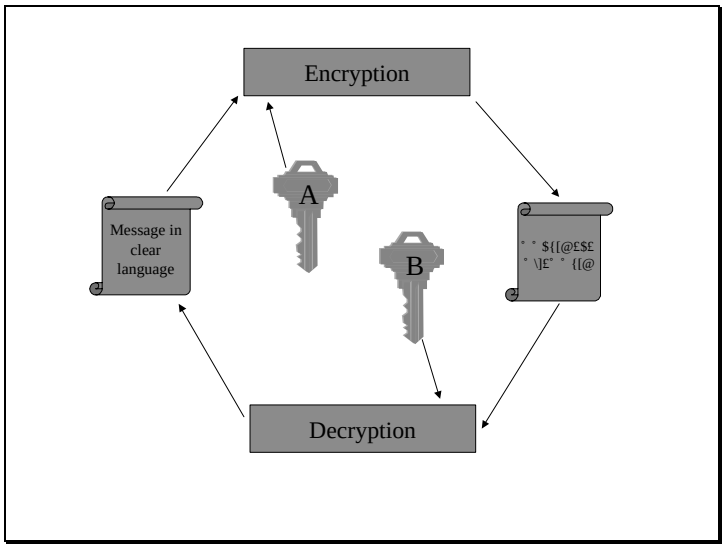

Figure 2 Asymmetrical encryption (Norman 1998)

5.2.1 PKIs

PKIs are based on asymmetrical encryption. In other words, there has to be a private, secret key and a public one. The private key is – as the name implies – kept private and secret. The public key is available to communication partners from a directory.

The PKI solution is based on the fact that there is a trusted third party, known as a Certification Authority (CA), which may prepare keys but which primarily guarantees their validity and authenticity,. In the case of external communication, the certificate issuer should be an independent third party whose task is to administer keys, issue keys, recall keys and guarantee the validity of keys. However, organisations may also issue their own certificates.

It must be possible for a communication partner to contact the CA in order to check whether the other party possesses a valid key, when the certificate was issued and for how long it will remain valid.
The CA issues what is known as a Certificate Policy (CP) in which it describes in detail the use of the certificate. The CA also issues what is known as a Certificate Policy Statement

(CPS). The CPS describes the CA's procedure for issuing certificates. Every CA must issue a CPS, and this may form the basis for legal agreements.

5.3 Sections in the audit model

The audit model is divided into fifteen subsections/domains. This division into subsections broadly follows the structures in the standards on which the model is based. The idea is for SAIs to be able to select specific elements / areas of the client's communication security for auditing. For this reason there are sometimes a number of similar questions which occur under a number of different headings / in a number of different sections in the model.

For each question that is included in the audit carried out by the auditor, the auditor should assess whether the answer received is satisfactory or not. These assessments should result in a non-conformance report that is then submitted to the client in accordance with the procedures of the respective SAIs. The observations should be accompanied by recommendations on what action should be taken to improve security in electronic communication.

Below are brief descriptions of each section in the audit model.

1. Management system for information security

This section deals with questions relating to the management's control and follow-up of issues relating to communication and information security in general terms, in the form of risk analyses, policies, continuity planning, and so on. These are basic criteria for authorities to be able to maintain good security in their communication solutions, and they can be said to form part of authorities' *general controls.*

2. Processes and procedures

Questions relating to work descriptions and the distribution of responsibilities are dealt with under this heading, as well as general procedures relating to the use of data communication and the use of functions for the compression and encryption of files.

3. Sending electronic documents

This section contains questions and preparations that should be observed in order to assess the level of security when electronic documents are to be communicated to external areas by the authority. Questions on compression and encryption, and questions for verifying the integrity of the data sent are also dealt with here.

4. Communication

This section deals with overall questions on the technical environment in which communication takes place, such as which communication solution has been selected and what protection has been set up in the form of firewalls, etc. The aim of these questions is primarily to assess how the authority is able to guarantee continuous operation of its communication solution.

5. Receiving electronic documents

This section contains questions and preparations that should be observed in order to assess the level of security when electronic documents are received from external parties. As in section 3, questions relating to decryption and data integrity are dealt with here.

6. System maintenance
This section deals with questions concerning the documentation and maintenance of the communication system, as well as available logging functions.

7. Security and protection
The questions in this section relate – among other things – to topics regarding procedures for reporting security incidents and how the operating environment for the communication system is established. They also establish whether this is in line with the recommendations that apply to the solution selected.

8. Contracts
This section deals with the issue of how contracts are drawn up with other parties in communication solutions. This may, for example, be relevant when it comes to solving any disputes between parties, and form a basis for which technical solutions should be applied.

9. Third parties
This deals with the issue of how guidelines, etc. are regulated in cases in which third parties are involved in parts of the operation or maintenance of the communication system. This may, for example, apply to questions on service level, and to the fact that it must be possible to handle data in a manner that ensures that integrity and confidentiality are maintained.

10. Standardised documents
This section deals with the issue of how to verify the integrity and accessibility of the templates used for official communication from the authority.

11. Version management
This section deals with questions concerning how changes and reconfigurations in the communication solution can be derived so that it is possible to verify which criteria were in force at the time when a specific a specific communication took place. This may be of interest from a legal point of view, or for internal checks.

12. Technology
This section deals with overall questions relating to the network environment in which the communication system operates, as well as procedures for the compilation of system descriptions and documentation, which help to ensure that continuous operation is maintained. Questions on user management, the storage of documents, etc. are also dealt with.

13. Audit
This section deals with questions on how to ensure that a satisfactory audit trail is available, such as in the form of logs, and procedures for handling these. This is one element that will later make it possible to analyse what actions led to a certain event occurring in the system.

14. Processing history
This section deals with questions on how a satisfactory processing history is maintained in the system. This means that it must be possible subsequently to follow the route a transaction or case has taken through the communication system.

15. E-mail

This section deals with questions on how the use of e-mail is regulated and monitored, with the objective of achieving a level of knowledge within the organisation on what internal criteria apply in respect of public access to official records and confidentiality, as well as risks that the use of e-mail may entail.

6. Experiences from testing the audit model

In this chapter we present the experiences we have made from the case studies where the model for auditing communication security was tested.

6.1 Case studies

The audit model has been tested by carrying out audits of three Swedish authorities. Below are brief descriptions of these authorities.

6.1.1 Migrationsverket (the Migration Board)

The Migration Board is a central administrative authority for issues relating to migration and citizenship in so far as these are not the responsibility of any other authority.

The authority is divided into several parts: its head office is in Norrköping, and it has five regional offices throughout the country. This authority employs around 1500 people.

Security issues are dealt with by the executive office, and two people work full-time with issues relating to security.

As things stand at present, the Migration Board does not use the Internet as a communication carrier for business-critical information between its regional offices. Instead, this information is sent over a fixed connection.

The Migration Board itself issues certificates, which means that it is its own Certification Authority (CA); that is to say, it issues and assures the quality of the keys used for asymmetrical encryption. Any authorities wishing to establish communication with the internal systems at the Migration Board have to accept and adopt the CPS, Certification Policy Statement, of the Migration Board. In 2001, the Migration Board will be working together with a number of other authorities to form a joint intranet for dealing with certain joint issues. A PKI solution for which the Migration Board is the CA has been produced for this purpose.

6.1.2 Patent- och Registreringsverket (the Swedish Patent and Registration Office)

The Swedish Patent and Registration office (Patent- och Registreringsverket, PRV) is a central administrative authority for matters relating to patents, trademarks and surnames and first names, and for registration matters relating to limited companies, branch offices and European economic interest groups. This authority is also a central administrative authority for matters relating to the trade register and register of associations.

This authority employs 950 members of staff. The authority is geographically decentralised, and a certain number of its staff are distance workers. There are fixed connections between offices, as well as to the EPO, the European Patent Office. Security work is carried out by the IT council, of which the authority's deputy director general[1] is the chairman.

6.1.3 Invest in Sweden Agency (the Delegation for Foreign Investments in Sweden)

The task of the Delegation for Foreign Investments in Sweden (ISA) is to use information and contacts to take an active part in helping foreign companies in various forms to invest in or join forces with Swedish companies in order to establish new companies and bring about new investments in Sweden.

This authority is represented in Sweden and abroad at certain consulates, as well as in Japan and the USA. The ISA employs 19 members of staff and a number of staff on a per-project basis.

6.2 Results of the case studies

In this section we will present the general results of the audits carried out, as well as a brief summary of the reports issued to the authorities audited.

6.2.1 General results

- Limitations in standards

In our opinion PD5000 assumes that some kind of PKI solution or similar has been installed. The questions based on this standard are formulated in a way that can seemingly only be answered satisfactorily by organisations that have tools for signing, authentication and encryption. This means that the standard is only partly applicable in organisations that do not have this type of tool. ISO/IEC 17799-1 and FA22 are not specifically aimed at communication security issues, and thus do not cover all aspects that are of interest.

- PKIs and e-mail systems

It is not possible to authenticate the sender and recipient of electronic communication without a PKI. The most common e-mail systems provide no support for authentication without adding electronic signatures. This means that many of the questions in the model are not really relevant to authorities that do not have a working PKI solution.

[1] The deputy director general is a deputy to the director general, approximately at the level of deputy managing director.

- Secure communication demands identical levels of security

The potential problem with a national CA and a national certificate hierarchy or a major hierarchy of any kind is how to bring about a uniform level of security for all the organisations in the hierarchy. For instance, how is it possible to persuade a smaller company to accept and build up the same level of security as that demanded by the banking and finance sector, for example?

Authentication and identification of users and documents presupposes that both the communicating parties have PKI solutions, which are compatible with one another. In practice, national CAs are needed which can guarantee the users' certificates. In Sweden, this may be the result of the Digital Signatures Act that came into force on 1 January 2001.

Cross-certification between organisations which act as their own CAs can work if they decide that they can trust one another. In practice, the communicating organisations should have equally stringent demands on security in their respective policies on information security. They do not both have to have the same technical solution installed, as long as the solutions they do have are compatible with one another. Cross-certification with other organisations allows the authorities themselves to ensure that the parties with which they are communicating maintain acceptable levels of security.

- No use of encryption in e-mail!

None of the three authorities audited admits to communicating business-critical or sensitive information by e-mail. Nevertheless, if the organisations were to want to protect their e-mail communication, which in certain circumstances they no doubt should do, they are able to supplement their existing e-mail systems with encryption products such as PGP (Pretty Good Privacy) or PEM (Privacy Enhanced Mail). None of the authorities audited has chosen to do this. It should also be noted that PEM or PGP solutions demand that both sender and recipient have the same tool in order to be able to read messages.

6.2.2 Reports to the authorities

Following the three audits where the model was tested, written reports were sent to two of the three authorities involved. These are the most significant findings that were reported:

In the view of the auditor, only one of the three authorities audited met the basic requirements in the audit model for communication security in the form of procedure and control documents established by the management, such as an established policy on information security. A certain amount of basic information existed in one case, but this had not been decided upon at management level and had no official status within the organisation. Foundations, such as a risk analysis, for creating meaningful policies were not present.

Only one of the three authorities audited is currently using some kind of encryption and PKI solution for its operations. As work on further developing this solution was in progress, it was recommended that once the audit had been carried out, a second audit should be carried out once supplementary parts of the PKI solution had been commissioned.

One of the authorities audited had no logging of incoming and outgoing e-mail traffic. Furthermore, at one of the audits, basic shortcomings in the operating environment were noted, such as in the form of protecting the computer hall from unauthorised access.

Finally, we reported on shortcomings in – or a lack of – continuity planning at the authorities.

7 Conclusions

In this section, we will implement a discussion on the basis of the shortcomings of a general nature identified while work progressed.

The conclusions drawn from the case studies do not so much concern security aspects in the actual communication systems and communication sessions, but rather more basic issues, namely the lack of policy documentation and guidelines for electronic communication.

If the basic criteria in the form of policies and guidelines do not exist or are not met, an assessment of the observations made in the more technical field is difficult to make. This is due to the fact that comparisons cannot be made with the documents that should form the basis from which the technical solutions are applied, namely controlling and policy documents established by the management.

Work on communication security has to start by setting up the objectives of IT security and security in communication. In order to connect these objectives to the overall objectives of the operations, it is essential that a proper investigation has been performed of the nature of the operations, and the environment in which they are performed, including the various risks the business faces in its different processes. Only once this has been done is it possible to check whether the control elements in the communication system are adequate for the actual operation being audited.

7.1 Need for an extended risk analysis

One basic criterion for security work is that an analysis must have been carried out of the authorities operations and its environment. The security level within the organisation should be set on the basis of the potential threats indicated by the risk analysis. Our recommendation is that this risk analysis should also include a risk analysis relating to information assets and data communication and result in action being implemented in order to safeguard such assets and communication.

7.2 Policy on information security

It is important for the issues relating to communication- and information security to be given sufficient attention by the management and to be controlled by the same.
Two of the three authorities audited in the case studies had no established policy on security. However, they may have an informal policy on security that is based on accepted practice and common sense. SAIs should not accept informal policies on security. Instead, it is recommended that their policies on security be written down and established by the management.

A policy on information security must contain a clear indication from the management of the aims of the said management as regards the policy.

The policy on information security should include a policy on the secure handling of e-mail, if this does not exist as a separate document.
The IS policy and policy on e-mail should be implemented and communicated in such a way that staff do not feel insulted or under suspicion. Staff must feel that they have clear, obvious guidelines on the rules that apply when using the resources of their employer. This will facilitate their work and reduce the risk of errors, both intentional and accidental. Giving staff an active part to play in information security work will make them feel a sense of responsibility for the resources of the organisation.

7.3 Public Key Infrastructure

The Internet protocol is commonly used, and other protocols that exist for data communication can, as a rule, communicate with the Internet protocol. Therefore, using the Internet for communication is an efficient, cost-effective way for government bodies to communicate. The alternative method currently employed for communicating business-critical information uses fixed, encrypted connections.

However, the Internet protocol does have shortcomings, which have to be compensated for in order to meet the demands on government bodies in respect of confidentiality, integrity and accessibility. The only way of doing this is to use PKI tools and to become part of an organisation or network in which communication is based on a PKI, which is something that few authorities currently do. As far as communication by e-mail and the option of attaching documents of a sensitive nature to messages are concerned, PKI is the only possibility by means of which this can be done reliably.

To avoid each authority coming up with its own communication solutions, it is important to discuss the option of introducing a government standard to which all authorities may subscribe. Otherwise, there is a risk that we will see the rise of many different security solutions which are not compatible with one another, the occurrence of compromises of security and, not least, the spending of huge sums of money on development and evaluation in a situation in which attempts should be made to find cost-effective solutions. The solution closest at hand is the one that involves using the infrastructure which is already available all over the world: the Internet.

It will never be possible to achieve 100 per cent security. Instead, it is a matter of risk management: organisations need to determine which risks they are prepared to take with their information.

7.4 ISO/IEC 17799-1, PD5000, FA22

Neither ISO/IEC 17799:1 nor FA22 are particularly detailed in respect of communication in general and e-mail communication in particular. PD5000 is a Best Practice for communication solutions and their legal aspects. The communication sections are applicable to the fullest extent only in cases in which the organisation being audited has a tool for and a communication infrastructure that supports strong authentication, signing and encryption: in other words, a PKI solution.

As far as generalists are concerned, standards like FA22 and ISO/IEC 17799 do not provide enough guidance. Experience of the field of information security is required in

order to be able to formulate audit programmes with questions that can give answers to the question of whether the control objectives set up by the standards are being met. PD5000 contains complete checklists, thereby giving the auditor some more help.

The standards are appropriate for auditors to use as a yardstick depicting the best-case scenarios, but at the same time it is necessary to realise what the standard assumes about the authority's infrastructure. Quite simply, it is not possible to meet all the auditing objectives if the authority has not built up its information infrastructure on the basis of ideas similar to those depicted in the standards.

In such cases, SAIs should recommend to the authorities that they consider an appropriate standard and work towards constructing a management system for information security.

The primary objective of such work does not necessarily have to be to gain accreditation in accordance with the standard, but to use it as a tool for organising and protecting information assets. At a later stage, the organisation can then opt for accreditation in accordance with a standard in order to gain a mark of quality along the lines of the other ISO accreditations that exist for quality management systems and environmental management systems. If, at that point, the organisation is already adapted to an accreditation standard, it is already halfway there.

The database belonging to this report contains questions of a general nature and can be used irrespective of the technical solution used for data communication. Some questions assume that the authority has a PKI solution or similar, but there are also questions that are generally applicable to more or less all audit subjects.

8. Additional development of the audit model

As mentioned in sector 2.2, the audit model has been developed further as a result of discussions during the 10th meeting of the INTOSAI Standing Committee on EDP Audit. As noted in sector 7.1, findings from the case studies included the need for extended risk analysis on behalf the authorities we audit. Since the issues of risk analysis and risk management were also central to the suggestions RRV received to improve the model during the Committee meeting, RRV decided to take a few steps in pointing out the way in which the audit model can be further developed. Two alternative ways of further developing the model has been approached. The first consists of applying the IT Service Management Model presented in SAI Norway's report "Auditing IT Service Management" (which was presented during 10th meeting of the INTOSAI Standing Committee on EDP Audit) to the model developed in this report. The second way deals with connecting to the model, preliminary matrixes of risks, potential impacts and risk management strategies for each of the 15 domains presented in 5.3. However, neither of these approaches has been empirically tested in case studies, and as a result makes no claim to fully cover all areas of interest concerning risk management in the area of communication security. This chapter should thus be seen only as a first step for further development of a thorough model for auditing communication security.

8.1 Risk management

Any communication system, e.g. e-mail, is, in various ways, exposed to risks which could lead to a situation where the communication system in not able to give requested contribution to the agency's business. In order to obtain efficiency (in the client's case efficient operations, in the auditor's case efficient use of audit resources) it is essential both to the clients, and to the auditor, to focus on areas of high risk, or rather areas where the risk could lead to a severe impact for the organization audited. To help the auditor focus more closely on these issues two steps have been taken.

The first step has been to apply the IT Service Management Model presented in SAI Norway's report "Auditing IT Service Management" (which was presented during the 10th meeting of the INTOSAI Standing Committee on EDP Audit) to the model developed in this report. There are several reasons for applying the IT Service Management Model to the model and the result of RRV's study. Primarily it further increases the focus on management responsibility in IT and communication issues. It also gives us a chance to obtain synergy effects between INTOSAI projects.

In the IT Service Management Model there are six main areas dealing with various IT-activities. Please note that slight terminological changes have been made compared to the original model:

- Necessary strategies and policies for IT-based communication systems
- Developing, running, maintaining, delivering and supporting an IT-based communication system

- ***Support of an IT-based communication system***

- External demands and requirements, from Parliament, the Government and various organisations, on IT-based communication systems

- The user's interaction with the IT-based communication system

- Consequences from IT-based communication systems on society, citizens and organisations.

A seventh area, the Entity area, is also presented in the model. This area can be seen as a representation of the interaction between the other six areas in the model, or rather the management's responsibility for managing the activities in the other six areas.

In the sectors 8.1.1-8.1.7 a short description of each area is included. To illustrate the connection between the IT Service Management Model and the model developed in this report, each of the 15 domains presented in chapter 5 has been applied to one of the areas in the IT Service Management Model.

As a second step, to increase focus on the assessment of various risks and their potential impact, each domain presented in chapter 5 has also been connected to a matrix description of:

- risks that could occur in situations pertaining to the respective domains, and which could affect the possibility of reaching management- or business objectives
- the possible impact if risks mentioned above are not managed
- strategies/measures that could be taken to manage the risks.

Some risks are common in the sense that they apply not only to several domains in the audit programme, but also to an organisation's overall IT-operations; other risks are more or less specific for a single domain. Please note that one risk can also be connected to several of the listed impacts and vice versa. The same applies for the relation between a domain and an area in the IT Service Management Model; certain domains can relate to more than one area in the model. For practical reasons, however, we have chosen to apply each domain to only one area in the IT Service Management Model.

8.1.1 Entity area

The Entity area reflects the Top Management's responsibility for managing the entity of - and interaction between - the other areas in the IT Service Management Model. The main risk in this area would best be described as not being able to manage the entity of IT-based communication systems, which could affect the organisation's ability of achieving organisational objectives. In this chapter we have chosen not to apply a domain to this area, but rather to apply each domain to one of the operational areas in sections 8.1.2-8.1.7.

8.1.2 Necessary strategies and policies for IT-based communication systems

This area deals with the operational strategies and policies that are considered necessary to run the IT-based communication systems in order to support business strategy and organisational objectives:

- Work description
- Distribution of responsibilities

Domain relevant to this area is:

Domain 2, Processes and procedures

Questions relating to work descriptions and the distribution of responsibilities are dealt with under this heading, as well as general procedures relating to the use of data communication and the use of functions for the compression and encryption of files.

RISK	IMPACT	RISK MANAGEMENT STRATEGY
Procedures for data communication has not been documented Procedures for data communication has not been communicated to all relevant personnel Procedures are not updated regularly Roles and responsibilities are not clearly defined Implementation of procedures are not performed in accordance with organisation policies	All relevant security activities are not performed Procedures do not match the organisation's need for security measures Security measures are not cost effective	A policy/standard should be implemented for documenting procedures for data communication. The policy should also include routines for reviewing and updating procedures, as well as a strategy for communicating procedures to all relevant parties. A periodic review, or audit, should be performed to ensure that procedures and routines are followed.

8.1.3 Developing, running, maintaining, delivering and supporting IT-based communication systems

This area deals with the part of IT-based communication systems that is related to the IT-departments' delivery of communication systems, for example:

- Communication solutions and communication protection
- Reporting security incidents
- Establishing the communication system environment
- Documentation and maintenance of the communication system
- Logging functions
- Level of security in communications (sending, receiving)
- Verifying the circumstances in a specific communication

Domains relevant to this area are:

Domain 4, Communication

This section deals with overall questions on the technical environment in which communication takes place, such as which communication solution has been selected and what protection has been set up in the form of firewalls, etc. The aim of these questions is primarily to assess how the authority is able to guarantee continuous operation of its communication solution.

RISK	IMPACT	RISK MANAGEMENT STRATEGY
Insufficient analysis of the demands on the communication environment of the organisation Security settings applied to the technical solution are insufficient	The technical solution does not match the actual demands of the organisation Continuous operations can not be performed (loss of service availability) Potential loss of data confidentiality or integrity Information does not reach intended recipient Loss of credibility	Procurement and implementation of technical solutions should be based on an organisational review and risk analysis. Depending on the nature of the operations, implementing other communication methods than the Internet should be considered (for example VAN)

Domain 7, Security and protection

The questions in this section relate – among other things – to topics regarding procedures for reporting security incidents and how the operating environment for the communication system is established. They also establish whether this is in line with the recommendations that apply to the solution selected.

RISK	IMPACT	RISK MANAGEMENT STRATEGY
Analysis of operating environment within the organisation is insufficient Operating environment of the communication system is not in line with the vendor's recommendations Procedures for log-analysis are insufficient or irrelevant Procedures for reporting security incidents are not established	Full system functionality can not be obtained Security breaches may occur due to poor system implementation All security incidents are not reported and followed up on	A policy/standard should be implemented for documenting procedures for data communication, based on an organisational review and risk analysis. Risk based procedures for analysing system logs should be implemented. Procedures for reporting all security incidents should be established.

Domain 6, System maintenance

This section deals with questions concerning the documentation and maintenance of the communication system, as well as available logging functions.

RISK	IMPACT	RISK MANAGEMENT STRATEGY
A relevant system maintenance schedule is not implemented Procedures for system maintenance have not been documented System maintenance is not logged	Service availability is not adequate Loss of credibility Unauthorised changes to system and security settings Loss of information confidentiality	Documentation of system maintenance procedures should be implemented to ensure that service is performed in accordance with vendor's recommendations. Logs of system maintenance access to the communication system should be followed up regularly, to ensure that security is not compromised

Domain 3, Sending electronic documents

This section contains questions and preparations, which should be observed in order to assess the level of security when electronic documents are to be communicated to external areas by the authority. Questions concerning compression and encryption, and questions for verifying the integrity of the data sent are also dealt with here.

RISK	IMPACT	RISK MANAGEMENT STRATEGY
Insufficient analysis of the demands on the communication environment of the organisation Procedures for secure data communication have not been documented Implementation of procedures and activities are not performed in accordance with organisation policies Procedures for data communication have not been communicated to all relevant personnel	Unauthorized disclosure or manipulation of data, which can lead to loss of confidence or even legal impacts. Data does not reach intended recipient Security measures are not cost effective All relevant security activities are not performed	A policy/standard should be implemented for documenting procedures for data communication, based on an organisational review and risk analysis. The policy should also include routines for reviewing and updating procedures, as well as a strategy for communicating procedures to all relevant parties. Depending on the nature of the operations, implementing other communication methods than the Internet should be considered (for example VAN) A periodic review, or audit, should be performed to ensure that procedures and routines are followed.

Domain 5, Receiving electronic documents

This section contains questions and preparations that should be observed in order to assess the level of security when electronic documents are received from external parties. As in section 3, questions relating to decryption and data integrity are dealt with here.

RISK	IMPACT	RISK MANAGEMENT STRATEGY
Insufficient analysis of the demands on the communication environment of the organisation Procedures for secure data communication have not been documented Implementation of procedures and activities are not performed in accordance with organisation policies Procedures for data communication have not been communicated to all relevant personnel	Unauthorized disclosure or manipulation of data, which can lead to loss of confidence or even legal impacts. Security measures are not cost effective All relevant security activities are not performed	A policy/standard should be implemented for documenting procedures for data communication, based on an organisational review and risk analysis. The policy should also include routines for reviewing and updating procedures, as well as a strategy for communicating procedures to all relevant parties. A periodic review, or audit, should be performed to ensure that procedures and routines are followed.

Domain 11, Version management

This section deals with questions on how changes and reconfigurations in the communication solution can be derived so that it is possible to verify which criteria were in force at the time when a specific a specific communication took place. This may be of interest from a legal point of view, or for internal checks.

RISK	IMPACT	RISK MANAGEMENT STRATEGY
There are no routines for change management in the communication environment	Criteria in force at the time when a specific a specific communication took place cannot be established	Procedures for change and version management should be established

8.1.4 Support of IT-based communication systems

This area deals with organisational, financial, humanly and technological support in order to make IT-based communication systems contribute as planned to business objectives:

- The network environment in which the communication systems operates
- Third parties' involvement in communication systems
- Contracts drawn up with other parties.

Domains relevant to this area are:

Domain 12, Technology

This section deals with overall questions relating to the network environment in which the communication system operates, as well as procedures for the compilation of system descriptions and documentation, which help to ensure that continuous operation is maintained. Questions on user management, the storage of documents, etc. are also dealt with.

RISK	IMPACT	RISK MANAGEMENT STRATEGY
System descriptions and documentation are not complete or up to date Routines for logging and analysing logs are not implemented Routines for authentication and access controls are not correctly implemented Control of the network environment is insufficient	Detection and correction of errors and malfunction are difficult Abnormal usage patterns or access attempts are not discovered Chances of preventing unnecessary downtime are reduced	Standards for producing, reviewing and updating system documentation should be established Risk based procedures for analysing system logs should be implemented. Procedures for implementing and reviewing network controls should be established.

Domain 9, Third parties

This deals with the issue of how guidelines, etc. are regulated in cases in which third parties are involved in parts of the operation or maintenance of the communication system. This may, for example, apply to questions on service level, and to the fact that it must be possible to handle data in a manner that ensures that integrity and confidentiality are maintained.

RISK	IMPACT	RISK MANAGEMENT STRATEGY
Service agreement does not cover all relevant aspects concerning operation and/or service	Third party supplier fail to accept responsibility Potential loss of confidentiality, integrity or availability of data and services No legal protection if third party fails to deliver services	Service requirements should be established in contract All contracts are subject to legal review before being signed

Domain 8, Contracts

This section deals with the issue of how contracts are drawn up with other parties in communication solutions. This may, for example, be relevant when it comes to solving any disputes between parties, and form a basis for which technical solutions should be applied.

RISK	IMPACT	RISK MANAGEMENT STRATEGY
The contract does not cover all relevant aspects of a communication agreement	Communication failure due to non-compatible installations etc Potential loss of confidentiality, integrity or availability of data, with the risk of resulting legal claims. Loss of credibility	All contracts are subject to technical and legal review before being signed

8.1.5 External demands and requirements, as from Parliament, the Government and organisations, on IT-based communication systems

This area is focused upon the authority's obligation and need to assess, adopt and implement external demands and formal regulations in the process of development, maintenance and running of IT-based communication systems:

- Basic criteria, demands and requirements for a good communication and communication systems.

Domain relevant to this area is:

Domain 1, Management system for information security

This section deals with questions relating to the management's control and follow-up of issues relating to communication and information security in general terms, in the form of risk analyses, policies, continuity planning, and so on. These are basic criteria for authorities to be able to maintain good security in their communication solutions, and they can be said to form part of authorities' *general controls.*

RISK	IMPACT	RISK MANAGEMENT STRATEGY
Poor management awareness of IS-security issues Policies and procedures are not updated regularly Organisation's stance on IS-security issues is not known among employees A proper risk assessment, based on the organisation's environment, has not been performed	All relevant areas of risk are not considered by management Reduced efficiency and cost-effectiveness in IS-operations Policies are not relevant to current environment Policies are not effected throughout the organisation. IT-security organisation is not organised to deal with security risks efficiently Potential loss of confidentiality, integrity or availability of sensitive data	An IT-strategy and an IT-policy should be created, based on the overall business plan and the business objectives. Procedures should be implemented for continuous review and updating of policies, procedures and organisation. A risk analysis should be performed, taking its basis in an overall review of the organisation and it's environment.

8.1.6 The user's interaction with the IT-based communication systems

This area focus on the user's meeting with the IT-based communication systems delivered. The user concept encompass both internal and external users of communication systems. In the context of managing this area, there is a need for focusing on accessibility of services and the user's participation in delivery/receipt of communication messages:

- Regulating and monitoring e-mail traffic and related objectives
- Official communication

Domains relevant to this area are:

Domain 15, E-mail

This section deals with questions on how the use of e-mail is regulated and monitored, with the objective of achieving a level of knowledge within the organisation on what internal criteria apply in respect of public access to official records and confidentiality, as well as risks that the use of e-mail may entail.

RISK	IMPACT	RISK MANAGEMENT STRATEGY
E-mail policy is insufficient or not implemented Extensive private usage of company e-mail	Increased risk of virus or spam intrusions Legal demands are not met, for example public information contained in e-mails are not registered properly The organisation's credibility is reduced by abuse of company e-mail	An e-mail policy should be created, which covers among other things: use of acknowledgement functions, private use of company e-mail, risks involved in using e-mail (virus, spam etc).

Domain 10, Standardised documents

This section deals with the issue of how to verify the integrity and accessibility of the templates used for official communication from the authority.

RISK	IMPACT	RISK MANAGEMENT STRATEGY
Layout standards for official communication from the authority are not implemented	Loss of credibility Concerns could be raised about official status of documents etc that are communicated	Policy and procedures should be implemented for communicating official documents; including who is authorised to official communication

8.1.7 Consequences of IT-based communication systems on society, citizens and organisations.

This area deals with consequences of IT-based communication systems on society, citizens and organisations. This means focusing on the needs of any person or organisation influenced by the communication system, rather than focusing on convenience for government departments:

- Audit trails in communication systems
- Processing communication history

Domains relevant to this area are:

Domain 13, Audit

This section deals with questions on how to ensure that a satisfactory audit trail is available, such as in the form of logs, and procedures for handling these. This is one element that will later make it possible to analyse what actions led to a certain event occurring in the system.

RISK	IMPACT	RISK MANAGEMENT STRATEGY
Routines for producing a sufficient audit trail are not implemented Integrity of the audit trail is not secured Routines for analysing logs are not implemented	Essential information is not recorded in the audit trail, or is lost/over written. Essential information cannot be traced through the audit trail, or is not reliable Abnormal usage patterns or access attempts are not discovered	The inclusion of a sufficient audit trail should be addressed in the early stages of designing or procuring systems. Routines should be established to ensure that the audit trail is not impaired by upgrades/changes in the system, and that the audit trail cannot be manipulated Risk based procedures for analysing system logs should be implemented

Domain 14, Processing history

This section deals with questions on how a satisfactory processing history is maintained in the system. This means that it must be possible to subsequently follow the route a transaction or case has taken through the communication system.

RISK	IMPACT	RISK MANAGEMENT STRATEGY
Routines for producing a sufficient audit trail and processing history are not implemented	Ability to perform follow-up controls are limited Legal demands on processing history cannot be met	The inclusion of a sufficient audit trail and processing history should be addressed in the early stages of designing or procuring systems. Routines should be established to ensure that the audit trail is not impaired by upgrades/changes in the system, and that the audit trail cannot be manipulated Risk based procedures for analysing system logs should be implemented

8.2 Suggestions for further use and development of the audit model

We hope that this report will help the reader to gain additional knowledge on the topic of communication security, to conduct a general discussion in this problem area and assess and report on shortcomings in communication security, irrespective of technical solution. However, in several aspects, we would like to see this report as a starting point for further activities concerning audit of communication security.

As has been pointed out earlier in this report, our aim has been to produce a general model for auditing communication security. However, there is a risk that having been developed in a Swedish environment influences the model. Therefore we think it would be useful if the model was tested, evaluated and possibly further developed by other SAIs, in order to ensure that it is reasonably applicable for other SAIs.

Also, the audit model in its present state has not been empirically tested applying the risk based approach as presented in section 8.1, and as a result we can give no assurance that all relevant risk aspects have been covered in the tables in 8.1.2-8.1.7. Further testing and development of the risk based approach to auditing communication security and of the audit model should be considered.

Applying the IT Service Management Model to the communication security model of this report, points to a need for further development concerning some areas. For example, the IT Service Management Model areas concerning External demands and User interaction need be investigated to make sure that all relevant aspects have been covered.

Finally, there are some questions concerning communication security on the Internet that has not been covered in this report. We have been limited to three case studies; the selection criteria for these studies have been presented in chapter 2.2. This limitation and the scope of the project mean that certain types of organisations and electronic communication have not been subject to testing through the case studies. An example of an area that ought to be further explored is the control of electronic trading/EDI in public authorities.

References

Standards etc.
BS 7799.1:1999 - AS/NZS 4444.1:1999 Information Security Management Standard

SIS: SS627799, 1999.

PD5000: An International Code of Good Practice in 5 Parts for Electronic Documents and e-Commerce Transactions as Legally Admissible Evidence, 1999.

DISC PD 0008:1999 Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically, 1999.

ISCF: Code of Practice for Netcentric Technologies vol. two Intranet/Extranet/Internet, 1999.

Literature, legislation etc:
van Biene-Hershey, Margaret E., Strous Leon; Integrity and Internal Control in Information Systems - Strategic Views on the Need for Control, Kluwer Academic Publishers, 1999.

Lavér, Johan och Toivonen, Juha-Pekka; Incorporating legal, evidentiary, and audit trail requirements into the BS7799 - AS/NZS 4444 Information Security Management Standard, Masters' series no. 00-52 DSV-SU(2000).

Pfleeger, Charles P.; Security in Computing, Prentice-Hall International, 1997.

Persson, Malin; Lindberg, Linda; Harvey, Christina (1999): VPN En studie om Virtuella Privata Nätverk, dissertation on Systems Science at the college in Trollhättan / Uddevalla.

SAI Norway, Auditing IT Service management, 2001.

Salamone, Salvatore; VPN: The Basics, Internet Week 1998-12-14.

Swedish Code of Statutes, no. 2000:832; Qualified Electronic Signatures Act (2000:832).

Swedish Code of Statutes, no. 2000:833; Qualified Electronic Signatures Ordinance (2000:833).

Swedish Code of Statutes, no. 1998:204; Personal Data Act.

Interviews, seminars:
10th Meeting of the INTOSAI Standing Committee on EDP Audit, May 2001

Björklund, Lars; Deputy Director General, Patent- och registreringsverket [the Swedish Patent and Registration Office]

Chambert, Ingrid; IT co-ordinator, ISA

Edenbro, Patrik; IT Engineer, Patent- och registreringsverket

Eriksson, Mats (IMS Data); Operations Manager, ISA

Helenelund, Kurt; Simberg & Partners at the seminar "En infrastruktur för samhällets e-tjänster", April 2000

Holmberg, Lars; Industrial Lawyer, Riksrevisionsverket [the Swedish National Audit Office]

Keisu, Thomas; Icon Medialab Parallel AB, Conference on PKI and electronic signatures, 13 December 2000.

Kihl, Erik; Acting Security Manager, Migrationsverket [the Migration Board]

Lekander, Bengt; IT strategist, Riksrevisionsverket

Norman, Ulrika; lecturer at DSV, KTH / SU

Skantze, Pernilla; Näringsdepartementet [the Ministry for Industry, Employment and Communications], Conference on PKI and electronic signatures, 13 December 2000.

Westmar, Jan; IT expert responsible for IT issues and IT infrastructure at Migrationsverket

Östling, Per; IT Manager, Riksrevisionsverket

Audit programme – communication security

BASED ON THE STUDY “COMMUNICATION SECURITY ON INTERNET”,
THE SWEDISH NATIONAL AUDIT OFFICE

Contents

Introduction

This audit programme deals with a number of different aspects of security in respect of data communication within organisations. For each question, the auditor should carry out an assessment of whether the client meets the demands that should be made, identify any shortcomings and formulate recommendations for improvements.

The audit programme is divided into a number of sections. The idea is for the auditor to be able to select specific elements / areas of the client's communication security for audit and then use only the relevant sections in the audit programme. For this reason there are a number of similar questions which occur under a number of different headings / in a number of different sections in the document.

It should be observed that some parts of the audit programme refer to Swedish legislation etc. Therefore we would like to stress the importance, when using the model, of adapting it to suit the unique conditions in force in the environment in which it is to be used.

Finally, it should be borne in mind that the audit programme largely deals with technical matters, which is why we recommend that the auditors who will be using it should have a good knowledge of IT.

1 Management system for information security

1.1 Policy on information security

1.1.1 Policy document

Does a policy on information security exist which has been documented and approved by the authority's management, and does this policy comply with laws and regulations and reflect the objectives of the management in respect of IT security in a clear manner? Have all staff within the organisation been informed of this policy?

1.1.2 Review and assessment

Is the policy on information security reviewed regularly within the organisation and updated in order to keep it current?

1.1.3 Classification of information

Is information classified, and are the associated security measures implemented on the basis of the needs of the organisation as regards gaining or restricting access to information?

1.1.4 User training

Do all employees, including third-party users, receive user-specific, regularly updated information about the guidelines and procedures of the organisation?

1.1.5 Responsibility

Is it clear from the policy who is responsible for information security?

1.1.6 Content of the policy on information security

Does the policy on information security deal with the following areas?
1. A definition of information security, its general objectives and scope
2. A statement on the management's overall ambition concerning security issues, which supports the objectives and principles of information security
3. A brief description of general policy on security, principles, guidelines and observance requirements of particular importance to the organisation, such as:
· observance of laws, regulations, agreements and other external security requirements;

· requirement for training in security;
· anti-virus protection and protection against other harmful software;
· breakdown plan for the activities
· consequences of disregarding the policy on security
4. A definition of responsibilities for information security, including the reporting of incidents
5. References to other controlling documentation and security regulations that have to be observed.

1.1.7 Electronic communication

Does the policy on information security include – in a structured, clear manner – responsibilities and the use of e-mail and other electronic forms of communication, or are these regulated in a separate document?

1.1.8 Observance

Do the managers of the organisation ensure that all procedures in their respective areas of responsibility are executed correctly, and are efforts made to ensure that guidelines and standards are observed?

1.1.9 Disciplinary action

Do rules exist for dealing with situations in which employees have contravened the organisation's policy on security or security procedures?

1.2 Risk analysis

1.2.1 Risk analysis in the event of third-party access

Has the organisation evaluated the security risks that would occur if a third party were to gain access to information? Have appropriate checks and measures been introduced?

1.2.2 Risk management by government authorities

Has the authority drawn up a risk analysis of the risks and threats in connection to the operations?

1.2.3 Risk analysis in respect of information assets

Has the authority included its information assets in this risk analysis, or does a separate document exist which deals with the risks in connection with IT operations?

1.2.4 Subcontracting of operation

In cases in which all or parts of information systems, networks or computer environments are subcontracted/outsourced, have the security requirements been included in these contracts?

1.3 Infrastructure for information security

1.3.1 Management group for information security

Is there a group at the highest management level that ensures that information security has a clear *direction* and which supports security initiatives?

1.3.2 Co-ordination

Does a joint forum exist which co-ordinates the *introduction* of measures for information security within the various units of the organisation?

1.3.3 Distribution of responsibility

Has responsibility for the various resources of the organisation and the *execution* of specific security procedures been defined clearly?

1.3.4 Decision-making process

Within the organisation, is there a decision-making process for dealing with new resources that are to be used for information processing?

1.3.5 Specialist advice

Does the organisation utilise its own experts or external specialists for dealing with matters relating to information security?

1.3.6 Co-operation with other organisations

Has the organisation established appropriate contacts with relevant authorities, with companies offering different kinds of information service, and with telecommunications operators?

1.3.7 Independent assessment
Has the introduction of the policy on information security been assessed by an independent third party?

1.4 Continuity planning

1.4.1 Procedure for continuity planning
Does a controlled process exist for developing and maintaining continuity within the various operations of the organisation?

1.4.2 Breakdown and consequence analysis
Does a strategic plan (breakdown and consequence analysis) exist, based on a risk analysis, which deals with the effects of not being able to maintain continuity of operations?

1.4.3 Preparation and introduction of continuity plans
Do plans exist for allowing the operations of the organisation to continue or be reset within the requisite time after a breakdown or error in critical procedures?

1.4.4 Framework for continuity planning
If the continuity plan consists of various subplans, does a system exist for ensuring that these subplans are consistent and compatible? Has an order of priority been defined for testing and maintenance?

1.4.5 Testing, maintenance and assessment
Are the continuity plans tested regularly, and are they maintained by means of regular checks in order to ensure that they are current and operational?

1.5 Consultations

1.5.1 Restrictions to electronic communication
Is there any risk at all of the organisation's communications coming into conflict with national or international restrictions? If so, has the organisation consulted the authorities and organisations responsible in order to guarantee the legitimacy of the communication system and communications?

2 Processes and procedures

2.1 Descriptions of procedures

2.1.1 Descriptions of roles and responsibilities

Does the information given on roles and responsibilities in job descriptions in respect of security tally with the information given in the organisation's policy on information security?

2.1.2 Description of procedure for the communication system

Does a description exist which deals with the procedures applicable when using the electronic
communication system?

2.2 Preparations for communication

2.2.1 Encryption of files

Does the organisation have a policy on the use of encryption technology for the protection of information?

2.2.2 Use of encryption

Is encryption used to safeguard the confidentiality of sensitive or critical information?

2.3 Malicious code

2.3.1 Hidden channels and Trojan code

Are the purchase, use and alteration of software checked and controlled in order to protect against any hidden channels or Trojan code?

2.3.2 Action against malicious code

Do controls exist which detect attacks from malicious programmes/code and protect the organisation's IT environment from the same, and do procedures exist which make users aware of the existence of such malicious programmes?

2.3.3 Anti-virus protection
Has anti-virus protection been installed on the communications equipment, and is this updated continuously?

2.3.4 Documented procedures
Do documented procedures exist for how to deal with malicious code?

2.4 File compression

2.4.1 Security aspects in respect of compression
Do procedures exist which ensure that authenticity and integrity are not lost when files are compressed?

2.4.2 Less reliable compression technology
Does the organisation use any less reliable compression technology for files to be communicated electronically?

2.4.3 Non-repudiation
Are functions used which aim to make it impossible for users to deny that a specific message or file has been received or to reject receipt of a specific message or file (prevention of message / file rejection or denial of receipt)?

2.5 File encryption

2.5.1 Use of encryption
Does the organisation use encryption technology on files that are to be communicated electronically?

2.5.2 Guidelines for encryption
Does the organisation have documented guidelines on when encryption is to be used, such as in the policy on information security or the policy on e-mail?

2.5.3 Need for encryption
Has the organisation identified the situations in which file encryption is required? What situations are involved?

2.5.4 Legitimacy
Has the organisation investigated and identified whether the encryption technology used at any time could be considered to be illegal?

2.5.5 Integrity
How does the organisation ensure that the integrity of a message or document is not lost on account of file encryption?

2.5.6 Dealing with keys
How does the organisation deal with encryption and decryption keys?

2.5.7 Information to communication partners
How does the organisation ensure that the recipient of an encrypted message or an encrypted document is able to read it?

2.6 Sender identity

2.6.1 Identification
How can the recipient of an electronic message or file identify the sender?

2.6.2 Digital signatures
Are digital signatures used to ensure the authenticity and accuracy of electronic information?

2.7 Information on integrity

2.7.1 Integrity of messages received
How can the recipient of a message or file verify that the message has not been distorted?

2.8 File format exchange

2.8.1 Readability
How does the organisation ensure that the recipient of the message or file is able to read it?

2.9 Storage / archiving

2.9.1 Guidelines for storage
Does the organisation have any guidelines on when and how electronic messages and documents are to be stored, and how long?

2.9.2 Metadata
What metadata is stored together with the message or document?

3 Sending electronic documents

3.1 Malicious code

3.1.1 User awareness
Are the employees within the organisation aware of the risks associated with electronic communication as far as destructive code is concerned? How have staff been made aware of this?

3.1.2 Action in respect of malicious code
Do controls exist which detect attacks from malicious programmes/code and protect the organisation's IT environment from the same, and do procedures exist which make users aware of the existence of such malicious programmes?

3.1.3 Anti-virus protection
Has anti-virus protection been installed on the communications equipment, and is this updated continuously?

3.1.4 Procedures
Do documented procedures exist for how to deal with malicious code?

3.2 File compression

3.2.1 Maintenance of integrity
Do procedures exist which ensure that authenticity and integrity are not lost when files are compressed?

3.2.2 Less reliable compression technology

Does the organisation use any less reliable compression technology for files to be communicated electronically?

3.3 Encryption

3.3.1 Dealing with keys

Is a key handling system used that is based on specific standards, procedures and methods for support for the organisation's use of encryption technology?

3.3.2 Regulation of encryption

Have control measures been introduced to avoid contravening legal requirements in order to control the use of encryption?

3.3.3 Use of encryption

Is encryption technology used on files that are to be communicated electronically?

3.3.4 Guidelines for encryption

Do guidelines exist regarding when messages or files have to be encrypted?

3.3.5 Non repudiation

Are functions used which aim to make it impossible for users to deny that a specific message or file has been received or to reject receipt of a specific message or file (prevention of message / file rejection or denial of receipt)?

3.3.6 Integrity

How does the organisation ensure that the integrity of a message or document is not lost on account of file encryption?

3.3.7 Information to communication partners

How does the organisation ensure that the recipient of an encrypted message or an encrypted file is able to read it?

3.4 Sender identity

3.4.1 Digital signatures
Are digital signatures used to ensure the authenticity and correctness of electronic information?

3.4.2 Identification
How can the recipient of an electronic message or file identify the sender?

3.5 Verification of integrity

3.5.1 Information on integrity
How can the recipient of a message or file verify that the message has not been distorted?

3.6 Notification of receipt

3.6.1 Non repudiation
Are functions used which aim to make it impossible for users to deny that a specific message or file has been received or to reject receipt of a specific message or file (prevention of message / file rejection or denial of receipt)?

3.7 File format exchange

3.7.1 Readability
How does the organisation ensure that the recipient of the message or file is able to read it?

3.8 Storage

3.8.1 Guidelines for storage
Does the organisation have firm guidelines on when and how electronic messages and documents are to be stored, and how long?

3.8.2 Metadata
What metadata is stored together with the message or document?

4 Communication

4.1 Communication system

4.1.1 Choice of communication system
Does the organisation have more than one communication system, and if so, do clear rules exist regarding when each system has to be used?

4.1.2 Manual
Does a manual exist which belongs to the communication system and which documents all possible manual actions required to initiate communication?

4.1.3 Network services
Does a clear description exist of the security attributes for all network services utilised by the organisation?

4.2 Exchange of information

4.2.1 Agreements on the exchange of information
Is the electronic or manual exchange of information with other organisations regulated in agreements with these organisations?

4.3 Firewalls

4.3.1 External connections
Does all TCP / IP communication to and from the organisation take place via a firewall, and is the configuration of this firewall documented and controlled by a policy? Has the system owner

established what is to be logged by the firewall, who is responsible for monitoring the logs and how often this is to be done?

4.3.2 Connections

Does an up-to-date list exist of all connections to the organisation? If remote diagnostics are used, does this take place in accordance with established / agreed procedures?

4.4 Protection in the event of data communication

4.4.1 Security measures

Has the system owner decided whether the services offered by the network operator are acceptable from the point of view of security, and what measures of its own must the organisation implement?

4.4.2 Responsibility

Has the system owner regulated responsibility for security for the transfer of data to and from computer systems and established and documented decisions on which internal and external connections may be permitted to telecommunications and computer networks (such as the Internet)?

5 Receiving electronic documents

5.1 Malicious code

5.1.1 Measures

Do controls exist which detect attacks from malicious programmes/code and protect the organisation's IT environment from the same, and do procedures exist which make users aware of the existence of such malicious programmes?

5.1.2 User awareness

Are the employees within the organisation aware of the risks associated with electronic communication as far as destructive code is concerned? How have staff been made aware of this?

5.1.3 Anti-virus protection
Has anti-virus protection been installed on the communications equipment, and is this updated continuously?

5.1.4 Procedures
Do documented procedures exist for how to deal with malicious code?

5.2 File compression

5.2.1 Maintenance of integrity
Do procedures exist which ensure that authenticity and integrity are not lost when files are compressed and unpacked?

5.2.2 Less reliable compression technology
Does the organisation use any less reliable compression technology for files to be communicated electronically?

5.3 Decryption

5.3.1 Dealing with keys
Is a key handling system used that is based on specific standards, procedures and methods for support of the organisation's use of encryption technology?

5.3.2 Rules for encryption
Have control measures been introduced to avoid contravening legal requirements in order to control the use of encryption?

5.3.3 Use of encryption
Is encryption technology used on files that are to be communicated electronically?

5.3.4 Guidelines for encryption
Do guidelines exist regarding when messages or files have to be encrypted?

5.3.5 Non repudiation
Are functions used which aim to make it impossible for users to deny that a specific message or file has been received or to reject receipt of a specific message or file (prevention of message / file rejection or denial of receipt)?

5.3.6 Integrity
How does the organisation ensure that the integrity of a message or document is not lost on account of file encryption?

5.3.7 Information from communication partners
Does the recipient receive information from the sender that specifies that an encrypted message or an encrypted file can be read?

5.4 Sender identity

5.4.1 Digital signatures
Are digital signatures used to ensure the authenticity and correctness of electronic information?

5.4.2 Identification
How can the recipient of an electronic message or file identify the sender?

5.5 Verification of integrity

5.5.1 Verification of messages
Does validation of the content of the applications (electronic transfers) take place where protection of the accuracy of such is a security requirement?

5.5.2 Non-distorted messages
How can the recipient of a message or file verify that the message has not been distorted?

5.6 Notification of receipt

5.6.1 Non repudiation

Are functions used which aim to make it impossible for users to deny that a specific message or file has been received or to reject receipt of a specific message or file (prevention of message / file rejection or denial of receipt)?

5.7 File format exchange

5.7.1 Readability

What information on file format does the recipient receive from the sender so that the message or file can be read?

5.8 Storage

5.8.1 Guidelines for storage

Does the organisation have firm guidelines on when and how electronic messages and documents are to be stored, and how long?

6 System maintenance

6.1 Maintenance

6.1.1 Professional system maintenance

Is the communication system covered by professional system maintenance?

6.1.2 Log book

Does a log book exist for system maintenance? What is documented in it?

6.1.3 Preventive maintenance
Does a detailed description of procedures exist for all preventive system maintenance?

6.2 System documentation

6.2.1 Documentation
Does complete documentation exist which includes system, operating and user documentation, and in which the operating documentation specifies – among other things – which security measures the administrator is able to influence and which permit him only to obtain information? Does this documentation contain instructions on how the system or product is to be installed and configured?

6.2.2 Security for system documentation
Is the system documentation within the organisation protected against unauthorised access?

6.3 Logging

6.3.1 Operator logs
Is all work carried out by the operators in the IT environment logged?

6.3.2 Error logs
How are errors reported from the error log? Do procedures exist for undertaking action on account of these reports?

7 Security and protection

7.1 Operating environment

7.1.1 Criteria for operation
Does the communication system operate under conditions stipulated by the organisation?

7.1.2 Security checks
Does the system contain security checks adapted to suit the environment in which the system is run, and does the physical and operating environment for the communication system comply with the recommendations of the supplier?

7.1.3 Procedures
Are security checks and procedures that have been implemented documented in a procedure description?

7.2 Controlling networks

7.2.1 Control measures for networks
Do control measures exist which make it possible to achieve and uphold security in networks and associated infrastructures?

7.3 Incident management

7.3.1 Reporting
Are security incidents reported immediately once they have been discovered, and are they reported via appropriate reporting routes?

7.3.2 Procedure in the event of an incident
Have responsibilities and procedures been established regarding how to deal with incidents?

7.3.3 Malfunctions in software
Do procedures exist for reporting software problems?

7.4 Logging

7.4.1 Operator logs
Is all the work carried out by the operators in the IT environment logged?

7.4.2 Error logs
Are errors reported from the error log, and is action undertaken?

7.4.3 Logging of security incidents

Do logs exist which record non-conformances and other incidents relevant to security? Are these logs saved for a specific period of time?

7.5 E-mail

7.5.1 Security in electronic mail

Does a policy exist within the organisation regarding the use of electronic mail, and do control measures exist in order to reduce the risks regarding the use of electronic mail?

8 Contracts

8.1 Contracts between communication partners

8.1.1 Agreement

Is communication between the organisation and a third party a consequence of an agreement, and does this contract then contain clauses of relevance to the electronic exchange of documents?

9 Third parties

9.1 Engaging third parties

9.1.1 Guidelines

Does the organisation engage third parties for servicing, maintenance or operation for the entire system or parts of it, and if so, is this work carried out on the basis of established agreements and guidelines?

10 Standardised documents

10.1 Public templates

10.1.1 Filing
Does the organisation use standardised templates as a framework for official documents, is it permitted to amend these, and if so, are integrity, confidentiality and accessibility taken into account?

11 Version management

11.1 Version management systems

11.1.1 Changes
Are all hardware, software and all procedure descriptions used during electronic communication included in a version management system, and does this system have appropriate logging in order to trace changes and configurations?

12 Technology

12.1 Networks and the Internet

12.1.1 Firewalls
What kind of firewall does the organisation use, and why?

12.1.2 Operating system
What operating system is installed on the server on which the Internet connection is stored?

12.1.3 Control measures for networks
Do control measures exist which make it possible to achieve and uphold security in networks and associated infrastructures?

12.1.4 Node authentication
Are all connections to external computer systems authenticated?

12.1.5 Protection of external diagnostics port
Is access to the diagnostics ports checked and controlled?

12.1.6 Division of networks
Have security measures been introduced into the network so as to be able to differentiate between groups of information services, users and information systems?

12.1.7 Control over networks
Are users' connection options in shared networks restricted in accordance with the organisation's access control policy?

12.1.8 Security in network services
Does a clear description exist of the security attributes for all network services utilised by the organisation?

12.1.9 Automatic terminal identification
Is automatic terminal identification used for the authentication of connections to specific locations and to portable equipment?

12.1.10 Security in login procedure
Is a secure login procedure used for access to information services?

12.1.11 Identification and authentication of users
Have all users been assigned unique identities so that activities can be traced to individuals responsible?

12.2 System description

12.2.1 Protection of system documentation
Is the system documentation within the organisation protected against unauthorised access?

12.2.2 Security requirements in respect of systems
Are requirements in respect of control measures and security measures defined in the requirement specifications of new systems or when existing systems are altered?

12.2.3 Components included
Does a list exist in the system description of the hardware and software elements included in the communication system?

12.2.4 Manuals
Does a manual exist which describes the various communication systems that exist and how these are to be used?

12.2.5 Service partners
If a service partner is used, does the manual deal with information essential to this service partner?

12.2.6 Historical data
Is it possible from the system description to read details which are or were of significance to the communication of various types of file, including from a historical perspective?

12.2.7 Data loss
Does the system description discuss whether or not the communication system is reliable from the point of view of data loss?

12.2.8 Authorisation levels
Is it clear from the system description that authorisation levels exist in the communication system?

12.2.9 Identification of senders and recipients
Is it clear from the system documentation that processes ensure that the senders and recipients of documents can be identified?

12.2.10 Filing of network information
Is the network information obtained by the communication system kept on file?

12.2.11 Identification of documents
Is it clear from the system description how it is possible to identify individual documents among other documents communicated?

12.2.12 Logging
Does the system description discuss the logging process used to document communication sessions?

12.2.13 Integrity of documents
Does the system description discuss the processes used to safeguard the integrity of documents that are to be sent?

12.2.14 Authentication of senders and recipients
Does the system description describe which technology is used for the authentication of senders and recipients?

12.2.15 Notification of receipt
Is it clear from the system description what the process is for notification of receipt?

12.2.16 Storage of documents
Does the system description contain a process description relating to how files and associated information (notification of receipt, acknowledgement, etc.) communicated are stored? Are any automated indexing processes also described?

12.2.17 Time aspect
Does the system description discuss processes for logging the date and time, filing checks for this information, and use of trusted time stamps?

12.2.18 Error handling
Does the system description discuss the error handling process?

12.2.19 Audit tracing
Does the system description describe the process for creating an audit trace?

12.3 Access rights

12.3.1 Identification of users
Have all users been assigned unique identities so that activities can be traced to the individuals responsible?

12.3.2 Restriction of access to information

Is access to information and application systems restricted in accordance with the organisation's policy on access rights?

12.4 Identification of users / recipients

12.4.1 Authentication of users

Are all external users authenticated before they are permitted to connect?

12.4.2 Automatic identification of terminals

Is automatic terminal identification used for the authentication of connections to specific locations and to portable equipment?

12.4.3 Identification of organisations

Is it possible to identify the organisation from which a message has been received?

12.5 Identification of documents

12.5.1 Identification

Is it possible to identify a specific document communicated? How is this done?

12.6 Initiation of communication

12.6.1 Logging

What information on communication sessions is logged?

12.6.2 Critical time

Does the organisation ever find itself in situations in which the actual time of communication may be considered to be critical, and if so, how is the information on the time guaranteed?

12.7 Sender / recipient integrity checks

12.7.1 Checks
What checks are carried out by the sender of the document or message in order to ensure its integrity?

12.7.2 Less reliable communication systems
Does the organisation use a less reliable communication system, and if so, what integrity checks are carried out?

12.8 Authentication of senders / recipients

12.8.1 Authentication technology
What technology is used to authenticate senders and recipients, and what does this involve?

12.9 Notification of receipt and acknowledgement

12.9.1 Receipt level
Does the notification of receipt make clear the organisational level at which the message or file has been received?

12.9.2 Details at document level
What information can be found in the notification of receipt?

12.9.3 Content in the acknowledgement
What information can be found in the acknowledgement, and how is this information dealt with?

12.10 Storage of documents

12.10.1 Process for storage
Are documents stored in such a manner as to guarantee confidentiality, integrity and accessibility?

12.11 Time aspect

12.11.1 Logging
What information regarding the time aspect for communication is stored, and how is this information dealt with?

12.12 Error handling

12.12.1 Implementation of error handling
How has the error handling process been implemented, and how are errors dealt with?

13 Audit

13.1 Audit trail

13.1.1 Operator logs
Is all work carried out by the operators in the IT environment logged?

13.1.2 Error logs
Are errors reported from the error log, and is action undertaken?

13.1.3 Monitoring via logging
Do logs exist which record non-conformances and other incidents relevant to security? Are these logs saved for a specific period of time?

13.1.4 Monitoring of system usage
Do procedures exist for the monitoring of the use of resources for information processing, and are the results audited regularly?

13.1.5 Security log
Does a security log exist which contains information on user identities, approved logins, logouts and the date and time? Has the system owner specified which events in addition to these are to be recorded in the computer system’s security log?

13.1.6 Log monitoring
Is it clear from the security instruction who is responsible for auditing security logs, the times at which security logs are to be analysed, how long security logs are to be retained and how these logs are to be stored?

13.2 Creating audit trails

13.2.1 Clock synchronisation
Are the computer clocks synchronised regularly?

13.2.2 Process for audit trails
How are audit trails created?

13.2.3 Full log
Do procedures and a procedure description exist for handling full logs so that information logged previously is not overwritten or event logging comes to a halt when the log is full?

13.3 Date and time

13.3.1 Logging
Do all logs in the system have date and time stamps for all system events?

13.3.2 Time-critical communication
Does the organisation have any communication which may be time-critical?

13.4 Storage

13.4.1 Storage of logs
What checks are carried out on the organisation’s logs, and what decisions are made regarding how long a log should be retained?

13.5 Access rights to logs

13.5.1 Procedure for access to logs
Does a procedure description exist regarding who is to be given access to logs, and when?

13.6 Security and protection

13.6.1 Filing of processing history
How is the processing history kept on file?

13.7 Decisions in respect of audits

13.7.1 Controlling audits
Is system-oriented auditing planned and agreed on in order to reduce the risk of downtime in the business processes?

13.7.2 Protection of audit tools
Is access to audit tools restricted to the relevant staff?

14 Processing history

14.1 System log

14.1.1 Information on the system log
What information does the system log contain?

14.1.2 Conversion
Does the information in the communication system need to be converted from one format to another?

14.2 Details on time

14.2.1 Time
What information is stored in the processing history regarding the time of communication?

14.3 Communication paths

14.3.1 Information on communication paths
What information does the processing history contain on communication paths?

14.4 Storage

14.4.1 Information on storage
What information does the processing history contain on storage?

15 E-mail

15.1 Policy on e-mail

15.1.1 Security for e-mail
Does a policy exist within the organisation regarding the use of electronic mail, and do control measures exist in order to reduce the risks involved with the use of electronic mail?

15.2 Creating e-mail messages

15.2.1 Instructions
What instructions does the policy on e-mail contain regarding the creation of e-mail messages?

15.3 Spam, filtering and viruses

15.3.1 Spam
Are matters concerning spam and viruses dealt with in the policy on e-mail?

15.3.2 Filtering
Does the organisation use filtering technology to prevent the receipt of unwanted e-mail?

15.4 Copyright and ownership

15.4.1 Decisions
Has the organisation made decisions on copyright issues in its policy on e-mail / information security?

15.5 Anonymity / integrity

15.5.1 Decisions
Has the organisation taken into account the integrity aspect in terms of personal and organisational identity in respect of communication?

15.6 Private use

15.6.1 Conditions for private use
Has the organisation made decisions on whether e-mail may be used privately and notified its staff of any conditions connected with private use?

15.7 Monitoring

15.7.1 Monitoring of activities
Has the organisation made an active decision on policy for the monitoring of e-mail?

15.8 Misuse

15.8.1 Misuse, procedure and penalties

Is it clear from the organisation's policy on e-mail / information security what responsibilities individuals have in respect of misuse and non-authorised use?

15.9 Journal keeping / filing

15.9.1 Procedure for journal keeping

Do clear guidelines exist regarding when an e-mail message is to be entered in a journal?

15.10 Destruction

15.10.1 Decisions

Has the organisation issued guidelines to staff on what should be borne in mind as regards the possible filing or destruction of e-mail messages?

15.11 Acknowledgement

15.11.1 Use of the acknowledgement function

Does the organisation's policy on e-mail deal with the use of acknowledgements, and if so, what aspects of acknowledgement does it discuss?