Edition 3

Basic Level for Information Security (BITS)

SEMA RECOMMENDS - 2006:1

KRISBEREDSKAPS
MYNDIGHETEN

Title: Basic level for information security (BITS)
Published by SEMA
Cover photo: Ablestock
Publication: 15 000 copies

ISSN: 1652-2893
ISBN: 91-85053-97-x
SEMA´s registration number: 1214/2005
Graphic design: AB Typoform
Print: Edita, Västerås 2006
Publication can be ordered for free from SEMA, materielförvaltning
E-mail: bestallning@krisberedskapsmyndigheten.se
The publication can also be downloaded from SEMA´s web site:
www.krisberedskapsmyndigheten.se

Sema recommends 2006:1

Foreword

To achieve and maintain suitable level of information security, it is necessary to work in a structured and uniform manner. Different standards and standard endeavour occur both national and internationally. An increasing information exchange has led to an increased need of international standards agreement. The International Organization for Standardisation (ISO) and International Electro technical Commission (IEC) compose together an international standardisation system. Within this framework, the standards have been approved as Swedish standards. The Swedish terms for those are SS-ISO/IEC 17799, and SS 627799-2.
Within the framework for management of “24-hour agency”, The Swedish Agency for Public Management has developed the product OffLIS that compose a management outline to fulfil those standards.

Important factors for the revision of the document “Basic Level for IT Security (BITS)” are that:

- The structure is compliant with the swedish standards, and
- The document is including essential parts of OffLIS.

The ambition is therewith to facilitate the more long-term work to fulfil the swedish standards, and also to be able to replace OffLIS.

Ann-Louise Eksborg
Director-general, The Swedish Emergency Management Agency.

1. Scope

1.1 BITS applicability

The BITS document (Basic level for Information security) provides a number of recommended administrative security measures that an organization should implement in order to achieve an acceptable security level for managing the information within an organization. This level designates as basic level. Primarily those recommendations are addressing the management of information within vital public sectors that must function even during various disturbances within the society. Ideally, the basic level will be well balanced and provide a general accepted security level. Only a security analysis can determine whether the basic level is sufficient for an organization.

1.2 Modifications in relation to the previous version

In relation to the previous BITS edition, the following modifications are made:

- The abbreviation BITS stands for “basic level for information security” instead of “basic level for IT security”. The well-known acronym BITS remain as well.
- Chapters and sections-introductions are in compliance with the Swedish standard SS-ISO/IEC 17799
- The span has been extended to include the conception information security
- The main content of the Swedish Agency for Public Management´s regularity document OffLIS is harmonized within BITS. This therefore means that BITS will replace OffLIS and will also be used as template to establish a regulation for information security in accordance with the swedish standard SS-ISO/IEC 17799.

2. Terms and definitions

If an organization applies BITS as a template for managing its information security, then SEMA suggest the following items on this area:

- Terms and definitions of value for the organization.
- Declaration of what parts of the Swedish standard SS-ISO/IEC 17799 are applicable for organization's need. Such formal declaration is mandatory for the certification of an operation adjacent the standard.

The following concepts are fundamental to BITS:

Information security: the ability to maintain desired confidentiality, integrity and availability level regarding information and/or information facilities.

System owner: the head of the organization, or one by the head elected person who has approved responsibility for the development, acquisition, administration, and responsibility for the operation requirements, security, and the use of an information system, within the framework of assumed goals and economic framework.

Corporate system owner: an organization´s system owner who has the overall responsibility for an information system used by many organization.

Information security co-ordinator/-operation: a person or a group of persons that is the uniting link between the operating activities for information security and leadership.

Information security policy: document that states goals and guidelines for the organization´s information security management.

System security analysis[*]: document that states gathered requirements on availability, integrity and secrecy (confidentiality) of an information system, or internal network. The security analysis should clarify what further security measures should be needed for the compliance of information system requirements. System security analysis should be checked against organization´s information security policy.

Security instructions: tangible rules and routines directed to the end users, operators, and administration and management personnel.

Basic level: an information system´s minimum-security level to be achieved to maintain the business activities on a suitable level.

Operations approval: formal organization decision-making to approve an information system operation.

[*] replace the notion "system security plan"

3. BITS structure

3.1 content

BITS is edited according the following:

- Chapters and sections introduction are in compliance with the Swedish standard SS-ISO/IEC 17799.
- Each section is introduced by a statement formulated similarly SS-ISO/IEC17799 section.
- After these intend formulations, a number of basic level recommendations will be accounted for.
- The following text illustrates, in varying range, certain supplementary information to the stated recommendations.

3.2 Consecutive steps in the operations process of the security

BITS commence from the following security operation processes:

- The organization defines the objectives and guidance for the security management within an information security policy. This is the widespread document that governs the management of the security.
- The information security policy is clarified in security instructions for the end-users, operators, and administration and management personnel. In some cases, specific system instructions could be needed.
- Starting from the information security policy, a system security analysis for every system that is considered vital for organization's business should be performed. The system security analysis describes what security requirements that should be imposed concerning secrecy, integrity and availability. If the requirement level exceeds the basic level described in SEMA´s recommendations, then supplementary security measures should be considered.
- An assessment should be carried out to see if the implemented security measures has intended function, and a standpoint for how further requirements on security measures should be handled. This gives a basis for the security evaluation on which a decision on operations approval could be based on.

4. Risk assessment and risk management

4.1. Starting point for information security management

As a starting point for information security management, a risk and vulnerability analysis should be carried out to determine the security level appropriate for protection of an organization's information and information system. The suggested basic level in BITS should only be considered as an absolute lowest level.

4.2. SEMA´s information security analysis tool

A security analysis should be performed to clarify whether a higher security level than SEMA's basic level is required. SEMA has developed a tool to implement such analysis (BITS Plus[*]). In this tool, additional two security levels besides SEMA´s basic level are defined. Briefly the tool contains the following items:

- Description of current information system, concerning demarcation, communication, and information content.
- Availability, integrity, and Secrecy (confidentiality) should be clarified.
- The tool
  - generates administrative measures as response to imposed requirements.
  - produces the system security analysis document
  - produces result reports
- Templates for documents that govern information security operations management should be accounted for.

[*] Further development of SEMA´s IT security guide

5 security policy

5.1 Information security policy

Objective: “provide management direction and support for information security in accordance with business requirements and relevant laws and regulations”

Basic level

- An information security policy determined by the management should be available.
- The policy should express:
  - The commitment of the management
  - Definition, scope, and the importance of information security
  - Structure for risk assessment and risk management

- Information security policy should at least include a short description of:
  - Long-term objectives for the information security
  - Organization’s role and responsibility for the management of information security
  - General security requirements on identified areas that are significant for the organization

- Management responsibilities:
  - To ensure that the information security policy is well documented
  - All personnel should be informed about the content of information security policy and other regulations for their particular area.
  - To verify that information security policy is revised at regular intervals or whenever significant changes occur.

Information security management is often operated by the security department, but the organization’s leadership must be closely involved because of their inspiration.

The policy should be brief and clearly stated; so that all personnel will be able to accept it, and so that it could be a landmark for the continual work. The policy should be comprehensive, relatively long termed so as to not-to-be updated too often.

Hint!
See example on the template of information security policy on SEMA´s web site (www.krisberedskapsmyndigheten.se).

6. The information security organization

6.1 internal organization

Objective: “To manage information security within the organization”

Basic level

- The Management’s area of responsibilities:
  - provide the adequate resources needed for managing information security
  - determine how information security management should be described, in the shape of objectives, organization, roles and responsibilities
  - ensure that the implementation of information security measures across the organization is co-ordinate
  - identify the potential need of expert advice whether internal or external
  - approve methods for risk assessment, information classification, and approval procedures.
  - identify significant changes of overall threatening scenario
  - initiate an independent review of how the organization is developing and managing its information security.

- The information security instructions for users, administration and operating, should be made available by the management.
- An information security officer, co-ordinator or function should be appointed.
- The co-coordinator/-function, in issues related to information security, should be subordinated to the organization’s managers
- All information systems should be identified, recorded and approved by the management
- System register should include systems that are significant for the business operation, and should be at hand even in case of disturbances and crisis.
- All information systems should comply with the basic level in accordance with BITS
- A system owner of every information systems should be elected by the management
- Each system owner is responsible for the establishment of system security analysis of own vital systems
- The management should determine what risk level could be acceptable
- all information should be classified in term of its secrecy (confidentiality), integrity, and availability
- A common continuity plan for the organization should be in place
- Necessary agreements on information security topics should be established.

In some areas within business operations, specific rules may be stated, e.g. concerning teleworking and use of Internet.

Management has always the overall responsibility for business operations and information system support. Delegation of information security responsibility should follow the same principles as the delegation of other business responsibility within the organization.

Details concerning particular information systems should be stated on the system security analysis related to each information system. System security analysis may be modified in case

of significant alteration e.g. change management, different scope, and major changes in systems design or other threats.
The consultative and co-ordinating function tasks should be to:

- Co-ordinate the information security operation within the organization
- Contribute to the development of information security policy, system security analysis, system security instructions and other steering documents.
- Inform of and give advices on information security policy issues
- contribute to the accomplishment of security measures
- Follow up that the security instructions are carried out and when needed suggest measures.
- Co-ordinate and participate in the development of general routines regarding information security within the organization, i.e. routines for incident management.
- Be accountable for business contacts/intelligence
- Co-ordinate resources and information for security incident management

Suggestion!
Use SEMA´s analysis tool (BITS Plus) to perform system security analysis. See examples of template for information security instructions on SEMA´s web site (www.krisberedskapsmyndigheten.se). BITS Plus can be used to establish system records

6.2 External parties

Objective: "To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties".

Basic level

- Documented rules for third parties access to information or information systems should be available
- External personnel like service staff, consultants, and craftsmen should be informed about acquisition, access control, fire-protection, etc.
- Risk analysis should be performed prior to decision on outsourcing information management or information systems.

If the organization outsources information processing to an external organization, the responsibility for information security should be regulated in an agreement. The agreement should take into consideration the following:

- How to fulfil the business and security requirements in accordance with relevant legislations e.g. the personal Data Act
- The measures that should be taken to ensure that all concerned parties, including subcontractors are aware of the accountability of their security.
- how to check and maintain the integrity and the confidentiality of organizations´ s business resources
- The physical and logical measures that should be carried out, so as to restrict access to the organization´ s sensitive information, towards authorised users only.
- How to maintain continuity in the event of disaster
- The validity of physical security level for outsourced equipment
- Audit rights – the organization should have the right to carry out security audit, at service suppliers´ premises

- If outsourcing includes information that concerns state security, an SUA-agreement should be outlined, e.g. privacy-protected purchasing agreement.

7. Asset management

7.1 responsibilities for assets

Objective: “To achieve and maintain appropriate protection of organizational assets”.

Basic level

- Information processing resources should be listed and labelled according to current regulations (security instructions, administration)
- Responsibility allocation of all organization’s information assets should be available (security instructions, administration)
- Moving and transferring IT equipments to other users should be carried out according to established routines (security instructions, administration and security instructions, business continuity and operations).
- Rules for how information processing resources should be used must be documented (security instruction, administration).

Examples of assets associated with information system are:

- Information assets: data bases, data files, system documentation, user instructions/-manuals, administrative routines, education materials, operating and service routines, business continuity plans, and filed information.
- Program assets: application programs, network applications and operating systems, development tools (debuggers, compilators).
- Physical assets: computer equipments (computers, monitors), communications equipment (modems, routers, telephone exchanges, fax machines, answering machines, mobile phones), recorded media (tapes, disks), other technical equipments (UPS, air-condition equipments).

7.2 information classification

Objective: “to ensure that information receives an appropriate level of protection”

Basic level

- Documented rules for classification of information (security instruction, user categories) should be accessible.
- Information processed in automated information systems should be classified according to the required protection level
- The system owner is responsible for the implementation of the classification and for ensuring that security requirements are met.
- Rules for data media (security instructions, business continuity and operation) should be available, and include:
    - **c**lassification of data media
    - how data media should be labelled and recorded.

If external requirements are forced on some information in b2b systems, the elimination of this information should be considered, and it could be processed in a specific order or managed separately. By this, system requirements could often be reduced.

It is important that the classification of data media is being carried out as the classification levels can differ for information in data media. The labelling and registration should apply on all data media that are handled within the organization, as well the users´ as the operational administrations. The aim of labelling and registration is to avoide mixing-up the data media. Security back ups should be labelled and registered as well.

To avoid routine-like use of classification, a regularly training, e.g. every two years, on how to apply the classification should be provided. New employees should also receive training in current rules for information classification before granting access to information systems.

In the public sector, the secrecy assessment should be performed prior to decision on whether to deliver confidential information.

Hint!
See the classification model in SEMA´s analysis tool (BITS Plus).

8 Human resources security

8.1 Prior to employment

Objective: “To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities”.

Basic level

- All candidates for employment should be adequately screened, in proportion to future tasks
- Line managers are responsible to update all employees and temporary personnel on policy and instructions of information security.
- The system owner should describe requirements on user who grant access to information system and are thereby also given entry to information. The requirements should:
  - be documented and communicated**.**
  - cover security as well as competence needed.

8.2 During employment

Objective: To ensure that employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.

Basic level

- Documented security instructions for users and approved by management (security instruction, user) should be available.
- Security awareness and training in information security should be carried out regularly
- User guidance for an information system should be available.

User security instructions state the general information security rules that involve the management of the organizations´ information system and IT resources. The instructions clarify the matter of development, classification and document saving, restrictions for electronic mail and Internet usage, etc.

It is important that the education and training are performed continuously. This ensures the validity of information security knowledge and retains the security consciousness and motivation to maintain security.

The personnel concerned should be providing particular information about the responsibility roles defined in the information security policy.

User guidance for system is formulated taking into account the user’s knowledge and needs, and could be composed of:

- Manual directed to end user
- Basic user guidelines directed to new users, e.g. crib.

User guidance should at least include:

- Overall description
- administration of system functions
- administrative organization system
- where to approach to get help, regarding error detected, proposal and incident reports, etc.
- security regules for the system and its information
- routines for information delivering

Hint!
Se example in template for “security instructions, users” on SEMA´s web site (www.krisberedskapsmyndigheten.se).

8.3 Termination or change of employment

Objective: “To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner”.

Basic level

- Employees, suppliers and external users should bear in mind that:
  - all equipment belonging to the organization shall be returned when mission is accomplished
  - access right to information and information handling resources will be with-drawn when the assignment is complete.

9 Physical and environmental security

9.1 Secure areas

Objective: “To prevent unauthorized physical access, damage, and interference to the organization’s premises and information”.

Basic level

- Decision on who should be granted access to computer rooms should be taken by system owner considering the need of the information protection.
- For access to sites where sensitive information is processed or access to critical computer and communications equipments, the following should be considered:
    - the access should be regulated (security instruction, administration)
    - the access log should be recorded and safely stored
    - vacant security area should be physically locked
    - maintenance and cleaning staff and other outsourced personnel should be controlled and be granted access only if required.

Physical access to rooms containing critical computer equipment and communications equipment for information system should be logged.

Printer, facsimile & copy machines, scanners, or other equipment processing confidential or sensitive information should be placed in secure area that only authorised personnel do have access to.

As complementary measurement for access control, protection against theft in shape of physically locking equipments could be used. Thus locking devices that fulfil the Swedish association for protection against theft norms should be selected.

Regarding access control, the following should also be taken into account:

- Official ID should be visibly worn
- Access rights should be granted and maintained according to a specific routines

If an unauthorised person is discovered, then this event should be reported as security incident.

9.2 Equipment security

Objective: “To prevent loss, damage, theft or compromise of assets and interruption to the organization’s activities”.

Basic level

- IT equipment requiring UPS should be identified and labelled.
- UPS equipment should be regularly tested according to supplier’s instructions
- Power supply to central operational environment should be kept separately
- Fire-suppression system should be connected to critical operational computers and communication equipments
- Alarm systems for Fire, temperature and humidity should be available

- Alarm system should:
  - be connected to alarm-recipient
  - be regularly tested
- fire inspection of computer rooms should be performed in consultation with fire service authority
- computer operating site:
  - should be located in fire sectioned area
  - walls should be fireproofed
  - the zone should be free from unnecessary combustible materials
- It should be possible to adjust and measure temperature and humidity
- Apply routine procedures for tracing if data media containing sensitive information has been removed from its ordinary place.

Examples of equipments that do require uninterrupted power supply are network servers and communications equipment. Generally it is acceptable that central-server and data communications equipment are protected against power failure for at least two hours.

In the event of fire, the fire department should have easy access instantly. Preferably, areas with important computers equipment and communications equipment should be equipped with automatic extinguish device.

To avoid interference, it may be suitable to separate strong current cables from telephone cables. Regarding sensitive or critical systems, initiating searches for unauthorised equipment connected to cables should be considered.

If equipment with sensitive information is disposed of, or reused, the included information must be securely erased. Uninstalled reserve equipment and new equipment, as well the equipment that will be reused or disposed of, should be stored in locked rooms. Regarding computer equipment/data media that will be disposed of, a formal disposal report should be established.

Due of the risk of theft, special attention should be taken when storing equipment outside the organization. Depending on what information is included in the equipment (PC, memory devices, USB memory, DVD, CD, etc.), particular security measures should be implemented. Similar security protection requirements should be applied within the organization prior to employment.

Maintenance agreements that are significant for the system should be carefully considered.

Information and equipment for information processing must not be removed from the organization’s premises without the consent of the responsible manager.

10 Communications and operations management

10.1 Operational procedures and responsibilities

Objective: “To ensure the correct and secure operation of information processing facilities”.

Basic level

- Documented security instructions for business operations should be approved by management and published (security instructions, business continuity and business operations)
- Business operations for information system should be published and as a minimum include:
    - security back up procedures
    - restart and restore routines
    - log information and audit trails management
- Operational documentation should include procedures for:
    - how information system should be installed and configured
    - a safe storage of a copy of operational documentation that is separate from business operations area
- operational documentation should include procedures for:
    - identification and record of significant changes
    - planning and test of changes
    - formal approval of proposed changes
- All operational documentation should in a reasonable degree be complete and up-to-date and updated when changes in information system occur
- System owner determine, in consultation with IT responsible, the point of time for installation of new software versions.
- An established plan for operations of information system should be available. The plan should include:
    - staffing
    - required qualifications
    - system administrator substitute

- Installation of new program versions should be recorded and documented
- Documented procedures for installation of network operations (security instructions, business continuity and operation) should be available.
- Procedure for security incident management and malfunctions (security instructions, business continuity and operation) should be available.
- Systems development and testing of modified systems should not be carried out in the operational environment.
- Different level of authorizations should be used for the operational- and development environment.
- Unique access rights for testing and system development should be provided
- Implementation of program in both operational and development environment should be performed by authorised personnel.
- Rules should be available, for delegation of
    - resources and responsibilities for operation in different conditions
    - resources for incident preparedness and management/actions in case of security incident

Business continuity and operation security instructions are intended for ongoing management of business operations, instructions for how interruptions of varying lengths should be handled, any priorities in the event of exceptional events, handling and storing of data media, etc.

Documentation is intended to the personnel who are responsible for the daily operation of information system, and should include:

- An outline that shows the information system´s location within the organizations entire data operations, as well as the included equipment.
- The physical network structure and its included components
- The logical network structure
- Operational instructions for all operational activities.
- Configuration, parameters setting in information system, e.g. changes of the default-setting in the operating system,
- Routing tables
- Supplier's telephone number
- procedures for the management of changes in business operations

When continuity of information system operations is required, measures must be introduced for handling staff shortages. The basis for operational security is that the organization and responsibilities for the regular operations of information systems are clearly defined, that documentations are available and that operational staff has adequate education. The responsibility for various control and follow-up phases should be allocated, as well as the responsibility for detecting and correcting errors.

As complement to existing log, an operational record should be available in every business operation area. The record should include security events that effect the operations. Operational records could be carried out either automatically or manually.

Changes in the operational environment, equipment and procedures should be carried out by a formal procedure, i.e:

- Identification and recording of significant changes
- Security impact analysis of such changes
- Formal approval procedure for proposed changes
- Business information requirements
- Procedure for terminating and recovering from unsuccessful changes.

If external suppliers are used for the operation of information processing systems, the following issues should be carried out:

- Identification of critical applications that should preferably be managed internally
- Approval by system owner
- Business continuity impact
- Security rules and methodes for controlling compliance
- Level of Monitoring and following-up
- Incident management forms, responsibilities, reporting and management

Operational staff (internal and suppliers) should be aware of current security rules and regulations. This should be included in a code of conduct or agreement with external suppliers.

Hint!

Se example in template for “security instructions, business continuity and operation” on SEMA´s web site (www.krisberedskapsmyndigheten.se).

10.2 Third party service delivery management

Objective: “To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements”.

Basic level

- Procedures for how to control and follow-up external delivery services should be available (security instruction, administration).
- A new security risk assessment should be performed when changes of implementation of external delivery services occur.

An important condition for assessing security management of external delivery services is that the organization has good acquisition skills.

10.3 System planning and acceptance

Objective: “To minimize the risk of systems failures”.

Basic level

- To guarantee information system performance:
  - the use of resources should be monitored and checked
  - the planning for future capacity requirements should be carried out
- Information system should be approved by the system owner
- It should be considered, from case to case, whether operations approval should be renewed when changes in information system occur.
- Corporate system owner should determine the common information system components that should be approved either centrally or locally.
- Information system should be delivered to the organization in accordance with the established procedure
- Acceptance test should be carried out prior to operations delivery.

Operations approval is the process that leads to a formal decision that confirms the fulfilment of information system requirements, within a given environment.

To approve operations of information system, control of requirements on general (not specific) information security and IT infrastructure measures, as a result of information system security analysis, should be carried out.

An operations approval could be performed with reservation; which means that a short-term plan should be established for the supplementary security measures that should be taken.

A corporate system owner is accountable for system used by several organizations. The Corporate system owner is responsible for reviewing the common information system components, and for compiling a basis for respective (local) information system owner to approve local system operations. Common components could be:

- Technical platform
- Infrastructure, network and network services
- Software, applications

Responsibility demarcations are significant, whish is why the basis for organizations´ operations approval should include a clear demarcation between central and local areas of responsibility.

10.4 Protection against malicious and mobile code

Objective: To protect the integrity of software and information.

Basic level

- Procedures for the protection of malicious software should be available and:
  - as minimum detect the presence of malicious software
  - continuously monitor and implement new updates, both for servers and clients
  - execute the protection automatically
- The right to install new programs, program versions or to download external files should be regulated and documented (security instructions and/or business continuity and operations)
- Procedures for the updating of protection against malicious software (patch-handling), for both operating systems and application programs, should be available
- Approval regulations for the use of mobile code should be available

Protection against malicious software should be correlated to the potential harms caused by attacks. The system owner should therefore, in consultation with IT staff, assess the risks and consequences of such attacks prior to taking actions. Current measures against malicious software are those that contribute, after the detection, to prevent the infection, restrain infection propagation, and restore infected system.

Because new types of virus are constantly detected, no antivirus program can guarantee complete protection. An important part of protection is having control over programs that are allowed into information system, and knowing how information is transferred to them, e.g. via data media or Internet. The right to install programs, new program versions or to download external files should therefore be regulated in the operational instructions. Other possibilities to be taken into consideration, regarding protection against malicious software are to partitionate organization’s network into segments or subnets, so that an attack only harms one part of the network, and also to filter Internet traffic. Software against virus or the like should be installed in several places in the IT environment. Software could be either active protection system or passive protection system. The active protection software starts automatically, e.g. at system start-up, and remain active searching virus and other virus-like activities. It could also control applications and data files. The passive program could be activated at specific times.

When possible, procedures that keep protection against malicious software on servers and clients updated should be automated.

Mobile code is software that is transmitted across a network from a remote source to a local system and is then executed on that local system, often without explicit action on

the part of the user. Such program code includes ActiveX controls, Java applets, script run within the browser, and HTML email (as attachment), and other software for Internet connection, e.g. Internet bank, etc. Mobile code could be used to manipulate or steal information or used for other malicious purposes.

10.5 Back-up

Objective: “To maintain the integrity and availability of information and information processing facilities”.

Basic level

- Security back-ups should be performed regularly.
- The system owner should determine and document (security instructions, business continuity and operations):
    - what information should be backuped
    - back-up intervals
    - how many generations or cycles of back-ups should be available
    - how the back-ups should be stored
    - whether some back-ups should be stored in a remote location, separately from the operations area.
- The system owner should, to ensure the readability, determine if and when the back-ups should be tested. The decision should be documented (security instruction, business continuity and operations).
- The storing of and access to source code for own-developed information systems should be determined by the system owner.
- The actions to be taken to ensure the readability of information during the storing period should be documented (security instruction, business continuity and operations).
- Rules for data media (security instruction, business continuity and operations) should be available, for:
    - data media storage period
    - data media classification
    - how data media should be labelled and recorded
- restart test of the information systems from back-up copies should be performed regularly.

Back-ups interval should be determined according to the operations business requirements on business operations when restarting from back-ups.
In most cases, back-ups of information systems, in a common operations area, are performed by nominated personnel. In such cases, the back-ups intervals should be issued from the business operations that comply with the highest requirements on up-to-dateness of the information, at system restart. Hence, the interval should be clarified in the system owner’s statement on back-ups, as well as how the back-ups are performed.
Back-up may include copy of all information or just copy of the altered information since the latest back-up.

The information system restart test, from the back-up copies, should preferably be performed at least ones a year.
Examples of data media are diskettes, disks in servers, clients, or memory in portable computers, but also transcriptions from information system.

Classification of data media should take into account the current laws and regulations, and the business operations´ requirements, as well as the value of the business information. Other specific requirements from external parties should be taken into account as well. Classification determines the data media that should be included in a specific storage procedure.

Examples of regulations that determine the storage period of information stored in media are “archive law” (arkivlagen) and “the national archives administrations gathering” (Riksarkivets förvaltningssamling). See also information from “the Swedish National Testing and Research Institute (SP)”.

10.6 Network security management

Objective: “To ensure the protection of information in networks and the protection of the supporting infrastructure”.

Basic level

- One person should be responsible for every part of the network, including network segments.
- Network administration should be separated from regular administration and information system maintenance
- It should be possible to log relevant security events.
- Cross-connect cabinet should be locked.

Administration of bridges and routers, etc. should be tied up to the responsibility of other parts of the network. Network administrator should have the responsible to e.g. configure the servers, routers and DNS, and cooperate with the security personnel, to maintain the security in the network. Furthermore, a substitute administrator having the appropriate skill and qualifications should be elected. Access control should be based on security domains. One domain is a specific security area that includes some information systems and users following the same security rules and having a common security administration.

Rules for the security domains interconnections should include information about potential transfer directions, protocol types and services. Usually, all system administrators are not allowed to have complete access rights to system, but only limited access rights to fulfil their duties. Routing tables, etc. must be protected against unauthorised access and modification with password, etc. Repeatedly user authentications are not necessary when using network application once the authentication is performed on the workstation. Network application could get information about the user identity via data from the client application, or by identifying the network address.

Special attention should be given to the following:

- Network operations´ responsibilities should if possible be separated from other operations´ responsibilities.
- Responsibilities and procedures for the management of all network equipments should be established.

- Particular protection measures should be taken into account, to protect secrecy and integrity when transferring data across the public network, and to protect connected systems and equipments.

It is important that multi-machines, printer, etc. that are connected to the network are protected against unauthorised access.

10.7 Media handling

Objective: "To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities".

Basic level

- System owner should determine which information stored in data media requires specific storage procedures to prevent unauthorised disclosure.
- Storage procedures for data media should be available (security instructions, business continuity and operations)
- Data media containing vital business information should be stored in a safe, secure environment.
- Data media and backup copies should be stored separately and in different band stations, or in special storage area.
- Procedure for how data media containing confidential information should be disposed of (security instruction, administration) should be available.
- The system owner should determine how the stored media containing system information should be disposed of.

In order to decide what data media should be protected against unauthorised access, the information stored in these data media must be labelled and classified. The security instructions should clarify how to store these data media, e.g. in a safe or cabinet. Data media should be stored in a safe or other form of security furniture that corresponds to minimum fire class D60 or the equivalent. Area or safe should comply with the fire law and any insurance company rules.

The system owner determines the storage area to be used. Specific access controls to data media storage area e.g. a safe or a cabinet should be available.

Information media can be vulnerable to unauthorised access, misuse or corruption during physical transport, for instance when sending data media via postal service or via courier. An assessment should therefore be made, based on information sensitivity, of how the data media should be packed and physically transported, and by whom. The usage of cryptographic and electronic signature should be considered.

Movable data media should be handled so that:

- Previous content from reused media should be erased, prior to leaving the organization, e.g. by over-writing, using techniques commensurate with the requirements for current classifications level.
- All media that leaves the organization should be recorded to maintain accountability.

- Storage should be housed in secure area and in an appropriate environment in accordance with the manufacture's specifications.

10.8 Exchange of information

Objective: "To maintain the security of information and software exchanged within an organization and with any external entity".

Basic level

- Documented procedures should be available (security instructions, users) and include the following:
  - the information to be sent by e-mail
  - transferred data by e-mail and attached files should at least be protected against virus
- The system owner's responsibility for data transferres to and from information system should be clarified.
- Exchange of information with any external entity should be regulated in an agreement
- Procedures for the approval of the publishing of information in systems that are available for public, should be in place
- The system owner will decide on measures for the physical transport of business critical information (Security instructions, administration)
- Procedures for protecting information shared by different information systems should be in place.
- Internet services should not be run prior to the security functions approval.
- Security functions instructions for public web service development should be documented (security instructions, administration).

The rules that apply for information that can be sent by e-mail should at least include information classification based on legislation and business requirements. They should also include procedures for:

- The information that should be encrypted, and the information that should have an electronic signature
- Encryption, key management and key transfer
- Network monitoring, access control system and protection against attacks.
- Selection of standard protocol and alternative data communications.
- The organization´s user support functions.

Regarding operations of organization's e-mail system, the internal e-mail system should be separated from the external network, e.g. by some form of firewall functions.
To avoid the risk of confidentiality violation, the following items should be considered:

- Automatic forwarding of connections should not be permitted when sending sensitive information (e.g. Personal data) in clear text.
- Restrictions in sending or forwarding large files
- Use caution when opening attached files
- Contact assigned support function if virus in e-mail is suspected.

The system owner should be aware of his security responsibility concerning the transfer of data to/from information systems, e.g. in case of failure or manipulation of data. If data is transferred between two organizations with different responsibilities, a

co-operation on security issues between the organizations should be carried out. Responsibility issues are complicated by the fact of that data transfer is often carried out by communication lines and other communications equipment that the system owner does not control. An additional network operator is often responsible for the technical performance of transferring, in accordance with agreed security specifications. This also means that the network operator is responsible for implementing the security requirements needed to protect the network equipment. The network operator in turn is dependent upon the network owner maintaining suitable security. The security level that is defined by the system security analysis requirements for an information system also place indirect demands on any external communications and communication services. The system owner needs to know what security requirements the techniques and purchased communication services should fulfil, and whether supplementary measures should be implemented. Alternative paths around the organization's firewall must be avoided. A current and up-to-date record of all network connections makes it possible to regularly identify authorised persons having access to the network. The establishment of unauthorised connections could then be supervised. This also includes all kinds of connections for maintenance, supplier services and remote diagnostics.

There are different types of authentication methods with various degrees of protections. The selection of methods is based on risk analyses. Authentication methods include those based on cryptographic technique, smart cards, challenge-response protocol and call back procedures.

Regarding electronic publishing systems (EPS) and electronic services (Internet), in particular those that permit rereporting and direct information input, the following items should be ensured:

- To obtain and process information in accordance with the regulations in the legislation concerning personal data legislation.
- Information that is obtained and processed by publishing system should be processed completely, accurately and in time.
- Sensitive information held in system should be protected during the transfer and storage.
- Access to the publishing system should not permit access to organization's internal networks.

Procedures and controls for protecting of information exchanges over voice, fax and video equipment, should be available.

Information exchange that is regulated in agreements should regulate the right of usufruct issues, economic issues as well as the security requirements (confidentiality, integrity and availability).

10.9 Electronic commerce services

Objective: "To ensure the security of electronic commerce services, and their secure use".

Basic level

- The security of information exchange should be applied for electronic commerce as well.

10.10 Monitoring
Objective: “To detect unauthorized information processing activities”.

Basic level

- Audit log for relevant security events should be available and as minimum records:
  - user identity
  - date and time of log-on and log-off
  - successful and unsuccessful attempts to gain access.

- administrator and operator logs should be available, and as minimum record:
  - accounts and the involved administrator/operator
  - involved computer processors
  - date and time of log-on and log-off
  - successful and unsuccessful attempts to gain access
- If the activities of the administrator and the system operator cannot be logged automatically, they will be logged manually.
- The system owner should determine the events, besides the above, that should be recorded in the information system log.
- The corporate system owner should ensure that the information system is constructed så that the audit log for relevant security events as minimum records:
  - user identity
  - date and time of log-on and log-off
  - successful and unsuccessful attempts to gain access
- Regarding the information system logs, the system owner should determine (security instructions, administration):
  - how often the logs should be reviewed
  - who is responsible for reviewing them
  - how long the logs should be saved
  - how the logs should be stored
- Instructions for the organization’s use and monitoring of log files at operations should be documented (security instructions, administration)
- Logs should:
  - be stored during a period of time in accordance with the thinning decision that even meets the necessity of incident investigation.
  - be checked regularly, taking into account the signs of abnormal conditions and security incidents.
- Procedures should:
  - be available for how the information system logs should be monitored
  - include instructions about how error messages and other information should be carried out, who should be informed, etc.
- Logging facilities and log information should be protected against tampering and unauthorised access.
- The clocks in information system should be synchronised with an agreed accurate time resource.

During the follow up process of security events through logs, it is important that the computer clocks are synchronised. The use of NTP (Network Time Protocol) via Internet service Provider (ISP) should be considered.

Accountability means the possibility to identify and follow up the course of different events through the records. A coordination of several logs may be needed, to acquire accountability witch is the real purpose of the logging.

To be able to perform accountability in an information system, knowledge of the system processes and their chronological order is necessary. Facilities for that are one or more monitoring functions in a form of logging. Procedures to ensure traceability, in relation to the protection value of the system, should be established.

Security logs should be followed up continuously. A security log analyses should be carried out taking into account all kinds of violation against current regulations.

Usually, the security logs are saved for a period of two years, but in some specific cases they may needed to be saved longer. For instance, the logs for financial systems and financial transactions should be saved for a period of 10 years, so that the bookkeeping regulation requirements on accountability and restoring are complied with. This requires the ability to be able to read the information during the log-storing period.

Logs that record divergences and other security-relevant events should include:

- user identities
- date and time of log-on and log-off
- terminal identity and location if possible
- records of successful and rejected system access attempts
- records of successful and rejected data and resources access attempts

System administrator and system operator activities should be logged. Logs should include:

- start and end time for system operation
- system errors and the taken corrective actions
- confirmation of accurate files and data output
- Name of the person who did introduce information in the log, at manual logging.

In case of a juridical process, it is important to prove that information system logs are unchanged. In those cases, the digital signature of current logs should be considered.

11 Access control

11.1 Business requirement for access control

Objective: “To control access to information”.

Basic level

- If possible, the users should be given authorisation profiles that only admit access to information systems that are necessary for solving their tasks.
- The system owner should determine whitch and what types of connections to telephone and data network are permitted.
- Decision on connections to telephone and data network should be documented.
- A current record of all external connections should be available.
- Connections to information system should be checked regularly.

11.2 User access management

Objective: “To ensure authorized user access and to prevent unauthorized access to information systems”.

Basic level

- Only appointed authorised person should have the right to install new softwares in the network
- Specific network access rights should be available.
- System administrator and technician should always have unique and individual user identities.
- Only the appointed administrator can access the access right file.
- The number and the extent of privileged accounts should be reduced.
- Administrators should not have access right to all system applications, but only to those applications that are necessary for their tasks.
- Routing tables etc. should only be accessible by authorised administrators.
- A documented (security instructions, administration) procedure for allocation of, following up and updating authorisations should be available.
- the system owner should determine who is entitled to make decisions on access rights
- Documented procedures for the management of access rights of users who have hanged roles or jobs or left the organization should be available (security instructions, administration).
- New users should be provided initially with a secure temporary password, which they are forced to change immediately.
- Before allocating access rights, the users should have sufficient knowledge of:
  - the security instructions that are generally applied for IT operations
  - the instructions, particularly those that are associated to the users own tasks
- When the authorisations are expired, the access rights should be blocked within a week.
- It should be checked, at least once a year, that only authorised users are registered in the authorisation system,
- Only appointed administrator should be able to register, change or remove users´ access rights

- Reserve personnel should be appointed; and reserve routines for authorisation management should be available.
- Authorised information system users should be registered in an access control system, with their determined rights. If possible, the user should be given an authorisation profile that only provides access to the information system that is relevant for their own tasks.
- For passwords, the following items should be considered:
  - each user should have a unique user identity and a private password
  - the password should be composed of, as minimum, 8 characters, for as well the users as the system administrator/operator (not based on anything somebody else could easily guess or obtain using person related information)
  - users should be forced to change the passwords at regular intervals, according to system owner's decision
  - limit the number of unsuccessful log-on attempts; allow three attempts prior to locking the user's account
  - the passwords should not be reused, within a period of 13 months, according to the security co-ordination functions´ regulation
- For workstations, the following items should be considered:
  - screen lock, with automatic locking should be activated when users leave their workstations.
  - the unlock should be executed by password.
- Secure user identification should be carried out prior to unlock the locked account.
- Store password in protected (e. g. encrypted) form.
- Routines that prevent the use of standard or default vendor password should be available.
- Regarding information system owned by a corporate system owner, the corporate system owner should ensure that the system is constructed in a manner that the access control rights satisfy the basic level recommendations.

Access rights refer to a user right to access an information system and its resources in a regulate manner. Achieving this requires joint administrative and technical measures. Access control right refers to administrative and technical measures for controlling user ID, managing user access rights, and following up the activities. These controls are usually performed within an access control system that enable the verification of the IDs, rules of access rights, and recording user's activities in the information system (logging). A password should be composed of a mix of letter, digits and special characters, to make it difficult to disclose. Access rights decisions should be documented and stored.

As additional measure, to ensure that workstations are not left unlocked because user forget to activate the screen lock, a general period of time for automatic activation should be considered.

Users should not have administrator access rights on their machines, be able to install programs themselves or have access to operating system and system equipment.

11.3 User responsibilities

Objective: "To prevent unauthorized user access, and compromise or theft of information and information processing facilities".

Basic level

- users is responsible for:
  - not disclosing their passwords or lending their access control rights to any other person
  - protecting their passwords
  - immediately changing the password, if it is suspected that the password has been disclosed
  - changing the password according to the rules
  - not reusing previous passwords
  - not using the same password externally
- information handling equipment in public areas should:
  - be deadlocked
  - only allow access to intended public applications
- paper documents and stored media in user's workrooms should be carried out in accordance with the classification of the information.

11.4 Network access control

Objective: "To prevent unauthorized access to networked services".

Basic level

- The firewall function should be the only channel for IP based data communication to and from the organization.
- Responsibility for administration of the firewall should be documented (security instructions, administration).
- The firewall design and configuration should be documented.
- The firewall should include safeguards against malicious software.
- Network's system owner should, in consultation with respective other system owner determine (security instructions, administration):
  - what should be logged in the firewall
  - who is responsible for following-up the logs
  - how often the follow-ups should be performed.
  - how long time the logs should be saved.
- If wireless LAN is used, the network system owner should determine if measures against unauthorised eavesdropping and system exploitation should be taken.
- Servers should be protected by control application in the operating system, or by accessing the server via network application.
- Documented procedures for what is allowed for connections between security domains should be documented.
- The use of remote diagnostics should be performed according to the fixed routines.
- Based on the system owner's requirements, the need for authentication methods for external connections should be clarified.
- Rules for how authentication should be performed, at external connections, should be available (security instructions, administration)
- Security architecture for internal and external networks and communication systems should be documented (security instructions, administration).
- Documented procedures for the connecting equipment to internal and external networks should be available (security instructions, administration).

- Rules and routines, for external network connections, including security functions, authentication, etc. should be documented (security instructions, administration).
- Guidelines for connecting wireless network equipment should be documented (security instructions, administration)
- Security guidelines for Internet connection should be documented (security instructions, administration).
- The administrator's activities should be logged. The logs should not be erased or manipulated.
- Verification that security functions are operating should be carried out prior to connecting to Internet.

Firewall is a common resource for an organization, which means that its security level must satisfy the security requirements of several different business areas. Example of issues that may be relevant when developing a firewall policy are the following:

- What services the firewall should offer
- What information the firewall should hide, e.g. organization's network structure, IP-address and user IDs.
- What should be logged in the firewall
- Should the firewall include e-mail scanning system
- Should the firewall include anti-virus protection system
- Internet access/logging control
- Should integrity control of firewall software be required.
- What physical protection is required for the firewall (limited access zone).
- How is firewall administration organized
- What authentication requirements apply for firewall access, e.g. at remote access
- What should be back-uped

More and more organizations build wireless networks for their business, WLAN (Wireless Local Area Network). Authentication of clients in a wireless network infrastructure is necessary; nevertheless the authentication of the infrastructure is mandatory.

Wireless network standards include a security solution that covers authentication, encryption and integrity control. This security solution is WEP (Wired Equivalent Privacy) WEP is not a complete security solution; therefore it should be combined with other security solutions.

The wireless access points should be closed down when they are not in use.
Internal/external networks and communication systems security architecture should include technical instructions for:

- Access to e-mail, file transmissions, and time/date of network.
- Network segregation
- Requirements on external suppliers of external network services
- Security architecture for using wireless communication networks.

Opportunities for automatically disconnecting Internet communications at exceptional events should be considered.

11.5 Operating system access control

Objective: "To prevent unauthorized access to operating systems".

Basic level

- Logging procedure
  - should not show the identity concept for the systems or applications prior to successfully complete log-on
  - should not provide messages during the logging process that could help an unauthorised user
  - should not validate the logging in information until all data is received
  - should records unsuccessful attempt in the log
- Rules for system facilities that ignore system and application blockages should be available (system instructions, administration)
- Sessions should automatically be disconnected, after a defined period of inactivity.
- The connection times for sensitive applications should be limited.

Workstations should have a unique ID in the network to provide a suitable control of the connections. Exceptions should be granted subsequent to the performed risk analysis. Exceptions should not be granted for systems with highly classified information (integrity and confidentiality) because these are subject to accountability and non-repudiation requirements.

The use of administration tools or system facilities that can ignore the system and application blockages should be restricted and controlled. Documented rules for how and when they can be used should be available. Activities of these tools/facilities should be logged.

Consol terminal should have the same level of physical protection as the computer that is controlled by the console.

To prevent misuse by unauthorized users, restricted connection time for high risk applications should be considered.

11.6 Application and information access control

Objective: “To prevent unauthorized access to information held in application systems”.

Basic level

- Well-defined access rules should be available. These rules should take into consideration that the access should:
  - be restricted according to the need to carry out a task
  - be granted with consideration for how information is classified
  - be tracable, if required by the level of information classification
  - not be carried out anonymous when using information handling resources.
  - be managed with different access rights
  - be determined and documented.
- Only authorized persons should have access to media containing critical business operations´ information.
- The system should be connected to the access control functions applied within the organization.
- It should not be possible to access databases with other services.

The following should be observed regarding access control to applications:

- Organization´s information should be stored in allocate systems, or in allocated catalogues in file server
- Storage of the organization´s information in local hard disks should be performed only if there is a copy on the file server.
- The laptops users must ensure that the organization's information that is stored locally is back-uped on the file server.
- Laptops should not be connected to external and internal network at the same time.
- Users hwo handle information locally should be aware of the information's security classification and handle the information accordingly.

The following principles should be considered access control:

- The system should, in the first instance, be constructed so that authorisation is linked to user identity, to determine the system functions that the users can access, and access to multiple users´ databases.
- In the second hand, the cobtrol of functions within the system, and access to multiple users' database should be performed with specifically defined access ID. This identity's password should be stored securely to avoid unauthorized disclosure of information.

11.7 Mobile computing and teleworking

Objective: "To ensure information security when using mobile computing and teleworking facilities".

Basic level

- Requirements on technicall security and practical handling of mobile equipment should be documented (security instructions, user).
- The system owner should determine whether an information system´s information can be processed remotely with stationary or mobile equipment.

Teleworking have been growing today. Thus, the handling of laptops and/or other mobile equipment and their connections to organization's network should be regulated. It should therewith be appropriate to enter into agreements with employees regarding teleworking. care must be exercised when using mobile equipment like laptops, palmtops, mobile telephones, etc. outside of the organization's premises.

Issues that need regulationin regard to teleworking could be:

- Physical protection in or outside the home (theft risk, risk of fire)
- Logical protection (inappropriate use)
- Whether the equipment should only be used for organization's business (virus contamination, etc.)
- Transcriptions management (inappropriate access)
- Whether storage and backups of information should be performed in the user's computer or in the organization´ server (risk of theft, inappropriate access and destruction, etc.)
- How remote support should be carried out (inappropriate intrusion).
- Protection against malicious program code (virus contamination, etc.).
- Encryption requirement when transferring data in some cases (inappropriate access and manipulation).

- Authentication when connecting to organization’s network (inappropriate access and manipulation).

There may be grounds to consider controlling clients to ensure updated anti virus software and imbedded security patches, etc. prior to connecting to internal network.

12 Information systems acquisition, development and maintenance

12.1 Security requirements of information systems

Objective: “To ensure that security is an integral part of information systems”.

Basic level

- A system security analysis should:
  - be performed for each system assessed vital for the organization
  - be established by the system owner and documented
  - point out the system owner
  - include the collected security requirements on the information system
  - be checked for compliance with the information security policy and the current policy declaration.
- Security instructions for administration should be determined by the management, documented and available (security instructions, administration).
- When using public network within the frame of the information system, the system owner should determine whether the network operator’s services meet the organization´s security requirements.
- The information system that is used should be checked for compliance with the organisation´s security requirements.

To be able to assess the security requirements on an information system, it is necessary to clarify the business activities that the the system supports, their degree of dependency and the requirements herewith.

The system security analysis identifies the security requirements that should be imposed to:

- Prevent or make it difficult for an unauthorised to access the information system (confidentiality)
- Make sure that the produced and processed information in the information system is correct, up-to-date and complete (integrity)
- That the information system functions and information are accessible when necessary (availability).

The risk analysis should be based upon the assessments of the threats against the information system, the likelihood of the threats realized, and their negative security impact to the organization.

Procedures for administration access rights, procedures for implementation, administration and disposal of system, and various system administrative measures, associated to information handling resources and communication resources, etc. should be clarified in the security instructions, administration.

Already in the development and purchasing phases of an information system it is important to study security requirements on the system and the need for reserve routines. This also applies after major changes to existing systems. Procedures are therefore urgent. They may include requirements on certified and evaluated products, tests, test environment, and the points of time of testing and introducing system, etc.

As basis, the purchased system and software should be certified by an independent body, or developed and provided by trusted supplier.

Procedures for purchasing and installing software in network environments are particularly important. The risk that a data virus is propagated to other environments in the local networks is imminent when one computer is infected.

12.2 Correct processing in applications

Objective: "To prevent errors, loss, unauthorized modification or misuse of information in applications".

Basic level

- Procedures for validation should be in place
  - of the information system's data input and output (security instructions, administration)
  - to detect information distortion.

- Documented procedures for data correction should be available (security instructions, business continuity and operation).
- Personal data sent over open networks should be encrypted.

Procedures for data correction should at least include:
- Who is responsible for the quality of data
- How often the controls should be performed.

12.3 Cryptographic controls

Objective: "To protect the confidentiality, authenticity or integrity of information by cryptographic means".

Basic level

- Encryption procedures for information should be documented (security instructions, administration).
- Instruction for cryptographic technique application should be documented (security instructions, administration)
- Key management supporting the organization's use of cryptographic technique should be in place.

Organization's need of cryptographic technique should be based on the implemented risk analyses. In case of such need, the organization should develop encryption rules to avoide inappropriate or incorrect usage.

Cryptographic technique should be applied within the organization and at external connection to/from the organization's network when data or information requires:
- protection against unauthorised interception
- protection against unauthorized disclosure
- production of electronic signature, and

- secure authentication (strong authentication)

Reliable and evaluated products for cryptographic technique should be used.
Instructions for key management should be carried out by the operational organization, in consultation with the functions for the information security coordination.

12.4 Security of system files

Objective: “To ensure the security of system files”.

Basic level

- procedures for software, application and system installation should be available
- test data should be checked and protected
- access to source code should be restricted

Installation of new programs in existing systems should follow the documented process/procedure. Installation should only be performed if the agreed test process is carried out, including test of security functions (system approval).

Test data should be protected and checked. The use of production database containing personal data is prohibited. Personal data should be anonymized prior to execute test data.

The following safeguards should be applied to protect production data, when they are performed for test purpose:

- Access management procedures that are applied for production systems should also be carried out when testing of such systems
- Access rights should be granted separately each time the production data is copied to test system.
- Production data should be erased from test systemas as soon as the test is completed.
- Replication of production data should be logged, to gain accountability.
-

12.5 Security in development and support processes

Objective: “To maintain the security of application system software and information”.

Basic level

- Appointed system administrators should be in place
- Personnel responsible for system maintenance should be available
- Contracts will regulate how sensitive information is handled in conjunction with service.
- Remote diagnostic should be performed in controlled manner
- Procedures for system and program development should be carried out and available (security instructions, administration).
- Decision on program alteration should be made by the system owner
- The system owner should determine when to install new program versions
- Program development and alteration should be documented
- Procedures for how knowledge of administration is fed back to the organization for its own programs that are developed externally should be available.

- Procedures for how training is implemented for purchased systems, including changes of programs and functions, should be available.
- Access to internal developed information system's source code should be regulated in a settlement.
- Copy right issues should be regulated in a settlement.
- System documentation for information system should be available and include:
    - What components the information system is composed of
    - overall description of the component functions´ purpose
    - a detailed system description
- A complete copy of system documentation should be stored separately from the original
- System documentation containing sensitive information should only be available to authorised personnel.
- All documentations should, to a reasonable extent and degree, be complete, up-to-date, and be updated when changes in information system occur.
- All software should be tested and approved, so that it does not harm other system functions or the common network, prior to being installed.
- Installation instructions and, in occurring cases, routines for program distribution should be established.

System maintenance includes the continual control and alteration of information system with the purpose of securing the system quality and business profit. Usually the remote diagnostic communications should be disconnected, and only reconnected subsequent to a direct agreement in every single case.

Administrative instructions for system development should include:
- System development responsibility
- System development design
- Administration model in line with system development model
- Access control.

The system owner is responsible for the security measures when developing the information system. New system development and program maintenance should be performed separately. For program maintenance, it is usually only necessary to check the security measures that are related to implemented measures. Verification of, that an information system fulfils the established security objectives should be performed at system test and in production process. The same commitments should be applied at information system changes, as well as acquisition. Source code should be deposit with a third party, if no other agreements can be reached. For security reason, it is important to regulate access to source program/-archive.

The system documentation is intended for information system maintenance and development personnel. Preferably the documentation should include both a general and a detailed system description.

The general system description will present a general view of the information system and system construction. It could include:
- An outline that shows the information system's location within the organization's data operations.
- The physical and logical network structure
- The parts/modules included in the system/program

- A description of the parts´ functions without details, preferably in the shape of figures that show their interdependency.
- essential data structures, preferably in the shape of figures

The detailed system description is intended for the personnel who will implement changes or introduce new functions. It may include:

- A separate description of each part/module
- A description of the data types
- A well described program code.

Parts of the system documentation can contain sensitive information about the information system's security instructions. Therefore, in some cases, access to documentation may need to be regulated.

System changes in production should be subject to a consequence analysis with regard to impact on security functions (secrecy, integrity and availability) and the existing business continuity planning.

Only well-reputed supplier should be chosen, at software packages acquisition.

12.6 Technical Vulnerability Management

Objective: "To reduce risks resulting from exploitation of published technical vulnerabilities".

Basic level

Roles and responsibilities for managing technical vulnerabilities should be defined and include:

- vulnerability monitoring
- vulnerability risk assessment
- program changes
- asset tracking
- co-ordination responsibilities.

13 Information security incident management

13.1 Reporting information security events and weaknesses

Objective: “To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken”.

Basic level

- Procedures for how user should react to function errors, suspected intrusion, or other disruption, should be documented and available (security instructions, user).

A formal reporting procedure for how suspected incidents are handled, where the point of contact for reporting is known throughout the organization, should be established.

13.2 Management of information security incidents and improvements

Objective: “To ensure a consistent and effective approach is applied to the management of information security incidents”.

Basic level

- Procedures for following-up function errors, suspected intrusion, or other disruptions should be established (security instructions, administration).

Security incidents are inevitable and occur in many organizations. Causes may be internal or external intrusion attempts, incorrect use of information systems and IT resources, etc. Feeding back experiences from different kinds of incidents for tracing defect and weaknesses in IT operations is important. Procedures for following-up incidents are therefore significant.

The incident management process should:

- Clarify how and to whom reporting
- Provide resources for prioritizing and managing occurred incidents
- Make it possible to follow up events and measures
- Provide procedures for restoration to normal operations, after an incident has been properly handled.

Organizations that run operations for other organizations in cooperation with each information system’s system owner, should establish procedures for extraordinary events. The procedures should include:

- How the users are informed, during disruptions
- How reporting of disruptions, errors and IT incidents should be carried out
- How to act in the event of simultaneous disruptions in several systems
- How prioritization between systems should be performed.

14 Business continuity management

14.1 Information security aspects of business continuity management

Objective: “To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption”.

Basic level

- The system owner should determine the longest estimated time that an information system can be down before the business is jeopardized.
- A documented contingency plan that includes restart and reserve routines for data operations that take place within the framework of ordinary operations, so that the information system can restart within the determined time, should be available.
- The restart procedures should be:
    - available for the information system
    - documented (security instructions, business continuity and operations)
- The existing reserve routine should be documented (security instructions, business continuity and operations).
- A documented joint contingency plan for IT activities that are harmonized with the individual information systems´ contingency plans should be in place
- A documented procedure for informing about interruptions and restarting actions should be available, and
    - is communicated and tested.
    - includes everything that directly or indirectly is dependent upon the information system functions
- Circumstances characterized as disaster for the business should be clarified.

For business continuity planning, business critical processes should be identified. The security requirements on business continuity should be integrated with other continuity requirements for operations, staffing, equipment, transport and resources. Information security should be an integrated part of the common process for continuity planning in the organization.

The continuity planning should include measures for identifying and reducing risks, minimising the consequences of malicious incidents, and ensuring availability and integrity of the information.

Continuity planning is a process that provides, among other things, a contingency and disaster plan.

The contingency plan should be adapted to the the importance of the information system for the organization, and be integrated part of all security activities. Information systems should be prioritized. Contingency planning process presumes that the performed restart will meet availability requirements for each information system. The contingency plan should describe the measures that will ensure the continued activities during disruptions or interruptions in IT operations. Most measures can then be relevant and apply to areas such as documentation, staffing, fire, protections against malicious program code, power supply, security backup, and storage of data media.

It is also important to regulate security relationships during disruptions, e.g. the responsibility for the measures needed to handle the situation at hand.

The management should consider whether there are specific reasons for establishing a disaster plan. As starting point for the development of a disaster plan, the management should assess the circumstances that could be disastrous for the organization. Disaster planning is a process that must be led by the managemen, and the goal is to create conditions for establishing a disaster management team that run the business.

15 Compliance

15.1 Compliance with legal requirements

Objective: “To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements”.

Basic level

- Software should only be used in accordance with the current agreements and licensing regulations.
- For compliance with copyright regulations, procedures for approval and distribution of program that are used by the organization should be available
- Information systems that handle public document should include:
    - the thinning decision.
    - the filing and thinning takes place according to thinning decisions.
- Procedures for system information delivery should be available for systems that handle public documents
- Licenses or other agreements on usufruct for all external integrated programs and program components in an information system should be available.
- Licenses agreements should be revised annually and will comply with the number of users, type of computer, etc.
- Procedures for protecting the organization’s register and documents for compliance with national laws and regulations should be documented (security instructions, administration) and include:
    - document identification principles
    - preservation, storing, handling, and cassation
    - storage time requirement, etc.
    - specific needs for protection from loss, destruction and forgery
- Information system that handle personal data should be registered and reported to the personal data representative (if one has been appointed).
- Processing of personal data, plus information concerning consent for processing, will take place as agreed with the personal data representative, or according to the Personal Data Act.

Important provisions concerning requirements for implemented protective measures are:

- Personal Data Act
- Freedom of information and secrecy legislation
- Copyright Act
- Patent Act
- Archive Act and Archive Ordinance and current thinning regulations
- Protective Security Act
- Specific regulatory legislation concerning information processing (Social Insurance Register Act, patient records Act, etc.)
- Bookkeeping Ordinance.

hint!
Some guidelines on the application of freedom of information and archive legislation are available from The Swedish Agency for Public Management (Statskontoret) publication “Offentlighet och IT 2002:1”.

15.2 Compliance with security policies and standards and technical compliance

Objective: “To ensure compliance of systems with organizational security policies and standards”.

Basic level

- Internal and external penetration tests should be performed regularly.
- Managers should regularly check compliance with security procedures, policy, and standards.
- Penetration tests on external communication systems (FW, etc.) and on internal information systems respectively, should be performed regularly.

15.3 Information systems audit considerations

Objective: “To maximize the effectiveness of and to minimize interference to/from the information systems audit process”.

Basic level

- Measures for controlling systems in operations should be planned, to minimize the risk of disruptions.
- Access to audit tools should be restricted.