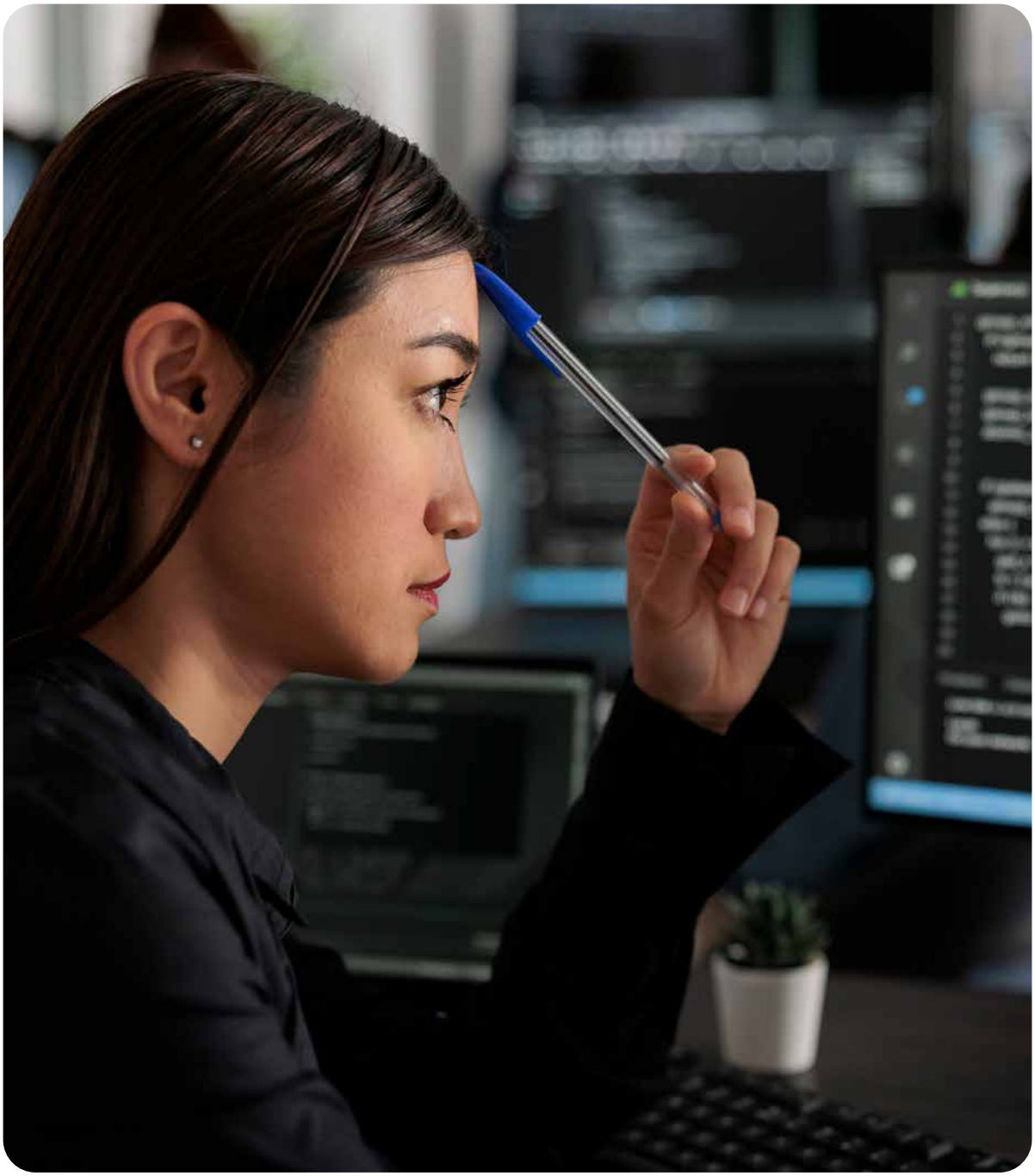
safespring

Information Security Guidelines

SECURITY BY DESIGN 2024



Applicability of the guidelines

This document sets normative organizational, administrative and technical security measures to be taken to achieve the information security baseline of protection for all of the organization's information assets and systems identified as missioncritical.

Table of contents

Applicability of the guidelines 2

Human resource security 4
Trusted roles 4
Qualifications, experience, and clearance requirements 5
Training requirements 5
Termination and change of employment 5
Segregation of duties 5

Asset management 6
Responsibility for assets 6
Information classification 6
Media handling 6

Access control 7
Identity management 7
Authentication 7
Authorization 8
Password management 8
Audit logging 8

Cryptography 9

Physical and environmental security 10
Physical access controls 10
Monitoring of secure areas 10
Power and environmental controls 10
Fire prevention and protection from water exposures 10
Alternative operating site 10

Operations security 11
Orderliness and automation 11
Responsibilities 11
Operating procedures 11
Operating systems security controls 11
Isolation of critical components 12
Configuration and change management 12
Information backup 13
Monitoring 13
Time synchronization 13

Network securities 14
Logical segregation and filtering 14
Network components 15
Wireless network communication 15
Remote access 15
Mitigating denial of service attacks 15

Outsourcing 16

Information security incident management 17

Contingency planning 18

Human resource security

Within the organization, there will be a number of people in trusted roles that have the ability to override or set aside the technical means for access control.

Trusted roles

Within the organization, there will be a number of people in trusted roles that have the ability to override or set aside the technical means for access control. The role of the system administrator is such a trusted role, which usually has full authorization for both logical access to the information systems and physical access to the facilities where the information systems are located. Any person who holds the trusted role of system administrator must have read and accepted by signing a separate liability and confidentiality agreement, before the person is assigned to the role and given administrative access to information systems and facilities.

Qualifications, experience, and clearance requirements

When hiring new personnel for trusted roles, there shall be a particularly thorough background check procedure in place which aims to ensure that the person is suitable for the task, can be considered reliable and have the necessary qualifications. The assessment will be based on:

- check of qualifications by specified and nonspecified references and academic records,
- check of claimed personal and contact information,
- economic risk assessment through credit checks,
- a check of public sources on the Internet, and
- interview with the subject aimed to identify potential conflicts of interest and other risk factors.

Assessment should be made for both contracted personnel as well as employees, whether it be a longer or shorter commitment. The results of each check shall be documented and retained. Staff who has worked within the organization for some time and proven to be competent and reliable, and have the necessary qualifications, is not required to be subject for a background check.

Training requirements

All staff should at hiring and periodically thereafter, at least every two years, undergo a brief training on information security matters. The training will address the following topics:

- reminder of confidentiality and responsibility,
- personal data protection,
- specific securityrelated customer requirements,
- incident management process,
- contingency plans,
- circumstances that could lead to conflicts of interest, and
- further provisions found in the employee handbook.

Agenda for the training and the attendee list shall be retained.

Termination and change of employment

When staff leave or are assigned other duties, a procedure shall be followed consisting of:

- reminder of the surviving terms of the confidentiality agreement,
- the return of equipment and any identity tokens, as well as
- revocation of all permissions that no longer apply.

Responsibility for following the procedures lies with the employee's immediate manager.

Segregation of duties

Segregation of duties should be applied where it is practically possible, to reduce the risk of omissions or deliberate abuse of the information systems. In particular, incorporating newly developed features into the production environment should require at least two persons working in collaboration. Either by one system administrator carrying out peer review of another system administrators work in a rapid deployment scenario, or by a formal handover procedure from the developers to the operations staff.

Asset management

Using the methodology described in the Information Security Manual, missioncritical information assets are identified and classified.

Responsibility for assets

Using the methodology described in the Information Security Manual, missioncritical information assets are identified and classified. Each such asset shall be assigned a system owner whose responsibility is to ensure the adequate protection of the information, the compliance with service agreements, regulatory requirements and applicable law, and the adherence to these information security guidelines.

Information classification

Structured information assets are classified using the methodology described in the Information Security Manual, founding the basis of the risk analysis by also relating the assets to the identified threats and the controls in place. For other types of information, there are three generic information classes established within the organization:

- Public information
- Internal information
- Confidential information

Each individual coworker who creates, obtains or compiles a document is responsible for
classifying it as confidential information if it contains information which, if the information is disclosed to unauthorized persons, may lead to significant harm to the organizations or to customers interests. Such documents shall be clearly marked as confidential and shall always be stored, transported, and communicated in encrypted form. The person managing the information is also responsible for only sharing it with other authorized persons.

All other unclassified information is by default internal information. Internal information is characterized by having a moderate sensitivity, whereas its disclosure to unauthorized persons may at worst lead to limited harm to the customers or the organizations interests. Internal information may be communicated in cleartext email, stored on general purpose devices and verbally spoken over the phone.

Only personnel working in public relations or with copywriting has the authority to classify information as public information. Information in this class is characterized by it being to the organizations advantage and in its best interest to disseminate the information.

Media handling

Disposal of storage media that may contain sensitive information requires professional
destruction, either carried out by the organizations own personnel or by a contracted party. Formal procedures shall exist to ensure such secure handling of media. If the media is handed to a contracted party for destruction, the media must be transported and destroyed maintaining an audit trail. Evidence from the destruction procedure shall be retained.

Access control

Staff with access to information systems, both users and administrators, should always be assigned unique personal system identities so that accountability is maintained.

Identity management

Staff with access to information systems, both users and administrators, should always be assigned unique personal system identities so that accountability is maintained.

Assignment and registration of such systems identities should also be done in an accountable manner and by a process that ensures that the right person is credibly linked to the system identity. Registration of identities and credentials used for subsequent identification should be made in a central registry against which all subsystems can verify a claimed identity.

Nonpersonal system identities must only be used when the accountability is maintained in other ways, such as through a physical access control system.

Authentication

Authentication is the process by which a claimed identity is proved. The authentication process may be based on one or more of the following identification factors:

- knowledge of something (such as a password),
- possession of something (e.g. a security token), or
- a certain inherent property (such as a fingerprint).

For missioncritical information systems, strong authentication is required. This implies at least two different of the above factors shall be recorded and then proved by the person.

Authorization

Authorization is the process whereas an identity is assigned certain privileges to an information system. The starting point for the management and assigning of authorization rules should always be based on the principle of least privilege for each system identity. Access control mechanisms should furthermore

- be able to control user access to information and systems according to a defined role profile, as well as
- allow accountability at the individual level on all operations and actions that users have requested in the system (both authorized and unauthorized).

Authorization rules should also be managed centrally in a register (e.g. directory service), against which the respective information system can verify the permissions associated with an identity. This facilitates the administration of authorization rules and reduces the risk of errors. All assignment, modification and revocation of privileges shall be approved by the responsible system owner. Approvals must be in writing to create an audit trail. Excerpts of all granted permissions shall be compiled on a quarterly basis and submitted to the system owner for review. This procedure aims to ensure that no stale permissions are assigned in information systems. Documentation from each review shall be retained.

Password management

Use of passwords may be used in different parts of the IT environment, possibly as part of a strong authentication procedure. Passwords should not be displayed, stored or transmitted in clear text or other inadequately protected form. Passwords should not be entered through untrusted devices where there is an increased risk that the password will be recorded or otherwise compromised. This applies especially to computers in public environments and mobile devices over which there are not sufficient control. Where only passwords are used for authentication there has to be particularly stringent requirements on password strength. A strong password is difficult to guess and takes a long time to crack even by bruteforce. There should be technical controls that assists staff in choosing strong passwords by:

- check that the selected password meets the length or complexity requirements, and
- prevent the reuse of previous passwords.

For password used for access to the organizations' information systems, the following complexity requirements apply:

- the password must contain at least 12 characters,
- the password should not appear in any dictionary or similar and must not be a simple combination of such words or names.
- the password must not contain simple keyboard patterns (e.g. qwerty).

To prevent information security incidents in one system from having cascade effects on other systems, passwords must never be reused between different systems, neither externally nor internally. Default passwords and other widely known passwords must be changed or removed before the system or equipment is connected to the network.

Audit logging

There should be an audit log that records all of the systems security events. Log information shall be transmitted in real time and concentrated to a separate log collection function in which the data can be protected separately from the sending system. Secure handling of the logs should be given particular attention in order not to destroy any evidence. This applies to the logging procedures as well as on subsequent review of security logs. The security log should be regularly analyzed after extraordinary system events.

Cryptography

Encryption can protect the confidentiality of the information as well as its authenticity and integrity.

Encryption systems and techniques should be used to protect information that is considered to be particularly at risk and for which other measures may not provide adequate protection. When using encryption techniques, emphasis should be given to the use of cryptographically strong and secure encryption algorithms. The software and products used for the encryption should be reliable, wellknown and scrutinized. As general rule, all network communications of sensitive information must be encrypted and authenticated. In addition, encryption on the application level should be employed as applicable with respect to the information's sensitivity and available encryption mechanisms.

Physical and environmental security

All of the missioncritical systems must be accommodated in secure areas within protected facilities using a defined physical perimeter with appropriate security barriers and entry controls.

The areas must be physically protected against unauthorized access, damage and disruption.

Physical access controls

Access to secured areas shall be restricted. Access controls may be provided manually (e.g. a staffed reception), or automated using electronic credentials. In both cases it is appropriate that both the entry as well as the exit is recorded to allow complete traceability. Within the organization there should be a central function for the management of access rights and credentials for physical access control.

Monitoring of secure areas

Secured areas inside the perimeter protection should be continuously monitored for unauthorized activity, using for example motion detectors and door contacts connected to the alarm system. Contractors, visitors and employees who do not normally have access to an area is required to be escorted or monitored continuously while in that area. This can be achieved by the presence of authorized personnel or by using the CCTV systems.

Power and environmental controls

Facilities must have backup power of sufficient capacity to power the missioncritical information systems during power outages. Facilities shall have a controlled environment that meets the technical equipment's requirements for temperature and humidity, which can compensate for the external effects such as those imposed through different weather conditions.

Fire prevention and protection from water exposures

Facilities shall have fire alarm and automatic fire suppression systems which are not liquid based. The technical equipment must also be protected against liquid flowing from leaks and flooding.

Alternative operating site

The organization shall maintain at least one alternative facility at a geographically separate location which is able to support a complete outage of any other facility used for missioncritical production. The alternative facility shall, in all material respects, comply with the same standards and requirements of physical protection, access control, environmental control, monitoring, emergency power and fire and water protection as the main site.

Operations security

The more order there is in the operating environment, the easier it is to detect and act upon critical security events.

Orderliness and automation

The more order there is in the operating environment, the easier it is to detect and act upon critical security events. Orderliness also reduces the risk of errors and serious information security incidents and facilitates the review of information systems security and functionality. For this reason, in the operating of the organizations information systems, as many tasks as practically possible should be automated.

Responsibilities

Responsibilities and procedures for the management and operations of all the missioncritical information systems should be established. For any such information system, there should be a person with designated primary responsibility for the technical operations of the system. The responsibility includes the development of appropriate operating procedures, automation of tasks, procedures for monitoring, documentation and implementation of security controls. System documentation should be available that describe the information system design, configuration, interfaces and dependencies.

Operating procedures

It is an integral part of information security to routinely develop and maintain the necessary operating procedures. All identified manual procedures related to the operations should be documented and contain clear step by step instructions.
This type of documentation shall cover the operation of the entire integrated system environment, including network communications, backup, maintenance and security of the operating systems.

Operating systems security controls

Protective measures at the operating system level is an important part in maintaining overall system security. In this, the organization should strive to use an as homogeneous and standardized operating environment as possible. These standard platforms should be delivered in a secure default configuration based on current best practice for the operating system.

The default setting should comprise of a minimum of services installed and activated. The default configuration should then be used for all production systems with minimal modifications. The advantages are a cleaner, clearer and simpler operating environment, easier administration, fewer patches to introduce and easier overall recovery of a failed system.

To reduce the risk for single vulnerabilities having severe consequences, the principle of security indepth should also be enforced. What combination of controls that should be included in such indepth protection varies depending on the information system function and its design.

The default setting of the standard operating system should however include functions to filter network communication flows in order to provide an extra layer of protection against networkdriven attacks. Operating system functions for the separation of services through the use of different system identities shall be enforces. Mandatory access control (MAC) functions should also be used to restrict certain services access to operating system functions.

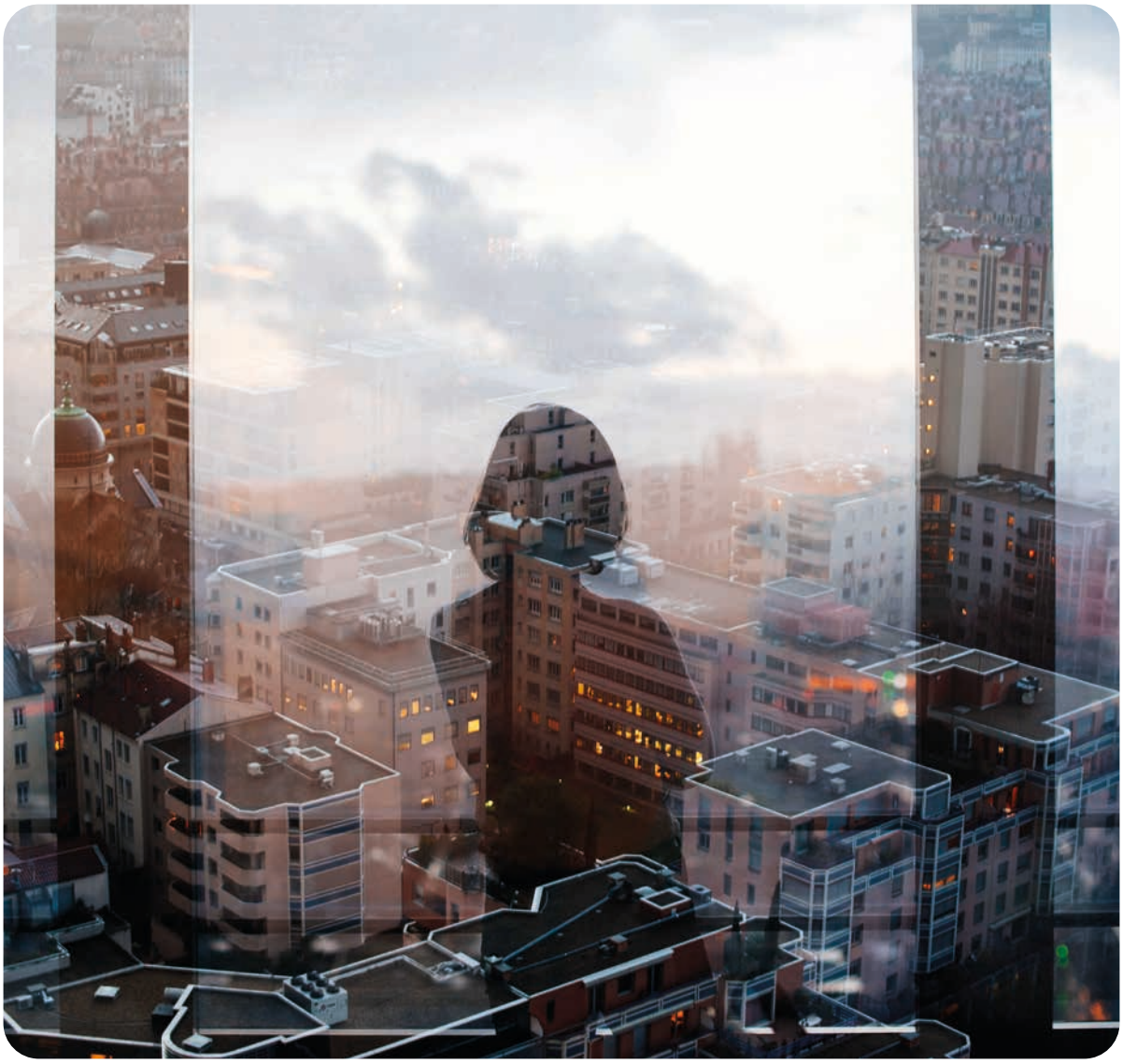
Isolation of critical components

Particularly sensitive or critical system components may require entirely or partly dedicated technical environments to reduce its exposure to various identified threats. The requirements for isolation shall for such systems be documented in a separate system security plan.

Configuration and change management

The system security must also be maintained as changes in configuration and new software are introduced in the operating environments. Any such changes should take place under strict control during planned and preannounced service windows.

At such a scheduled service window, the changes to be introduced should have been scoped, tested and accepted in a staging environment before being introduced in the missioncritical production environment. There should also be quick and easy rollback procedures in place, which enables the operators to back out of changes which later was determined to have negative side effects. Particularly critical changes to the systems should be carried out by at least two system administrators in tandem, to reduce the risk of mistakes.



There must also be an emergency procedure to follow for the immediate introduction of securitycritical software patches. Such patches may be introduced outside of the normal service intervals. Configuration should be managed through an automated configuration management system, which remotely monitors, controls and changes all production platforms.

Information backup

It is of utmost importance that the organization always has access to a number of generations of backups of missioncritical information assets. Procedures for backup must therefore be established. System documentation should indicate what is to be backed up, how often backups should be done and for how long backups should be retained.

Backups should be protected by cryptographic controls from disclosure and unauthorized manipulation. The key materials required for restore of information must be kept separate from the backups and only accessible to authorized system administrators.
Backups are also required to be stored at a secondary location, separate from the primary operating facility. The same security requirements for storage must be applied on all storage sites.

The disaster recovery planning should include regular testing of restore procedures in order to ensure that the backups are working and that restore can be completed within the required timeframes. In order to ensure that the requirements are met, the following topics should each year be checked and tested:

- the procedures for the backup and restore of information are correct and in compliance with business requirements, particularly regarding what is being backed up, how often backups are made and the number of generations which is retained, and
- the backups are readable and that missioncritical systems can be restored within the required timeframes.

In all restore operations, backups authenticity and integrity are required to be checked.

Monitoring

Monitoring of information systems is necessary for both efficiency reasons and for maintaining the security of the system. Monitoring enables by automatic means to detect important system events and define alerts to be triggered for notifying the system administrators.

Specific areas to be monitored from a security standpoint shall include:

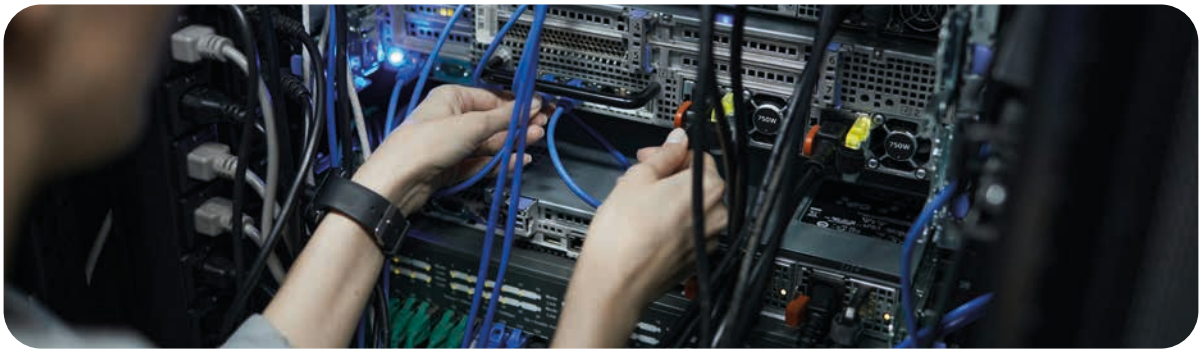
- utilization of system resources,
- frequency of unauthorized access attempts,
- anomalies (abnormal system events)
- systems and intrusion alarms, as well as
- time synchronization.

Monitoring should be done in real time and alerts shall be followed up upon within an agreed timeframe.

Time synchronization

Proper synchronization and exact function of system clocks is important to ensure the proper function of information systems and the validity of the security log information.

All system clocks should be set to an agreed standard time and synchronized with reliable time sources. The time synchronization must be monitored continuously.



Network securities

The controls for the security of the network environments should include logical and physical separation into security zones with filtering mechanisms limiting the nature and source of network activities that may access missioncritical computing resources.

Further controls shall include fault tolerant network designs and incorporating strategies to counter severe denial of service attacks. The responsibility for implementing, maintaining and improving these controls lies with the network managers.

Logical segregation and filtering

Logically sectioned networks and separation into security zones with filtered communication between them should be applied as a general method to address threats and vulnerabilities associated with communication over open networks.

The firewall systems are the organization's logical perimeter and security barrier to the Internet and other nontrusted networks. Firewall systems also extend into the production environment, maintaining the filtering policies between the organization's different logical security zones.

Firewall systems are therefore a crucial part of the organization's protection against network driven attacks and require careful management. The design of the combined firewall system should be consistent with good network planning resulting in a clear and reviewable ruleset.

Access to the firewall system and its configuration must be limited to the designated network managers whose responsibility is to monitor, control and maintain the firewall systems function and security.

Access to the management interfaces shall be limited to a few wellprotected sources. Administration interfaces should also be protected with available encryption mechanisms. All changes in the firewall configuration shall be conducted in accordance with the established procedures for change management.

Changes of the ruleset which may have material impact on information security shall be formally approved by the Security Manager before they are introduced. Documentation supporting such approvals must be retained.

Network components

The network components that supports the firewall system and maintains its function should be considered an integral part of the combined firewall system. The same requirements which applies to the firewall system should also be applied on other such missioncritical network components.

Wireless network communication

Wireless network communications can be used as a supplement to the wired LAN. The organization's critical systems and processes should however not be dependent on the wireless network confidentiality, integrity or availability.

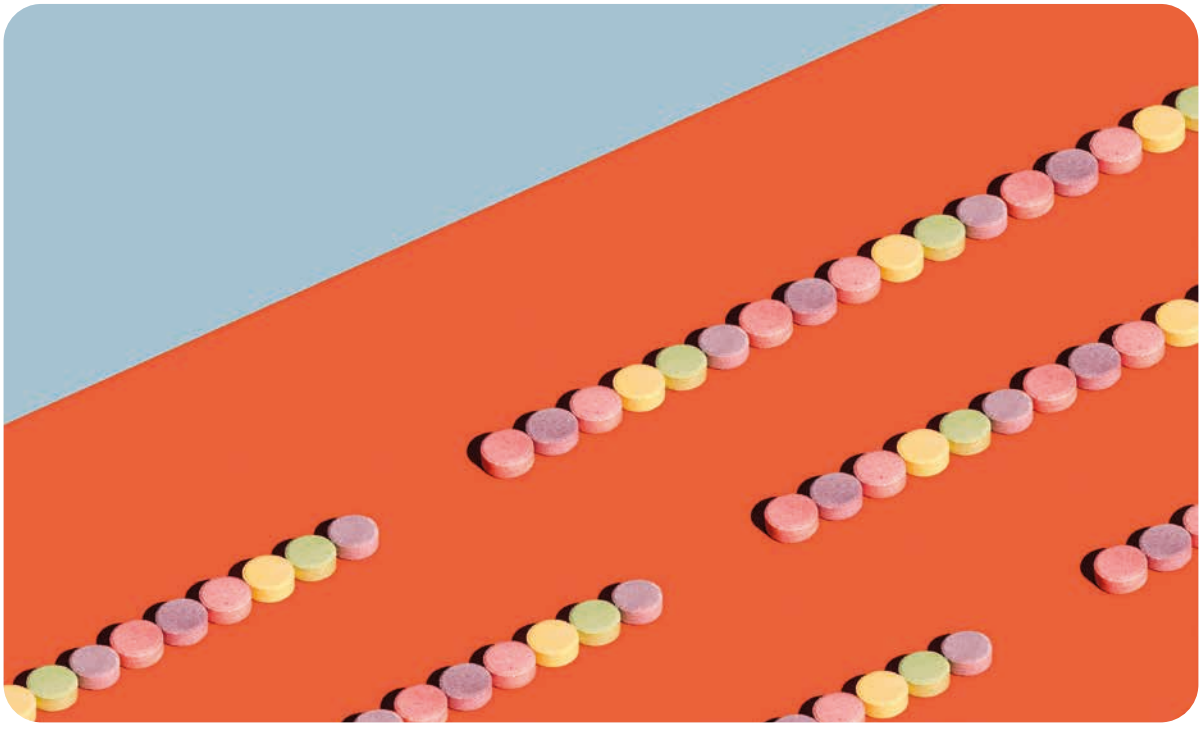
In any case where communication with internal missioncritical resources takes place over the air, such communication shall be subject to the same protection mechanisms as if it had originated from the Internet.

Remote access

The communication with remote missioncritical resources, such that any part of the communication flow extends outside of the organization's physical protected perimeter, shall be mutually authenticated and protected against eavesdropping and manipulation by strong cryptographic means. Focal points for such remote connections should also be filtered on the network level with the granularity and extent deemed practical from a management point of view.

Mitigating denial of service attacks

The organization must establish strategies to maintain preparedness for managing and mitigating severe and persistent denial of service attacks, including relevant technical countermeasures on the network level and established channels of contact with upstream providers and the national IT security incident center CERTSE. The state of readiness should be based on the currently identified level of threat against the organization. The strategies and procedures should be documented and regularly practiced.



Outsourcing

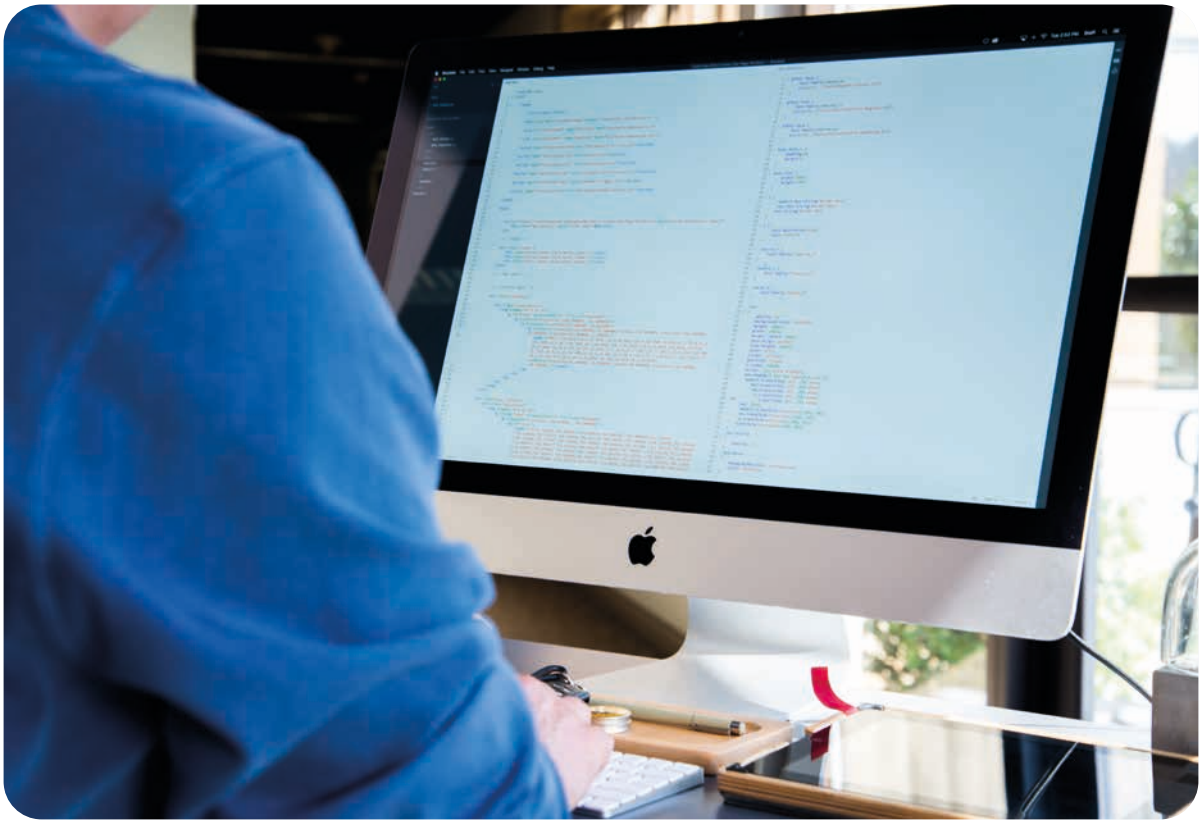
If mission-critical functions or processes are outsourced to another party, it shall be ensured that the outsourcing does not undermine the organization's ability to manage its risks.

Requirements imposed on providers shall include these guidelines for information security. The ability of monitoring compliance through audits shall be ensured.

When evaluating a new provider's ability to meet the security requirements, the following risk factors shall be taken into consideration:

- supplier's maturity in the management and control of information security risks,
- the maturity in the suppliers' internal controls,
- experience and ability to deliver the required services,
- financial position, and
- experience of compliance with regulatory requirements, security frameworks and standards.

Other indicators that may be included as parameters of a risk assessment of the supplier is previous experience of the provider, geographical presence, jurisdiction and regulatory regime, et cetera.



Information security incident management

An information security incident is defined as a real or perceived event of securitycritical nature that led or could have led to:

- disruptions or failure in information systems (including deliberately caused events),
- errors due to incorrect data, or
- compromise of confidentiality.

In order to effectively manage incidents, a number of measures shall be taken both during the urgent course of the incident event and in the subsequent work to restore normal operations. The incident management process is divided into four phases:

Damage control

When an incident becomes known, the highest priority action is to limit the event's negative effects. Since some incidents may imply laws or other regulations have been violated, it is important not to destroy evidence and this fact must be taken into account in the damagecontrol phase. Serious security incidents with high impact on the business should be notified without delay to the Security Manager.

Restoring of operations

The next phase of the incident management process aims to restore normal operations.

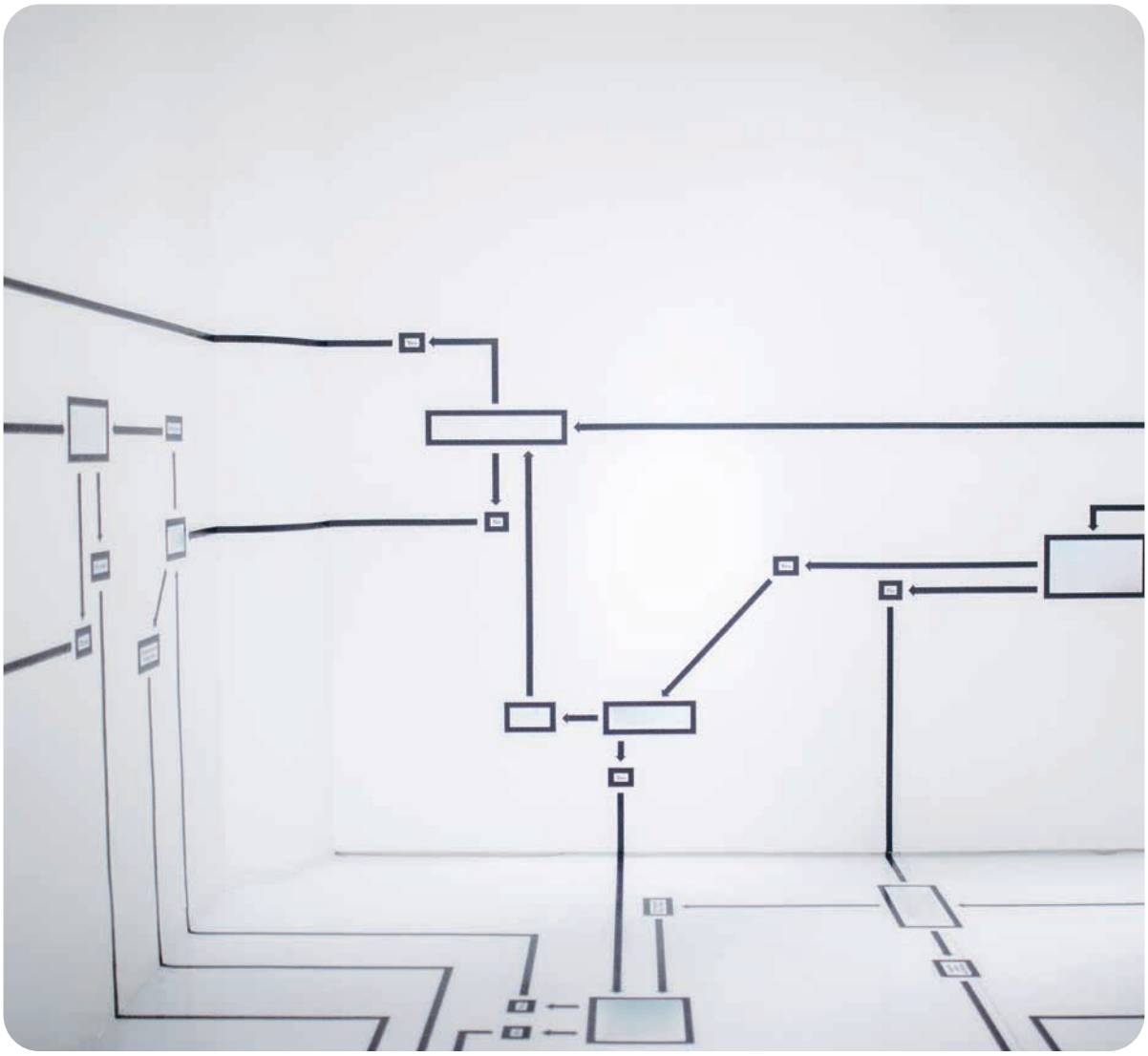
Rootcause analysis

As operations have been restored, the root cause of the incident shall be investigated, and measures shall be taken to prevent the event from reoccurring.

Reporting

When the rootcause analysis is done, a report describing the incident, its origin, extent and consequences shall be provided to the Security Manager. The report shall also include the actions taken (or planned to be taken) to prevent the incident from reoccurring.

Control evidence documentation for the incident management process shall be retained to create an audit trail for every occurrence of incidents.



Contingency planning

Contingency planning is the ability and preparedness to manage a major disruption in IT operations.

A contingency plan shall be established for all missioncritical information systems, so that it can be ensured that essential business processes can be completely restored within an agreed timeframe in the event of an emergency. The readiness of the emergency organization and ability to manage various forms of disruptions and recovery of information systems should be tested regularly, at least every two years. The result of such tests shall be documented, and the documentation shall be retained.

Safespring is a sustainable platform for secure cloud services

Safespring is a European provider of cloud and infrastructure as a service. Our platform is based on Open Source and open standards. Experience the benefits of the cloud where you retain control and digital sovereignty.

www.safespring.com/en

safespring

+46 (0)8-55 10 73 70 | hello@safespring.com
Rättarvägen 3, 169 68 Solna, Sweden

www.safespring.com