Threats

Responsibility

1 Lack of direction on information security from management.

The management does not focus on information security. Responsibilities towards line managers are not assigned. An information security policy and/or ISMS is missing.

Availability: p Integrity: p Confidentiality: p

Relevant controls from NEN-ISO/IEC 27002:2022: 5.1, 5.4, 5.5, 5.9, 5.29, 5.35, 5.36

2 Line managers do not take their responsibility for information security.

Line managers do not sufficiently ensure that information security is implemented correctly within their department. The ownership of information systems is not well invested. Security is not a permanent part of projects.

Availability: p Integrity: p Confidentiality: p

Relevant controls from NEN-ISO/IEC 27002:2022: 5.2, 5.4, 5.5, 5.9, 5.10, 5.12, 5.35, 5.36, 6.3

3 Insufficient attention to security within projects.

Insufficient attention to security within projects. Within projects (excluding software development) there is insufficient attention to security. This has negative consequences for new systems and processes that are introduced within the organization.

Availability: p Integrity: p Confidentiality: p

Relevant controls from NEN-ISO/IEC 27002:2022:
5.8, 5.19, 5.20, 5.21, 5.22, 5.23, 5.30, 5.37, 8.6, 8.27, 8.28, 8.32

4 Employees do not act according to what is expected of them.

The employees lack awareness towards information security and do not feel the need to contribute to it.

Availability: p Integrity: p Confidentiality: p

Relevant controls from NEN-ISO/IEC 27002:2022: 5.2, 5.4, 6.1, 6.2, 6.3, 6.4

Continuity and reliability of systems

5 Insufficient attention to security during software development.

Insufficient attention to security when developing software yourself or having it developed leads to a breach of information security.

Availability: p Integrity: p Confidentiality: p

Relevant controls from NEN-ISO/IEC 27002:2022: 5.32, 8.4, 8.25, 8.29, 8.30, 8.31, 8.33

6 Access to information is blocked.

Information on a system has been made inaccessible because malware (ransomware, wipers) or an attacker has encrypted or deleted this information.

Availability: p Integrity: - Confidentiality: s

Relevant controls from NEN-ISO/IEC 27002:2022:
5.6, 5.7, 5.15, 5.17, 5.21, 5.36, 6.3, 8.7, 8.8, 8.13, 8.22, 8.23

7 Network services are overloaded.

A network service is reduced in availability due to a malicious attack (DoS) or due to an unforeseen increase in the amount of requests or the resources required to handle a request. Requests can come from users, but also from other systems.

Availability: p Integrity: - Confidentiality: -

Relevant controls from NEN-ISO/IEC 27002:2022: 5.7, 5.20, 5.23, 8.6, 8.14

8 Attacks via systems that are not under their own control.

Due to insufficient control over the security of private and home equipment and other equipment from third parties, there is a risk of contamination with malware, for example.

Availability: p Integrity: - Confidentiality: p

Relevant controls from NEN-ISO/IEC 27002:2022: 5.19, 5.20, 6.7, 8.1, 8.7, 8.20, 8.21, 8.22

9 Failure of systems due to hardware errors.

Insufficient quality hardware can lead to system failure.

Availability: p Integrity: - Confidentiality: -

Relevant controls from NEN-ISO/IEC 27002:2022: 5.21, 7.8, 7.13, 8.13, 8.14

10 Failure of systems due to configuration errors.

Incorrect configuration of an application can lead to incorrect processing of information.

Availability: p Integrity: p Confidentiality: -

Relevant controls from NEN-ISO/IEC 27002:2022: 5.8, 5.21, 8.19, 8.27, 8.28, 8.29, 8.31, 8.32

11 Failure of systems due to software errors.

Errors in software can lead to system crashes or corruption of information stored in the system.

Availability: s Integrity: p Confidentiality: -

Relevant controls from NEN-ISO/IEC 27002:2022: 5.8, 5.21, 5.37, 8.9, 8.32, 8.34

12 Errors due to changes in other systems.

Errors arise in a system as a result of changes in linked systems.

Availability: p Integrity: p Confidentiality: -

Relevant controls from NEN-ISO/IEC 27002:2022: 5.8, 5.9, 5.22, 8.8, 8.19, 8.30, 8.32

Human behaviour

13 User errors.

Insufficient knowledge or too little control over other people's work increases the risk of human errors. User interfaces that are not tailored to the user level increase the chance of errors.

Availability: s	Integrity: p	Confidentiality: -

Relevant controls from NEN-ISO/IEC 27002:2022: 5.8, 6.3, 8.2, 8.12, 8.13, 8.23

14 Systems are not used for their intended purpose.

The lack of a policy on internet use, for example, increases the risk of abuse.

Availability: p	Integrity: -	Confidentiality: s

Relevant controls from NEN-ISO/IEC 27002:2022:
5.3, 5.10, 5.18, 5.32, 5.36, 6.2, 6.3, 6.4, 8.15, 8.19, 8.23

15 Taking away company assets.

Due to insufficient checks on the issue and incorrect inventory of company assets, there is a chance that the theft will not be noticed or will be noticed too late.

Availability: s	Integrity: -	Confidentiality: p

Relevant controls from NEN-ISO/IEC 27002:2022:
5.9, 5.11, 6.1, 7.2, 7.3, 7.4, 7.5, 7.8, 7.9, 8.1, 8.10, 8.12, 8.13

16 Policy is not followed by lack of sanctions.

Due to the lack of sanctions for violating rules, there is a chance that employees will not take the policy measures seriously.

Availability: s	Integrity: p	Confidentiality: p

Relevant controls from NEN-ISO/IEC 27002:2022: 6.3, 7.7, 7.9, 8.1, 8.21

17 Allowing external parties into the building or onto the network.

The admission of external parties, such as suppliers and project partners, can have consequences for the confidentiality of the information available within the premises or via the network.

Availability: -	Integrity: -	Confidentiality: p

Relevant controls from NEN-ISO/IEC 27002:2022: 5.19, 5.20, 6.1, 6.6, 7.3, 7.4

18 Loss of mobile devices and storage media.

The loss of mobile devices and storage media can lead to a breach of the confidentiality of sensitive information.

Availability: s	Integrity: -	Confidentiality: p

Relevant controls from NEN-ISO/IEC 27002:2022: 6.6, 7.9, 7.10, 8.1, 8.10, 8.12, 8.24

19 Abuse of someone else's identity.

Due to insufficient (possibility of) checking an identity, unauthorized access can be obtained to confidential information. This also includes social engineering, such as phishing and CEO fraud.

Availability: - Integrity: p Confidentiality: p

Relevant controls from NEN-ISO/IEC 27002:2022:
5.14, 5.16, 5.17, 6.1, 6.3, 6.4, 7.4, 7.7, 8.1, 8.2, 8.15, 8.26

20 Abuse of special rights.

Due to insufficient control of employees with special rights, such as system administrators, there is a risk of unauthorized access to sensitive information.

Availability: - Integrity: p Confidentiality: p

Relevant controls from NEN-ISO/IEC 27002:2022:
5.3, 5.10, 5.16, 5.19, 5.20, 6.1, 6.4, 6.5, 6.6, 8.2, 8.12, 8.15, 8.16, 8.17

21 Access rights set incorrectly.

Due to a missing, incorrect or unclear process for allocating and taking rights, a person can inadvertently have more rights. These rights can be abused by this person or by others (eg via malware).

Availability: - Integrity: p Confidentiality: p

Relevant controls from NEN-ISO/IEC 27002:2022:
5.9, 5.11, 5.15, 5.16, 5.17, 5.18, 6.5, 8.2, 8.3, 8.4, 8.9, 8.12, 8.18, 8.31

Access to information

22 Bad password usage.

Lack of password policies and employee awareness can lead to the use of weak passwords, the writing of passwords, or the use of the same password across multiple systems.

Availability: - Integrity: p Confidentiality: p

Relevant controls from NEN-ISO/IEC 27002:2022: 5.17, 6.3, 8.5, 8.12

23 Leaving workplaces unattended.

In the absence of a clear-desk and/or clear-screen policy, access can be gained to sensitive information.

Availability: - Integrity: s Confidentiality: p

Relevant controls from NEN-ISO/IEC 27002:2022:
5.9, 5.10, 5.12, 5.13, 5.14, 5.15, 5.33, 8.12, 8.26, 8.33

24 Uncertainty about classification and powers.

Due to a lack of clarity about the confidentiality of information and authority of persons, there is a risk of unauthorized access to sensitive information.

Availability: - Integrity: - Confidentiality: p

Relevant controls from NEN-ISO/IEC 27002:2022: 5.9, 7.10, 7.13, 7.14, 8.10, 8.12

25 Information on systems upon repair or disposal.

Sensitive information may leak if storage media or systems containing storage media are discarded or offered to third parties for repair.

Availability: - Integrity: p Confidentiality: p

Relevant controls from NEN-ISO/IEC 27002:2022:
5.6, 5.7, 5.8, 5.21, 5.22, 5.36, 8.7, 8.8, 8.12, 8.15, 8.16, 8.22, 8.23, 8.27, 8.28, 8.29, 8.32

26 Exploitation of vulnerabilities in applications or hardware.

Abuse of vulnerabilities in applications or hardware. Vulnerabilities in applications or hardware are misused (exploits) to gain unauthorized access to an application and the information stored therein.

Availability: - Integrity: p Confidentiality: p

Relevant controls from NEN-ISO/IEC 27002:2022:
5.6, 5.7, 5.21, 5.22, 7.12, 8.5, 8.8, 8.16, 8.20, 8.22, 8.29

27 Exploiting network security vulnerabilities.

Weaknesses in the security of the (wireless) network are misused to gain access to this network.

Availability: - Integrity: - Confidentiality: p

Relevant controls from NEN-ISO/IEC 27002:2022:
5.6, 5.7, 5.19, 5.20, 7.12, 8.5, 8.7, 8.8, 8.9, 8.12, 8.22, 8.32

28 Insufficient attention to security when outsourcing work.

Because external parties / suppliers do not have their information security in order, infringements can occur on the information to which they have access.

Availability: - Integrity: - Confidentiality: p

Relevant controls from NEN-ISO/IEC 27002:2022: 5.8, 5.19, 5.20, 5.21, 5.22, 5.23, 8.34

29 Information outside the protected environment.

Information that is taken outside the office for permitted use, for example, is no longer properly protected. Also consider Bring Your Own Device (BYOD).

Availability: - Integrity: - Confidentiality: p

Relevant controls from NEN-ISO/IEC 27002:2022: 5.23, 6.7, 7.9

30 Eavesdropping equipment.

Sensitive information is retrieved by means of keyloggers or network taps.

Availability: - Integrity: - Confidentiality: p

Relevant controls from NEN-ISO/IEC 27002:2022: 7.1, 7.2, 7.8, 7.12, 8.7, 8.12

Exchanging and storing information

31 Sending sensitive information insecurely.

Breach of confidentiality of information by sending information unencrypted.

Availability: - Integrity: s Confidentiality: p

Relevant controls from NEN-ISO/IEC 27002:2022: 5.12, 5.13, 5.14, 5.21, 6.4, 6.6, 7.10, 8.24, 8.26

32 Sending sensitive information to incorrect person.

Breach of confidentiality of information due to insufficient control of recipient.

Availability: - Integrity: - Confidentiality: p

Relevant controls from NEN-ISO/IEC 27002:2022: 5.14, 6.6, 7.10, 8.12, 8.24, 8.26

33 Loss of information due to expiration of the shelf life of the storage method.

Information is lost due to the medium becoming unreadable or the file format becoming outdated.

Availability: p Integrity: - Confidentiality: -

Relevant controls from NEN-ISO/IEC 27002:2022: 5.33, 7.10, 8.13

34 Incorrect information.

Unwanted actions as a result of incorrect company information or receiving incorrect information. This could be as a result of willful act or a mistake.

Availability: - Integrity: p Confidentiality: -

Relevant controls from NEN-ISO/IEC 27002:2022: 5.14, 5.19, 8.24, 8.26

35 Misuse of cryptographic keys and/or use of weak algorithms.

There is a risk of misuse of cryptographic keys due to incorrect or missing key management. The use of weak cryptographic algorithms provides a false sense of security.

Availability: - Integrity: p Confidentiality: p

Relevant controls from NEN-ISO/IEC 27002:2022: 5.31, 8.11, 8.24

36 Losing cryptographic keys

Losing cryptographic keys due to problems with the hardware in which they are stored, due to malicious actions, or due to human error, which makes the information encrypted with them inaccessible.

Availability: p Integrity: - Confidentiality: -

Relevant controls from NEN-ISO/IEC 27002:2022: 8.13, 8.24

Laws and regulations

37 Legislation on information in the cloud.

Legislation in some countries allows the government of such a country to view information stored in the cloud.

Availability: - Integrity: - Confidentiality: p

Relevant controls from NEN-ISO/IEC 27002:2022: 5.21, 5.22, 5.23, 5.31

38 Foreign law when visiting a country.

Legislation in some countries allows the government to require access to the data on systems included when visiting that country.

Availability: - Integrity: - Confidentiality: p

Relevant controls from NEN-ISO/IEC 27002:2022: 5.31, 6.3, 6.7, 8.1

39 Legislation on the use of cryptography.

Legislation in some countries allows governments to demand a copy of cryptographic keys.

Availability: - Integrity: - Confidentiality: p

Relevant controls from NEN-ISO/IEC 27002:2022: 5.31, 8.24

Incident handling

40 Incidents are not dealt with in a timely manner.

The consequences of incidents are unnecessarily large as a result. Within the company there is insufficient network monitoring and there is no central reporting point for security incidents.

Availability: - Integrity: s Confidentiality: p

Relevant controls from NEN-ISO/IEC 27002:2022: 5.24, 5.25, 5.26, 6.8, 8.7, 8.15, 8.16

41 Information for dealing with incidents is lacking.

System administrators do not have enough technical information about the problem to solve it. There is no action plan, which means that the incident continues unnecessarily long.

Availability: p Integrity: p Confidentiality: p

Relevant controls from NEN-ISO/IEC 27002:2022:
5.5, 5.9, 5.25, 5.26, 5.27, 5.28, 5.29, 8.15, 8.16, 8.17

42 Recurrence of incidents.

Causes of incidents are not held accountable for their actions. Managers have insufficient insight into recurring incidents, so that they do not manage them.

Availability: p Integrity: s Confidentiality: p

Relevant controls from NEN-ISO/IEC 27002:2022: 5.24, 5.27, 5.36, 6.4, 6.8

Physical security

43 Unauthorized physical access.

The lack of access passes, visibility of entrances and awareness among employees increases the chance of unauthorized physical access.

Availability: - Integrity: - Confidentiality: p

Relevant controls from NEN-ISO/IEC 27002:2022: 5.29, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8

44 Fire.

The lack of fire detectors and fire extinguishing equipment increases the consequences of a fire.

Availability: p Integrity: - Confidentiality: -

Relevant controls from NEN-ISO/IEC 27002:2022: 5.29, 5.30, 7.1, 7.2, 7.3, 7.5, 7.8, 7.11, 8.13, 8.14

45 Explosion.

Explosions can cause damage to the building and equipment and casualties.

Availability: p Integrity: - Confidentiality: -

Relevant controls from NEN-ISO/IEC 27002:2022: 5.29, 5.30, 7.1, 7.5, 7.7, 7.8, 8.13, 8.14

46 Flooding.

Flooding can damage computers and other business assets.

Availability: p Integrity: - Confidentiality: -

Relevant controls from NEN-ISO/IEC 27002:2022: 5.29, 5.30, 7.1, 7.5, 7.7, 7.8, 7.11, 8.13, 8.14

47 Pollution of the environment.

Contamination of the environment can lead to the organization being (temporarily) unable to work.

Availability: p Integrity: - Confidentiality: -

Relevant controls from NEN-ISO/IEC 27002:2022: 5.29, 5.30

48 Failure of facility resources (gas, water, electricity, air conditioning).

Failure of facility resources can mean that one or more business units can no longer do their job.

Availability: p Integrity: - Confidentiality: -

Relevant controls from NEN-ISO/IEC 27002:2022: 5.30, 7.11, 7.12, 8.14

49 Vandalism.

Damage to or destruction of company property as a result of an undirected action, such as vandalism or rodents.

Availability: p Integrity: - Confidentiality: -

Relevant controls from NEN-ISO/IEC 27002:2022: 7.4, 7.5, 7.8, 7.11, 7.12

Business continuity

50 Unavailability of third-party services.

The unavailability of third-party services due to system failure, bankruptcy, unplanned contract termination or unacceptable changes in services (for example, due to a company takeover).

Availability: p Integrity: - Confidentiality: -

Relevant controls from NEN-ISO/IEC 27002:2022: 5.8, 5.22, 5.23, 5.30, 5.37, 8.14

51 Software is no longer supported by the publisher.

Security patches will no longer be issued for software that is no longer supported. Also think of Excel and Access applications.

Availability: p Integrity: - Confidentiality: -

Relevant controls from NEN-ISO/IEC 27002:2022: 5.8, 5.22, 5.30, 5.37, 8.28, 8.30

52 Losing important knowledge when employees are unavailable.

Employees who leave the company or who cannot be deployed for a long time due to an accident possess knowledge that is therefore no longer available.

Availability: p Integrity: - Confidentiality: -

Relevant controls from NEN-ISO/IEC 27002:2022: 5.22, 5.37