(How) does NEN 7510 contribute to getting ready for NIS2?

Health and Youth Care Inspectorate

Johan Krijgsman, coordinating/specialist inspector

Agenda

- The work of the inspectorate
- NIS 2 highlights
- NIS 2 Risk management measures
- NEN 7510
  - Basics
  - How does it fit to NIS2?
  - Knowing you are compliant

Our field of work

Social care sector

Nursing homes, home care institution, institutions for the disabled, mental healthcare institutions, care for asylum seekers and detainees

Public health

Local health authorities, prevention, emergency response teams

Youth care

Curative care

Hospitals, private clinics, rehabilitation institutions

Manufacturers, distributors and laboratories

Blood (products) and tissue, medication (as well as research), medical devices and technology

Primary care providers and independent care professionals

General practitioners, pharmacies, oral and dental care, obstetricians and maternity care

A large and diverse field of work

30 laws

Thousands of guidelines
drawn up by care providers

EUR 100 billion
healthcare budget

1.3 million
healthcare professionals

What follows from NIS2?

Register

- Entities must register themselves.
- There will be a registration portal for this

Take Measures

- Entities are responsible for organising their information security.
- Entities must perform risk management
- Entities must take appropriate measure to manage risks and to avoid and handle incidents.

Report incidents

- Entities must report significant incidents within 24 hours.
- Factors that determine if an incident is significant:
  - severe operational disruption
  - financial loss
  - considerable damage to others

What follows from NIS2?

Inform

- Entities must :
  - inform the recipients of services about impact on these services from significant incidents;
  - inform the recipients of services how they can respond in case they may be affected by a significant cyber threat

Management body

- Management bodies of entities can be held liable for infringements of duties on cybersecurity risk measures.
- Members of the management bodies must follow training.

Assistance

- The Cyber Security Incident Response Team (CSIRT) responds to incidents and provides assistance the entities concerned.
- **Z-CERT** is the CSIRT for the healthcare sector.

Risk management measures (art. 21)

a. policies on risk analysis and information system security;

b. incident handling;

c. business continuity, such as backup management and disaster recovery, and crisis management;

d. supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

e. security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

f. policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

g. basic cyber hygiene practices and cybersecurity training;

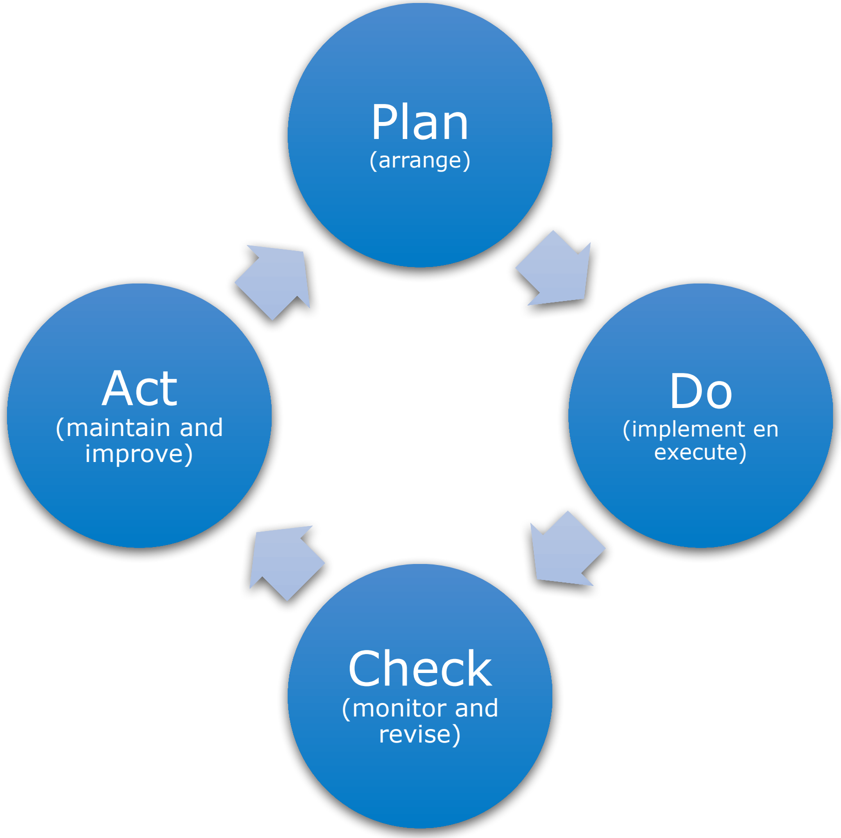
h. policies and procedures regarding the use of cryptography and, where appropriate, encryption;

i. human resources security, access control policies and asset management;

j. the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

NEN 7510: Information security in healthcare

NEN 7510: ISMS and the quality cycle



Plan
(arrange)

Do
(implement en execute)

Check
(monitor and revise)

Act
(maintain and improve)

Risk analysis and control measures

RISK ANALYSIS AND RISK MANAGEMENT

APPROPRIATE CONTROL MEASURES: ‘DECLARATION OF APPLICABILITY’

NORMATIVE APPENDIX A LISTS POSSIBLE CONTROL MEASURES

Most article 21 areas are covered in NEN7510

NIS2

- policies on risk analysis ...
  - ...and information system security;
- Incident handling

NEN 7510

- 6.1.2 risk evaluation for information security
- 6.13 treatment of information security risks
- 5.2 policy
- A16 management of information security incidents

More examples

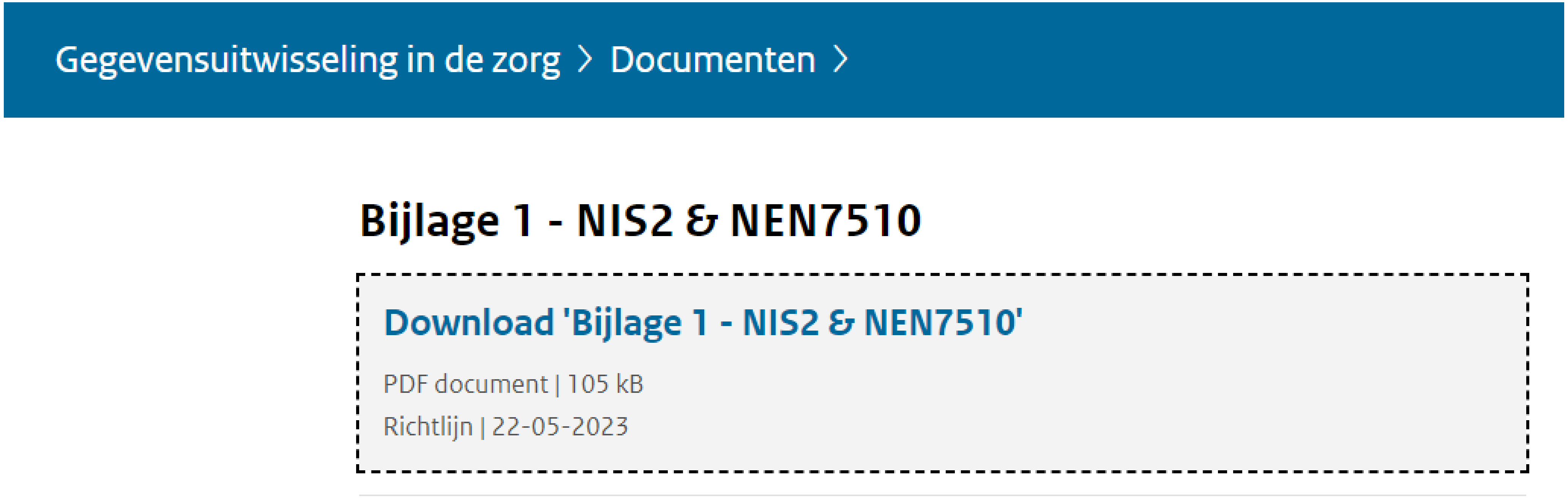
NIS2

- supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
- human resources security, access control policies and asset management;

NEN 7510

- A15 Supplier relationships
- A7 Secure Personnel
- A9 Access control
- A8 Management of company resources

Mapping efforts can be found online



Gegevensuitwisseling in de zorg › Documenten ›

Bijlage 1 - NIS2 & NEN7510

Download 'Bijlage 1 - NIS2 & NEN7510'

PDF document | 105 kB

Richtlijn | 22-05-2023

[Bijlage 1 - NIS2 & NEN7510 | Richtlijn | Gegevensuitwisseling in de zorg]

What may need additional attention?

Business continuity and crisis management;

- ➔ NEN-EN-ISO 22301 (Security and resilience - Business continuity management systems – Requirements) offers additional guidance

Reporting significant incidents

- ➔ You already report data protection incidents

Training for management

- ➔ NEN 7510 already requires training for all personnel

Knowing if you are compliant with NEN 7510

Independent assessment

Appropriate scope

Regular / with planned intervals
On significant change

Independent
- Internal auditor (?) or independent manager (?)
- External organisation

Expert
- Appropriate skills and experience

How to avoid common pitfalls?

- Make sure management is involved / avoid purely technical focus
- Make sure your information security policy status is clear
- Up to date risk analysis
- Clear instructions for personnel
- Clear status of risk management measures
- Manage your suppliers, don’t just trust them blindly
- Plan (!) monitoring and audits
- Arrange independent assessments

For the kind of good and safe care we wish for the ones we love.