NIS2 DIRECTIVE

ISO 27001

Riadh Brinsi www.linkedin.com/in/riadhbrinsi

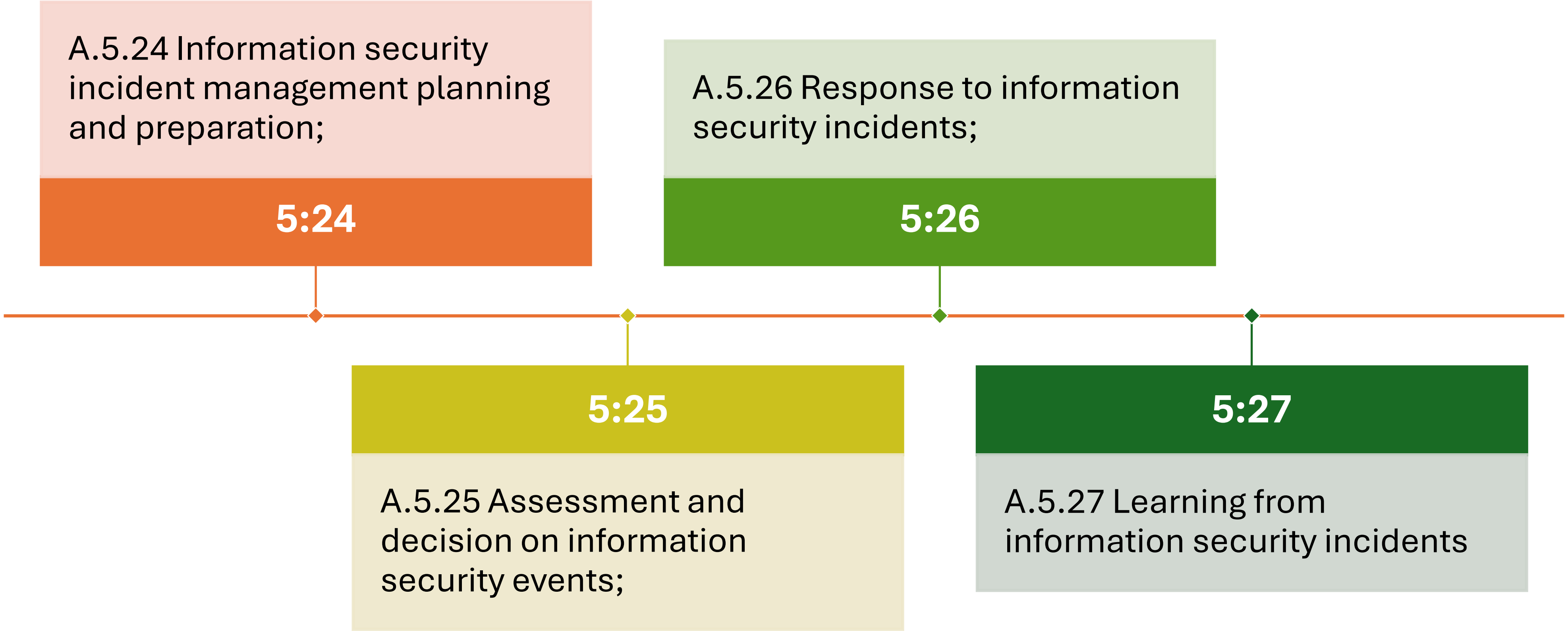
Policies on risk analysis and information system security

ISO 27001

- 5.2 Policy;
- 6.1.2 Information security risk assessment;
- 6.1.3 Information security risk treatment;
- A.5.1 Policies for information security

Riadh Brinsi www.linkedin.com/in/riadhbrinsi

Incident handling



5:24

A.5.24 Information security incident management planning and preparation;

5:25

A.5.25 Assessment and decision on information security events;

5:26

A.5.26 Response to information security incidents;

5:27

A.5.27 Learning from information security incidents

Riadh Brinsi www.linkedin.com/in/riadhbrinsi

Business continuity, such as backup management and disaster recovery, and crisis management

- A.5.29 Information security during disruption
- A.5.30 ICT readiness for business continuity;
- A.8.13 Information backup;
- A.8.14 Redundancy of information processing facilities

Riadh Brinsi www.linkedin.com/in/riadhbrinsi

NIS2 DIRECTIVE

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

ISO 27001

A.5.19 INFORMATION SECURITY IN SUPPLIER RELATIONSHIPS;

A.5.20 ADDRESSING INFORMATION SECURITY WITHIN SUPPLIER AGREEMENTS;

A.5.21 MANAGING INFORMATION SECURITY IN THE ICT SUPPLY CHAIN

NIS2 DIRECTIVE

Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure

ISO 27001

A.5.19 Information security in supplier relationships;

A.5.20 Addressing information security within supplier agreements

NIS2 DIRECTIVE

Policies and procedures to assess the effectiveness of cybersecurity risk-management measures

ISO 27001

- 9.1 Monitoring, measurement, analysis and evaluation;
- 9.2 Internal audit;
- 9.3 Management review;
- A.5.35 Independent review of information security;
- A.5.36 Compliance with policies and standards for information security

ISO 27001

Basic cyber hygiene practices and cybersecurity training

A.5.1 Policies for information security;

A.6.3 Information security awareness, education and training

NIS2 DIRECTIVE

Policies and procedures regarding the use of cryptography and, where appropriate, encryption

ISO 27001

A.8.24 Use of cryptography

Riadh Brinsi www.linkedin.com/in/riadhbrinsi

Human resources security, access control policies and asset management

- A.5.15 Access control;
- A.5.16 Identity management;
- A.5.17 Authentication information;
- A.5.18 Access rights;
- A.5.9 Inventory of information and other associated assets;
- A.6.1-A.6.8 People controls

Riadh Brinsi www.linkedin.com/in/riadhbrinsi

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

ISO 27001

- A.5.14 Information transfer;
- A.5.17 Authentication information;
- A.8.5 Secure authentication;
- A.8.20 Network controls;
- A.8.21 Security of network services

References:

- Images :

  - https://miro.medium.com/v2/resize:fit:940/1*W1jAaMMs7GrykzfZcOyb_w.png
  - https://global-engineering-technologies.com/wp-content/uploads/2017/05/iso-27001-logo.gif

- Webographie:
  - NIS 2 and ISO 27001 | Instant 27001
  - Public
  - Network & Information Security Directive (NIS2) (kpmg.com)ations Office (europa.eu)
  - NIS 2 Directive: A Guide to EU's Latest Security Requirements (cobalt.io)