NIS 2 INFORMATION SECURITY CHECKLIST

INFORMATION SECURITY POLICY

Policy Framework

- ✓ Set out the approach to managing network and information system security
- ✓ Ensure alignment with business strategy and objectives
- ✓ Define clear network and information security objectives
- ✓ Establish risk tolerance levels based on the risk appetite

Commitment and Resources

- ✓ Commit to meeting all applicable security requirements
- ✓ Commit to continual improvement of security measures
- ✓ Ensure availability of necessary resources (staff, finances, tools)

Communication & Acknowledgment

- ✓ Communicate the policy to employees and stakeholders
- ✓ Obtain acknowledgment and understanding from relevant parties

Roles and Responsibilities

- ✓ Define roles and responsibilities
- ✓ Ensure roles are aligned with company needs

Monitoring and Approval

- ✓ Implement measures to monitor policy implementation
- ✓ Note the formal approval date by management

Documentation and Policies

- ✓ List all required documents
- ✓ Specify and list topic-specific policies

CENTRIPETAL

NIS 2 INFORMATION SECURITY CHECKLIST

ROLES, RESPONSIBILITIES AND AUTHORITIES

Assignment of Roles

- ✓ Define and assign security responsibilities
- ✓ Communicate roles to management

Review and Update

- ✓ Regularly review roles and responsibilities
- ✓ Document the results of reviews

Reporting

- ✓ Ensure all personnel and third parties follow security policies

Policy Adherence

- ✓ Ensure all personnel and third parties follow security policies

Conflict Management

- ✓ Segregate conflicting duties and responsibilities, where applicable

Role Coverage

- ✓ Ensure security roles are adequately covered, based on company size

This checklist can be used as a guideline to start implementing a NIS2 compliant information security policy. Reach out to Centripetal to see how we can help your organization improve the security posture of your network and information systems.

CENTRIPETAL