유럽 연합

NIS2 지침

(Directive EU 2022/2555)

유럽 연합 전역의 높은 공통 사이버보안 수준을 위한 조치

CISO 및 컴플라이언스 담당자를 위한 한국어 요약

문서 참조 정보

항목	내용
공식 명칭	Directive (EU) 2022/2555
채택일	2022년 12월 14일
공포일	2022년 12월 27일 (OJ L 333/80)
발효일	2023년 1월 16일
각국 국내법 전환 기한	2024년 10월 17일
폐지 대상	Directive (EU) 2016/1148 (NIS1)

> 본 문서는 2022년 12월 14일 채택된 EU NIS2 지침의 비공식 요약본으로, 권위 있는 번역본이 아닙니다. 구속력 있는 해석을 위해서는 OJ L 333/80, 27.12.2022의 공식 원문을 참조하시기 바랍니다.

목차

1. 경영진 요약

NIS2 지침 (Directive EU 2022/2555)은 2022년 12월 14일 유럽 의회 및 이사회가 채택한 EU의 범용 사이버보안 기준 지침입니다. 2024년 10월 18일부로 기존 NIS1 지침(Directive 2016/1148)을 폐지하고 대체합니다.

검토 결과, NIS1이 연합 전반의 사이버 복원력 향상에 기여하기는 하였으나, 현재 및 미래의 사이버보안 위협에 대응하기에는 불충분하다는 결론이 내려졌습니다. NIS2는 적용 범위를 대폭 확대하고, 통일된 기준을 도입하며, 리스크 관리 및 사고 보고 의무를 강화하고, 보다 강력한 집행 조항을 마련합니다.

지침의 다섯 가지 기둥

1. **확대된 적용 범위**: 더 많은 분야와 기업이 규제 대상에 포함됩니다.
2. **강화된 리스크 관리**: Article 21에 따라 10가지 최소 기술적·조직적 조치가 의무화됩니다.
3. **신속하고 단계적인 사고 보고**: 24시간 조기 경보, 72시간 사고 통보, 1개월 최종 보고서.
4. **경영진의 책임**: 고위 경영진이 개인적 책임을 질 수 있습니다.
5. **억제력 있는 제재**: 연간 전 세계 매출의 최대 2% 또는 최대 1,000만 유로의 행정 제재금.

2. 목적 및 법적 근거

지침의 법적 근거는 내부 시장의 기능 확립 및 보장을 위해 각국 규정의 근접화 조치를 허용하는 **유럽 연합 기능 조약(TFEU) Article 114**입니다.

지침의 주요 목표는 다음과 같습니다.

- 회원국 간의 큰 편차를 해소하고 공통 최소 사이버보안 규칙을 수립합니다.
- 국경을 초월한 협력 및 정보 공유를 위한 효과적인 메커니즘을 구축합니다.
- 오늘날의 위협 환경을 반영하여 사이버보안 의무 대상 분야 및 활동 목록을 갱신합니다.
- 의무의 효과적인 이행을 보장하는 집행 및 구제 메커니즘을 제공합니다.
- 중요 인프라 운영자 및 디지털 서비스 제공자의 사이버 복원력을 강화합니다.

이 지침은 개인 데이터 보호에 관한 EU 법률(GDPR, Regulation EU 2016/679) 및 전자 통신 프라이버시(Directive 2002/58/EC)의 적용을 침해하지 않고 이에 부합하는 방식으로 적용됩니다.

3. NIS1에서 NIS2로: 새 규제가 필요한 이유

2016년에 발효된 NIS1은 EU 최초의 수평적 사이버보안 규제였습니다. 검토 과정에서 적용 범위 결정이 회원국 재량에 상당 부분 맡겨져 회원국 간 이행 방식에 심각한 차이가 나타났으며, 이로 인해 내부 시장이 분열된 것으로 드러났습니다.

NIS1의 주요 문제점

문제 영역	NIS1 상황	NIS2 해결책
적용 범위 결정	회원국 재량에 맡김; 실무상 편차 심각.	EU 전역에 통일된 '규모 기준' 규칙 적용 (중소기업 및 대기업).
분야 목록	대상 분야 수 제한; 디지털 경제의 상당 부분 제외.	분야 적용 범위 대폭 확대; 디지털 인프라, 공공행정, 우주 등 포함.
사고 보고	단일 단계; 마감 기한 및 내용이 회원국마다 상이.	다단계 보고: 24시간 조기 경보 + 72시간 통보 + 1개월 최종 보고서.
리스크 관리	일반적 표현; 구체적인 최소 조치 불명확.	Article 21에 10가지 의무적 최소 조치 범주 명시.
제재금	회원국마다 매우 다른 수준으로 이행.	EU 전역 조화된 최대 제재금 (1,000만 유로 / 매출의 2%).
고위 경영진 책임	불명확.	경영진이 컴플라이언스에 대해 개인적 책임을 지며 의무 교육 수료.

NIS2는 NIS1의 업데이트가 아니라, 연합 전역에 **단일하고 조화된 집행 가능한 사이버보안 프레임워크**를 구축하기 위해 설계된 완전한 대체 법령입니다.

4. 적용 범위 및 제외 영역

지침은 주로 EU 내에서 **Annex I (고위험) 또는 Annex II (기타 중요)** 분야에서 운영되며 중소기업 이상의 규모 요건을 충족하는 기관에 적용됩니다. 집행위원회 권고 2003/361/EC 부속서 Article 2에 따르면, 중소기업은 직원 250인 미만이고 연간 매출이 5,000만 유로 이하(또는 대차대조표 총액 4,300만 유로 이하)인 기업입니다. NIS2는 중소기업 기준 이상의 기관을 포착합니다. 즉, 적용 대상의 실질적 최저 기준은 직원 50인 또는 매출 1,000만 유로(동일 권고에서 "소기업"의 상한선)입니다.

규모에 관계없이 적용 대상인 기관

- 공중 전자 통신망 사업자 및 공개적으로 이용 가능한 전자 통신 서비스 제공자
- 신뢰 서비스 제공자 (eIDAS Regulation EU 910/2014 적용 대상)
- 최상위 도메인(TLD) 등록 기관 및 DNS 서비스 제공자
- 회원국 내 서비스의 유일한 제공자이거나, 서비스 중단이 공공 안보, 보건 또는 안전에 중대한 영향을 미칠 수 있는 기관
- 모든 중앙 공공행정 기관 (회원국이 국내에서 정의)

적용 범위 제외 영역

주로 **국가 안보, 공공 안보, 국방 또는 법 집행** (범죄 예방, 수사, 탐지 및 소추) 분야에서 활동하는 공공 기관은 지침의 적용 범위에서 제외됩니다. 제3국에 있는 회원국의 외교 및 영사 공관, 그리고 폐쇄형 시스템에서 사용되는 신뢰 서비스도 제외됩니다.

5. 주요 정의

지침의 올바른 해석을 위해 몇 가지 기본 개념을 명확히 이해해야 합니다.

용어	정의
네트워크 및 정보 시스템	전자 통신 네트워크, 디지털 데이터를 처리하는 모든 장치 또는 장치 그룹, 그리고 그 운영·사용·보호·유지를 위해 처리되는 모든 디지털 데이터.
사이버보안	네트워크 및 정보 시스템, 사용자 및 기타 사람들을 사이버 위협으로부터 보호하기 위해 필요한 모든 활동.
사고	저장·전송·처리되는 데이터 또는 네트워크 및 정보 시스템을 통해 제공되거나 접근 가능한 서비스의 가용성, 진위성, 무결성 또는 기밀성을 침해하는 사건.
중대 사고	관련 기관의 서비스에 심각한 운영 중단 또는 재정 손실을 초래했거나 초래할 수 있거나, 다른 자연인 또는 법인에게 상당한 물질적 또는 비물질적 피해를 야기했거나 야기할 수 있는 사고.
사이버 위협	네트워크 및 정보 시스템을 손상시키거나, 방해하거나, 그 외의 방식으로 불리한 영향을 미칠 수 있는 잠재적인 상황, 사건 또는 행위.
중대 사이버 위협	기술적 특성상 기관의 네트워크 및 정보 시스템, 사용자 또는 기타 사람들에게 상당한 물질적 또는 비물질적 피해를 야기함으로써 심각한 영향을 미칠 잠재성을 가진다고 가정할 수 있는 사이버 위협.
취약점	사이버 위협에 의해 악용될 수 있는 ICT 제품 또는 서비스의 약점, 취약성 또는 결함.
아차사고 (Near miss)	저장·전송·처리되는 데이터 또는 네트워크 및 정보 시스템을 통해 제공되거나 접근 가능한 서비스의 가용성, 진위성, 무결성 또는 기밀성을 침해할 수 있었으나, 실제 발생이 성공적으로 차단된 사건.
CSIRT	Computer Security Incident Response Team. 사고 처리를 담당하는 기술 팀.
ENISA	European Union Agency for Cybersecurity. 지침 이행에 있어 중심적인 자문·지원 역할을 수행.

6. 기관 분류: 필수 기관과 중요 기관

지침은 적용 대상 기관 전체를 두 가지 주요 범주로 구분합니다. 이 구분은 의무사항과 감독·집행 체계가 어떻게 적용되는지를 결정합니다.

기준	필수 기관	중요 기관
분야	Annex I, 고위험 분야	Annex II, 기타 중요 분야 (및 Annex I의 중소기업)
규모	대기업 (직원 250인 이상 또는 매출 5,000만 유로 이상)	중소기업 (직원 50인 이상 249인 이하)
감독 체계	사전 및 사후 감독 모두 적용	증거 또는 민원에 기반한 사후 감독만 적용
최대 행정 제재금	1,000만 유로 또는 전 세계 연간 매출의 2% 중 높은 금액	700만 유로 또는 전 세계 연간 매출의 1.4% 중 높은 금액
고위 경영진 제재	임시 직무 정지 적용 가능	임시 직무 정지 미적용

> **중요 참고사항:** NIS1에 따라 '필수 서비스 운영자'로 지정된 기관의 경우, 회원국은 해당 기관을 NIS2에 따른 필수 기관으로 직접 분류하도록 결정할 수 있습니다. 또한 Directive 2022/2557 (CER)에 따라 '중요 기관'으로 지정된 모든 기관은 자동으로 NIS2의 필수 기관으로 간주됩니다.

7. 적용 대상 분야 (Annex I 및 Annex II)

Annex I, 고위험 분야

해당 분야의 대기업은 필수 기관이며, 중소기업은 중요 기관입니다.

분야	하위 분야 / 기관 유형
에너지	전력 (발전, 송전, 배전, 공급); 지역 냉난방; 석유 (파이프라인, 생산, 저장, 송유); 천연가스; 수소 생산, 저장 및 송수
운송	항공 (항공사, 공항, 항공 교통 관제); 철도 (인프라 관리자, 철도 운영자); 수상 (해운/내수로 운영자); 도로 (지능형 교통 시스템, 도로 운영자)
은행업	Regulation (EU) 575/2013에 따른 신용 기관
금융 시장 인프라	거래소 및 중앙청산소(CCP)
보건	의료 제공자; EU 참조 실험실; 의약품 R&D 수행 기관; 의약품 제조업체; 공중 보건 비상 사태 시 중요 의료 기기 제조업체 (Regulation (EU) 2022/123 기준)
음용수	인간 음용 목적의 용수 공급자 및 배급자
하수	도시 하수, 가정 하수 또는 산업 하수를 수집, 처리 또는 정화하는 기관
디지털 인프라	인터넷 교환 지점(IXP); DNS 서비스 제공자 (루트 DNS 제외); TLD 등록 기관; 클라우드 컴퓨팅 서비스 제공자; 데이터 센터 서비스 제공자; 콘텐츠 전송 네트워크(CDN) 제공자; 신뢰 서비스 제공자; 공중 전자 통신망/서비스 제공자
ICT 서비스 관리 (B2B)	관리 서비스 제공자(MSP); 관리 보안 서비스 제공자(MSSP)
공공행정	회원국이 정의한 중앙 및 지역 정부 기관
우주	회원국 또는 민간이 운영하는 지상 인프라 운영자

Annex II, 기타 중요 분야

분야	하위 분야 / 기관 유형
우편 및 택배	우편 서비스 제공자 (택배 서비스 포함)
폐기물 관리	폐기물 수거, 재활용 및 처리 서비스 제공 기관
화학물질	화학물질 생산, 가공 및 유통에 종사하는 기관
식품	식품 생산, 가공 및 도매 유통에 종사하는 대기업
제조	의료 기기/체외 진단 의료 기기; 컴퓨터, 전자 및 광학 제품; 전기 장비; 기타 기계 및 장비; 자동차, 트레일러 및 세미트레일러; 기타 운송 장비 제조
디지털 서비스 제공자	온라인 마켓플레이스; 온라인 검색 엔진; 소셜 네트워킹 서비스 플랫폼
연구	상업적 목적의 연구를 수행하는 연구 기관

8. 회원국 의무사항

지침은 민간 기관뿐만 아니라 회원국에도 의무를 부과합니다. 각 회원국은 다음 조치를 취해야 합니다.

국가 사이버보안 전략. 명확한 전략적 목표, 우선순위 및 거버넌스 프레임워크를 갖춘 국가 사이버보안 전략을 채택합니다. 전략은 공급망 보안, 랜섬웨어, 중소기업 지원, 오픈소스, 적극적 사이버 방어 등의 주제를 다룹니다.

관할 당국. 지침의 이행 및 감독을 보장하기 위해 하나 이상의 관할 당국을 지정하거나 설립합니다.

단일 창구(SPOC). EU 차원의 국경 간 조정을 담당할 단일 연락 창구를 지정합니다.

CSIRT. 사고 처리, 사전적 모니터링, 조율된 취약점 공개, 국내외 협력을 담당하는 하나 이상의 CSIRT를 설립하거나 지정합니다.

기관 목록. 필수 기관, 중요 기관 및 도메인 등록 서비스 제공 기관의 목록을 유지·정기 갱신하고 집행위원회에 전달합니다.

조율된 취약점 공개. CSIRT를 조율 기관으로 지정하고 취약점 연구자를 위한 법적 명확성을 증진합니다.

상호 지원. 국경 간 감독 및 집행에서 다른 회원국에 상호 지원을 제공합니다.

중소기업 지원. 소기업 및 마이크로기업을 위한 지침, 무료 도구, 국내외 연락 창구를 제공합니다.

9. 사이버보안 리스크 관리 조치 (Article 21)

지침의 가장 중요한 기술적 조항은 Article 21입니다. 필수 기관 및 중요 기관이 이행해야 하는 최소 기술적·운영적·조직적 조치를 열거합니다. 이 접근 방식은 **'전위험(all-hazards)' 관점**에 기반합니다. 사이버 공격뿐만 아니라 물리적 피해, 자연재해, 장비 고장, 인적 오류와 같은 위협도 포함됩니다.

Article 21, 10가지 최소 조치

#	조치	설명
1	리스크 분석 및 정보 시스템 보안 정책	모든 리스크 분석 및 일반 정보 보안 정책의 서면 수립.
2	사고 처리	사고 예방, 탐지, 대응 및 복구 프로세스.
3	업무 연속성	백업 관리, 재해 복구 및 위기 관리.
4	공급망 보안	공급업체의 보안 관행 포함; 직접 공급업체와의 계약에 사이버보안 조항 포함.
5	네트워크 및 정보 시스템 획득, 개발 및 유지 관리의 보안	취약점 처리 및 공개를 포함한 전체 수명 주기에 걸친 보안.
6	조치 효과성 평가	리스크 관리 조치의 효과성 정기 평가.
7	기본 사이버 위생 관행 및 보안 교육	직원 대상 사이버 위생 관행 및 인식 교육.
8	암호화 및 암호화 정책	암호화 사용 정책; 적절한 경우 종단 간 암호화 적용.
9	인적 자원 보안, 접근 통제 및 자산 관리	인사 보안 점검, 권한 부여 및 자산 목록 관리.
10	다중 인증 및 보안 통신	적절한 경우 MFA 적용, 지속적 인증, 보안 음성/영상/텍스트 통신, 비상 시 보안 통신 시스템.

이러한 조치는 기관의 리스크 노출도, 규모, 분야별 중요성 및 사고의 잠재적 영향을 고려하여 **비례의 원칙**에 따라 적용됩니다.

10. 사고 보고 의무 (Article 23)

지침의 가장 중요한 운영적 혁신은 다단계 사고 보고 체계입니다. 필수 기관 또는 중요 기관은 심각한 운영 중단, 재정 손실 또는 타인에 대한 상당한 영향을 초래하는 것으로 정의된 **중대 사고**를 다음의 기한 내에 CSIRT 또는 관할 당국에 보고해야 합니다.

단계	기한	내용
조기 경보	사고 인지 후 24시간 이내	사고가 불법적/악의적 행위로 인한 것이라는 의혹; 국경 간 영향 가능성; CSIRT 인지를 가능하게 하는 기본 정보.
사고 통보	사고 인지 후 72시간 이내	조기 경보 갱신; 심각도, 영향 및 가능한 경우 침해 지표(IoC).
중간/최종 보고서	사고 통보 후 1개월 이내	사고에 대한 상세한 설명, 심각도 및 영향; 악용된 위협 유형; 취해진 완화 조치 및 계획; 해당 시 국경 간 영향.
진행 보고서	최종 보고서 기한 시점에 사고가 여전히 진행 중인 경우	사고의 현재 상태에 대한 진행 보고서; 사고 처리 완료 후 1개월 내 최종 보고서 제출.

서비스 수신자에 대한 통보: 중대 사이버 위협이 발생할 가능성이 있는 경우, 기관은 부당한 지체 없이 무료로 서비스 수신자에게 가능한 완화 조치와 적절한 경우 위협 자체를 명확하고 이해하기 쉬운 언어로 통보해야 합니다.

아차사고 및 자발적 보고

사고 외에도, 기관은 CSIRT 또는 관할 당국에 **아차사고 및 중대 사이버 위협을 자발적으로 보고할 수 있습니다**. 지침의 적용 범위에 해당하지 않는 기관도 자발적으로 보고할 수 있습니다. 자발적 보고는 보고자에게 추가적인 의무를 부과하지 않습니다.

> **실무적 영향:** 24시간 조기 경보 기한은 기관이 사고 탐지 즉시 활성화할 수 있는 사이버 사고 대응 계획과 커뮤니케이션 흐름을 미리 갖추도록 강제합니다. 수동적이고 분산된 프로세스로는 이 기한을 맞추기 매우 어렵습니다.

11. 공급망 보안

최근 몇 년간 발생한 주요 사이버 공격의 대부분은 조직 자체에 대한 직접 공격이 아니라, 공급업체 및 소프트웨어 제공자를 통해 목표 조직에 도달했습니다. 따라서 지침은 공급망 리스크를 리스크 관리 의무의 핵심에 둡니다.

- 기관은 공급업체 및 서비스 제공자의 제품/서비스에 대한 **품질, 보안 관행 및 안전한 개발 프로세스**를 평가해야 합니다.
- **직접 공급업체와의 계약에 사이버보안 요건을 포함**해야 합니다.
- **관리 보안 서비스 제공자(MSSP)** 선정 시 특별한 주의를 기울여야 합니다. 이러한 제공자는 공격자에게 고가치 표적입니다.
- 협력 그룹은 집행위원회 및 ENISA와 함께 중요 공급망에 대한 **조율된 보안 리스크 평가**를 수행합니다 (5G 네트워크에 대해 수행한 것과 같은 방식으로).
- **비기술적 리스크 요인**도 평가 범위에 포함됩니다. 제3국의 공급업체에 대한 부당한 영향력 가능성, 숨겨진 취약점/백도어, 제공자 의존성 등이 해당됩니다.

12. 경영진의 책임

지침은 사이버보안이 기술 부서에만 국한된 주제에서 벗어나 **고위 경영진의 직접적인 책임 영역**으로 이관되도록 보장합니다. Article 20에 따라, 필수 기관 및 중요 기관의 경영진은 다음의 역할을 수행합니다.

- Article 21에 따른 **리스크 관리 조치를 승인**하고 그 이행을 감독할 책임이 있습니다.
- 해당 의무 위반에 대해 **개인적인 책임을 질 수 있습니다**.
- 충분한 지식과 역량을 갖추기 위해 사이버보안 교육을 정기적으로 받아야 합니다.
- 직원들도 유사한 교육을 받도록 장려해야 합니다.

> **중요:** 필수 기관의 경우, 관할 당국은 고위 경영진(CEO 또는 법적 대표자 수준)에게 **임시 직무 정지**를 적용하도록 요청할 수 있습니다. 이는 다른 모든 집행 수단이 소진된 이후에만 적용 가능한 최후의 수단입니다.

13. EU 차원의 협력 구조

지침은 회원국 간의 효과적인 협력을 보장하는 다양한 구조를 규율하거나 강화합니다.

구조	기능
협력 그룹	전략적 수준의 협력 지원; 격년 작업 프로그램 수립; 지침 문서 발간; 중요 공급망에 대한 조율된 리스크 평가 수행.
CSIRTs Network	운영 수준의 협력; 사고 정보 공유; 상호 지원; 공동 대응.
EU-CyCLONe	유럽 사이버 위기 연락 기관 네트워크; 대규모 사고 및 위기에서 기술적 수준과 정치적 수준을 연결; 영향 분석 수행.
ENISA	유럽 취약점 데이터베이스 설립 및 유지; 기술 지원 제공; 지침 개발; 회원국 사이버 위생 정책 모니터링.
IPCR 체계	EU 통합 정치 위기 대응 체계 (Council Implementing Decision 2018/1993); 대규모 위기에 대한 연합 차원의 위기 관리.
EU-CSIRTs CVD 조율 기관	각 회원국의 CSIRT가 국경 간 조율된 취약점 공개를 관리하는 조율 기관으로 지정.

제3국과의 협력: EU는 TFEU Article 218에 따라 제3국 또는 국제 기구와 국제 협정을 체결할 수 있습니다. 이러한 협정은 연합의 이익 및 데이터 보호를 보장하면서, 해당 당사자가 협력 그룹, CSIRTs Network 또는 EU-CyCLONe의 활동에 참여하도록 허용할 수 있습니다.

14. 감독 및 집행

지침은 두 기관 범주에 대해 서로 다른 감독 체계를 규정합니다. **필수 기관**은 사전 및 사후 감독 모두에 적용되는 반면, **중요 기관**은 증거 또는 민원에 기반한 사후 감독만 받습니다.

관할 당국의 감독 권한

- 현장 조사 및 원격 감독 실시
- 표적화된 보안 감사 요청 (기관이 비용을 부담할 수 있음)
- 보안 스캔 명령
- 리스크 관리 조치 준수에 관한 문서 요청
- 지침 위반이 의심되는 행위에 관한 정보 요청
- 필요한 경우 개인 데이터 및 트래픽 데이터 접근을 포함한 정보 요청

적용 가능한 집행 조치

- 경고 및 구속력 있는 지시 발부
- 지정된 기간 내에 특정 조치 또는 취약점 개선 이행 명령
- 리스크 관리 조치 검증을 위한 독립 감사 명령
- 위반의 성격에 관해 서비스 수신자에게 통보하도록 기관에 명령
- 공개 성명 발표 (기관명 및 위반 성격 공개)
- 필수 기관에 대해 (최후 수단으로): 인증 또는 인가의 임시 정지 및 고위 경영진에 대한 임시 직무 정지
- 행정 제재금 부과 또는 부과 요청

15. 행정 제재금

지침은 회원국이 적용하는 행정 제재금에 대해 **EU 전역에 조화된 최대 한도**를 설정합니다. 이 한도는 GDPR과 유사하게 기관의 전 세계 매출에 연동됩니다.

기관 유형	최대 금액 (높은 금액 적용)
필수 기관	1,000만 유로 또는 전 세계 연간 매출의 2%
중요 기관	700만 유로 또는 전 세계 연간 매출의 1.4%

제재금 결정 요소

- 위반의 성격, 심각도 및 기간
- 야기된 물질적 또는 비물질적 피해
- 위반이 고의적인지 과실에 의한 것인지 여부
- 피해 예방 또는 완화를 위해 취해진 조치
- 책임 정도 및 이전 위반 이력
- 관할 당국과의 협력 정도
- 기타 가중 또는 감경 요소

제재금은 **비례의 원칙**에 따라야 하며, 적용 시 방어권, 무죄 추정의 원칙, 효과적인 구제 권리 등 기본권을 준수해야 합니다. 회원국은 국내법 위반에 대해 형사 제재를 규정할 수도 있으나, **일사부재리(ne bis in idem)** 원칙에 따라 동일한 행위에 대해 누구도 두 번 처벌받을 수 없습니다.

16. 이행 일정 및 전환

날짜	사건
2022년 12월 14일	유럽 의회 및 이사회의 지침 채택
2022년 12월 27일	EU 관보 공포 (OJ L 333/80)
2023년 1월 16일	지침 발효 (공포 후 20일)
2024년 10월 17일	회원국의 국내법 전환 기한
2024년 10월 18일	지침 적용 개시
2024년 10월 18일	Directive (EU) 2016/1148 (NIS1) 폐지
2025년 4월 17일	회원국의 필수 기관 및 중요 기관 목록 집행위원회 제출 기한
2027년 10월 17일 이후	집행위원회의 지침 이행 정기 검토 (매 36개월)

> **중요:** NIS2는 지침이므로 직접 적용되지 않습니다. 각 회원국이 지침을 자국 법률로 전환해야 합니다. 따라서 기관에 적용되는 구체적인 의무와 제재는 해당 기관이 운영되는 회원국이 채택한 국내 전환법에 따라 달라집니다.

17. EU 역외 기업에 대한 영향

NIS2는 EU 지침이지만, EU 시장에 서비스를 제공하거나 EU 소재 중요 기관에 공급하는 기업을 중심으로 EU 역외 기업에도 상당한 영향을 미칩니다.

직접적인 영향을 받는 EU 역외 기업

- EU에서 서비스를 제공하는 비EU 소재 **DNS 제공자, 클라우드 서비스 제공자, 데이터 센터 운영자, CDN 제공자, 관리 서비스 및 관리 보안 서비스 제공자, 온라인 마켓플레이스, 검색 엔진, 소셜 네트워킹 플랫폼**은 EU 대리인을 선임하고 지침 의무를 준수해야 합니다.
- EU 자회사 또는 지사를 보유한 비EU 기업은 해당 법인을 통해 지침의 적용을 받을 수 있습니다.
- EU 필수 기관 또는 중요 기관에 제품/서비스를 공급하는 비EU 공급업체는 고객사가 부과하는 **공급망 보안 계약 요건** (Article 21(2)(d))의 적용을 받습니다.
- EU 디지털 인프라 또는 금융 기관에 서비스를 제공하는 비EU MSP/MSSP는 직접 적용 범위에 포함될 수 있습니다.

간접적인 영향

- EU 고객사의 공급망 리스크 평가로 인해 비EU 공급업체는 사이버보안 기준을 높여야 합니다.
- 지침이 도입하는 기준(ISO/IEC 27001, ENISA 가이드라인 등)은 글로벌 시장에서 **사실상의 참조 기준**으로 자리잡고 있습니다.
- 비EU 국가들도 자국 사이버보안 법제 개발 시 NIS2를 참조 기준으로 활용하는 사례가 증가하고 있습니다.

18. 실무 컴플라이언스 로드맵 (10단계)

다음 10단계 로드맵은 EU 내에서 운영되는 기업과 NIS2 기준에 자발적으로 준하고자 하는 기업 모두를 위한 실무 지침입니다.

단계	활동
1. 적용 범위 확인	회사가 Annex I 또는 Annex II 분야에 해당하는지 확인하고, 규모 기준을 충족하는지 판단하며, 범주(필수/중요)를 식별합니다.
2. 갭 분석	기존 정보 보안 관리 체계를 Article 21의 10가지 조치 범주와 비교하여 평가하고 갭을 파악합니다.
3. 거버넌스 구조	이사회/고위 경영진 수준에서 책임, 보고 체계 및 승인 프로세스를 수립하고 정기 교육 프로그램을 마련합니다.
4. 정책 및 문서화	정보 보안 정책, 리스크 관리 정책, 사고 대응 정책, 허용 사용 정책 및 기타 문서를 작성하거나 갱신합니다.
5. 리스크 평가	자산 목록 작성, 위협 분석 및 전위험 접근 방식의 리스크 평가를 수행하고 리스크 수용 기준을 수립합니다.
6. 기술적 통제 이행	MFA, 암호화, 네트워크 분할, 제로 트러스트 아키텍처, 로그 관리, SIEM, EDR/XDR, 백업 및 재해 복구 솔루션을 구현합니다.
7. 사고 대응 역량	사고 대응 계획 문서화; 역할/책임 배정; 24시간 조기 경보 커뮤니케이션 흐름 수립; 모의 훈련 실시.
8. 공급망 관리	공급업체 목록 작성; 리스크 수준별 분류; 계약 템플릿에 사이버보안 조항 추가; 정기 감사 실시.
9. 교육 및 인식 제고	전 직원 대상 연간 사이버 위생 교육 실시; 경영진 특화 교육 제공; 피싱 시뮬레이션 수행.
10. 지속적 개선	내외부 감사 실시; KPI 추적; 각 사고에서 교훈 도출; 리스크 평가 연간 갱신; 인증 취득 추진 (ISO/IEC 27001, EU 사이버보안 인증).

19. 결론 및 평가

NIS2 지침은 유럽 연합의 사이버보안 기준을 대폭 높입니다. 단순히 기술적 요건을 부과하는 데 그치지 않고, 사이버보안을 **기업의 거버넌스 구조와 사업 운영의 통합적 요소**로 만듭니다.

지침의 강점

- **광범위한 적용 범위**: EU-27 전역에서 약 18개 분야, 100,000개 이상의 기관이 적용 대상.
- **조화화**: EU 전역에 통일된 기준과 집행 체계를 통해 내부 시장에서의 공평한 경쟁 환경 조성.
- **거버넌스 중심**: 고위 경영진에게 책임을 부여함으로써 사이버보안이 기업의 모든 계층에 침투하도록 보장.
- **공급망 강조**: 현대 공격의 대부분이 공급망을 통해 이루어진다는 현실에 대응.
- **협력 구조**: 협력 그룹, CSIRTs Network 및 EU-CyCLONe을 통한 다층적 EU 차원의 조율.

비판 및 과제

- 회원국의 전환 지연 및 편차로 인해 실무상 EU-27 전반의 균일한 이행이 불충분한 상황.
- 특히 중소기업의 경우 컴플라이언스 비용과 기술 역량 격차 해소가 심각한 과제.
- 충분한 성숙도가 갖추어지기 전에 24시간 조기 경보 기한이 이행될 경우 보고 흐름이 형식적이거나 오류가 발생할 수 있음.
- 분야별 규제(DORA, 금융; eIDAS, 신뢰 서비스; 분야별 항공 규제 등)와의 중복 영역이 기관에 복잡성을 야기할 수 있음.

종합 평가

NIS2는 사이버보안을 기술적 문제에서 **업무 연속성, 기업 거버넌스, 고객 신뢰**의 문제로 재정의합니다. EU에서 운영되거나 EU와 상호작용하는 기관에게 컴플라이언스는 법적 의무이자 운영 복원력을 강화하는 수단입니다.

비EU 기업에게 NIS2는 EU 시장 접근을 위한 새로운 **사실상의 기준**으로 자리잡고 있으며, 전 세계적으로 사이버보안 기대치를 높이고 있습니다. 조기 컴플라이언스는 계약상 의무 이행을 용이하게 하고 전반적인 사이버 복원력을 향상시킵니다.

> **최종 안내:** 본 문서는 지침의 주요 조항을 요약한 것입니다. 귀 기관에 특정한 컴플라이언스 요건을 확인하려면 공식 원문 (OJ L 333/80, 27.12.2022), 귀 회원국의 국내 전환법, 분야별 규정을 검토하시고 필요한 경우 법률 및 사이버보안 전문가의 조언을 구하시기 바랍니다.

출처

- Directive (EU) 2022/2555, EUR-Lex CELEX number 32022L2555
- Official Journal of the EU L 333/80, 27 December 2022
- ENISA, European Union Agency for Cybersecurity (www.enisa.europa.eu)
- European Commission Digital Strategy portal (digital-strategy.ec.europa.eu)

Rediacc의 NIS2 추가 자료

본 요약서는 지침의 구조와 의무사항을 정리한 것입니다. rediacc.com의 동반 가이드는 해당 의무사항을 구체적인 운영 및 조달 결정으로 전환하는 방법을 설명합니다.

세 가지 동반 가이드

- **Article 21(2)(d)와 자체 호스팅.** 데이터 플레인이 귀사의 테넌시를 벗어나지 않을 때 제3자 ICT 등록부가 줄어드는 이유. 2026년 DPA를 재협상하는 CISO 및 조달 담당자를 위한 안내.
- **형식 없는 지속적 효과성.** Article 21(2)(e), (f) 및 23을 종합적으로 검토. 주간 훈련을 현실적으로 만드는 일정 시간 포크(fork), 그리고 포렌식 수준의 아티팩트 없이는 맞출 수 없는 Article 23 보고 일정. SRE 및 운영 담당자를 위한 안내.
- **NIS2 컴플라이언스의 구조적 비용.** 중간 규모 필수 기관이 조용히 구축하고 있는 5가지 도구 스택, 자체 호스팅 컨트롤 플레인이 없애주는 것, 그리고 어느 방향이든 귀사가 부담하는 항목. 갱신 주기를 앞둔 CFO 및 구매 담당자를 위한 안내.

자료 위치

세 가지 가이드 모두, 본 요약서의 PDF 다운로드와 함께 아래에서 확인하실 수 있습니다.

rediacc.com/resources/nis2-directive-summary

Rediacc OÜ는 에스토니아에 등록된 자체 호스팅 인프라 플랫폼입니다 (법인 등록번호 17363830, 부가가치세 번호 EE102920091). 본 제품은 보안 프로그램의 대체재가 아니라, 기존의 백업, DR 및 테스트 데이터 도구가 제거할 수 없는 데이터 플레인 공급업체 리스크를 없애주는 툴링 레이어입니다. 무료 커뮤니티 티어 및 월 $349부터 시작하는 유료 티어가 있습니다.

> 본 문서 및 동반 가이드는 교육 목적의 자료입니다. 귀 기관에 특정한 컴플라이언스 결정을 위해서는 법률 전문가의 조언과 귀 관할 국가의 국내 전환법을 참조하시기 바랍니다.