KPMG

EU 네트워크 & 정보 보안 지침 (EU NIS2)

EU NIS2 대응을 위한 IT와 OT 보안 이해하기

EU NIS2 Directive 대비서

—

2023년 6월

Abstract

본 문서에서는 EU NIS (The Network and Information Security) 를 개정한 NIS2에 대한 개요와 NIS2의 범위에 속하는 기업들이 준비해야 할 IT보안 및 OT보안에 대한 정보를 제공합니다.

추가로, NIS2에 대한 KPMG의 의견과 생각을 공유하고, NIS2 지침과 국제 산업 표준들을 비교하며 IT와 OT를 모두 보유하고 있는 기업들이 고민해야 할 내용들에 대해서 논의할 것입니다.

새로운 요구사항이 반영된 NIS2 규제들을 준수하고 사이버 리스크를 줄여 비즈니스를 지속적으로 운영할 수 있는 방법으로 사이버보안 전략, 거버넌스, 커뮤니케이션을 통제하고 개선하는 방법에 대해서 설명합니다.

마지막으로 본 문서는 NIS2 지침을 위한 과제들을 알아보는 것과 동시에 기업들의 사이버보안 역량을 강화할 수 있는 내용을 제공합니다.

Contents

핵심 요약서

초기 NIS 지침(2016)을 개정

16개의 핵심 분야가 범위 내에 포함

세계가 점점 더 연결되고, IT 및 OT 인프라가 통합되면서 기업들은 사이버 보안 사고의 가능성이 커지고 있음을 알게 되었습니다. NIS2 지침은 유럽연합(EU)이 사이버 보안 문제에 적극적으로 대응하면서 공표되었고, 전반적으로 NIS2 지침은 주요기반시설의 공급망과 밀접한 조직 및 기업들에 초점을 두고 있습니다.

- 2016 | NIS1 발표
- 2022년 12월 | NIS2 공표
- 2023년 7월 | 현재
- 2024년 10월 | NIS2 세부 요구사항 발표
- 2025년 1월 | NIS2 적용

현재 NIS2 지침의 세부 요구사항 발표가 아직 1년 이상 남아있기 때문에 주요 기업들은 현재 NIS2를 대응해야 하는 것에 의문을 가질 수 있습니다. 하지만 우리가 제안을 드리고 싶은 것은 사이버 보안 거버넌스와 위험관리에 대한 대응 수준을 높이고 새로운 의무에 대비해야 한다는 것입니다. 예를 들어 OT보안을 위해서 사용되는 국제 표준인 IEC 62443 시리즈와 같은 규정으로 향후의 사이버 보안지침에 대해 준비해야만 합니다.

NIS2는 아래 16개의 핵심 분야를 포함하고 있습니다.

위험분석	사고대응	백업/복구
공급망보안	네트워크 보안	정보시스템 보안
위험관리	인식 & 교육	암호화
인적보안	접근통제	자산관리
다중인증	유지보수	감사 & 추적
시스템 & 통신 보안		

NIS2 16개 도메인

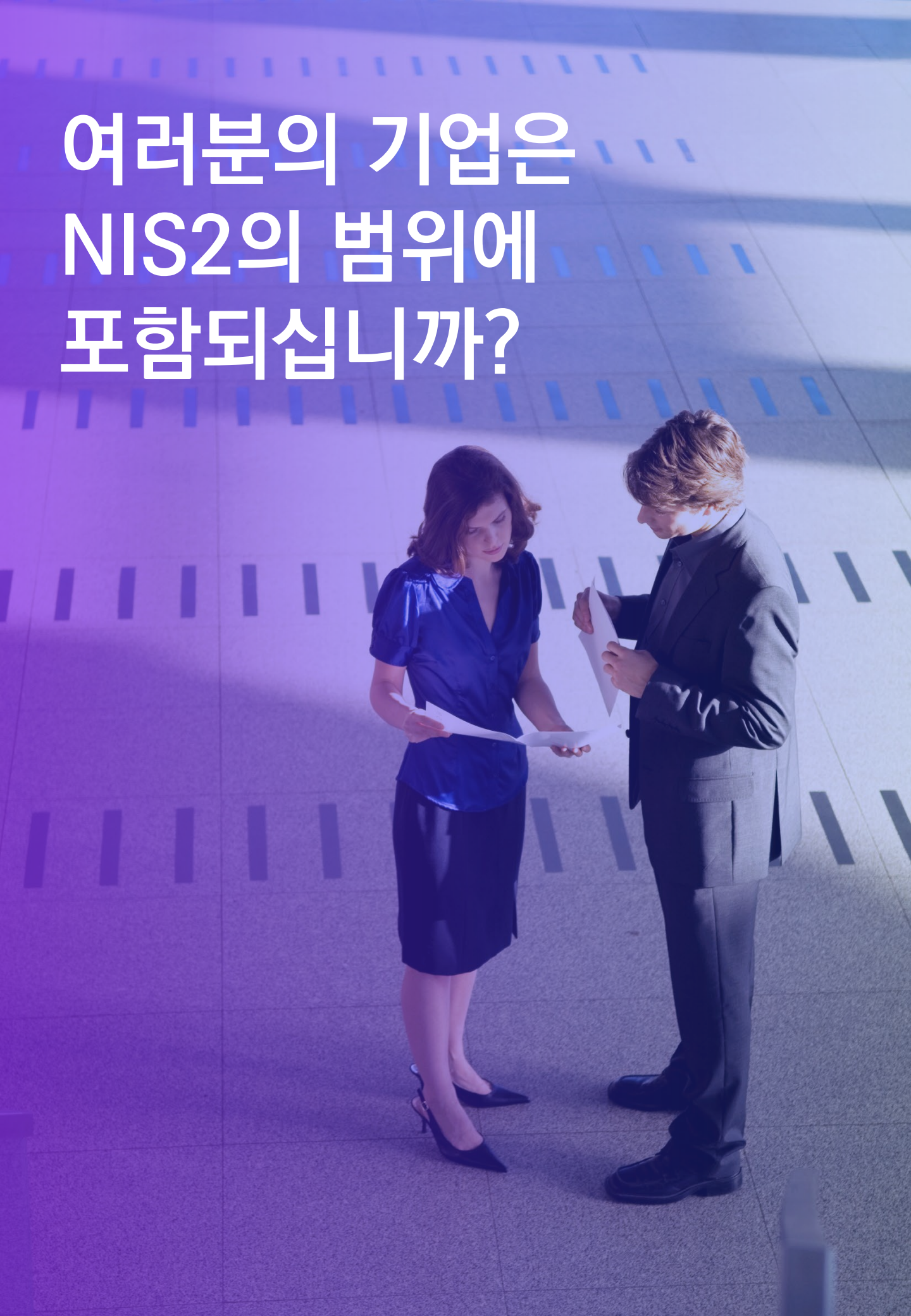
조직에 미치는 영향

NIS2는 기존 NIS 지침의 요구사항에 비해 자율적이지 않습니다. 우리는 EU가 주어진 기간내에 NIS2 지침을 준수하지 않는 조직에 대해 GDPR 법안과 유사한 재정적 페널티를 부과할 것이라는 것을 알게 되었습니다. 또한 세부 요구사항을 통해 배포될 내용들은 비즈니스의 IT에만 집중되는 것이 아니라 기업의 산업시설이 안전하게 운영하고 있는지에 대한 다양한 기술적 내용도 포함될 것입니다. 마지막으로, NIS2 지침을 준수하지 않는 조직의 C급 임원에 대한 처벌 가능성도 있을 것이고, 임원진에 포함된 조직의 개인들에게도 제한을 가할 수 있습니다.

기업이 수행하고 있는 비즈니스 라인에서 규정을 준수하면서 수 많은 지침을 따라야 하는 유럽 기업의 경우, 규정 준수를 하기 위한 환경이 지속적으로 성장하고 있는 것처럼 느껴집니다. 이를 관리하기 위해 한번의 테스트만으로 많은 지침들을 준수 할 수 있는 아이디어(15 페이지)는 점점 더 어려워지는 규제 환경속에서 조직에 큰 도움이 될 것입니다.

위 언급된 10개의 분야는 본 지침에서 가장 엄격한 감독을 받게 될 분야들이며 이외 다른 조직도 범위에 포함될 수 있습니다 (7 페이지). 만약 귀하의 조직이 NIS2 지침의 범위에 포함될 경우, 법률에 대응하는 방법을 설명하는 우리의 세부적인 접근 방식(17 페이지)을 통해 기업이 적시에 효과적으로 규정을 준수할 수 있는 올바른 방법을 지원합니다.

여러분의 기업은 NIS2의 범위에 포함되십니까?



NIS 지침 초기 개정 (2016)

2022년 12월, EU는 개정된 NIS2 지침을 공표하면서, 기존 2016년에 제정된 NIS 지침은 폐지하고 NIS2 지침으로 대체될 예정입니다. NIS2 지침에서는 전반적으로 사이버 복원력을 향상시키기 위한 EU의 적극적인 노력이 보입니다. 이는 NIS 지침이 핵심 산업 인프라의 공급망에 필수적인 기업에 새로운 산업군들이 포함되도록 범위를 확대한 것으로 알 수 있습니다.

2016년 초기 NIS 지침은 7개의 핵심 분야를 다루었습니다만, 이후 EU에서 안전하고 효율적이며 효과적인 사회에 중요한 것으로 간주되는 부문까지 관점을 확장했습니다. 이에 따라 NIS2 지침 범위는 9개의 부문이 추가되어 그 대상이 확대되었습니다.

기업이 확인해야 할 사항

여러분의 기업은 8페이지에 언급된 예시와 같이, 중요한 서비스나 제품 혹은 필수 기능을 최종 고객에게 직접 제공하거나 혹은 공공 안전이나 경제 안정에 영향을 미칠 수 있는 주요 공급업체에 제공하고 있습니까?

여러분의 기업은 8페이지에 언급된 예시와 같이, NIS2 지침이 명시한 산업분야와 관련되어 운영되고 있습니까?

기업은 EU 외부에 있으나, EU 내에서 중요한 서비스를 제공하고 있습니까? 그러한 경우에는 본 지침을 적용해야 합니다.

특별법 우선 원칙이 적용됩니까?
(DORA, PSD2처럼 다양한 분야의 EU 법적 행위가 사이버 보안 요구사항과 동등하거나 사고 발생시 통보해야 하는 의무를 제공하는 경우 우선 적용되어야 합니다.

KPMG 사이버보안 서비스

Cyber 전략 & 위험 | 운영 | 평가 | 데이터 보호

KPMG 사이버보안 서비스는 기본 평가부터 전략 구현까지 모든 사항에 대해 제공 가능합니다.

본 문서에서는 조직의 구체적인 요구 사항에 따라 조정될 수 있는 NIS2 지침에 따라, 산업별 OT 및 IT 보안 개선에 대한 KPMG의 접근 방식을 확인할 수 있습니다.

조직이 NIS2 범위에 해당됩니까?

그렇다면, 본 문서가 필요할 것입니다.

그렇지 않은 경우에도, 조직을 더 안전하게 만들 수 있는 방법을 제시하므로 본 문서는 도움이 될 것입니다.

중요 부문: 부록 I & 부록 II

NIS2 지침의 범위는 두 개의 부록에서 정의됩니다. NIS2 지침은 아래 그림과 같이 부록 I 과 II에 언급된 공공기관과 민간기업 모두에 적용됩니다.

부록 I에는 기업의 총 연간 수익 및 규모에 따라 필수 또는 중요 항목이 될 수 있는 부문이 나열되어 있습니다.
(이 페이지 아래 '참조' 부분을 확인하세요)

부록 II는 EU에서 규정한 기타 주요 산업군을 제공하며, 이것 또한 중요한 범위에 해당됩니다.

범위 내 조직: 필수 및 중요 조직

NIS2 지침은 적용 범위에 속하는 조직을 "필수"와 "중요"의 두가지 산업으로 구분하고 있습니다.
중요한 차이점은 "필수 그룹"의 서비스 중단은 국가 사회 전반에 심각한 결과를 초래할 것으로 예상된다는 것입니다.

두 조직 그룹 모두 동일한 보안 조치를 준수해야 합니다. 하지만, "필수 그룹"에 속하는 조직에 대해서는 적극적으로 감독(사전 예방)을 실시하고 있으며, " 중요 그룹 " 에 속하는 조직에 대해서는 위반 사항이 보고된 후에만 보안조치를 준수하였는지 모니터링(사후 관리)하고 있습니다. 기업들은 "필수 그룹"에 속하는지 혹은 "중요 그룹"에 속하는지를 즉시 확인하고 조치해야 합니다.

필수 그룹 | 사전 예방

- 부록 I – 대기업(a)
- 공인 신뢰 서비스 공급자, TLD 이름 레지스트리, DNS 서비스 공급자
- 공공행정기관
- 필수 서비스 운영자
- 필수 서비스 운영자(2016/1148 지침)
- 회원국에서 선정한 조직

중요 그룹 | 사후 관리

- 부록 I – 중견기업(b)
- 부록 II – 중견기업 및 대기업
- 회원국에서 선정한 조직(c)

참조: (a) 대기업: 연간 매출 5천만 유로 이상; 직원 250명 이상
(b) 중견기업: 연간 매출 1천만 유로 이상; 직원 50명 이상
(c) 회원국에서 선정한 조직: 임의의 규모; 리스크 기반 선정

EU가 사이버보안을 강화하기 위한 조치

유럽연합(EU)의 의지

NIS2의 세부 요구사항이 공개되는 2024년 10월까지, 기업들과 그들의 필수 공급업체는 조직의 정책 및 운영 절차 마련과 관련 지원 기술을 준비하기까지 16개월도 남지 않았습니다. 이 기간은 기업이 자신들의 복원력을 나타내고, 고객과 더 강력한 관계를 구축하고, 사이버 위협으로부터 보호할 수 있는 유일한 기회입니다.

기업들은 비즈니스가 디지털화됨에 따라, NIS2는 최고 운영 책임자(COO)들에게 기업의 사이버보안 역량을 강화하고 컴플라이언스를 충족시킬 수 있는 기회와 과제를 모두 제공합니다.

NIS2가 적용되는 2025년부터는, EU 전역의 수천개의 조직과 필수 그룹들은 사이버보안 역량을 강화하고 중요 인프라 보호에 대한 약속을 보여줄 기회를 가지게 됩니다.

유럽연합(EU)은 왜 NIS2를 개정했을까요?

유럽연합은 기존 NIS 지침에 대해 검토를 수행하여 4가지 주요사항을 도출할 수 있었습니다:

1. 기업의 사이버 복원력 부족;
2. 회원국 및 기업 간의 공동 위기 대응 부족;
3. 주요 위협 및 과제에 대한 공통된 이해 부족;
4. 회원국 간의 일관되지 않은 사이버 복원력.

출처: 네트워크 및 정보시스템 보안 지침 (Directive on security of Network and Information Systems)

초기 NIS 지침은 주목할 만한 성과에도 불구하고, 분명한 한계점을 보여주었습니다. 코로나19 팬데믹의 결과로 인한 디지털 혁신의 가속화는 사이버위협 환경을 확장시켰습니다. 게다가, 주요 산업시설에서 발생하는 사고의 수는 줄어들지 않고 있습니다.

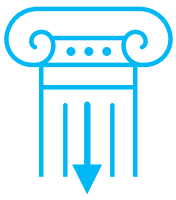
정부기관은 이러한 상황에 충분히 엄격하게 대응하지 못하였고, 이는 조직의 사고 대응 및 복구가 늦어지는 결과로 이어져 법률적 지침의 개정이 불가피하게 되었습니다.

NIS2는 초기 NIS 지침의 기초를 형성한 세 가지 주요 요소를 기반으로 합니다.

7개 초기 분야에 걸친 사이버 보안 조치 이행

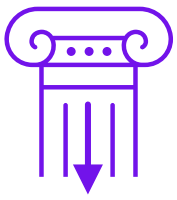
NIS2는 범위를 확장했습니다

회원국에 대한 높은 수준의 대비 (국가 사이버 전략, CSIRT) 구축



NIS2는 유럽연합의 보다 엄격한 감독을 선언합니다

전략적 협력과 정보교류를 지원하고 촉진하기 위한 NIS 협력단



NIS2는 새로운 보고 및 정보 공유 메커니즘을 도입합니다

기업이 지켜야하는 주요 요구사항은 무엇입니까?

원문을 확인하시려면 여기를 클릭해 주세요.

제 20조
거버넌스

제20조는 필수/중요 조직의 관리기관이 제21조를 준수하기 위해 적용하는 사이버 보안 위험 관리 조치를 승인하고, 이러한 조치의 이행을 감독하며, 조항 위반에 대해 책임을 질 수 있도록 보장하는 것을 회원국들에게 요구합니다.

또한, 관리기관은 관련 교육을 수행하고, 이와 유사한 교육을 임직원에게 정기적으로 제공하는 것을 권장합니다. 이를 통해, 임직원은 위험을 식별하고 사이버보안 위험 관리 경험을 얻을 수 있으며, 기업이 제공하는 서비스에 미치는 영향을 평가할 수 있는 충분한 지식과 기술을 얻을 수 있습니다.

제 21조
사이버보안 위험관리 조치

제21조는 회원국으로 하여금 필수/중요 조직이 네트워크 및 정보시스템의 보안에 발생하는 위험을 관리하기 위해 기술적, 운영적 그리고 조직적 조치를 취하도록 요구합니다. 비례성은 조직이 위험에 노출되는 정도, 조직의 규모 그리고 경제적, 사회적 영향을 포함하여 발생가능한 사고의 가능성과 심각성을 기준으로 합니다. 조직은 모든 범위의 사고 및 비상상황에 대비하고 네트워크 및 정보시스템과 해당 시스템의 물리적 환경을 보호할 수 있는 모든 위험 접근 방식을 취해야합니다.

조치들은 최소한 다음 사항이 포함되어야 합니다:

- 위험 분석 & 정보보안 정책;
- 사고 처리;
- 비즈니스 연속성;
- 공급망 보안;
- 취약점 처리 및 공개;
- 사이버 위험관리 조치의 효과성에 대한 평가 절차;
- 사이버안전 유지 사례 및 사이버보안 교육;
- 암호화 관련 정책 및 절차;
- 인적자원 보안, 접근통제 정책 및 자산관리;
- 다중인증 및 보안 통신 시스템 사용.

제 23조
보고 의무

제23조는 회원국들이 서비스 제공에 중대한 영향을 미치는 모든 사고에 대해 기업이 CSIRT 또는 해당하는 경우 관할 당국에 통보하도록 요구합니다.

중대한 사이버위협이 발생한 경우, 조직은 잠재적으로 침해되었을 수 있는 서비스 사용자들이 위협에 대응할 수 있는 조치방안과 해결책을 통보해야 합니다. 필요한 경우, 조직은 서비스 사용자들에게 위협 자체를 통보할 수 있습니다.

중대한 사이버 위협은 다음과 같습니다:

a. 서비스 운영상 심각한 영향을 주거나 기업의 재정적 손실을 유발할 수 있는 경우;

b. 상당한 물질적 또는 비물질적 피해로 기업이나 외부인에게 영향을 줄 수 있는 경우.

조직은 관할 당국 또는 CSIRT에 다음과 같은 사항을 제출해야 합니다:

a. 중대한 사고를 인지한 후 24시간 이내, 사건이 불법 또는 악의적인 행위에 의해 발생한 것으로 의심되는 경우와 다른 국가에 영향을 미칠 수 있는지 여부를 나타내는 조기경보;

b. 중대한 사고를 인지한 후 72시간 이내, (a)항의 조기 경보 내용 최신화 및 중대한 사고의 심각성과 영향, 그리고 가능한 경우에는 손상 지표를 포함한 초기사고 평가를 포함한 보고서

c. CSIRT 혹은 가능한 경우 관할 당국의 요청에 따라 관련 상황을 최신화한 중간 보고서;

d. (b)항에 따른 사고 통지 제출 후, 1개월 이내 최종보고서.

제 24조
유럽 사이버보안 인증 제도의 활용

제21조의 특정 요구사항의 보안 의무가 충족되었음을 입증하기 위해, 회원국은 유럽 사이버보안 인증제도에 따라 인증된 ICT 및 OT 제품, 서비스 및 프로세스를 사용하도록 기업들에게 요구할 수 있습니다.

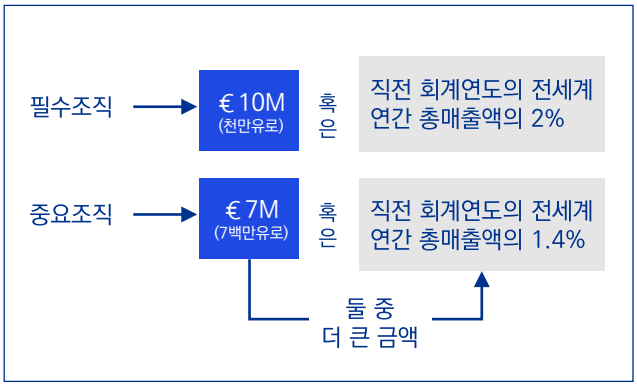
나아가, 회원국들은 필수/중요 조직으로 하여금 신뢰성 있는 서비스를 사용하도록 독려해야 합니다.

기업은 어떠한 영향을 받을까요?

NIS2에 있어서 가장 큰 질문은 해당 지침에 대한 각 회원국의 집행 방법입니다. GDPR 입법을 통해 알 수 있듯이, 기업은 시간이 지남에 따라 더 많은 데이터 보호 요구사항과 조치에 대해 철저한 이해가 필요합니다. NIS2의 경우에도 마찬가지일 가능성이 높으므로, 조직은 현재 가지고 있는 정보를 바탕으로 가능한 필수적 조치를 취해야 합니다.

컴플라이언스로 인한 내부적 영향

새로운 규정의 복잡성으로 인해 조직은 이 규정이 비즈니스에 미치는 범위와 잠재적 영향을 이해하기 위해 지금부터 준비를 시작해야 합니다. 규정을 준수하지 못하는 경우, 필수/중요 조직은 다음과 같은 금전적 처벌을 받을 위험이 있습니다.

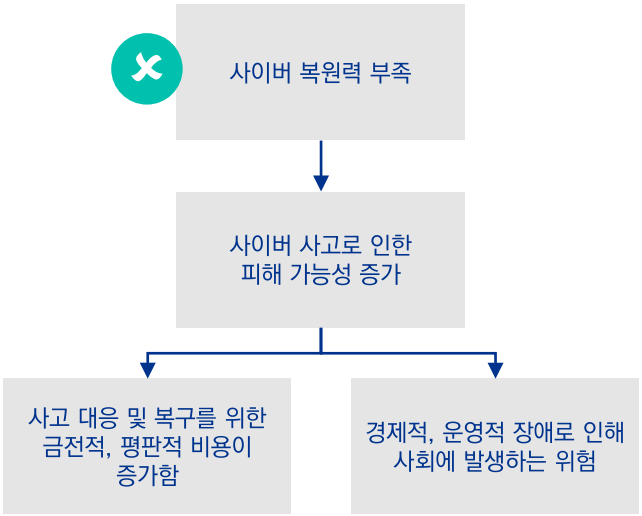


눈 여겨 보세요!

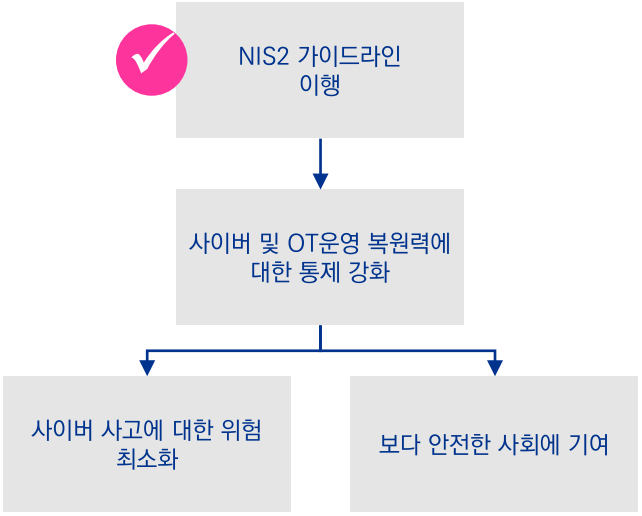
다국적 기업은 기업이 속해 각 회원국에서 중요 인프라 또는 중요 인프라 공급망의 일부로 간주되는지 확인해야 합니다.또한 소속 회원국에서 준수해야 하는 법률이 무엇이 있는지 확인해야 합니다. 유럽연합 회원국(EU)에 속하지 않지만, 유럽연합에 중요 서비스를 제공하는 기업들도 해당 지침이 적용되기 때문에 주의를 기울여야 합니다.

외부적 영향

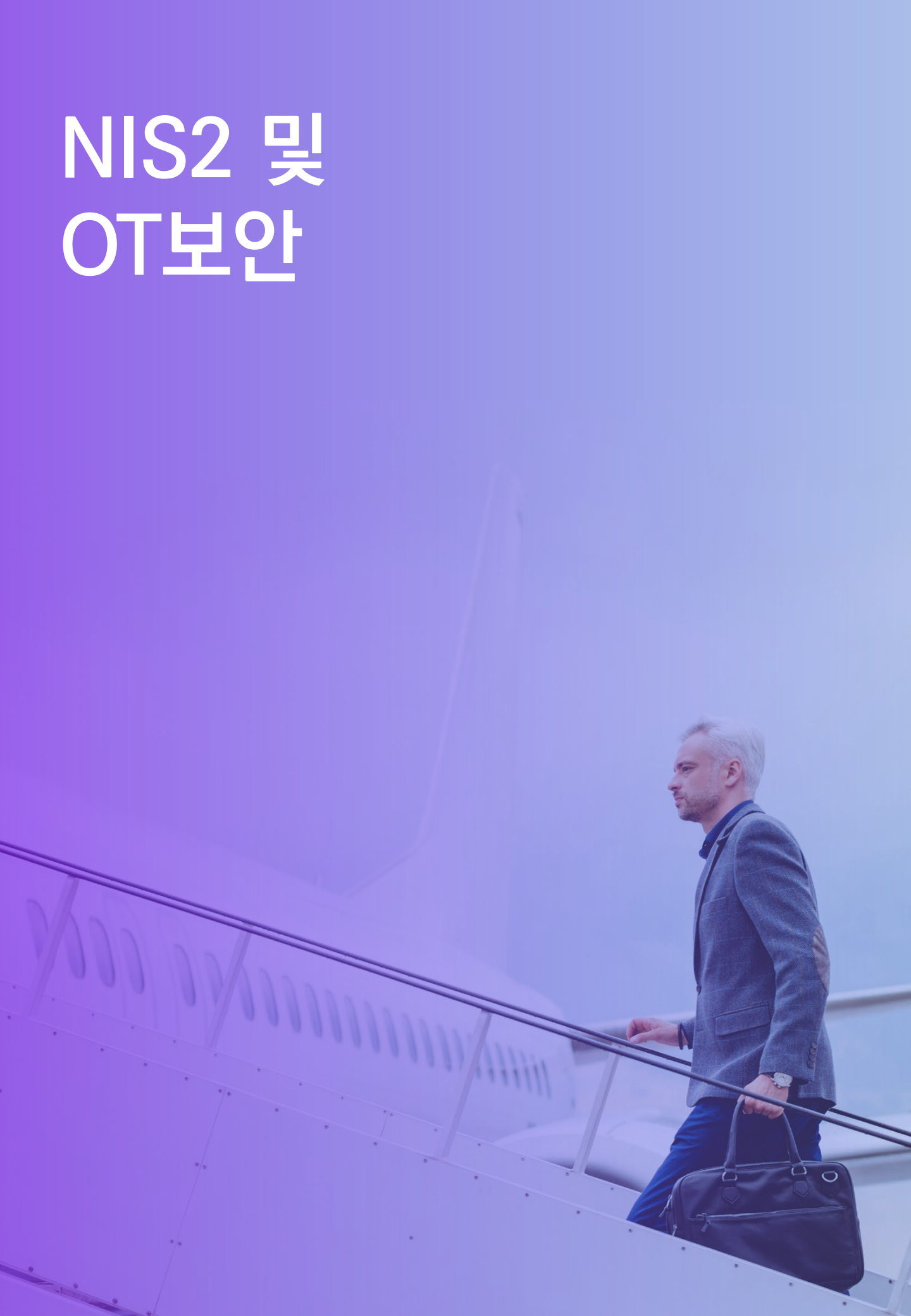
NIS2의 범위에 해당하는 조직은 안전하고 효과적이며 효율적인 사회에 기여하는 중요한 주체 간주된다는 사실을 인식해야 합니다.



핵심 조직이 스스로를 보호하지 못한다면 사회에 넓은 영향력으로 위험에 빠지게 할 수 있습니다. NIS2의 보안 의무를 충족하는 것은 문서상으로 훌륭해 보이는 규정 준수 외에도, 조직의 보안으로 회복력 있는 사회를 만드는데 기여할 수 있습니다.



NIS2 및 OT보안



IT와 OT의 연결이 많아질수록, 기업은 더욱 공격받기 쉬워집니다.

IT와 OT환경의 상호연결이 지속적으로 증가함에 따라, 사이버 위협은 두 영역을 보다 자유롭게 넘나들 수 있게 되었습니다. 이러한 결과는 공격을 받을 있는 경계가 확장되어, 공격이나 사고로 인해 IT와 OT 운영에 동시에 일어날 수 있는 충격이 현저하게 증가하게 됩니다. 이러한 부분은 부상 등의 인명피해, 환경에 대한 영향 뿐 아니라 보다 심각한 부정적 결과를 초래할 수 있습니다.

게다가 IT에서 시작된 사이버위협이 OT로 전이되거나 그 반대로 위협이 이동하는 경험으로 인해서, OT를 운영하는 많은 기업과 조직들은 산업분야의 공정 운영과 안전에 사이버보안을 우선적으로 검토하고 있습니다.

OT 전문가가 사이버보안의 전문지식이 없는 경우가 대다수이고, 확연하게 다른 업무 목표를 가지고 있는 IT팀과 OT팀 사이의 부족한 의사소통은 약점을 알아내고 명확한 해결책을 수립하는데 한계가 있습니다.

EU의 NIS2 지침은 물리적인 환경과 사람을 사이버보안 리스크로부터 보호하기 위한 요구사항들을 직접적으로 언급하고 있으며, 특히
이를 위해 OT시스템의 디지털안전 확보가 중요함을 강조하고 있습니다.

기업은 NIS2의 규정 준수와 사이버보안의 수준을 개선하기 위한 노력을 통해 IT와 OT영역의 시스템, 프로세스를 안전하게 통합할 수 있습니다.

그러나 이를 위해서는 사이버공격에 피해가 예상되는 부분을 파악하여 해결하고, 교육과 활용가능한 기술에 투자하며, IT와 OT부서 간의 효과적인 의사소통과 협업을 통해 사고 예방적인 접근이 우선 필요합니다.

IEC 62443 표준과의 연관성

많은 기업들은 NIS2 지침을 대비하면서 현 시점에서 많은 것들이 불분명하기 때문에 이 새로운 규정을 준수하기 위해 준비하는 것이 쉽지 않다고 느끼고 있습니다.

그러나, NIS2 규정 준수를 위한 대응을 이미 준비하기 시작한 기업들에게는 효과적인 통제와 적용가능한 산업표준이 이미 존재하고 있으며, EU 포함하여 국제적으로 인정되고 있다는 것은 매우 좋은 소식입니다.

회원국과 운영주체들은 OT환경을 위해서 IEC62443과 이를 참조한 산업별 OT보안 표준과
같은 동급 최고의 산업표준의 장점을 적극 활용해야만 합니다.

IEC62443을 활용한 기업들은 OT시스템의 취약점을 미리 식별하고 해결할 수 있으며, 직원들이 안전한 환경을 유지할 수 있도록 교육을 받고 장비를 갖추도록 할 수 있습니다.

따라서 NIS2의 세부 요구사항이 모두 확정되기까지 기업은 IEC 62443을 채택하여 사이버보안 태세를 개선하기 위한 조치를 미리 준비할 수 있습니다.

	NIS2 20, 21조에서 명시한 주요 기업의 준수사항	IEC 62443 표준을 활용한 현재 대응방안
거버넌스와 프로세스	• 리스크 분석과 정보시스템 보안 정책 • 사이버 리스크 관리의 효과성 평가 • 비즈니스 연속성 확보	• 정책과 절차 수립 • 리스크 관리 체계 도입과 개선 • 재난 복구 대비와 비즈니스 연속성 확보 • 보안 요구사항 이해 • 국제표준 기준 네트워크 아키텍처
조직과 인력	• 사이버 리스크 관리 방법에 대한 최고 경영진의 승인과 감독 • 컴퓨터 바이러스 예방 및 사이버 보안 교육 • 공급망 보안	• 역할과 책임 상세 정의 • 보안 인식 개선과 교육 진행 • 협력업체 보안
기술과 보안역량	• 사고처리 • 암호학과 암호화 • 취약점 처리와 투명한 공개 • 자산 관리와 접근 통제 정책 • 안전한 통신 시스템과 다중 인증 사용	• 자산 식별과 정보 최신화 • 네트워크 분할과 분리 • 업데이트 및 취약점 관리 • 원격 접근 보안

한번의 테스트로 다수의 컴플라이언스 준수

오늘날 기업들은 점점 더 어려운 규제 환경에 직면하고 있습니다. 조직은 내부 통제, IT 및 OT 통제, SOX 통제 및 잠재적인 산업별 규제를 처리해야 합니다; 예를 들어, 에너지 산업은 ENTSO-E 가 있습니다. NIS2를 준수해야 하는 조직의 경우, 규제에 추가할 또 다른 항목입니다. 별도의 테스트를 통해 이러한 모든 요구 사항을 단편적인 방법으로 관리하면 노력과 비용이 낭비됩니다.

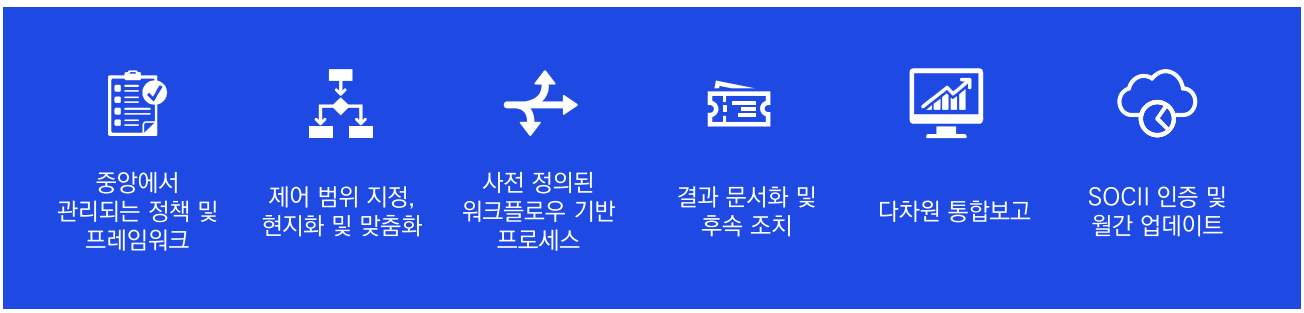
따라서, '한 번 테스트하고 여러 항목을 준수'하는 통합된 접근 방식을 통해 규정 준수 노력을 간소화하고 비용을 절감할 수 있습니다. 자동화된 GRC/IRM 솔루션에서 지원할 수 있는 통합 제어 프레임워크를 구축하고 모니터링함으로써 기업내 여러 조직에 프레임워크를 배포하여 단 한 번의 테스트로 여러 규제 프레임워크에 대한 규정 준수를 보장할 수 있습니다. 이 접근 방식은 여러 프레임워크를 독립적으로 관리하는 혼란을 없애고 조직이 효과적인 방식으로 규정 준수를 달성할 수 있도록 합니다.

통합 통제 항목	통합 통제 내용	ISO 27001/2	CRA	IEC 62443	NIS2
사이버보안 역할 및 책임	역할과 책임은 사이버 보안과 관련된 조직 전체의 기능에 대해 명확하게 정의됩니다. 특정 역할이 존재하고 경영진이 임명했으면 관련 당사자에게 전달되고 명확하게 문서화되었음을 입증합니다.	ISO 27001:2022 Clause 5.3	CRA Article 10 for Manufacturers	IEC 62443-2-1 Element 4.3.2.3	NIS2 Article 7 & 20
ISMS/CSMS 범위	범위를 정의하는 주요 목적은 조직이 보호하려는 정보를 이해하는 것입니다. ISMS를 설정하는 조직은 사이버 보안과 관련된 모든 거버넌스 및 프로세스를 고려하고 정의해야 합니다.	ISO 27001:2022 Clause 4.3	CRA Article 6-9	IEC 62443-2-1 Element 4.3.2.2	NIS2 Article 7 & 21
재3자 위험관리	타사에 대한 종속성과 이러한 당사자가 액세스할 수 있는 귀중한 자산을 고려하십시오. 아웃소싱과 관련된 위험을 관리하기 위한 통제가 마련되어 있습니다	ISO 27001:2022 Annex A.15	CRA Article 10 & 11	IEC 62443-2-4	NIS2 Article 12 & 21
멀웨어 방지	시스템에는 악성코드 방지 소프트웨어가 설치되어 있고 최대 7일 된 탐지패턴으로 실행되어야 합니다.	ISO 27002 8.7 Protection against malware	CRA Article 6	IEC 62443-3-3 SR 3.2 Malicious Code Protection	NIS2 Article 21

GRC 도구 지원 사례: KPMG Sofy GRC

기업은 IRM/GRC 도구를 구현하여 조직에 규정 준수 모니터링을 포함시켜야 합니다. 예를 들어, KPMG Sofy GRC 솔루션은 조직이 관련 규제, 위험 및 제어 프레임워크와 그 효과를 중앙에서 저장, 유지, 배포 및 모니터링할 수 있도록 지원합니다.

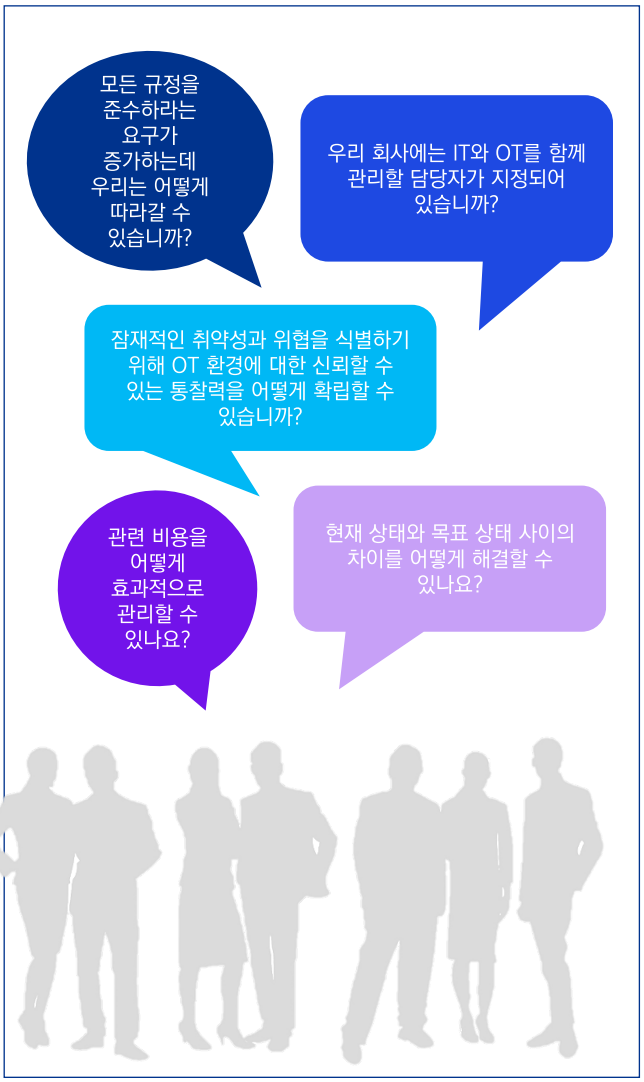
Sofy는 실시간 컴플라이언스 보고를 위해 프레임워크에 대한 규정 매핑을 지원합니다. 이 앱은 모든 방어선이 단일 환경에서 함께 작동하도록 지원하도록 개발되었으며 사전 구축된 워크플로우 및 보고서와 직관적인 사용자 인터페이스 덕분에 몇 달 만에 구현할 수 있습니다.



여러분의 기업은 어떻게 준비하겠습니까?

NIS2 지침에 대한 준비

규정과 관련하여 많은 조직은 규정 준수를 최종 목표로 보고 있습니다. 즉, 규정을 준수해야 하므로 최소 요구 사항을 충족하는 것을 목표로 하지만 실제로는 더 높은 수준의 사이버 보안을 달성하기 위한 기반이자 수단이 될 수 있습니다. 규제는 조직의 회복력에 중요한 역할을 하지만 조직에 맞게 조정되어야 합니다. 규제 범위가 회사의 공급망을 포함하도록 확장된 것은 COO가 직면한 가장 큰 과제 중 하나입니다. 이제 비즈니스 리더는 공급업체 및 기타 주요 파트너에 대한 영향과 관련 규정 준수 여부도 고려해야 합니다. 또한 회사의 컴플라이언스 현황에 대해 무지할 수 있는 고객 및 투자자들에게도 주의를 기울여야 합니다. 이에 따라, 조직은 아래와 같은 질문에 직면합니다.



우리는 이러한 질문에 대한 답변을 4가지 주요 조치로 제공합니다.

4가지 주요 전략적 조치

1. 최고경영진(C-Suite) 내에서 인식을 촉진하다

- 2016 | NIS1 발표
- 2022년 12월 | NIS2 공표
- 2023년 7월 | 현재
- 2024년 10월 | NIS2 세부 요구사항 발표
- 2025년 1월 | NIS2 적용

새로운 사이버 보안 법률의 책함에 있어, 조직적인 측면에서 예산과 전략에 대한 내용이 우선적으로 논의되어야 합니다. NIS2가 발효되기까지의 짧은 시간을 감안할 때 이 지침은 COO의 최우선 과제가 될 것입니다. 특히, 규정을 준수하지 못하는 경우 개인적으로 책임을 지는 것은 C급 임원이며, 그 결과는 벌금, 기소가 될 수 있습니다. CISO는 NIS2가 가져오는 문제에 대해 기업내에 알려야 하며 IT와 OT가 함께하는 방법에 대해 책임을 가지는 자원과 조직을 디자인해야 합니다.

2. 기준선 & 통찰력에 대한 계획

NIS2는 유럽 연합 내 조직의 사이버 보안 회복력을 강화하고 악의적인 행위자들이 가하는 위협에 대해 빠르게 인식하는 것을 목표로 합니다. 이 계획은 사이버 위험 관리 조치를 의무화하여 조직의 회복력과 연속성을 보장하고, 사이버 보안 요구사항을 준수하는 것을 기본으로 합니다. 따라서 조직의 인프라 내 취약점을 식별하고 신속하게 해결하는 것이 중요합니다.

그러나 NIS2에서 요구하는 특정 요구 사항은 여전히 모호합니다. 따라서 IEC 62443과 같이 세계적으로 인정되는 업계 OT보안 표준을 따를 것을 권장합니다. 조직은 평가를 통해 기준을 설정하기 전에 이러한 표준 및 프레임워크 구현을 우선적으로 처리해야 합니다.

어려운 사항

현재 IT 및 OT 환경은 어떻습니까?

현재 비즈니스를 하는 기업들은 전반적으로 사이버 성숙도 수준에 대해 제대로 평가하기 어렵습니다.

접근 방법

베이스라인

효과적인(Smart) 평가

사이버 성숙도 기준을 설정하려면 사이버 보안 위험에 대한 통찰력으로 평가를 수행해야 합니다. 짧은 기간에 거버넌스 및 위험 관리와 같은 조직적 측면과 기술 보안 위험을 모두 검토하여 주요 위험을 식별하기 위한 평가를 수행할 수 있습니다. 이 방법은 IEC 62443, C2M2 (Cybersecurity Capability Maturity Model) 및 CRA와 같은 국제적으로 인정된 OT보안 프레임워크 및 표준을 사용하여 효과적으로 수행할 수 있습니다.

예를 들어, C2M2 프레임워크는 사이버 보안 평가에 대한 구조화된 접근 방식을 제공하여 사이트 간 비교 또는 여러 국가에 걸쳐 비교를 할 수 있습니다. 이를 통해 조직은 상대적으로 취약한 영역을 식별하고 위험 수준을 개선하기 위한 우선순위를 지정할 수 있습니다. 이러한 평가를 수행함으로써 조직은 사이버 보안 상태에 대한 기준을 설정하고 잠재적인 위협을 해결할 수 있도록 적절하게 준비할 수 있습니다.

찾은 취약점을 어떻게 수정하는가?

평가 단계에서 도출한 시사점을 바탕으로 계획을 수립해야 합니다.

사이버보안 통찰력(insight)을 위한 계획

전략적 계획 개발(수립)

기준 설정 단계에서 사이버 보안 평가를 수행하게 되면 조직은 현재 보안 상태에 대해 의미 있는 통찰력을 얻을 수 있습니다. 이러한 통찰력은 식별된 위험과 취약점을 해결하기 위한 단기 및 장기 조치 계획을 개발하고 준비하는데 사용할 수 있습니다.

단기 실행 계획의 경우 즉각적인 위험을 줄이기 위해 신속하게 실행할 수 있는 빠른 성과에 중점을 둡니다.

장기 실행 계획에는 기본 원칙을 통한 보안 정책 개발, 산업 환경을 위한 보안 아키텍처 개발, 또는 보안 사고 감지 및 대응을 위한 보안 도구 구현과 같이 보다 포괄적인 보안 조치가 포함됩니다.

3. 가속화된 Fix-it (긴급개선)

어려운 사항

한정적인 기한 내에 문제를 어떻게 해결할 것인가?

주요 추진사업은 전략적 계획을 통해 정의되며, 실행될 수 있습니다.

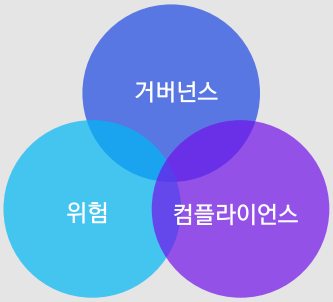
접근 방법

가속화된 Fix-it

심각한 취약점을 해결하기 위한 Fix-it 프로젝트

우리는 보안 취약점을 즉시 수정하여 사이버보안 수준을 향상시킬 수 있습니다. 통찰력을 가진 fix-it 프로그램으로 효율적이고 효과적인 조치를 취할 수 있습니다. 또한 이러한 fix-it 프로그램은 보안 아키텍처 구현을 지원하는 것부터 조직개편 지원까지 다양한 형태로 이루어집니다.

4. 소유권 부여 및 의무(책임) 확대



Risk Ownership은 기업의 거버넌스와 책임을 보장하는 것이 매우 중요합니다. OT 보안의 경우 IT 위험에서 볼 수 있는 만큼 성숙하지 않습니다. OT보안에서 리스크 담당자가 지정되지 않으면, 위험요소가 발견되거나 확산이 될 때 해결하지 못할 가능성이 높습니다. 앞서 언급한 바와 같이 NIS2에서는 보고 요건이 강화되었습니다. 현재 보고 의무는 데이터에 침해가 발생한 경우에는 적용되지만, NIS2에서는 지정된 시간내에 모든 사건을 보고해야 합니다. 한발 앞서 나가기 위해서는 Risk Ownership을 할당하는 것이 필요하고 중요합니다.

IRM/GRC 솔루션을 구현하면 조직 내 소유권 포함을 지원하고 IT 및 OT의 위험 관리 도메인에 필요한 통찰력을 제공합니다. 이러한 솔루션은 명확한 일정 및 알림을 통해 소유자에게 필요한 조치를 자동으로 배포하는 데 용이합니다. 경영진은 조직 전체(예: 벤치마크 위치)의 진행 상황을 모니터링하고 식별된 모든 위험에 실시간으로 대응함으로써 프로세스의 이점을 누릴 수 있습니다. 기업과 관련된 외부 이해관계자를 위한 솔루션인 Sofy GRC는 필요한 정보 수집을 지원하고 보고 프로세스를 간소화할 수 있습니다.

NIS2 지침의 결과로 사이버 보안은 경영 이사회 안건의 필수 구성 요소가 될 것입니다. NIS2에서 경영진은 위험을 식별하고 사이버 보안 위험 관리를 평가하는 데 필요한 올바른 지식과 기술을 보유해야 한다고 명시되어 있습니다. 또한 경영진은 직원이 정기적으로 교육을 받도록 권장해야하며, 실제로 사이버 공격이 발생한 경우 이사회는 조직 내에 적절하고 검증된 사이버 보안 프로그램이 있음을 입증할 수 있어야 합니다. 즉, 경영진은 NIS2의 영향에 대해 교육을 받아야 할 뿐만 아니라 직원들에게도 사이버 보안에 대해 알리고 교육하기 위한 프로그램을 마련한다는 것입니다.

기업의 빠른 준비를 위한 KPMG의 지원

KPMG는 표준들을 활용하여 조직이 NIS2 지침을 준수할 수 있도록 지원하는 업계 최고의 전문가입니다. KPMG는 사고 대응 계획 및 위험 평가를 개발하고 효과적인 OT 보안을 보장하기 위한 기술 및 조직 보안 조치를 구현하는 데 전문성을 제공합니다.

우리가 하는 일

앞에서 살펴본 바와 같이, NIS2는 범위 내의 주체들에게 다수의 사이버 보안 요구사항을 규정하고 있습니다.
다음 예시는 우리가 기업의 업무 향상을 위해 어떻게 도움을 줄 수 있는지를 보여줍니다.

KPMG에 문의사항이 있는 경우, 아래로 연락을 주시면 도움을 드리도록 하겠습니다.

Business Contacts

최민화
상무 / Partner
Digital – OT Security
mchoe@kr.kpmg.com
+82 10 3882 8700

이병각
이사 / Director
Digital – OT Security
byungkaklee@kr.kpmg.com
+82 10 4720 7489

Ronald Heil
상무 / Partner
ENR Global Risk Advisory Lead
Cyber & Privacy
heil.ronald@kpmg.nl
+31 (0) 20 656 80 33

1 사이버 보안 인식 프로그램

- 컴퓨터 바이러스 예방 및 사이버 보안 교육

2 비즈니스 연속성 관리 & 재해 복구 계획

- 비즈니스 연속성

3 ISMS/CSMS 구현

ISMS용 KPMG Sofy GRC 플랫폼

- 사고 처리
- 사이버 위험 관리의 효율성 평가 절차
- 공급망 보안
- 취약점 처리 및 탐색
- 인적 자원에 대한 보안, 접근 제어 정책 및 자산 관리
- 다중 인증 및 안전한 통신 시스템 사용

4 사이버 정책 설계

- 위험 분석 및 정보보안 정책
- 암호화 및 암호화 정책 및 절차

5 사이버 성숙도 평가

침투 테스트 포함 및 전략적 로드맵

KPMG 네덜란드: www.kpmg.com/nl/cyber

삼정KPMG: home.kpmg/kr

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2023 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. The KPMG name and logo are trademarks used under licence by the independent member firms of the KPMG global organisation. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.