

DQS Korea

ISO/IEC 27001로 강화하는 조직의 정보보호

PECB REGIONAL WEBINARS

Agenda

1. *ISO/IEC 27001의 필요성*
2. *ISO/IEC 27001의 효과적인 실무 적용 방안*
   - *보안운영의 성과 도출을 위한 ISMS 적용*
   - *실용성 있는 리스크 평가 및 관리*
   - *ISMS 구현 시, 주요 과제 및 대응 방안*
3. *ISO/IEC 27001과 ISO/IEC 42001 연계*
4. *ISO/IEC 27001 부적합 사례*

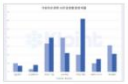
1. ISO/IEC 27001의 필요성

■2026년 사이버보안, 어떤 변화가 필요한가

2025년 주요 사고를 한 문장으로 요약하면 "기술이 아니라 운영이 뚫렸다"는 결론으로 수렴했다. GS리테일은 계정 재사용과 자동화 공격 방어 미흡이 유통 플랫폼 리스크로 확대될 수 있음을 보여줬고, SK텔레콤은 평문 계정·장기 잠복·로그 공백이 통신 인증 인프라를 장기간 흔들 수 있음을 드러냈다. 롯데카드와 쿠팡 사례는 '피해 산정의 정확성'과 '조사 협조·증거 보존·공시의 일관성'이 사고 이후 기업 신뢰를 좌우한다는 점을 확인시켰고, 예스24·SGI서울보증은 랜섬웨어가 곧 서비스·금융 인프라의 중단으로 이어지며 사회적 피해로 확장된다는 현실을 보여줬다.

Home > 뉴스검색





'6억명 시대' 가상자산 시장, 사기·해킹도 함께 진화... 피해액 30억달러 돌파
2025년 가상자산 시장이 전례 없는 성장세를 보인 가운데, 해킹·사기·자금 세탁 등 범죄 위험도 동시에 커진 것으로 나타났다. 클로인트는 7일 '2025년 가... 여이레 기자 | 2026년 01월 07일 13:35

CISA '알려진 취약점' KEV, 1년 새 20% 증가... 랜섬웨어 악용 취약점만 24개
지난해 미국 사이버보안청(CISA)이 공개하는 '알려진 취약점'(KEV) 등록 보안 결함이 2024년 말 1239건에서 2025년 말 1484건으로 늘어 약 20... 여이레 기자 | 2026년 01월 06일 14:07



美 연방 계약업체 세드윅 피격... CISA 등 정부 보안 부처 데이터 유출 비상
미국 대형 보험 및 리스크 관리 기업 세드윅(Sedgwick)이 자사 정부 전용 서비스 부문 자회사가 사이버 보안 사고를 겪고 있음을 공식 확인했다. 이번 사건... 여이레 기자 | 2026년 01월 05일 11:25



"이스라엘 고위층 텔레그램 뚫렸다!" 이란 해킹 조직 '문어 작전'... 1900개 대화내용 유출
2025년 12월, 이란과 연계된 해킹 조직 한다라(Handala)가 이스라엘의 주요 정치인 2명의 모바일 기기를 완전히 장악했다고 주장했다. 그러나 사이버 인텔... 여이레 기자 | 2026년 01월 05일 11:07



"미 재무부 깜짝 행보"... '프레데터' 스파이웨어 배후 조직 핵심 관계자 3인 제재 해제, 왜?
미국 재무부 해외자산통제국(OFAC)이 상업용 스파이웨어 프레데터의 지주회사인 인텔렉사 컨소시엄과 연결된 개인 3명을 특별제재대상(SDN) 목록에서 제외했다. 여이레 기자 | 2026년 01월 05일 09:13



유럽우주국, 서버 침투로 200GB 데이터 유출... 해커 888 "소스 코드 등 탈취" 주장
유럽우주국(ESA: European Space Agency)은 최근 서버 중 일부가 사이버 공격을 받아 200GB가 넘는 데이터가 유출됐다고 공식 발표했다. 권준 기자 | 2026년 01월 02일 15:15



[쿠팡 해킹] 쿠팡, "정부 지시" vs 정부, "지시 없어" 평행선 달린 청문회
쿠팡 개인정보 유출 사태와 관련해 해롤드 로저스 쿠팡 대표이사가 정부 지시에 따른 조사가 이뤄졌다고 재차 강조한 가운데, 정부는 어떤 기관도 조사를 지시한 적 없... 여이레 기자 | 2025년 12월 30일 17:20



[쿠팡 해킹] 배경훈 부총리 "정보유출 3300만건 이상"...쿠팡 주장 정면 반박
'쿠팡 사태 범정부 TF' 팀장인 배경훈 부총리 겸 과학기술정보통신부 장관이 30일 쿠팡의 개인정보 유출 범위가 3300만 건 이상이라고 밝히며 쿠팡의 3000... 여이레 기자 | 2025년 12월 30일 12:59



랜섬웨어 조직 '건라', 인하대 내부 자료 650GB 탈취 주장
랜섬웨어 그룹 '건라'가 인하대학교 학사정보시스템을 노린 랜섬웨어 공격의 배후를 자처하고 나서며 그룹이 650기가바이트(GB) 분량의 내부 자료를 탈취했다고 주장... 여이레 기자 | 2025년 12월 30일 10:21



유비소프트, 사상 최악 보안참사... '레인보우 식스 시즈' 통제권 일시 상실
프랑스에 본사를 둔 세계적인 비디오 게임 개발업체 유비소프트의 대표작 '레인보우 식스 시즈'가 해커 그룹의 공격을 받아 서버 통제권을 일시적으로 상실하는 초유의... 여이레 기자 | 2025년 12월 29일 10:08



[쿠팡 해킹] 쿠팡 김범석 의장, 유출 공개 한 달 만 사과... "두려움·불안 드려 죄송"
쿠팡 창업주 김범석 쿠팡 Inc 이사회 의장이 3300만명 이상 가입자 정보 유출 사고와 관련해 창업자이자 이사회 의장으로서 처음으로 공식 사과문을 냈다. 유출 ... 여이레 기자 | 2025년 12월 28일 14:12

Source: 보안뉴스, 2026-01-07

1. ISO/IEC 27001의 필요성

2025년부터 2026초까지 대한민국은 통신, 금융, 유통 분야에서 대규모 정보보안 침해사고가 잇따라 발생하며 사상 최대의 보안 위기를 겪었습니다.

1. **통신사 대규모 가입자 정보 유출:** 2025년 4월, 국내 주요 통신사(S사)에서 약 2,324만 명의 가입자 정보(휴대전화번호, IMSI 등)가 해킹으로 유출되었습니다.

2. **금융·카드사 데이터 유출 및 부정사용:** 2025년 9월, 카드사(L사)에서 해킹 사고가 발생하여 약 297만 명의 고객 정보가 유출되었습니다. 온라인 결제 서버 침투로 인해 성명/주민번호는 유출되지 않았으나, 28만 명은 카드 번호와 CVC 등이 노출되어 부정 사용 가능성이 제기되었습니다.

3. **유통·플랫폼 로그인 공격(Credential Stuffing):** 2025년 유통 및 플랫폼 기업을 타깃으로 대량의 로그인 공격이 지속되어 회원 계정이 탈취되고 2차 피해(포인트 도용 등)가 발생했습니다.

4. **의료·민감 정보 유출:** 해킹 포럼에서 성형외과, 지방흡입 전문 병원 등 환자들의 민감한 의료 정보와 대학 기숙사생들의 3년치 외출 기록 등 개인 데이터가 판매되는 사건이 발생했습니다.

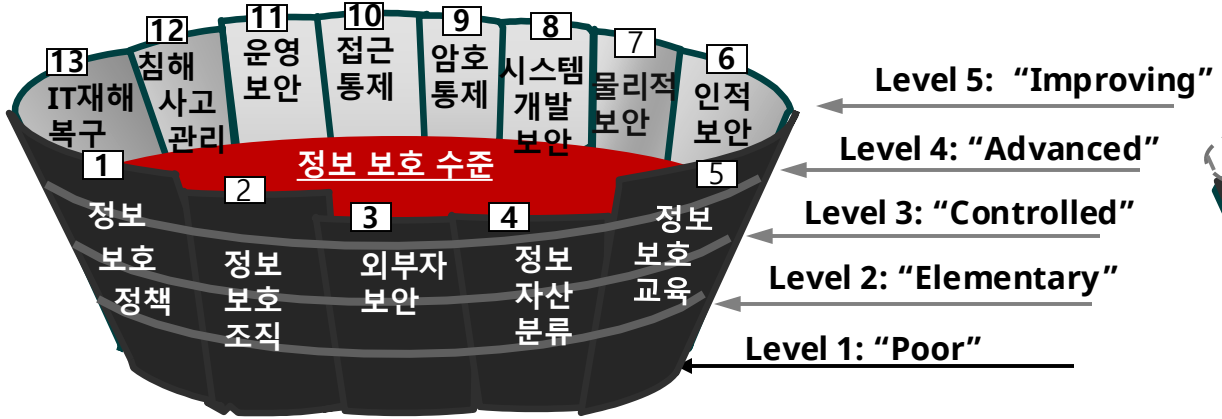
5. **금융권 랜섬웨어 및 업무 중단:** 금융사(S사) 등을 대상으로 한 랜섬웨어 공격이 발생하여 데이터가 암호화되거나, 금융 거래 시스템이 마비되는 업무 중단 사고가 보고되었습니다.

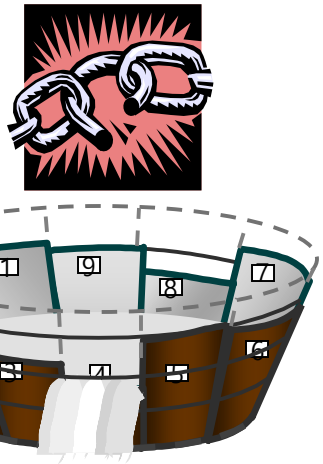
1. ISO/IEC 27001의 필요성

종합적인 정보보호 관리의 필요성

"조직의 보안은 각 분야의 유기적인 협조와 노력에 의해
지켜질 수 있으며, 한 분야의 취약점은 조직 전체의 보안수준을 저하"

(리비히의 최소율의 법칙-나무 물통의 법칙)



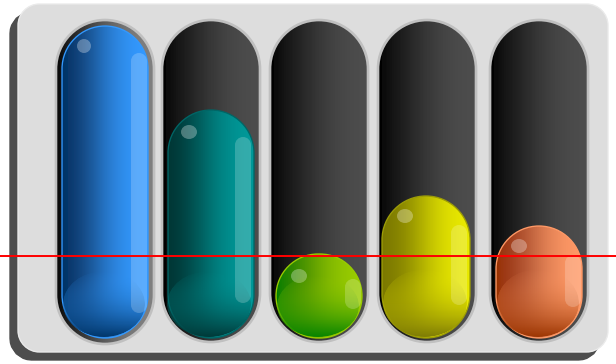


1. ISO/IEC 27001의 필요성

· 부분적 보안 · 일회성 관리 · 산발적 대응

<보안수준>

평가수준



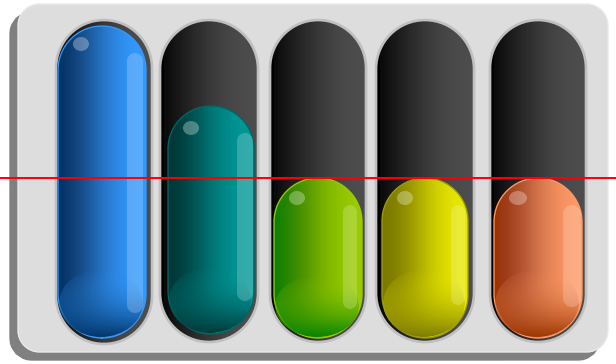
Islanded



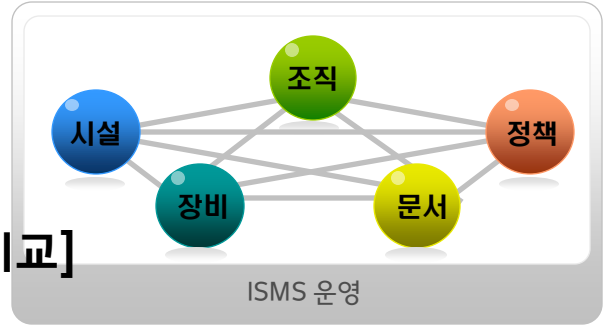
· 균형적 보안 · 지속적 관리 · 체계적 대응

<보안수준>

평가수준



Integrated



[ISMS 적용 전 후 비교]

1. ISO/IEC 27001의 필요성

1

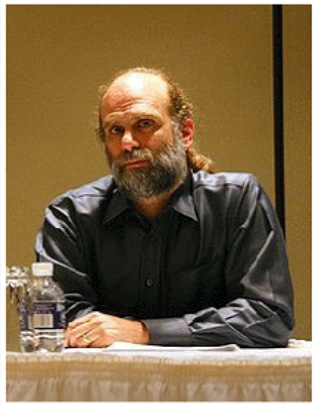
“Security is a process, not a product”
- 보안은 제품(기술)이 아니라, 프로세스이다.

2

"Security is a chain; it's only as secure as the weakest link”
- 보안은 사슬이다. 사슬의 가장 약한 고리만큼만 안전하다.
- 정보보호란 사슬처럼 연결되어 있어서 전체 정보보호 수준은 가장 취약한 연결 부분의 수준을 넘을 수 없다는 것

3

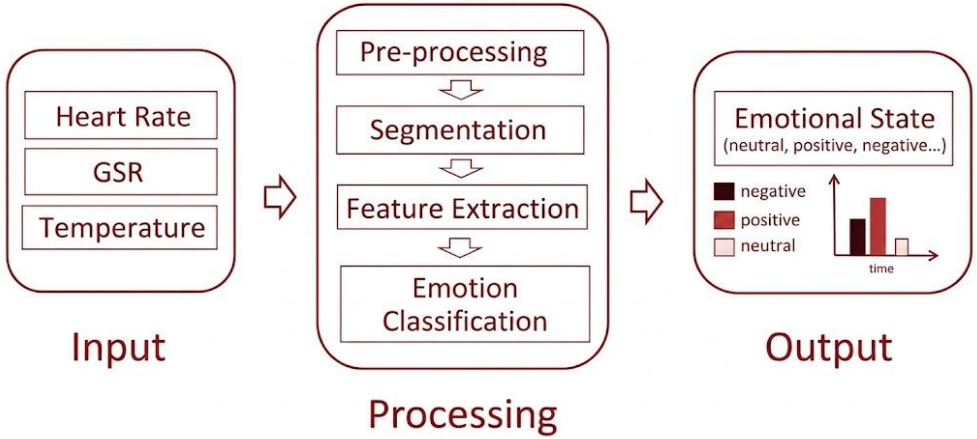
“완벽한 보안은 없다. 그러나 보안은 .. 있다”
- 완벽한 보안이 불가능해도 최선을 다 해야 하며, 그것은 보안에 대한 올바른 인식으로부터 출발



▲ 브루스 슈나이거 박사

1. ISO/IEC 27001의 필요성 > ISMS Framework

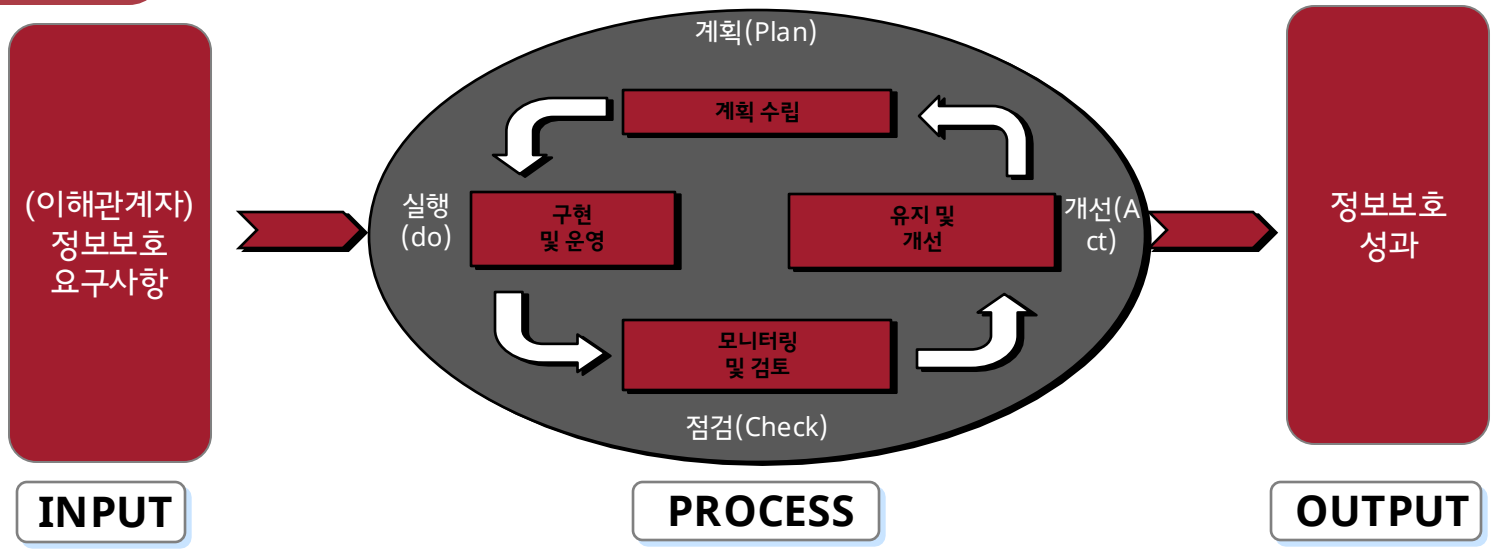
ISMS Process



[ISMS의 관리방법 2가지]
1. 데이터 중심의 IPO(Input – Process – Output)모델
- 데이터를 기반으로 보안관점의 처리와 해석을 통해 객관적인 결과 도출
2. 프로세스 중심의 PDCA 사이클
- PDCA(계획(Plan) – 실행(Do) – 점검(Check) – 조치(Action)) 사이클을 통해 보호 수준을 달성

1. ISO/IEC 27001의 필요성 > ISMS Framework

ISMS Process



ISMS 구축을 일련의 프로세스로 간주하여 각각의 프로세스를 프로세스 접근방법에 따라 명확화하고, 상호관계를 파악하여 시스템화 하여 운영 관리하는 접근방법

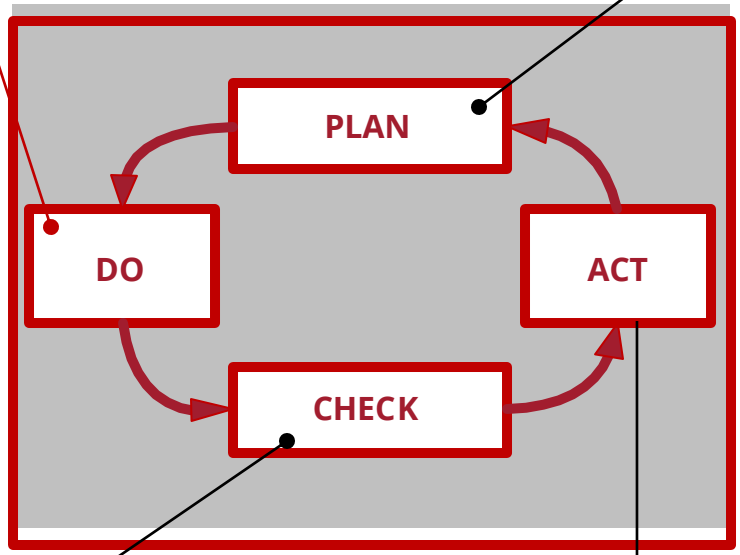
1. ISO/IEC 27001의 필요성 > ISMS Framework

프로세스 접근 방법은 ISMS에 꼭 필요한 사고로 프로세스를 명확히 하고 상호 연계와 프로세스를 시스템으로서 조직내에 적용하여 운영 관리하는 것이다.

Plan 계획 (ISMS 구축)	조직의 전반적인 비즈니스와 연계하여 정보보호 정책, 목적, 프로세스 등 수립
Do 실행 (ISMS 도입 및 운영)	정보보호 정책, 관리방안, 프로세스 등 도입 및 운영
Check 점검 (ISMS 모니터링 및 검토)	정보보호 정책, 목적 및 실제경험에 비추어 본 프로세스의 성과평가 및 그 결과검토를 위한 경영진에 대한 보고
Act 개선 조치 (ISMS 유지 및 개선)	ISMS의 지속적인 개선을 위한 ISMS의 내부감사 및 관리검토 결과 또는 시정조치 및 예방조치 실시

1. ISO/IEC 27001의 필요성 > ISMS Framework

ISMS 각 프로세스에 대한 목적 및 요구사항을 명확히 이해하는 것이 중요하다.



각 프로세스를 위한 자원분배

의사소통 경로 수립

대내외의 정보제공

피드백 수용

자료 수집

기록 유지

정확한 프로세스의 측정과 그 이행을 모니터링

수집된 정보 분석(정량적, 정성적) 분석 결과 평가

프로세스를 위한 입력과 출력 규정

프로세스별로 범위를 정의하고 고객의 요구사항을 규정

프로세스 책임자 규정

프로세스 네트워크의 전반적인 흐름과 구성도 전개

프로세스간 상호작용 규정

의도되거나 그렇지 않은 결과의 특성지정

기준에 대한 측정, 모니터링과 분석을 위한 방법 지정

경제적 문제 고려 (비용,시간,손실 등)

자료 수집을 위한 방법 규정

시정 및 예방 조치 실행

시정 및 예방 조치의 유효성과 이행에 대한 검증

2. ISO/IEC 27001의 효과적인 실무 적용 방안

보안성과 도출을 위한 ISMS 적용

보안성과는 단순히 ' ISMS 운영 ' 을 넘어, 구축된 ISMS 가 조직에 실제 어떤 기여를 하고 있는지 경영진과 이해관계자에게 증명하는 과정입니다.



① 정량적 보안지표(KPI)의 고도화

② 보안 ROI 가시화

③ 지속적 개선의 내재화

2. ISO/IEC 27001의 효과적인 실무 적용 방안

보안성과 도출을 위한 ISMS 적용

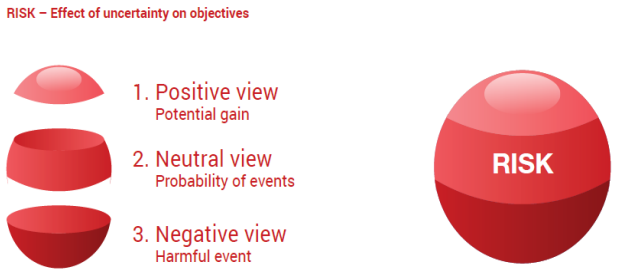
조직의 ISMS 운영에 대한 보안성과를 도출을 위하여 정량적 보안지표 고도화, 보안 ROI 가시화, 지속적 개선은 다음과 같은 방법으로 수행합니다.

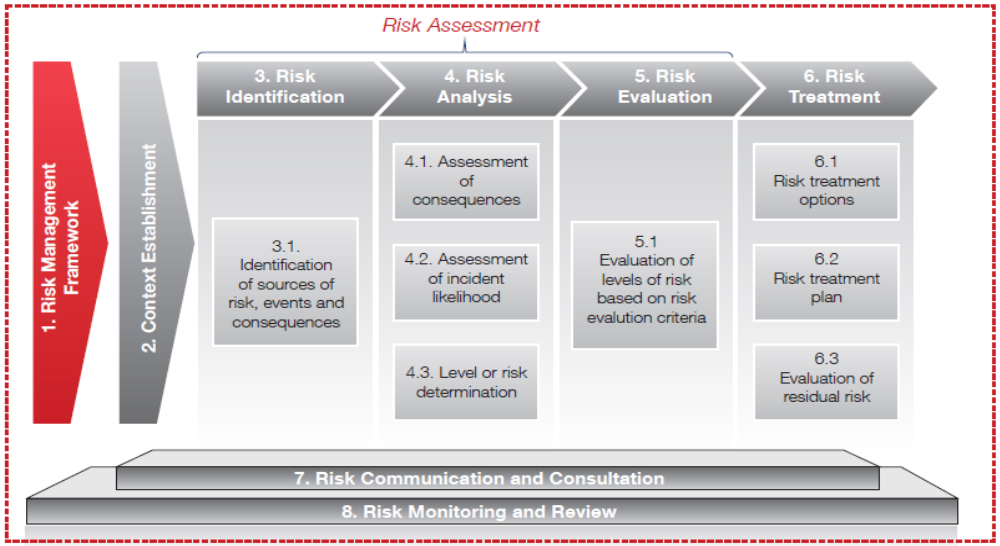
① 정량적 보안 지표(KPI) 고도화	② 보안 ROI 가시화	③ 지속적 개선의 내재화
• '보안교육 이수률'과 같은 1차원적 지표를 넘어 비즈니스 영향도와 직결되는 성과 지표를 도출해야 합니다. • (예1) 모의 악성메일 훈련 시, 열람 및 감염률 감소 추이 • (예2) 크리티컬 취약점 발견 후 조치까지의 소요시간(MTTR) 단축 • (예3) 개발단계에서의 보안 결함 사전 식별률 등	• 경영진의 언어로 보안의 가치를 표현하는 방법으로 정보보안 투자에 대한 결과를 경영진이 이해하기 쉽게 제시해야 합니다. • 보안 솔루션 도입, 인력 채용 등의 보안 투자가 동종 업계 또는 과거의 조직 현황과 비교하여 보안 사고의 손실액(ALE)을 얼마나 경감 시켰는지 객관적인 데이터를 기반으로 보고 합니다.	• ISMS PDCA 사이클이 문서화 된 것에 그치지 않고, 내부 감사 또는 보안 사고 등에서 도출된 시정 조치가 다음 해의 보안 투자 계획 및 정책, 프로세스 등의 개정으로 반드시 이어지도록 보안 업무 프로세스 간의 연결 고리를 적절하게 만들어야 합니다. • 특히, 주기적인 내부 감사를 통해 보안 업무 프로세스의 문제점을 도출하고 개선하여 ISMS 운영의 효율성과 효과성을 향상 시킵니다.

2. ISO/IEC 27001의 효과적인 실무 적용 방안

실용성 있는 리스크 평가 및 관리

일반적으로 정보보안 관련 위험을 식별, 분석, 평가 및 조치를 수행하는 방법론 ISO 31000 가이드라인을 많이 준용하며, 다음과 같이 불확실한 영향(위험)을 3가지 관점으로 바라봅니다.





Source: PECB

2. ISO/IEC 27001의 효과적인 실무 적용 방안

실용성 있는 리스크 평가 및 관리

기존의 기계적인 자산 식별과 위협/취약점 매핑을 넘어, 다양한 관점 위험을 도출하고 각 이벤트에 대하여 유연하게 대응할 수 있는 리스크 관리 체계를 만드는 것이 핵심입니다.

동적(상시) 위험평가 제도 도입

- 연 1회 정기적으로 수행하는 형식적인 위험 평가에서 벗어나, 최근 위험 동향(랜섬웨어, 공급망 공격 등)이 조직에 미치는 영향을 파악하여 시나리오 기반의 리스크 평가를 수행합니다.
- 신규 서비스 론칭, 클라우드 환경으로의 대규모 마이그레이션, 중요한 조직 개편 등 비즈니스 환경에 유의미한 변화가 발생할 때 즉각적으로 리스크를 식별하고 평가하는 '상시 리스크 관리'로 전환해야 합니다.
- 조직의 중요 데이터 관점의 위험평가 수행을 위하여 위험평가 대상, 범위, 기간, 방법, 인력 등을 조직의 IT 인프라 보안 환경에 적절하도록 Tailoring(상황에 맞는 맞춤형 방식)해야 합니다.

현업 친화적인 위험 수용 및 완화

- 정보 보안 부서의 일방적인 통제 요구나 시스템 차단은 현업의 반발(Shadow IT)을 부릅니다.
- 위험을 완화할 때 현업의 업무 가용성을 크게 저해하지 않는 '대체 통제(Compensating Control)' 방안을 함께 고민하고 제시해야 실효성 있는 위험 관리가 가능합니다.
- KPI 연계 및 경영진 참여를 위하여 정보 보안 부서만의 목표가 아닌, 전사적 핵심성과지표(KPI)에 보안 컴플라이언스 준수율을 반영해야 합니다.
- 이를 통해 정보보안이 비즈니스 연속성을 위한 투자임을 인식시키고 경영진의 지속적인 관여를 이끌어내는 것이 실무 적용의 첫걸음입니다.

2. ISO/IEC 27001의 효과적인 실무 적용 방안

ISMS 구현 시, 주요 과제 및 대응 방안

다음은 ISMS의 모델을 실제 조직에 구축 및 운영할 때 고려하여야 하는 사항이며, 이 사항들을 통해 조직의 ISMS 성숙도가 결정되며, ISMS의 지속적인 운영이 가능합니다.

① 부서별 R&R의 분산과 통합

② 한정된 리소스와 예산의 최적화

③ 신기술 표준으로의 확장 유연성

2. ISO/IEC 27001의 효과적인 실무 적용 방안

ISMS 구현 시, 주요 과제 및 대응 방안

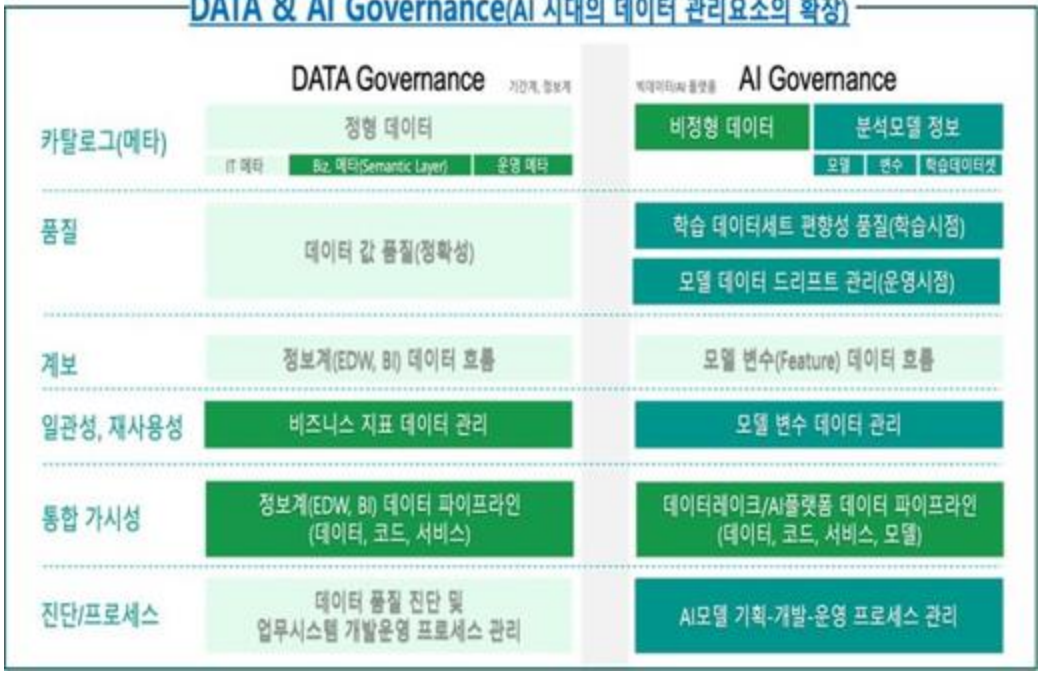
1. **부서별 R&R의 분산과 통합:** HR(입퇴사자 권한 관리), 개발/IT(시큐어 코딩 및 DevSecOps), 구매(수탁사 보안 점검) 등 각 부서의 기존 업무 매뉴얼에 ISO/IEC 27001의 요구사항을 스며들게 해야 합니다. 실무진이 '보안 업무'를 별개로 하는 것이 아니라, 본연의 업무 지침에 따르는 것만으로도 통제가 이루어지게 하는 것이 핵심입니다.

2. **한정된 리소스와 예산의 최적화:** 모든 통제 항목에 동일한 자원을 투입할 수는 없습니다. 핵심 정보 자산과 중요 서비스에 예산과 인력을 집중하는 '선택과 집중' 전략이 필수적이며, 단순 반복적인 보안 점검 업무는 자동화 도구(RPA, CSPM 등)를 도입해 리소스 부족을 타개해야 합니다.

3. **신기술 표준으로의 확장 유연성:** 향후 인공지능 경영시스템(ISO/IEC 42001)이나 클라우드/프라이버시 정보보호(ISO/IEC 27017, 27701) 등 새로운 경영시스템을 도입할 것에 대비하여, ISO 표준의 공통 상위 구조(High Level Structure, HLS)를 철저히 준수하여 뼈대를 튼튼히 구축해 두어야 확장 시 충돌을 막을 수 있습니다.

2. ISO/IEC 27001의 효과적인 실무 적용 방안

Data and AI Governance



[데이터 거버넌스에서 AI 거버넌스로 고도화]

-> 데이터 카탈로그 중요성 부각

데이터를 효과적으로 수집·저장·통합·관리·활용하는 것은 모든 기업의 최우선 과제다. 이 중 어느 것 하나 중요하지 않은 영역이 없다. 최근에는 생성형 인공지능(AI) 시대가 도래함에 따라 AI를 이용해 데이터 활용을 극대화하는 데 기업들이 많은 역량과 자원을 할애하고 있다. 기존 데이터 전략으로는 생성형 AI를 온전히 담을 수 없다는 점 때문에 기업들의 고심은 깊어지고 있다.

Source: 컴퓨터월드, 2024.06.30 기사

2. ISO/IEC 27001의 효과적인 실무 적용 방안

Data and AI Governance

< 참고 : 데이터 보호기술 개발 로드맵 >



*생성적 적대 신경망(Generative Adversarial Network): 두 개의 AI 알고리즘이 서로 경쟁적으로 데이터의 특성을 학습하여 가장 유사한 데이터를 생성하는 방식

Source: 과학기술정보통신부 제공, 2011

2. ISO/IEC 27001의 효과적인 실무 적용 방안

Data security risks caused by generative AI

NIST는 AI 거버넌스 관점에서 데이터 보안 위험을 줄이기 위하여 몇가지 원칙을 제시하고 있으며, 생성형 AI를 활용한 서비스를 개발 및 제공하는 조직은 반드시 확인 할 필요가 있습니다.

Data security risk

- ❑ 생성형 AI를 학습시키려면 다양한 소스로부터 수집한 엄청난 양의 데이터가 필요함
  ex) ChatGPT4: 인터넷의 책, 웹 텍스트, 기사 및 기타 글에서 570GB를 학습하였음
  (약 3,000억 개의 단어 -> 대부분 개인정보)
- ❑ 생성형 AI는 요청이 있는 경우, 학습한 데이터 내의 모든 정보를 공개함
- ❑ 생성형 AI는 LLM을 이용하여 추론을 할 수 있는데, 추론된 정보를 공개하거나 차별이 가능함

Consideration

- ❑ 데이터 프라이버시, 지식 재산, 게시 및 배포와 관련된 법률에 따라 생성형 AI 사용 범위 조정
- ❑ 데이터 프라이버시 위험과 관련된 다양한 유형의 생성형 AI 콘텐츠 분류
- ❑ 데이터 보안사고 대응 계획 수립 및 정기적인 테스트
- ❑ 데이터 프라이버시 위험을 포함하는 생성형 AI 관련 공급업체 평가 프로세스 수립 및 이행
- ❑ 정기적인 감사 실시 및 보안 위험 모니터링

Source: NIST

3. ISO/IEC 27001과 ISO/IEC 42001 연계

ISMS vs AIMS

구분(Aspect)	ISO/IEC 42001 (AIMS)	ISO/IEC 27001 (ISMS)
범위(Scope)	인공지능 관리 시스템(AIMS)의 구축, 운영, 유지 및 지속적 개선에 중점	정보보호 관리 시스템(ISMS)의 구축, 운영, 유지 및 지속적 개선에 중점
적용 대상(Application)	AI 시스템을 개발하거나 활용하는 조직에 적용 (특히 의료, 금융, 기술 분야 등)	모든 규모 및 산업의 조직에 적용 가능 (사이버 위협 및 데이터 유출로부터 정보자산 보호)
리스크 관리 초점 (Risk Management Focus)	윤리적 이슈, 개인정보 보호, 의사결정 편향, 예기치 않은 결과 등 AI 특화 리스크에 집중	무단 접근, 데이터 유출, 데이터 무결성 손실 등 정보보안 리스크에 집중
통제(Controls)	AI 거버넌스, 윤리적 활용, 리스크 관리에 대한 요구사항 제시 (세부 통제는 명시적으로 규정하지 않음)	접근통제, 암호화, 네트워크 보안, 사고 대응 등 구체적인 정보보안 통제 제공
규제 연계 (Regulatory Influence)	AI 관련 규제 및 윤리 가이드라인과 정렬 (예: EU AI Act, NIST AI RMF)	데이터 보호 및 개인정보 관련 법규 준수 지원 (예: GDPR, HIPAA, CCPA)

3. ISO/IEC 27001과 ISO/IEC 42001 연계

ISMS vs AIMS



ISMS vs AIMS

Interrelated Management Systems

Security Control Area	ISMS	AIMs
Risk Management	✓	✓
Transparency & Accountability	✓	✓
Continuous Improvement	✓	✓
Secure Development	✓	✓
Ethical Conduct	✓	✓
Data Governance	✓	✓
Asset Management	✓	✓
Third Party (Supply Chain) Security	✓	✓

3. ISO/IEC 27001과 ISO/IEC 42001 연계

ISMS vs AIMS – 핵심 공통점

구분 (Aspect)	ISO/IEC 27001 (ISMS)	ISO/IEC 42001 (AIMS)
관리 시스템 구조 (Management System Structure)	Annex SL(고수준 구조) 기반	Annex SL(고수준 구조) 기반
리스크 기반 접근 (Risk-Based Approach)	정보보안 리스크 식별 및 처리에 중점	AI 리스크 식별 및 대응에 중점
자산 중심 (Asset Focus)	정보 및 IT 시스템	AI 시스템, 데이터셋 및 모델
이해관계자 고려 (Stakeholder Consideration)	내부 및 외부 이해관계자	내부 및 확장된 외부 이해관계자
지속적 개선 (Continuous Improvement)	ISMS의 지속적 개선에 중점	AIMS의 지속적 개선에 중점

3. ISO/IEC 27001과 ISO/IEC 42001 연계

ISMS vs AIMS – 핵심 차이점

구분 (Aspect)	ISO/IEC 27001 (ISMS)	ISO/IEC 42001 (AIMS)
목적 (Objective)	정보의 기밀성, 무결성, 가용성(CIA) 보호	책임 있는 AI 활용 보장
리스크 기반 접근 (Risk-Based Approach)	정보보안 리스크 식별 및 처리에 중점	AI 리스크 식별 및 대응에 중점
자산 중심 (Asset Focus)	정보 및 IT 시스템	AI 시스템, 데이터셋 및 모델
거버넌스 (Governance)	정보보안 거버넌스	AI 신뢰성(보안, 안전성, 공정성, 투명성, 품질) 기반 거버넌스
통제 (Controls)	정보보안 통제	AI 라이프사이클 전반을 포함한 AI 특화 통제 (편향, 설명가능성 대응)
영향 평가 범위 (Impact Assessment Scope)	기밀성, 무결성, 가용성	법적 지위 또는 삶의 기회, 신체적·심리적 복지, 보편적 인권, 사회 전반

4. ISO/IEC 27001 부적합 사례

요구사항(Requirements)

(8.2) 위험평가

- 사례 1 : 수립된 위험관리계획서에 위험평가 기간 및 위험관리 대상과 방법이 정의 되어 있으나, 위험관리 수행 인력과 소요 예산 등 구체적인 실행계획이 누락되어 있는 경우

- 사례 2 : 전년도에는 위험평가를 수행하였으나, 금년도에는 자산의 변경이 없었다는 사유로 위험 평가를 수행하지 않은 경우

- 사례 3 : 위험관리 계획에 따라 위험 식별 및 평가를 수행하고 있으나, 범위 내 중요 정보자산에 대한 위험 식별 및 평가를 수행하지 않았거나 정보보호 관련 법적 요구 사항 준수여부에 따른 위험을 식별 및 평가하지 않은 경우

- 사례 4 : 위험관리 계획에 따라 위험 식별 및 평가를 수행하고 수용 가능한 목표 위험수준을 설정하였으나 관련 사항을 경영진(정보보호 최고책임자 등)에 보고하여 승인 받지 않은 경우

4. ISO/IEC 27001 부적합 사례

요구사항(Requirements)

(8.3) 위험처리

- 사례 1 : 이행계획 시행에 대한 결과 정보보호 최고책임자 및 개인정보 보호책임자에게 보고 하였으나 일부 미이행된 건에 대한 사유 보고 및 후속 조치가 이루어지지 않은 경우

- 사례 2 : 법에 따라 의무적으로 이행하여야 할 사항, 보안 취약성이 높은 위험 등을 별도의 보호조치 계획 없이 위험수용으로 결정하여 조치하지 않은 경우

- 사례 3 : 정보보호 및 개인정보보호 대책에 대한 이행완료 결과를 정보보호 최고책임자 및 개인정보보호책임자에게 보고하지 않은 경우(미보고)

- 사례 4 : 위험조치 이행결과보고서는 '조치 완료'로 명시되어 있으나, 관련된 위험이 여전히 존재하거나 이행결과의 정확성 및 효과성이 확인되지 않은 경우

- 사례 5 : 전년도 정보보호대책 이행계획에 따라 중 장기로 분류된 위험들이 해당년도에 구현이 되고 있지 않거나 이행결과를 경영진이 검토 및 확인하고 있지 않은 경우

4. ISO/IEC 27001 부적합 사례

부속서(Annex) A

(A.5.31) 법률, 법적, 규제 및 계약상의 요건

(A.5.34) 프라이버시 및 개인식별정보 보호

- 사례 1 : 정보통신망법 및 개인정보 보호법이 최근 개정되었으나, 개정사항이 조직에 미치는 영향을 검토하지 않았으며 정책서 및 시행문서에도 해당 내용을 반영하지 않아 정책서 및 시행문서의 내용이 법령의 내용과 일치하지 않은 경우

- 사례 2 : 조직에서 준수해야 할 법률이 개정되었으나, 해당 법률 준거성 검토를 1년 이상 수행하지 않은 경우

- 사례 3 : 법적 준거성 준수 여부에 대한 검토가 적절히 이루어지지 않아 개인정보 보호법 등 법규위반 사항이 다수 발견된 경우(개인정보 보유기간 경과, 미파기, 필수/선택 미구분)

- 사례 4 : 개인정보 보호법에 따라 개인정보 손해배상책임 보장제도 적용 대상이 되었으나, 이를 인지하지 못하여 보험 가입이나 준비금 적립을 하지 않은 경우 또는 보험 가입을 하였으나, 이용자 수 및 매출액에 따른 최저가입금액 기준을 준수하지 못한 경우

- 사례 5 : 개인정보 다운로드 사유 작성/사후 확인 미시행, 확인 절차/기준 없는 경우

4. ISO/IEC 27001 부적합 사례

부속서(Annex) A

(A.8.15) 로그 기록

- 사례 1: 로그 기록 대상, 방법, 보존기간, 검토 주기, 담당자 등에 대한 세부 기준 및 절차가 수립되어 있지 않은 경우

- 사례 2: 보안 이벤트 로그, 응용 프로그램 및 서비스 로그(Windows 2008 서버 이상) 등 중요 로그에 대한 최대 크기를 충분하게 설정하지 않아 내부 기준에 정한 기간 동안 기록 보관되고 있지 않은 경우

- 사례 3: 중요 Linux/UNIX 계열 서버에 대한 로그 기록을 별도로 백업하거나 적절히 보호하지 않아 사용자의 명령 실행 기록 및 접속 이력 등을 임의로 삭제할 수 있는 경우

- 사례 4: 개인정보처리시스템에 접속한 기록을 확인한 결과 접속자의 계정, 접속 일시, 접속자 IP주소 정보는 남기고 있으나 처리한 정보주체 정보 및 수행업무(조회, 변경, 삭제, 다운로드 등)와 관련된 정보를 남기고 있지 않은 경우

- 사례 5: 로그 서버의 용량의 충분하지 않아서 개인정보처리시스템 접속기록이 3개월 밖에 남아 있지 않은 경우(1년이상 보존, 월1회 이상 검토, 5만명 이상 등인 경우 2년 보존)

- 사례 6 : 어플리케이션의 로그생성 기능 미흡、로그기록에 대한 접근 권한 최소화、통합로그시스템 운영하는 경우 연동 누락/제외 시스템 여부

4. ISO/IEC 27001 부적합 사례

부속서(Annex) A

(A.8.16) 모니터링 활동

- 사례 1: 중요 정보를 처리하고 있는 정보시스템에 대한 이상접속(휴일 새벽 접속, 우회경로 접속 등) 또는 이상행위(대량 데이터 조회 또는 소량 데이터의 지속적 연속적 조회 등)에 대한 모니터링 및 경고 알림 정책(기준)이 수립되어 있지 않은 경우

- 사례 2: 내부 지침 또는 시스템 등에 접근 및 사용에 대한 주기적인 점검 모니터링 기준을 마련하고 있으나 실제 이상접속 및 이상행위에 대한 검토 내역이 확인되지 않는 경우

- 사례 3 : 외부로부터의 서버, 네트워크, 데이터베이스, 보안시스템에 대한 침해 시도를 인지할 수 있도록 하는 상시 또는 정기적 모니터링 체계 및 절차를 마련하고 있지 않은 경우

- 사례 4 : 외부 보안관제 전문업체 등 외부 기관에 침해시도 모니터링 업무를 위탁 하고 있으나, 위탁업체가 제공한 관련 보고서를 검토한 이력이 확인되지 않거나 위탁 대상에서 제외된 시스템에 대한 자체 모니터링 체계를 갖추고 있지 않은 경우

- 사례 5 : 내부적으로 정의한 임계치를 초과하는 이상 트래픽이 지속적으로 발견되고 있으나 이에 대한 대응조치가 이루어지고 있지 않는 경우(임계치 설정 오류, 알람 미설정, 대응조치 미비 등)

4. ISO/IEC 27001 부적합 사례

부속서(Annex) A

(A.8.20) 네트워크 접근통제

- 사례 1: 네트워크 구성도와 인터뷰를 통해 확인한 결과, 외부 지점에서 사용하는 정보시스템 및 개인정보처리시스템과 IDC에 위치한 서버간의 연결 시 일반 인터넷 회선을 통해 데이터 송수신을 처리하고 있어 내부 규정에 명시된 VPN이나 전용망 등을 이용한 통신이 이루어지고 있지 않은 경우

- 사례 2: 내부망에 위치한 DB서버 등 일부 중요 서버의 IP주소가 내부 규정과 달리 공인 IP 로 설정 되어 있고, 네트워크 접근 차단이 적용되어 있지 않은 경우

- 사례 3: 서버팜이 구성되어 있으나 네트워크 접근제어 설정 미흡으로 내부망에서 서버팜으로의 접근이 과도하게 허용되어 있는 경우

- 사례 4: 외부자(외부 개발자, 방문자 등)에게 제공되는 네트워크를 별도의 통제 없이 내부 업무 네트워크와 분리하지 않은 경우

- 사례 5: 주기적 검토 미흡 -> 방화벽 룰 – 미사용 IP 대역, 기간만료 룰, 미사용 정책(Hit-Count 0)

Q&A Session



Contact

- Website: www.pecb.com
- Phone: +1-844-426-7322
- Email: support@pecb.com |events@pecb.com