ISO/IEC 27001:2022 전환 FAQ

BSI 와 함께 귀사의 미래를 준비하세요.

1. 개정된 표준 문서의 중요한 변경 사항은 무엇인가요?

이번 개정의 주요 변경 사항은 다음과 같습니다.

- **부록 A을 완전히 개정**하여, ISO/IEC 27002:2022 변경 사항을 반영하였습니다.
  - **전체 참조 통제 집합에 대한 검토 및 개정**을 통해, 11개의 신규 통제를 도입하고 총 통제의 수가 114개에서 93개로 감소하였습니다.
  - **4개의 주요 통제 영역의 구조로 통합하였습니다**. 이전 버전에서 사용하던 14개 분류 대신 조직적 통제, 사람에 대한 통제, 물리적 통제, 기술적 통제 영역으로 분류합니다.
  - **속성의 개념을 도입했습니다.** 이로 인해 다양한 측면에서 통제 조합을 관리할 수 있습니다.
- ISO harmonized approach에 맞추기 위해 중요 변경 사항은 다음과 같습니다.
  - ISMS와 상호작용하는 표준으로 구현하기 위해 프로세스를 정의하도록 요구합니다.
  - **운영 프로세스 및 해당 프로세스 통제를 구현하기 위한 기준을 설정하도록 요구합니다(신규).**
  - 넘버링을 재구성하였습니다.
  - 조직내 정보 보안과 관련 있는 역할 커뮤니케이션에 대해 명시적인 요구합니다.
  - 신규 조항 6.3 - 변경 계획
  - 조항 7.4의 일부로 조직에서 커뮤니케이션 방법을 정하도록 요구합니다(신규).

  중요 사항: 처음 두 가지 내용은 세심한 주의가 필요합니다. 참조 통제 사항의 구조 대부분은 효과적인 프로세스 중심 접근 방식 구현에 기반하여 수정되었습니다.
- 또한, 편집상의 변경 내용은 다음과 같습니다.
  - '국제 표준'이란 단어를 '문서'로 변경하였습니다.
  - 원활한 번역을 위해 일부 영문 구조를 재배치하였습니다.

2. **이번 변경의 영향은 무엇인가요?**

이번 표준 개정은 조직의 ISMS 에 중대한 영향을 미칩니다. 조직의 ISMS 가 현재 비즈니스 관행 및 관련 위험과 일치하는지 확인하는 데 필요한 중요한 변경 사항을 포함하고 있기 때문입니다. 또한 중요 구조가 변경되면서 ISMS 가 더욱 명확하고 일관성 있게 유지될 것입니다.

조직에 따라 표준의 구현 영향력은 다를 수 있으나, 조직의 정보 보안 상태가 현재 비즈니스 운영 및 관련 위험과 정확하게 일치하는지 확인하는 것은 매우 중요합니다. 따라서 변경 사항의 세부 사항을 이해하고, 조직에 미칠 영향을 평가하여 귀사 조직에서 보유한 위험과 필요한 변경 사항을 최대한 빨리 구현하는 데 필요한 노력을 평가해야 합니다. 이렇게 하면 위험과 노력에 따른 우선순위에 기반한 통제된 방식으로 구현을 계획할 수 있습니다. BSI 의 전환 가이드-로드맵이 도움이 될 수 있습니다.

3. **전환 기간은 언제인가요?**

2022년 11월 1일에 시작하여 2025년 10월 31일까지 총 3년의 전환 기간이 있습니다. 최초 인증 및 재인증은 2024년 5월 1일부터 2022년 버전으로 이루어지며, 모든 인증서는 2025년 10월까지 전환해야 합니다. 그러나 비즈니스를 적절하게 보호하고 원활하게 전환하기 위해서는 가능한 빨리 변경 사항과 해당 변경이 조직에 미치는 영향을 이해해야 합니다. 자세한 내용은 아래 질문 7번 및 8번을 확인하세요.

4. **아직 전환 준비가 되지 않았습니다. 어떻게 해야 하나요?**

비즈니스를 효과적으로 보호하고 원활하게 전환하기 위해서는 가능한 빨리 변경 사항의 범위와 해당 변경이 조직에 미치는 영향을 이해하는 것이 중요합니다. 그래야 그 후에 위험별 우선순위에 따라 변경 사항 구현을 계획하고, 조직에 가장 적합한 전환 일정을 결정하여 효과적으로 대비할 충분한 시간을 만들 수 있습니다. BSI 의 전환 가이드-로드맵이 도움이 될 수 있습니다.

5. **교육에 대한 요건이 있으며 전환 업무에 투입하기 전에 직원을 교육시키고 싶습니다.**

좋습니다. BSI에서는 2022 버전에 대한 변경 사항을 다루는 교육을 포함하여 다양한 수준의 집체 교육,

온라인 교육, 온디맨드 이러닝 등의 교육 솔루션을 제공합니다. 비즈니스를 효과적으로 보호하고 원활하게 전환하기 위해서는 가능한 빨리 변경 사항의 범위와 해당 변경이 조직에 미치는 영향을 이해하는 것이 중요합니다. 위의 질문 1번을 확인하세요. 그렇기 때문에 교육 일정을 먼저 잡고 가능한 빨리 BSI의 전환가이드를 참고하여 진행할 것을 권장합니다. 그래야 조직에 미치는 변경 영향을 이해할 수 있습니다. 그 후에 위험 및 필요 노력에 따른 우선순위에 기반하여 다음 단계를 계획하세요.

6. **전환에 관심이 있습니다. 다음 심사와 합쳐서 진행할 수 있나요?**

당연히 가능합니다. 다만 다음 번 심사에 앞서 변경 사항과 해당 변경이 비즈니스에 미칠 영향을 이해하고, 효과적으로 비즈니스를 보호하며, 원활한 전환을 위한 대비를 마쳐 놓아야 합니다. 위의 질문 1 번, 2 번, 4 번을 확인하세요.

7. **2025년 10월까지 시간이 있는데 꼭 지금 뭘 해야 하나요?**

규정 준수를 위해 많은 작업이 필요할 수 있습니다. 또한 현재의 위험을 반영하도록 글로벌 모범 사례를 업데이트한 것으로써 중요성을 무시하면 귀사의 비즈니스가 불필요한 위험에 노출될 수도 있습니다. 모든 조직에서 가능한 빨리 변경 사항을 이해하고, 해당 변경이 조직에 미치는 영향을 이해해야 합니다. 그래야 위험과 우선순위에 기반한 통제 방안 계획 및 구현을 계획할 수 있습니다. 자세한 내용은 위의 질문 1번, 2번을 확인하세요.

8. **표준 변경 사항이 거의 없는 것 같은데, 짧은 기간 내에 전환을 해야 하는 이유가 무엇인가요?**

조항 내 변경의 숫자는 적어 보여도, 조직의 맥락에서 시작하여 필요한 모든 프로세스 및 상호 작용 결정, 이후 운영 부문의 프로세스 기준 설정 및 해당 기준에 따른 구현 작업에 이르기까지 상당한 양의 작업이 발생할 수 있습니다. 또한, 위험 평가 및 적용성 보고서(SoA)를 작성할 때 고려해야 할 통제 사항을 다루는 부록 A는 11개의 신규 통제 외에도 광범위하게 변경되었습니다. BSI에서는 모든 통제 사항을 검토하고 업데이트하였습니다. 이번 업데이트를 효과적으로 구현하려면 위험 평가 및 SoA에 대한 전체 검토가 필요합니다. 또한 변화하는 비즈니스 환경과 진화하는 위협을 반영하도록 변경하였으므로, 조직의 정보 보안 상태가 현재 비즈니스 관행 및 관련 위험을 반영하도록 신속하게 처리해야 합니다.

위의 질문 1번, 2번, 4번을 확인하세요.

9. **전환하기 전에 격차가 무엇인지 알고 싶습니다. BSI에서 도와줄 수 있나요?**

예, BSI에서 갭분석을 제공해 드릴 수 있습니다. BSI는 조직이 격차를 식별하고, 적절한 일반 교육을 통해 스스로 그 차이를 메우며, 앞으로 ISMS에 대한 높은 신뢰를 유지할 수 있도록 도와드립니다.

10. **ISO/IEC 27001:2022로 전환하려면 ISO/IEC 27002:2022 준수가 필수인가요?**

필수는 아니지만 기존 통제 사항에 대한 변경 및 신규 도입 통제 내용을 고려할 때, ISO/IEC 27002를 준수하는 것은 필요한 통제를 효과적으로 구현하는데 상당한 도움이 됩니다. 업데이트된 ISO/IEC 27002:2022는 새로운 그룹화, 속성 및 설명을 적용하는 등 '대폭 변경'되었습니다. 이를 통해 ISO/IEC 27001:2022 통제 사항을 효과적으로 구현하면서 사이버보안 프레임워크 및 기타 위험 관리 방법과 일치시키는 것이 용이 해졌습니다.

11. **ISO/IEC 27001:2013을 구현 중입니다. 그래도 2013 버전에 대한 ISMS를 인증받을 수 있나요?**

그렇습니다. 그러나 2024년 4월 30일 이전에 해야 합니다. 그 이후에는 전환 기간 이내에 2022 버전으로 전환을 마쳐야 합니다.

12. **인증서를 전환하고 업데이트하기 위해 무엇을 해야 하나요?**

인증 기관의 전환 심사를 통해 귀사 조직에서 변경 사항을 효과적으로 구현했는지 여부를 평가받아야 합니다. 그러나 변경 사항과 해당 변경이 조직에 미치는 영향을 완전히 이해하고 효과적으로 이를 구현해야 성공적으로 전환할 수 있습니다. 귀사의 ISMS가 정보 자산을 효과적으로 보호하고 성공적으로 전환하기 위해, 먼저 표준을 읽고, BSI에서 교육을 받으며, 준비 검토 과정을 진행할 것을 강력히 권장합니다. https://www.bsigroup.com/ko-KR/iso27001/training/