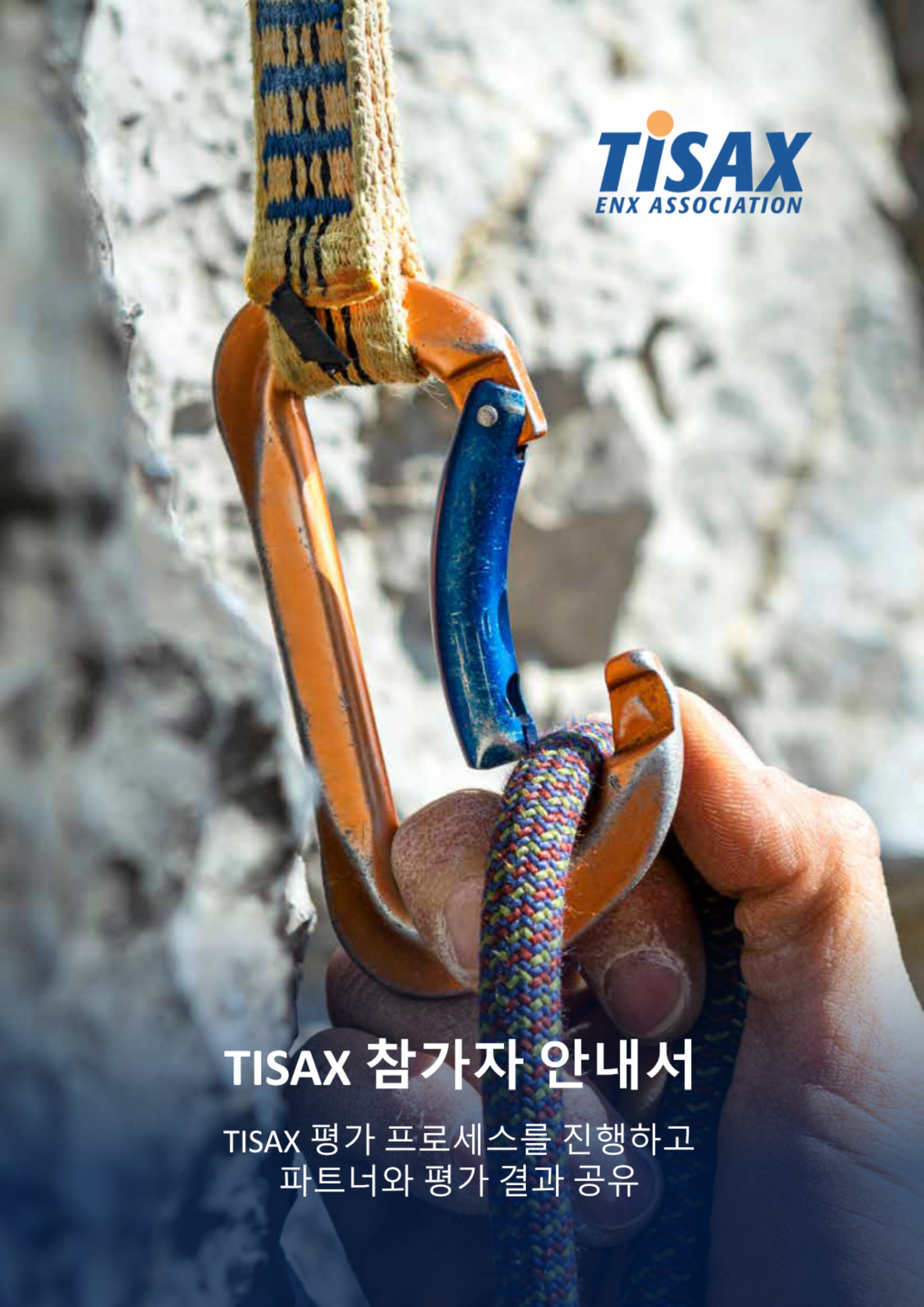


TISAX
ENX ASSOCIATION

TISAX 참가자 안내서

TISAX 평가 프로세스를 진행하고
파트너와 평가 결과 공유

게시자

ENX 협회
1901년 프랑스 법에 따라 프랑스 불로뉴비양쿠르의
수프레펙튀르에서 w923004198번으로 등록된 협회

주소
20 rue Barthélémy Danjou, 92100 Boulogne-Billancourt, France
Bockenheimer Landstraße 97-99, 60325 Frankfurt am Main, Germany

작성자

Florian Gleich

문의

tisax@enx.com
+49 69 9866927-77

버전

날짜:	2023-12-07
버전:	2.7
분류:	Public
ENX doc ID:	602-KR

저작권 고지

목차

1. 개요

1.1. 목적

TISAX(Trusted Information Security Assessment Exchange)에 오신 것을 환영합니다.

귀사의 정보 보안 관리가 “정보 보안 평가”(ISA)의 요구 사항에 따라 정의된 수준을 준수함을 입증해 달라는 파트너의 요청을 받았습니다. 그래서 이제 이 요청을 이행할 방법을 알고 싶으실 것입니다.

본 안내서는 귀사에서 파트너의 요청을 이행하거나, 파트너의 요청을 받기 전에 미리 예측하여 경쟁력을 확보할 수 있도록 하기 위한 목적으로 작성되었습니다.

본 안내서에서는 TISAX 평가에 합격하고 평가 결과를 파트너와 공유하기 위해 취해야 하는 조치에 대해 설명합니다.

정보 보안 관리 시스템(ISMS)을 구축하고 유지하기만 하는 것도 이미 복잡한 일입니다. 귀사의 정보 보안 관리가 제 기능을 수행할 수 있음을 파트너에게 입증하려면 일이 더욱 복잡해집니다. 본 안내서는 귀사의 정보 보안을 관리하는 데 도움이 되지 않습니다. 하지만 파트너에게 귀사의 노력을 입증하는 일을 최대한 쉽게 할 수 있도록 하는 것이 목표입니다.

1.2. 범위

본 안내서는 참가하실 수 있는 모든 TISAX 프로세스에 적용됩니다.

안내서는 TISAX 프로세스를 거치기 위해 알아야 하는 모든 내용을 포함합니다.

안내서에서는 평가의 핵심에 있는 정보 보안 요구 사항에 대처하는 방법에 대한 조언을 몇 개 제시합니다. 하지만 정보 보안 평가에서 합격하기 위해 해야 하는 일에 대해 전반적으로 설명하는 것은 안내서의 목적이 아닙니다.

1.3. 대상

본 안내서의 주 대상은 “정보 보안 평가”(ISA)의 요구 사항에 따라 정의된 정보 보안 관리 수준을 입증해야 하거나 입증하고자 하는 회사입니다.

TISAX 프로세스에 능동적으로 관여하는 즉시, 본 안내서에 제시된 정보는 귀사에 유익이 됩니다.

이 정보는 정의된 정보 보안 관리 수준을 입증할 것을 공급업체에 요청하는 회사에도 유익이 됩니다. 이런 회사는 본 안내서를 통해 공급업체가 요청을 이행해야 하기 위해 무엇을 해야 하는지 알게 됩니다.

1.4. 구조

TISAX에 대한 간단한 소개로 시작한 다음, 필요한 작업을 수행하는 방법에 대한 설명으로 곧바로 넘어갑니다. 프로세스를 거치기 위해 필요한 모든 정보가 알아야 하는 순서대로 나옵니다.

문서를 읽는 데 걸리는 예상 시간은 75~90분입니다.

1.5. 본 문서를 사용하는 방법

언젠가는 본 문서에 서술된 내용을 대부분 이해하고 싶을 수 있습니다. 충분히 준비하려면 안내서 전문을 읽는 것이 좋습니다.

안내서는 TISAX 프로세스의 주요 3단계를 따르는 구조로 작성되었으므로, 필요한 섹션을 읽은 후 나머지는 나중에

읽어도 됩니다.

안내서에서는 이해를 돕기 위해 도해를 사용합니다. 이런 그림의 색상에는 추가적인 의미가 있는 경우가 많습니다. 그러므로 문서를 컴퓨터 화면에서 읽거나 컬러 인쇄본으로 읽는 것이 좋습니다.

피드백은 감사히 받겠습니다. 안내서에 누락되었거나 쉽게 이해할 수 없는 내용이 있다고 생각될 경우 언제든지 알려 주십시오. ENX 협회와 향후에 안내서를 읽는 모든 독자가 피드백에 대해 감사하게 생각할 것입니다.

TISAX 참가자 안내서의 이전 버전을 이미 사용한 적이 있는 경우, 문서의 끝부분에 있는 다음 섹션에서 유용한 참고 사항을 몇 개 찾을 수 있습니다. 섹션 8, “문서 수정 내역”.

1.6. 문의

ENX 협회는 TISAX 프로세스를 안내하고 질문에 답해 드릴 준비가 되어 있습니다.

이메일 문의: tisax@enx.com
전화 문의: +49 69 9866927-77

독일(UTC+01:00)의 일반 영업 시간 동안 문의가 가능합니다.

영어 및 독일어 상담이 지원됩니다. 동료 한 명은 이탈리아어가 모국어입니다.

다음 섹션을 참조하십시오. 섹션 7.13, “부록: 불만 사항 관리”.

1.7. TISAX 참가자 안내서의 다른 언어 및 형식

TISAX 참가자 안내서는 다음 언어와 형식으로 제공됩니다.

언어	버전	형식	링크
영어	2.7	온라인	https://www.enx.com/handbook/tisax-participant-handbook.html
		오프라인	https://www.enx.com/handbook/tisax-participant-handbook-offline.html
		PDF	https://www.enx.com/handbook/TISAX%20Participant%20Handbook.pdf
독일어	2.7	온라인	https://www.enx.com/handbook/tisax-teilnehmerhandbuch.html
		오프라인	https://www.enx.com/handbook/tisax-teilnehmerhandbuch-offline.html
		PDF	https://www.enx.com/handbook/TISAX-Teilnehmerhandbuch.pdf

언어	버전	형식	링크
프랑스어	2.7	온라인	https://www.enx.com/handbook/tph-fr.html
		오프라인	https://www.enx.com/handbook/tph-fr-offline.html
		PDF	https://www.enx.com/handbook/tph-fr.pdf
중국어	2.7	온라인	https://www.enx.com/handbook/tph-cn.html
		오프라인	https://www.enx.com/handbook/tph-cn-offline.html
		PDF	https://www.enx.com/handbook/tph-cn.pdf
스페인어	2.7	온라인	https://www.enx.com/handbook/tph-es.html
		오프라인	https://www.enx.com/handbook/tph-es-offline.html
		PDF	https://www.enx.com/handbook/tph-es.pdf
일본어	2.7	온라인	https://www.enx.com/handbook/tph-jp.html
		오프라인	https://www.enx.com/handbook/tph-jp-offline.html
		PDF	https://www.enx.com/handbook/tph-jp.pdf
포르투갈어(브라질)	2.7	온라인	https://www.enx.com/handbook/tph-pt.html
		오프라인	https://www.enx.com/handbook/tph-pt-offline.html
		PDF	https://www.enx.com/handbook/tph-pt.pdf
이탈리아어	2.7	온라인	https://www.enx.com/handbook/tph-it.html
		오프라인	https://www.enx.com/handbook/tph-it-offline.html
		PDF	https://www.enx.com/handbook/tph-it.pdf
한국어	2.7	온라인	https://www.enx.com/handbook/tph-kr.html
		오프라인	https://www.enx.com/handbook/tph-kr-offline.html
		PDF	https://www.enx.com/handbook/tph-kr.pdf

중요한 참고 사항:

영어 버전이 우선합니다.
그 외 모든 언어는 영어 버전을 번역한 것입니다.
내용에 차이가 있는 경우 영어 버전이 우선합니다.

1.7.1. 한국어 번역

본 TISAX 참가자 안내서는 영어 버전의 번역본입니다.

TISAX의 기초를 이루는 모든 문서(예: 모든 TISAX 감사 서비스 제공자 계약서 및 요구 사항)는 영어로 작성되었습니다. 따라서 파트너 또는 감사 제공자가 일부 TISAX 관련 용어를 영어로 사용할 수 있습니다.

언어를 연결할 수 있도록 하기 위해, TISAX 참가자 안내서의 번역본에는 영문 TISAX 용어를 그대로 사용하거나 번역문 바로 뒤에 괄호로 묶어서 표시했습니다.

1.7.2. 온라인 형식에 대한 설명

각 섹션마다 고유 ID(형식: ID1234)가 있습니다.
ID는 언어에 관계없이 특정 섹션을 참조합니다.

다음과 같은 방법으로 특정 섹션에 연결할 수 있습니다.

- 섹션 제목을 마우스 오른쪽 단추로 클릭하고 링크 복사, 또는
- 섹션 제목을 클릭하고 브라우저의 주소 표시줄에서 링크 복사.

대부분의 그림은 여기에 기본적으로 표시된 것보다 더 큰 크기로 확인할 수 있습니다. 그림을 클릭하면 더 큰 그림이 열립니다.

1.7.3. 오프라인 형식에 대한 설명

오프라인 형식에는 온라인 형식의 기능이 대부분 유지됩니다. 대표적인 예로, 그림이 HTML 파일에 포함되어 있습니다. 오프라인 형식을 사용하려면 파일이 하나만 필요합니다.

온라인 형식과 달리, 오프라인 형식에는 다음이 포함되지 않습니다.

- 더 큰 이미지
- 온라인 형식의 원래 글꼴
  브라우저의 기본 설정에 따라 글꼴이 정의됩니다.

1.7.4. PDF 형식에 대한 설명

PDF 형식을 컴퓨터에서 사용해도 참조 링크를 모두 클릭할 수 있습니다. 하지만 PDF 버전을 인쇄하면 페이지 번호 같은 것이 없고, 참조를 직접 찾아봐야 합니다.

2. 소개

이어지는 내용에서는 TISAX의 개념을 소개합니다.

시간이 많지 않으면 이 내용을 건너뛰고 다음 섹션에서 곧바로 시작해도 됩니다. 섹션 4.3, “등록 준비” .

2.1. TISAX가 왜 필요할까요?

이 글을 보고 계신 이유가 무엇일까요?

이 질문에 답하기 위해, 비즈니스에 대한 전반적인 설명과 특히 정보 보호에 대한 설명으로 시작하겠습니다.

파트너가 있다고 상상해 보십시오. 파트너에게 비밀 정보가 있습니다. 파트너가 이 정보를 공급업체인 귀사와 공유하려고 합니다. 귀사와 파트너가 협력하면 가치가 창출됩니다. 파트너가 귀사와 공유하는 정보는 이 가치 창출의 중요한 일부분입니다. 그래서 파트너는 이런 정보를 적절하게 보호하길 원합니다. 그리고 귀사에서 정보를 파트너와 똑같은 수준으로 주의를 기울여서 처리하고 있다고 확신할 수 있기를 원합니다.

하지만 어떻게 하면 파트너가 정보를 귀사에 믿고 맡겨도 된다고 확신할 수 있을까요? 귀사를 그냥 "믿을" 수만은 없습니다. 파트너가 어떤 증거를 확인해야 합니다.

그러면 두 가지 문제가 제기됩니다. 정보의 "안전한" 처리가 무엇을 의미하는지 누가 정할까요? 안전한 처리를 어떻게 증명할까요?

2.2. "안전(보안)"의 의미를 누가 정의할까요?

귀사와 귀사의 파트너만 이런 문제에 처음 부닥치는 것은 아닙니다. 거의 모두가 이런 문제에 대한 답을 찾아야 하고, 대부분의 답에는 유사점이 있을 것입니다.

공통적인 문제에 대한 솔루션을 매번 따로 만들지 않고 문제를 해결하는 표준 방식이 있으면 모든 것을 처음부터 만들어야 하는 부담이 없어집니다. 표준을 정의하려면 많은 노력이 필요하지만, 한 번만 하면 되고 표준을 따르는 사람이 매번 유익을 얻게 됩니다.

올바른 정보 보호 방법 무엇인지에 대한 생각은 분명 다양합니다. 하지만 앞에서 언급한 이점 때문에 대부분의 회사는 표준을 정합니다. 표준은 특정한 문제를 해결하는 효과가 입증되고 오랜 시간에 걸쳐 검증된 최선의 방법의 압축된 형태입니다.

귀사의 경우, (정보 보안 관리 시스템, 즉 ISMS에 대한) ISO/IEC 27001 같은 표준과 그 이행은 비밀 정보를 최첨단으로 안전하게 처리하는 방법이 됩니다. 이와 같은 표준을 사용하면 매번 같은 일을 반복해야 하는 낭비가 없어집니다. 표준은 두 회사가 비밀 데이터를 교환해야 할 때 공통된 근거를 제시한다는 더 중요한 장점이 있습니다.

2.3. 자동차 산업의 방식

산업과 무관한 공통 표준은 본질적으로 자동차 회사의 구체적인 필요에 맞춰지지 않고 모든 산업에 적용 가능한 솔루션으로 개발됩니다.

오래 전에 자동차 산업은 업계의 보다 구체적인 필요에 적합한 표준을 정의하고 개선하는 등의 목표를 달성하기 위해 협회를 설립했습니다. VDA(Verband der Automobilindustrie)는 그 중 하나입니다. 정보 보안을 다루는 워킹그룹에 참여한 자동차 산업의 몇몇 회사는 각사에 필요한 사항이 비슷해서 기존 정보 보안 관리 표준을 자동차 산업에 맞게 수정할 수 있겠다는 결론을 내렸습니다.

이 회사들은 자동차 산업에서 널리 인정되는 정보 보안 요구 사항에 관한 설문지를 함께 만들었습니다. 이것을 "정보 보안 평가"(ISA)라고 합니다.

ISA를 통해 이제는 “안전(보안)의 의미를 누가 정의하는가?” 라는 질문에 대한 답을 얻게 되었습니다. VDA를 통해, 자동차 산업은 이 답을 구성원들에게 직접 제시합니다.

2.4. 보안을 어떻게 효율적으로 입증할까요?

ISA를 내부용으로만 사용하는 회사가 있는가 하면, 자사 공급업체의 정보 보관 관리의 성숙도를 평가하기 위해 사용하는 회사도 있습니다. 경우에 따라서는 자가 평가가 비즈니스 관계에 충분합니다. 하지만 특정한 경우에는 회사가 자사 공급업체의 정보 보안 관리를 전체적으로 평가(현장 감사 포함)하는 경우도 있습니다.

정보 보안 관리의 필요성에 대한 인식이 전반적으로 높아지고 ISA가 정보 보안 평가 도구로 더 널리 채택됨에 따라 여러 파트너에게 유사한 요청을 받는 공급업체가 많아지고 있습니다.

이런 파트너는 계속 다른 표준을 적용했고, 표준 해석 방법에 대한 의견이 다양했습니다. 하지만 공급업체들은 근본적으로 같은 것을 증명해야 했고, 방법만 달랐습니다.

그리고 파트너들에게 정보 보안 관리 수준을 증명해 달라는 요청을 받는 공급업체가 많아질수록 반복되는 노력에 관한 불만이 점점 커졌습니다. 여러 감사관에게 같은 정보 보안 관리 조치를 계속 보여주는 것은 결코 효율적이지 않습니다.

어떻게 하면 효율을 높일 수 있을까요? 감사관의 보고서를 여러 파트너에 다시 사용할 수 있으면 도움이 되지 않을까요?

ENX 워킹그룹에서 ISA를 유지관리하는 책임을 지는 OEM 및 공급업체들은 자사 공급업체들의 불만 사항에 귀를 기울였습니다. 이제 이들은 자사 공급업체와 자동차 산업의 다른 모든 회사에 "보안을 어떻게 입증하는가?" 라는 질문에 대한 답을 제시합니다.

답은 “Trusted Information Security Assessment Exchange”(🇰🇷 “신뢰할 수 있는 정보 보안 평가 교환”)의 약자인 TISAX입니다.

3. TISAX 프로세스

3.1. 개요

TISAX 프로세스는 일반적으로[1] 파트너 중 하나가 “정보 보안 평가”(ISA)의 요구 사항에 따라 정의된 정보 보안 관리 수준을 입증해 달라고 요청하는 것으로 시작됩니다. 이 요청에 따르려면 3단계로 구성된 TISAX 프로세스를 완료해야 합니다. 이 섹션에서는 이행해야 하는 단계를 요약합니다.

TISAX 프로세스를 구성하는 3단계는 다음과 같습니다.

그림 1. TISAX 프로세스 개요

1. 1 단계
   등록
2. 2 단계
   평가
3. 3 단계
   교환

1. 등록
   ENX 협회에서 귀사와 평가에 포함되어야 하는 사항에 대한 정보를 수집합니다.
2. 평가
   TISAX 감사 제공자가 실시하는 평가를 받습니다.
3. 교환
   평가 결과를 파트너와 공유합니다.

각 단계는 부단계로 구성됩니다. 부단계는 아래의 세 섹션에 약술되어 있고, 더 아래에 있는 각 섹션에 자세히 설명되어 있습니다.

참고:

당연히 TISAX 평가 결과를 얻는 데 얼마나 걸릴지 알려드리고 싶지만, 이 기간을 신뢰할 수 있는 방법으로 예측하기는 불가능하다는 점을 양해해 주시기 바랍니다. 전체 TISAX 프로세스 소요 시간을 좌우하는 요인이 너무 많고, 회사 규모 및 평가 목표와 각 회사의 정보 보안 관리 시스템 준비 상태가 매우 다양해서 이렇게 하는 것이 불가능합니다.

3.2. 등록

첫 단계는 TISAX 등록입니다.

TISAX 등록의 주된 목적은 귀사에 대한 정보를 수집하는 것입니다. ENX 협회는 이 정보를 제공하는 데 도움이 되는 온라인 등록 프로세스를 사용합니다.

등록은 모든 후속 단계의 전제 조건입니다. 등록 수수료가 부과됩니다.

온라인 등록 프로세스를 진행하는 동안:

- 자세한 연락처 및 대금청구 정보가 요청됩니다.
- 이용 약관에 동의해야 합니다.
- 정보 보안 평가의 범위를 정의할 수 있습니다.

이 단계부터 곧바로 시작하려면 다음을 참조하십시오. 섹션 4, “등록(1 단계)”.

온라인 등록 프로세스에 대한 자세한 설명은 다음을 참조하십시오. 섹션 4.5, “온라인 등록 프로세스”. 하지만 곧바로 시작하려면 다음 웹 페이지로 이동하십시오. enx.com/en-US/TISAX/.

3.3. 평가

두 번째 단계에는 정보 보안 평가를 거칩니다.

이 단계에는 부단계가 네 개 있습니다.

a. 평가 준비
평가를 준비해야 합니다. 준비해야 하는 정도는 귀사 정보 보안 관리 시스템의 현재 성숙도 수준에 따라 다릅니다. 준비는 ISA 카탈로그를 근거로 해야 합니다.

b. 감사 제공자 선택
ENX 협회의 TISAX 감사 제공자 중에서 선택해야 합니다.

c. 정보 보안 평가
선택한 감사 제공자가 파트너의 요구 사항과 일치하는 평가 범위에 따라 평가를 실시합니다. 평가 프로세스에는 최소한 첫 감사가 포함됩니다.
귀사가 평가에 곧바로 합격하지 않으면 평가 프로세스에 추가 단계가 필요할 수 있습니다.

d. 평가 결과
평가에 합격한 후에는 감사 제공자가 공식 TISAX 평가 보고서를 귀사에 제공합니다. 평가 결과에는 TISAX 레이블도 부여됩니다[2].

이 단계에 대한 자세한 내용은 다음을 참조하십시오. 섹션 5, “평가(2 단계)”.

3.4. 교환

세 번째이자 마지막 단계에는 평가 결과를 파트너와 공유합니다. TISAX 평가 보고서의 내용은 수준별 구조를 따릅니다. 파트너가 액세스할 수 있는 수준을 귀사에서 결정할 수 있습니다.

평가 결과는 3년 동안 유효합니다. 3년 후에도 귀사가 계속 파트너의 공급업체인 경우, 이 3 단계 프로세스를 다시 거쳐야 합니다[3].

이 단계에 대한 자세한 내용은 다음을 참조하십시오. 섹션 6, “교환(3 단계)”.

이제 TISAX 프로세스가 무엇인지에 대한 기초적인 개념에 대해 알아보았으므로, 각 단계를 완료하는 방법에 대한 설명을 이어지는 내용에서 확인할 수 있습니다.

4. 등록(1 단계)

등록 섹션을 읽는 데 걸리는 예상 시간은 30~40분입니다.

4.1. 개요

TISAX 등록은 첫 단계입니다. 등록은 모든 후속 단계의 전제 조건입니다.

이어지는 내용에서는 등록 과정을 안내합니다.

1. 필수적인 새 용어에 대한 설명으로 시작합니다.
2. 그런 다음 온라인 등록 프로세스를 준비하기 위해 해야 할 일에 대해 알립니다.
3. 그런 다음 온라인 등록 프로세스를 안내합니다.

4.2. 귀사 = TISAX 참가자

알아야 하는 새 용어를 먼저 소개하겠습니다. 지금까지 귀사는 “공급업체” 였습니다. 여기까지 온 이유는 “고객” 의 요구 사항을 충족하기 위해서입니다. 하지만 TISAX에서는 이 두 역할이 사실상 구별되지 않습니다. 등록하면 누구나 TISAX “참가자” 가 됩니다. 귀사와 귀사의 파트너는 모두 정보 보안 평가 결과 교환에 "참가"합니다.

그림 2. 등록하여 TISAX 참가자 되기

1. 귀사
2. TISAX 등록
3. TISAX 참가자

처음부터 두 역할을 구별하기 위해, 여기서는 공급업체인 귀사를 “능동적 참가자” 라고 지칭합니다. 귀사의 파트너는 “수동적 참가자” 라고 지칭합니다. 귀사는 “능동적 참가자” 로서 TISAX 평가를 받고 평과 결과를 다른 참가자들과 공유합니다. “수동적 참가자” 는 TISAX 평가를 받을 것을 귀사에 요청한 참가자입니다. “수동적 참가자” 는 귀사의 평가 결과를 수신합니다.

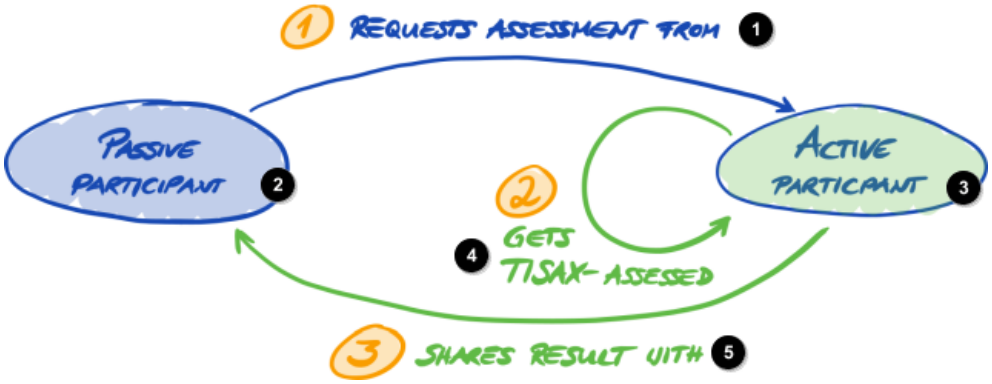


그림 3. 수동적 참가자와 능동적 참가자

1. 1 평가를 받을 것을 요청
2. 수동적 참가자
3. 능동적 참가자
4. 2 TISAX 평가를 받음
5. 3 결과 공유

모든 회사는 두 역할을 모두 수행할 수 있습니다. 귀사는 평가 결과를 파트너와 공유함과 동시에 공급업체에 TISAX 평가를 받으라고 요청할 수 있습니다.

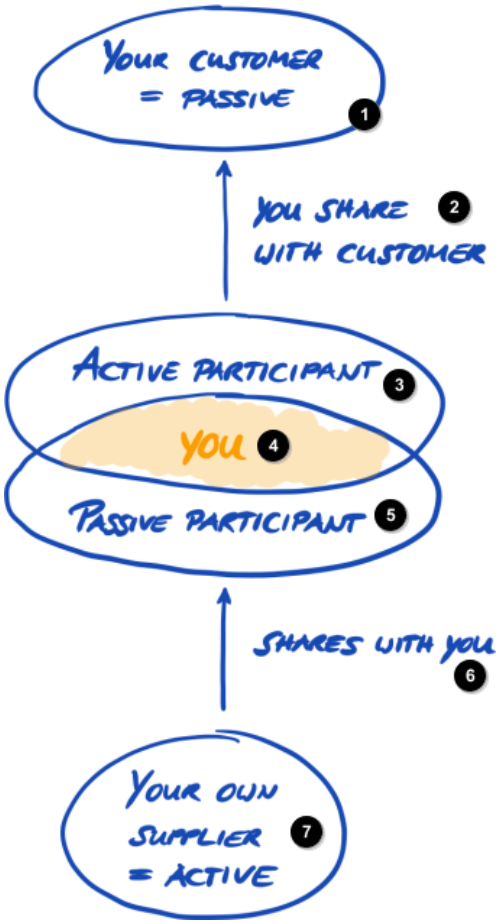


그림 4. TISAX 참가자는 동시에 능동적이고 수동적일 수 있음

1. 귀사의 고객
   = 수동적
2. 고객과 공유
3. 능동적 참가자
4. 귀사
5. 수동적 참가자

6 귀사와 공유

7 귀사의 자체 공급업체
= 능동적

귀사의 공급업체가 보호해야 할 필요가 있는 귀사 파트너의 정보도 처리하는 경우에는 특히 귀사의 공급업체에도 TISAX 평가를 받을 것을 요청하는 것이 좋습니다.

4.3. 등록 준비

이 섹션에서는 등록을 준비하는 방법에 대한 권장 사항을 제시합니다. 등록 프로세스 자체에 대해서는 다음 섹션에서 자세히 설명합니다. 섹션 4.5, “온라인 등록 프로세스”.

온라인 등록 프로세스 진행을 시작하기 전에 다음과 같은 준비 작업이 적극 권장됩니다.

- 정보 미리 수집
- 몇 가지 결정 내리기

4.3.1. 법적 기초

일반적으로 두 가지 계약에 서명해야 합니다. 첫 계약은 귀사와 ENX 협회가 체결하는 “TISAX 참가 일반 약관”(TISAX 참가자 GTC)입니다. 두 번째 계약은 귀사와 TISAX 감사 제공자가 체결합니다. 등록에 관해서는 첫 번째 계약만 살펴보겠습니다.

TISAX 참가자 GTC는 ENX 협회와 귀사의 상호 관계와 귀사와 다른 TISAX 참가자의 관계에 적용됩니다. 이 약관은 모두의 권리와 의무를 규정합니다. 대부분의 계약에 있는 일반적인 조항 외에, 약관에서는 TISAX 프로세스 도중에 교환 및 수집되는 정보의 처리에 대해 자세히 규정합니다. 이런 규칙의 핵심적인 목표는 TISAX 평가 결과를 비밀로 유지하는 것입니다. 모든 TISAX 참가자에게 같은 규칙이 적용되므로, 파트너가 (수동적 참가자 역할을 수행하면서) 귀사의 TISAX 평가 결과를 적절하게 보호할 것이라고 기대할 수 있습니다.

ENX 협회는 온라인 등록 프로세스의 이른 초기에 귀사에 TISAX 참가자 GTC 동의를 요청합니다. 이 약관은 실제 계약이므로 온라인 프로세스를 시작하기 전에 TISAX 참가자 GTC를 읽어보는 것이 좋습니다. 그 이유 중 하나는 사내 또는 외부 변호사의 허가를 받아야 하는 사내 직책이 있을 수 있기 때문입니다.

“TISAX 참가자 일반 약관”은[4] ENX 협회 웹 사이트에서 다운로드할 수 있습니다. 주소:
enx.com/en-US/TISAX/downloads/

PDF 직접 다운로드:
enx.com/tisaxgtcen.pdf

온라인 등록 프로세스를 진행하는 동안 다음과 같은 필수 확인란 두 개를 선택해야 합니다.

☒ We accept the TISAX Participation General Terms and Conditions (TISAX 참가 일반 약관에 동의합니다)

☒ We confirm knowledge of Applicant’s release of Audit Providers’ professional duties of secrecy acc. to Sec. IX.5. and X.3 of the TISAX Participation General Terms and Conditions; (TISAX 참가 일반 약관 IX.5. 및 X.3항에 따른 감사 제공자의 직업상 비밀유지 의무를 신청인이 면제함을 알고 있음을 확인합니다.)

이 두 번째 확인란이 있는 이유는 ENX 협회의 몇몇 TISAX 감사 제공자가 공인회계사이기 때문입니다. 이들에게는 직업상 비밀유지에 관해 특별히 요구되는 사항이 있습니다. 일반적으로, 공인회계사이기도 한 감사 제공자는 직업상 비밀유지에 관해 특별히 요구되는 사항 때문에 정보를 ENX 협회와 공유할 수 없습니다. 이 경우, 특히 ENX 협회의 거버넌스 역할에 필요한 통제 옵션이 취소됩니다. 그러므로 이 동의가 필요합니다. 상자를 선택하기 전에 해당 조항에 특별히 주의를 기울여야 합니다.

귀사에서 비밀 정보 처리자와 비밀유지 계약(NDA)을 체결해야 한다고 일반적으로 요구하는 경우, GTC의 해당하는 조항을 각각 살펴보십시오. 모든 우려 사항에 대한 답을 얻게 될 것입니다. 또한 귀사에서는 일반적으로 ENX 협회에 비밀 정보를 전혀 제공하지 않아도 됩니다.

법률 섹션 끝에서는 시스템이 제대로 작동하려면 모두가 같은 규칙에 동의해야 함을 양해해 줄 것을 요청합니다. 그러므로 ENX 협회는 추가적인 일반 약관에 동의할 수 없습니다[5].

4.3.2. TISAX 평가 범위

TISAX 프로세스의 두 번째 단계에 TISAX 감사 제공자 중 한 명이 정보 보안 평가를 실시합니다. 제공자는 어디서 시작하고 어디서 멈춰야 하는지 알아야 합니다. 그렇기 때문에 "평가 범위"를 정의해야 합니다.

"평가 범위"는 정보 보안 평가의 범위를 서술합니다. 간단히 말해, 파트너의 비밀 정보를 처리하는 귀사의 모든 부분이 평가 범위에 포함됩니다. 평가 범위는 감사 제공자의 직무를 구성하는 중요한 요소라고 간주할 수 있습니다. 평가 범위는 감사 제공자가 평가해야 하는 것을 정합니다.

평가 범위가 중요한 두 가지 이유는 다음과 같습니다.

a. 평가 결과는 각각의 평가 범위에 귀사에서 파트너 정보를 처리하는 모든 부분이 포함되는 경우에만 파트너의 요구 사항을 충족합니다.

b. 정확하게 정의된 평가 범위는 TISAX 제공자가 비용을 유의미하게 계산하기 위한 필수적인 전제 조건입니다.

중요한 참고 사항:

ISO/IEC 27001과 TISAX 비교

첫째, 다음 두 가지 유형의 범위를 구별해야 합니다.
1) 정보 보안 관리 시스템(ISMS)의 범위
2) 평가의 범위
이 두 범위는 동일하지 않을 수 있습니다.

ISO/IEC 27001 인증을 위해서는 ISMS의 범위를 (“범위 명세” 에서) 정의합니다. ISMS의 범위는 완전히 자유롭게 정의할 수 있습니다. 하지만 평가 범위("감사 범위"라고도 함)는 귀사의 ISMS 범위와 동일해야 합니다.

TISAX의 경우 ISMS도 정의해야 합니다. 하지만 평가 범위는 다를 수 있습니다.

ISO/IEC 27001 인증의 경우 ISMS 범위를 정의하는 방법을 통해 평가 범위를 자유롭게 정할 수 있습니다.

반대로, TISAX의 경우 평가 범위가 미리 정의됩니다. 평가 범위는 ISMS의 범위보다 작을 수 있습니다. 하지만 평가 범위는 ISMS 범위 안에 있어야 합니다.

4.3.2.1. 범위 설명

범위 설명은 평가 범위를 정의합니다. 범위 설명은 다음 두 가지 유형 중에서 하나를 선택해야 합니다.

1. Standard scope (🇰🇷 표준 범위)
2. Custom scope (🇰🇷 맞춤 범위)
    a. Custom extended scope (🇰🇷 맞춤 확장 범위)
    b. Full custom scope (🇰🇷 전체 맞춤 범위)

표준 범위에 대해서는 다음 섹션에서 설명합니다. 표준 범위는 거의 모든(99% 이상) 참가자에게 적합한 선택입니다. 그러므로 맞춤 범위에 대해서는 다음 섹션에서만 설명합니다. 섹션 7.8, “부록: 맞춤 범위” .

4.3.2.2. 표준 범위

표준 범위 설명은 TISAX 평가의 근거입니다. 다른 TISAX 참가자들은 표준 범위 설명에 근거한 평가 결과만 수락합니다.

표준 범위 설명은 미리 정의되어 있어 변경할 수 없습니다.

표준 범위를 사용하면 정의를 직접 생각해 낼 필요가 없다는 중요한 이점이 있습니다.

다음은 표준 범위 설명(2.0 버전)입니다.

The TISAX assessment scope defines the scope of the assessment. The assessment includes all processes, procedures and resources under responsibility of the assessed organization that are relevant to the security of the protection objects and their protection goals as defined in the listed assessment objectives at the listed locations.
The assessment is conducted at least in the highest assessment level listed in any of the listed assessment objectives. All assessment criteria listed in the listed assessment objectives are subject to the assessment.

TISAX 평가 범위는 평가의 범위를 정의합니다. 평가에는 평가 받는 조직이 책임지고 나열된 위치의 나열된 평가 목표에 정의된 보호 개체의 보안과 각각의 보호 목표와 관련이 있는 모든 프로세스, 절차 및 리소스가 포함됩니다.
평가는 최소한 나열된 평가 목표에 나열된 가장 높은 평가 수준으로 수행됩니다. 나열된 평가 목표에 나열된 모든 평가 기준이 평가 대상입니다.

표준 범위 선택이 적극 권장됩니다. 모든 TISAX 참가자는 표준 범위에 근거한 정보 보안 평가 결과를 수락합니다.

4.3.2.3. 범위 지정

범위 유형을 정의한 다음에는 평가 범위에 포함되는 위치를 결정하는 작업을 수행해야 합니다.

귀사의 규모가 작은 경우(위치 1개) 이 일은 쉽습니다. 간단히 해당 위치를 평가 범위에 추가하기만 하면 됩니다.

회사 규모가 큰 경우 평가 범위를 한 개보다 많이 등록하는 방법을 고려할 수 있습니다.

귀사의 모든 위치를 포함하는 범위가 하나만 있으면 다음과 같은 장점이 있습니다.

- 평가 보고서, 평가 결과, 만료 날짜가 하나씩만 있습니다.
- TISAX 감사 제공자가 귀사의 중심 프로세스, 절차 및 리소스를 한 번만 평가하면 되므로 평가 비용이 절감되는 이점이 있습니다.

하지만 범위가 하나뿐이면 다음과 같은 단점이 있을 수 있습니다.

- 모든 위치의 평가 목표가 같아야 합니다.
- TISAX 감사 제공자가 모든 위치를 평가한 후에만 평가 결과가 제공됩니다. 이 사실은 평가 결과가 긴급하게 필요한 경우에 중요할 수 있습니다.
- 평가 결과가 좋으려면 모든 위치에서 평가에 합격해야 합니다. 불합격하는 위치가 하나만 있어도 긍정적인

평가 결과를 받을 수 없습니다. 해결 방법은 다음과 같습니다. A) 불합격한 위치를 범위에서 제거, b) 문제 해결하고, c) 해당 위치를 이후에 범위 확장 평가로 추가합니다.

4.3.2.4. 범위 맞춤 조정

범위를 하나만 지정할지 아니면 몇 개 지정할 것인지의 문제에는 귀사만 답할 수 있습니다. 하지만 다음 도표에 있는 질문에 답하면 결정하는 데 도움이 될 수 있습니다.

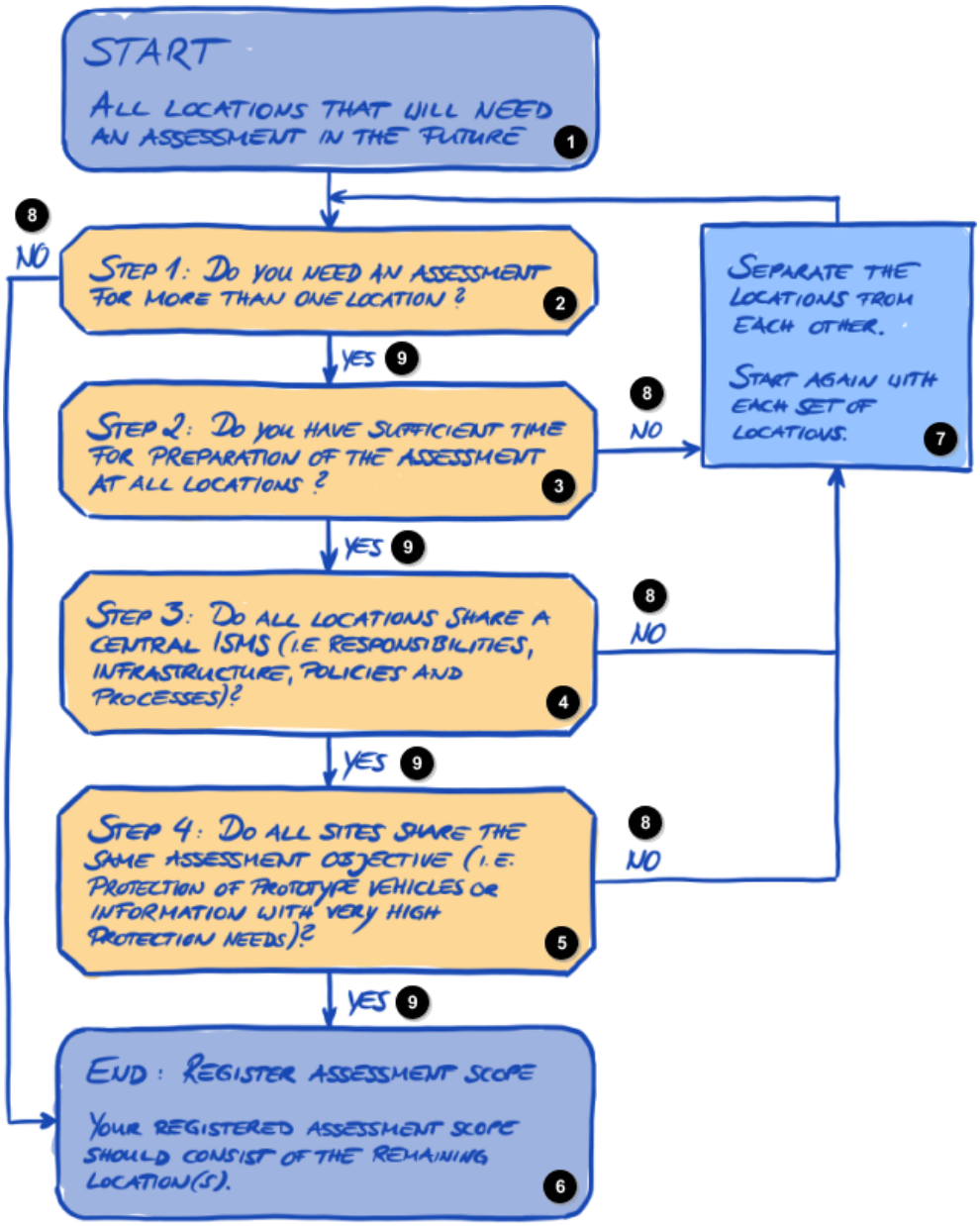


그림 5. 범위 맞춤 조정 결정 트리

1. 시작
   향후에 평가가 필요할 모든 위치
2. 1 단계: 평가가 필요한 위치가 하나보다 많습니까?
3. 2 단계: 모든 위치에서 평가를 준비할 시간이 충분합니까?
4. 3 단계: 모든 위치에서 중앙 ISMS(책임, 인프라, 정책 및 프로세스)를 공유합니까?

5. 4 단계: 모든 현장의 평가 목표가 같습니까(매우 높은 보호 수준이 필요한 프로토타입 차량 또는 정보의 보호)?
6. 끝: 평가 범위 등록
   등록된 평가 범위에는 나머지 위치가 포함되어야 합니다.
7. 위치를 서로 분리합니다.
   각 위치 집합으로 다시 시작합니다.
8. 아니요
9. 예

참고:

이 결정을 두려워하지 마십시오. 감사 제공자가 평가를 미칠 때까지 범위를 변경할 수 있습니다.

예를 들어 평가를 준비하는 동안 범위가 적합하지 않음을 알게 되고, 그래서 범위를 적절히 변경할 수 있습니다. 아니면 감사 제공자가 평가의 초기 단계에 범위 변경을 권장할 수도 있습니다.

추가 참고 사항:

- 엄밀히 말하면 ENX 포털에서 온라인 등록 프로세스 도중에 정의했던 평가 범위는 변경할 수 없습니다. 하지만 감사 제공자가 평가 결과를 ENX 포털에 업로드할 때 평가 범위를 업데이트할 수는 있습니다.
- 범위에 항목을 추가하면 수수료가 많아지고, 위치를 범위에서 제거해도 환불되지 않습니다. 감사 제공자는 원래의 범위를 비용 계산의 기준으로 사용하므로, 귀사에서도 비용 변경을 예상해야 합니다.

4.3.2.5. 범위 위치

이제 평가 범위에 포함되는 위치를 결정했으므로 위치 관련 정보를 계속 수집할 수 있습니다.

각 위치마다 회사 이름과 주소 같은 정보가 요청됩니다. TISAX 감사 제공자가 회사 구조를 더 잘 알 수 있도록 몇 가지 추가 정보도 요청됩니다. 답변을 근거로 제공자의 작업량이 추산됩니다.

각 위치에 대해 다음과 같은 세부 정보를 제공할 수 있도록 준비하십시오(빨간색 별표 * 는 온라인 프로세스에서 필수인 정보를 나타냄).

필드	옵션
위치 이름 *	해당 없음
D&B D-U-N-S NUMBER	해당 없음
위치 유형 *	회사가 단독으로 소유 및 사용하는 건물 회사가 임차하는 건물 공유 건물에서 회시가 임차하는 층/사무실 다른 회사들과 공유하는 사무실 자체 소유 데이터센터 공유하는 데이터센터
수동적 현장 보호 *	예 아니요

필드	옵션
산업 (복수 선택 가능)	정보 기술(IT) ☒ IT 서비스 ☒ 통신 서비스 ☒ 소프트웨어 개발
	경영 ☒ 컨설팅
	미디어 ☒ 마케팅 ☒ 대행사 ☒ 인쇄 서비스 ☒ 사진 ☒ 번역 서비스
	연구 개발 ☒ 차량 테스트 ☒ 차량 시뮬레이션 ☒ 프로토타입 제작 ☒ 자동차 축소 모델 ☒ 개발 서비스 ☒ CAx 개발 서비스
	생산 ☒ 생산 서비스 ☒ 계약 제조 ☒ 생산 현장 ☒ 물류
	영업 및 AS ☒ 수입, NSC ☒ 영업소 ☒ 금융 서비스 ☒ 보험 ☒ 보험금 지급
	기타 산업 (기입 요망)

필드	옵션
위치의 직원 수: 전체 *	0 1~10 11~100 101~1,000 1.001~5,000 5,001명 이상
위치의 직원 수: IT *	0 1~10 11~25 26~50 51명 이상
위치의 직원 수: IT 보안 *	0 시간제 1~5 6~25 26명 이상
위치의 직원 수: 위치 보안 *	0 시간제 1~3 4~10 11명 이상
이 위치의 인증	ISO 27001 기타(기입 요망) ISAE 3402 SOC2

표 1. 위치 관련 세부 정보

참고:

“산업”은 아는 범위 내에서 가장 가깝게 일치하는 항목을 선택하십시오. 위 보기에서 선택할 때 정답이나 오답은 없습니다. 귀사의 사업 유형과 일치하는 보기를 찾을 수 없으면 “기타” 아래에 적절한 내용을 입력하십시오.

각 위치마다 “location name”(🇰🇷 “위치 이름”)을 지정해야 합니다. 위치 이름은 위치를 평가 범위에 할당할 때 위치를 더 쉽게 지칭하기 위한 목적으로 사용됩니다.

다음 패턴에 따라 위치 이름을 지정하는 방법이 권장됩니다.

패턴: [지역명]

예시: “ACME”라는 가상 회사

- 프랑크푸르트
  (위치가 독일 프랑크푸르트 시에 있는 경우)

4.3.2.6. 범위 이름

각 범위마다 “scope name”(🇰🇷 “범위 이름”)을 지정해야 합니다. 범위 이름은 주로 ENX 포털의 범위 요약 목록에서 범위를 쉽게 식별하기 위한 목적으로 사용됩니다. 독자와 동료들에게 도움이 되는 이름을 지정해야 합니다. 외부 통신에는 범위 ID를 사용해야 합니다.

원하는 이름을 지정할 수 있습니다. 하지만 같은 범위 이름을 한 개보다 많은 범위에 지정해서는 안 됩니다.

나중에 TISAX 평가를 갱신하고 싶으면 새 범위(현재 범위와 동일할 수 있음)를 만들어야 합니다. 그러므로 범위 이름에 평가 연도를 추가하는 것이 좋습니다.

다음 패턴에 따라 범위 이름을 지정하는 방법이 권장됩니다.

패턴: [지역명 또는 기능명] [평가 연도]

예시: “ACME” 라는 가상 회사

- 2024
  (회사 위치가 하나뿐인 경우 지역명 없이)
- 프랑크푸르트 2024
  (범위에 독일 프랑크푸르트 시의 여러 위치가 포함된 경우)
- 니더작센 2024
  (범위에 독일 니더작센 주의 여러 위치가 포함된 경우)
- 독일 2024
  (범위에 독일이라는 국가의 모든 위치가 포함된 경우)
- EMEA 2024
  (범위에 EMEA 지역(“유럽, 중동, 아프리카”)의 모든 위치가 포함된 경우)
- 프로토타입 개발 2024
  (프로토타입 개발에 관여하는 모든 위치가 범위에 포함된 경우의 기능명)

4.3.2.7. 연락 담당자

ENX 협회는 귀사와 연락을 주고받기 위해 귀사의 연락 담당자에 대한 정보를 수집합니다.

귀사(TISAX 참가자)의 전체 연락 담당자 한 명 이상과 각 평가 범위의 연락 담당자 한 명 이상에 대한 정보가 요청됩니다. 추가 연락 담당자 정보를 제공하기로 선택할 수 있습니다.

등록을 준비하는 동안 누가 귀사의 연락 담당자가 될 것인지 결정해야 합니다.

연락 담당자에 대한 다음과 같은 세부 정보가 요청됩니다.

	연락 담당자 세부 정보	필수?	예시
1.	호칭	예	Mrs., Mr.
2.	학위		의학 박사, 박사 등
3.	이름	예	존
4.	성	예	도우
5.	직책	예	IT 책임자
6.	부서	예	정보 기술(IT)
7.	주 전화번호	예	+49 69 986692777
8.	부 전화번호		
9.	이메일 주소	예	john.doe@acme.com
10.	선호하는 언어	예	영어(기본)
11.	기타 언어		독일어, 프랑스어
12.	개인 주소 식별자		HPC 1234
13.	거리 주소	예	Bockenheimer Landstraße 97-99

	연락 담당자 세부 정보	필수?	예시
14.	우편번호	예	60325
15.	시	예	프랑크푸르트
16.	주/도		
17.	국가	예	독일

표 2. 연락 담당자 세부 정보

중요한 참고 사항:

각 연락 담당자의 대체자를 하나 이상 지정하는 것이 좋습니다. 연락 담당자가 일시적으로 연락이 불가하거나 퇴사하는 경우, 대체자가 귀사의 참가자 데이터를 관리할 수 있습니다. 새 연락 담당자를 지정해야 하는 경우 (다른 유효한 담당자가 남아있지 않으면) 복잡한 프로세스를 거쳐야 합니다. ENX 협회의 프로세스는 회사를 법적으로 대표할 권한이 있다고 입증할 수 있는 사람만 새 주 연락 담당자 지정을 승인할 수 있도록 보장합니다.

4.3.2.8. 게시 및 공유

TISAX의 주 목적은 평가 결과를 다른 TISAX 참가자를 위해 게시하고 평가 결과를 파트너(들)와 공유하는 것입니다.

평가 결과 게시 및 공유에 대해서는 등록 프로세스 도중이나 그 후 언제든지 결정할 수 있습니다.

선제 조치로서 TISAX 프로세스를 진행하는 경우, 평가 결과를 TISAX 참가자 커뮤니티를 위해 게시하기로 미리 결정할 수 있습니다. 그렇지 않으면 이 단계에 준비할 것이 없습니다.

파트너가 귀사에 TISAX 프로세스 진행을 요청한 경우, 평가 결과를 더 빨리 공유해야 합니다. 등록하는 동안 상태 정보를 파트너와 미리 공유할 수 있습니다. 평가 결과를 확인할 수 있게 되면 파트너가 평가 결과에 액세스할 권한을 자동으로 갖게 됩니다[6].

상태 정보를 공유하려면 다음 두 가지가 필요합니다.

1. 파트너의 TISAX 참가자 ID

   TISAX 참가자 ID는 파트너를 TISAX 참가자로 식별합니다.

   일반적으로 파트너는 귀사에 자사의 TISAX 참가자 ID를 제공해야 합니다.

   편의를 위해, 등록 양식에는 공유된 평가 결과를 자주 수신하는 몇몇 회사를 위한 참가자 ID 드롭다운 목록이 있습니다.[7]

2. 필수 공유 수준

   공유 수준은 파트너가 귀사의 평가 결과에 액세스할 수 있는 깊이를 정의합니다.

   파트너가 특정 공유 수준을 요청하거나, 귀사에서 평가 결과에 대해 파트너에 부여할 액세스 수준을 결정할 수 있습니다.

   공유 수준에 대한 자세한 내용은 다음을 참조하십시오. 섹션 6.5, “공유 수준” .

따라서 이 정보를 갖고 있는지 확인해야 합니다.

참고:

- 평가 결과를 나중에 언제든지 게시하기로 결정할 수 있습니다.

- 파트너를 위한 공유 권한을 나중에 언제든지 만들 수 있습니다.

중요한 참고 사항:

평가 결과를 게시하지 않거나 공유하지 않으면 아무도 평가 결과를 볼 수 없습니다.

중요한 참고 사항:

게시 또는 공유를 취소할 수 없습니다.

자세한 내용은 다음을 참조하십시오. 섹션 6.4, “교환된 결과의 영속성” .

참고:

이상한 말처럼 들릴 수 있지만, 실제로 평가 프로세스를 아직 시작하지 않은 경우에도 “평가 결과”를 공유할 수 있습니다. 이 초기 단계에는 “평가 상태”만 공유하게 됩니다. “평가 결과”를 공유 받는 참가자에게는 평가 프로세스가 어디까지 진행되었는지 표시됩니다.

일부 TISAX 참가자는 귀사에서 TISAX 레이블을 보여줘야 하지만 아직 평가 프로세스를 마치지 않은 경우 특별 면제를 허가해야 합니다. 이런 경우에는 파트너가 자신의 ENX 포털 계정에서 귀사의 “평가 상태”를 확인해야 할 수 있습니다.

평가 상태에 대한 자세한 내용은 다음을 참조하십시오. 섹션 7.6, “부록: Assessment status(🇰🇷 평가 상태)” .

평가 결과 게시 및 공유에 대한 자세한 내용은 다음을 참조하십시오. 섹션 6, “교환(3 단계)” .

4.3.3. 평가 목표

등록 프로세스를 진행하는 동안 평가 목표를 정의해야 합니다. 평가 목표(🇬🇧 assessment objective)는 정보 보안 관리 시스템(ISMS)이 충족해야 하는 해당하는 요구 사항을 결정합니다. 평가 목표는 전적으로 파트너 대신 처리하는 데이터의 유형에 따라 결정됩니다.

이어지는 내용에서는 평가 목표에 대해 설명하고 올바른 평가 목표를 선택하는 방법에 대해 조언합니다.

평가 목표를 사용하면 파트너 및 TISAX 감사 제공자와 TISAX에 관해 더 쉽게 소통할 수 있습니다. TISAX 평가 프로세스에 투입되는 정의된 정보가 평가 목표에 언급되기 때문입니다.

참고:

일부 파트너는 평가 목표를 지정하지 않고 특정 “평가 수준”(AL)으로 TISAX 평가를 받을 것을 대신 요청할 수 있습니다.

평가 수준에 대한 자세한 내용은 다음을 참조하십시오. 섹션 4.3.3.5, “필요한 보호 수준과 평가 수준”(“추가 정보” 하위 섹션)

4.3.3.1. 평가 목표 목록

현재 12개의 TISAX 평가 목표가 있습니다. 평가 목표를 하나 이상 선택해야 합니다. 한 개보다 많이 선택할 수 있습니다.

평가 목표가 정보 보안 관리 시스템에 대한 벤치마크라고 생각하십시오. 평가 목표는 TISAX 프로세스에 투입되는 핵심 정보입니다. 모든 TISAX 감사 제공자는 주로 평가 목표를 근거로 평가 전략을 결정합니다.

현재의 TISAX 감사 평가 목표는 다음과 같습니다.

번호	이름	설명
1.	Info high	Handling of information with high protection needs 높은 보호 수준이 필요한 정보의 처리
2.	Info very high	Handling of information with very high protection needs 매우 높은 보호 수준이 필요한 정보의 처리
3.	Confidential	Handling of information with high protection needs in the context of confidentiality (access to confidential information) 비밀 유지(비밀 정보 액세스)의 맥락에서 매우 높은 보호 수준이 필요한 정보의 처리
4.	Strictly confidential	Handling of information with very high protection needs in the context of confidentiality (access to strictly confidential information) 비밀 유지(비밀을 철저히 유지해야 하는 정보 액세스)의 맥락에서 매우 높은 보호 수준이 필요한 정보의 처리
5.	High availability	Handling of information with high protection needs in the context of availability (high availability of information) 가용성(높은 정보 가용성)의 맥락에서 매우 높은 보호 수준이 필요한 정보의 처리
6.	Very high availability	Handling of information with very high protection needs in the context of availability (very high availability of information) 가용성(매우 높은 정보 가용성)의 맥락에서 매우 높은 보호 수준이 필요한 정보의 처리
7.	Proto parts	Protection of Prototype Parts and Components 프로토타입 부품 및 구성 요소 보호
8.	Proto vehicles	Protection of Prototype Vehicles 프로토타입 차량 보호
9.	Test vehicles	Handling of Test Vehicles 테스트 차량 취급
10.	Proto events	Protection of Prototypes during Events and Film or Photo Shoots 이벤트와 영화 또는 사진 촬영 중에 프로토타입 보호

번호	이름	설명
11.	Data	Data protection according to Article 28 (“Processor”) of the European General Data Protection Regulation (GDPR) 유럽 연합 일반 데이터 보호 규칙(GDPR) 28조("프로세서")에 따른 데이터 보호
12.	Special data	Data protection according to Article 28 (“Processor”) of the European General Data Protection Regulation (GDPR) with special categories of personal data as specified in Article 9 of the GDPR 유럽 연합 일반 데이터 보호 규칙(GDPR) 28조(“프로세서”)에 따른 데이터 보호(GDPR 9조에 명시된 개인 데이터의 특별 범주 포함)

표 3. 현재의 TISAX 감사 평가 목표

예: 공공 도로에서 시험 운행을 하는 경우, 평가 목표 “Test vehicles”가 평가 목표 중 하나입니다.

참고:

평가 목표 “Info high” 및 “Info very high”는 2024년 3월 31일까지만 선택할 수 있습니다.

평가 목표 “Confidential” 및 “Strictly confidential”은 2024년 4월 1일부터 선택할 수 있습니다.

이 변화에 대한 자세한 내용은 ENX 협회 웹 사이트에서 다음 뉴스 기사를 참조하십시오.
CHANGES TO TISAX LABELS ACCOMPANYING ISA 6 RELEASE
enx.com/en-US/news/Changes-to-TISAX-Labels-ISA-six-Release/

중요한 참고 사항:

TISAX 안에서 “평가 목표”는 일반적으로 프로세스에 투입되는 정보입니다. 하지만 몇몇 파트너는 특정 “평가 수준”(AL)으로 TISAX 평가를 받을 것을 요청할 수 있습니다.

필요한 보호 수준과 평가 수준의 관계에 대한 자세한 내용은 다음을 참조하십시오. 섹션 4.3.3.5, “필요한 보호 수준과 평가 수준”.

4.3.3.2. 평가 목표와 ISA

ISA는 기준 카탈로그 세 개(정보 보안, 프로토타입 보호, 데이터 보호)를 포함합니다. 각 기준 카탈로그는 소위 “통제 문항”과 관련 요구 사항으로 구성됩니다.

각 평가 목표는 다음을 정의합니다.

- 해당하는 ISA 기준 카탈로그
- 답해야 하는 통제 문항
- 충족해야 하는 요구 사항

일부 평가 목표에는 통제 문항과 요구 사항의 부분 집합만 해당됩니다.

TISAX 평가 목표와 해당하는 통제 문항 및 요구 사항에 대한 배경 정보를 더 확인하려면 다음을 참조하십시오. 섹션 5.2.2, “ISA 문서 이해”.

4.3.3.3. 평가 목표와 TISAX 레이블

파트너가 “TISAX 레이블”에 대해 얘기할 수 있습니다. “평가 목표”와 “TISAX 레이블”은 거의 같은 것입니다. “평가 목표”를 갖고 평가 프로세스를 시작하고 평가에 합격하면 해당하는 “TISAX 레이블”을 받는다는 차이점이 있습니다.

예: 파트너가 “Info high” TISAX 레이블을 받아야 한다고 귀사에 요구합니다. 그러면 “Info high”를 귀사의 평가 목표로 선택합니다.

아래 그림에는 TISAX 프로세스의 투입물과 산출물이 나와 있습니다.

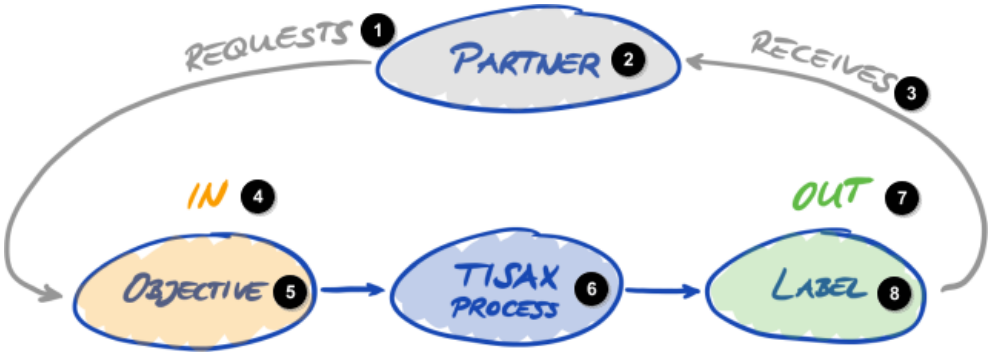


그림 6. 평가 목표와 TISAX 레이블

1. 요청
2. 파트너
3. 수령
4. 투입물
5. 목표
6. TISAX 프로세스
7. 산출물
8. 레이블

TISAX 레이블에 대한 자세한 내용은 다음을 참조하십시오. 섹션 5.4.14, “TISAX 레이블”.

4.3.3.4. 평가 목표 선택

이상적인 경우에는 귀사에서 달성해야 하는 평가 목표를 파트너가 정확하게 얘기합니다.

다음과 같은 경우 평가 목표를 직접 판단하여 선택해야 합니다.

a. 파트너가 요청하기 전에 TISAX 평가를 받으려는 경우, 또는
b. 달성해야 하는 평가 목표를 파트너가 얘기하지 않는 경우

중요한 참고 사항:

이 시점에는 다른 파트너를 고려하도록 적극 권장됩니다. 기존 파트너 중에 요구 수준이 같거나 더 높은 파트너가 있습니까? 미래 파트너의 요구 수준이 더 높을 것이라 예상됩니까?

더 높은 필요한 보호 수준이 포함된 평가 목표를 선택할지 고려해야 합니다. 그러면 다른 파트너의 요구 수준이 더 높은 경우에 문제를 방지할 수 있습니다.

귀사의 자체적인 판단에 따라 평가 목표를 선택해야 하는 경우, 다음과 같은 측면을 고려하면 도움이 될 수 있습니다.

번호	평가 목표	정보
1.	Info high	필요한 보호 수준(높음, 매우 높음)을 파트너의 문서 분류 등급에서 추론할 수 있습니다.
2.	Info very high	
3.	Confidential	비밀유지의 맥락에서 높은 보호 수준이 필요하거나 일반적으로 회사 자체의 분류 체계에 따라 비밀로 분류되는 정보를 수령하고 처리하는 모든 회사(예: VDA 백서 “Harmonization of classification levels(비밀 등급의 조화)”). 특히 정보가 허가 없이 공개될 경우 상당한 피해(예: 명예 훼손, 형사 처벌, 또는 금전적 손실)가 초래될 수 있는 경우 이 TISAX 레이블을 선택해야 합니다.
4.	Strictly confidential	비밀유지의 맥락에서 매우 높은 보호 수준이 필요하거나 일반적으로 회사 자체의 분류 체계에 따라 철저한 기밀 또는 비밀로 분류되는 정보를 수령하고 처리하는 모든 회사(예: VDA 백서 “Harmonization of classification levels(비밀 등급의 조화)”). 특히 정보가 허가 없이 공개될 경우 존재에 위협이 되거나 재앙적인 피해(예: 심각한 명예 훼손, 심각한 형사 처벌, 또는 매우 많은 금전적 손실)가 초래될 수 있는 경우 이 TISAX 레이블을 선택해야 합니다.
5.	High availability	고객의 생산 또는 납품 능력이 회사 제품 또는 서비스의 가용성에 좌우되고 불이행 시에 고객에 상당한 피해를 단시간 내에 초래하게 될 모든 회사. 예: 생산 재료 적기 공급업체
6.	Very high availability	고객의 생산 또는 납품 능력이 회사 제품 또는 서비스의 단기적인 가용성에 좌우되고 불이행 시에 매우 짧은 시간 안에 고객에 상당히 많은 피해를 초래하게 될 모든 회사. 예: 불이행 시 단시간 내에 광범위한 생산 중단이 발생하고 다시 시작하는 데 시간이 매우 오래 걸리는 결과를 초래할 수 있는 적기 공급업체.
7.	Proto parts	자체 위치에서 보호해야 한다고 분류된 고객이 제공한 구성 요소 또는 부품을 제조, 보관 또는 사용하는 모든 회사. 물리적 보안과 주변 구역을 고려한 보안에 대한 요구 사항, 조직의 요구 사항, 그리고 프로토타입 취급에 대한 구체적인 요구 사항은 평가의 일부입니다.

번호	평가 목표	정보
8.	Proto vehicles	자체 위치에서 보호해야 한다고 분류된 고객이 제공한 차량을 제조, 보관 또는 사용하는 모든 회사. 물리적 보안과 주변 구역(보호되는 차고와 워크샵 구역의 존재 포함)을 고려한 보안에 대한 요구 사항, 조직의 요구 사항, 그리고 프로토타입 취급에 대한 구체적인 요구 사항은 평가의 일부입니다. 평가에 합격한 후에는 “프로토타입 부품 및 구성 요소 보호” TISAX 레이블을 자동으로 받습니다.
9.	Test vehicles	보호해야 한다고 분류된 고객 제공 차량으로 테스트와 시험 운행(예: 공공 도로 또는 테스트 트랙에서의 시험 운행)을 실시하는 모든 회사. 조직의 요구 사항, 프로토타입 취급(공공 및 테스트 트랙에서 시험 운행하는 동안 차량을 위장하고 취급하는 것 포함)에 대한 구체적인 요구 사항은 평가의 일부입니다. 물리적 보안과 주변 구역을 고려한 보안에 대한 요구 사항은 평가에 포함되지 않을 수 있습니다. 위치에 적절한 장비가 갖춰진 경우 “프로토타입 차량 보호” 평가 목표도 선택하는 것이 좋습니다.
10.	Proto events	보호가 필요하다고 분류된 고객 제공 차량, 구성 요소 또는 부품을 사용하여 프레젠테이션 또는 이벤트(예: 시장 조사, 이벤트, 마케팅 이벤트)와 영화 및 사진 촬영을 진행하는 모든 회사. 조직의 요구 사항과 프로토타입 취급에 대한 구체적인 요구 사항(보호되는 실내와 공공 장소에서 진행되는 프레젠테이션, 이벤트, 영화 및 사진 촬영에 대한 요구 사항 포함)은 평가의 일부입니다. 물리적 보안과 주변 구역을 고려한 보안에 대한 요구 사항은 평가에 포함되지 않을 수 있습니다. 위치에 적절한 장비가 갖춰진 경우 “프로토타입 차량 보호” 평가 목표도 선택하는 것이 좋습니다.
11.	Data	귀사가 GDPR 28조에 따라 프로세서로서 개인 데이터를 처리하는 경우, “Data”를 선택해야 할 수 있습니다.
12.	Special data	귀사가 GDPR 28조에 따라 프로세서로서 특별 개인 데이터 범주(건강 또는 종교 등)를 처리하는 경우, “Special data”를 선택해야 할 수 있습니다.

표 4. 평가 목표 선택에 관한 조언

추가 설명:

- 파트너의 정확한 요구 사항을 갖고 있는 경우, 일반적으로 평가 목표를 파트너와 논의할 필요가 없습니다. 하지만 파트너의 정확한 요구 사항이 없는 경우 평가 프로세스를 시작하기 전에 파트너와 상의하도록 적극 권장됩니다.
- ISA에서는 필요한 보호 수준 “높음”과 “매우 높음”인 경우 이행에 어떤 차이점(있는 경우)이 있는지 각 요구 사항마다 서술합니다.
  이에 대한 자세한 내용은 다음을 참조하십시오. 그림 11, “스크린샷: ISA 기준 카탈로그 “정보 보안”에 있는 문항의 주 요소”.

4.3.3.5. 필요한 보호 수준과 평가 수준

파트너에게는 다양한 유형의 정보가 있을 수 있고, 이 중에는 다른 정보보다 더 높은 보호 수준이 필요한 정보가 있을 수 있습니다. ISA는 이에 맞춰 “필요한 보호 수준”(“protection needs”)을 세 개(일반, 높음 및 매우 높음)로 나눕니다. 파트너는 정보를 분류하고, 대개 각 정보에 필요한 보호 수준을 지정합니다.

필요한 보호 수준이 높을수록 파트너가 정보 처리를 귀사에 맡겨도 안전한지 확인하는 데 더 관심이 있을 것입니다. 그러므로 TISAX에서는 “평가 수준”(AL)을 세 개로 구분합니다. 평가 수준은 감사 제공자가 적용해야 하는 평가 방법을 정의합니다. 평가 수준이 높을수록 평가에 더 많은 노력이 필요합니다. 따라서 주의를 더 기울여서 더 정확하게 평가하게 됩니다.

아래 표에는 TISAX 평가 목표에 해당하는 평가 수준이 나와 있습니다.

번호	TISAX 평가 목표	평가 수준(AL)
1.	Info high	AL 2
2.	Info very high	AL 3
3.	Confidential	AL 2
4.	Strictly confidential	AL 3
5.	High availability	AL 2
6.	Very high availability	AL 3
7.	Proto parts	AL 3
8.	Proto vehicles	AL 3
9.	Test vehicles	AL 3
10.	Proto events	AL 3
11.	Data	AL 2
12.	Special data	AL 3

표 5. TISAX 평가 목표와 평가 수준 매핑

평가 수준 1(AL 1):

평가 수준 1에 해당하는 평가는 주로 진정한 의미의 자가 평가(self-assessment)에서 내부 용도로 사용됩니다.

평가 수준 1에 해당하는 평가에 대해, 감사관은 완료된 자가 평가가 있는지 여부를 확인합니다. 감사관은 자가 평가의 내용을 평가하지 않습니다. 감사관은 증거를 더 요구하지 않습니다.

평가 수준 1에 해당하는 평가의 결과는 신뢰 수준이 낮아서 TISAX에서 사용되지 않습니다. 하지만 파트너는 물론 이런 자가 평가를 TISAX 밖에서 요청할 수 있습니다.

평가 수준 2(AL 2):

평가 수준 2에 해당하는 평가에 대해, 감사 제공자는 귀사의 자가 평가에 대해 타당성 점검을 (평가 범위에 포함된 모든 위치에 대해) 수행합니다. 제공자는 증거를 확인하고[8] 정보 보안을 책임지는 자와 면접 조사를 실시하여 이를 뒷받침합니다.

감사 제공자는 일반적으로 웹 회의를 통해 면접 조사를 실시합니다. 요청 시에 제공자는 면접 조사를 직접 만나서 실시할 수도 있습니다.

감사 제공자에게 보내고 싶지 않은 증거가 있는 경우, 현장 점검을 요청할 수 있습니다. 이 경우에도 감사 제공자는

이 방법으로 “대외비”인 증거를 확인할 수 있습니다.

참고:

평가 수준 2에 해당하는 평가를 실시하는 다른 방법이 있습니다. 감사 제공자는 타당성 점검 대신 전체 원격 평가를 실시합니다. 이 방법을 때로는 “평가 수준 2.5”라고 합니다.

평가 수준 2에 해당하는 평가와 달리, 감사관은 ISMS가 해당하는 요구 사항을 충족하는지 여부를 확인합니다. 하지만 평가 수준 3에 해당하는 평가와는 반대로, 감사관이 아래의 평가 수준 3에 대한 섹션에 약술되어 있는 현장 활동을 수행하지 않습니다.

공식적으로, 이런 평가는 AL 2에 해당하는 평가로 평가될 것입니다.

AL 2.5는 접근방식이 AL 3과 계통적으로 호환된다는 장점이 있습니다. 그러므로 나중에 많은 노력을 기울이지 않고도 완전한 AL 3 평가로 업그레이드할 수 있습니다. 업그레이드의 경우, 감사관은 아래에 AL 3에 대한 섹션에 약술된 현장 활동만 수행하면 됩니다.

다음과 같은 경우에는 평가 수준 2.5에 해당하는 평가가 권장됩니다.

1. 현재는 평가가 AL 2임을 나타내는 TISAX 레이블만 필요하지만, 다른 파트너들이 평가가 AL 3임을 나타내는 TISAX 레이블을 요구할 수 있는 가능성을 배제할 수 없습니다. AL 2.5에 해당하는 평가는 나중에 AL 3로 업그레이드할 수 있는 길을 열어 둡니다.
2. 귀사에서 충분히 타당해 보이는 자가 평가를 준비하는 데 어려움을 겪고 있습니다. 타당성 점검을 위해, 자가 평가는 확실하고 잘 이해할 수 있고 입증되어야 합니다. 이런 자가 평가를 준비하려면 기초적인 입지가 좋은 회사에서도 내부적으로 많은 노력이 필요할 수 있습니다.

평가 수준 업그레이드에 대한 자세한 내용은 다음을 참조하십시오. 섹션 7.10, “부록: 범위 확장 평가”.

이 대안(AL 2.5)은 선택 사항이며, AL 2 요구 사항을 충족하는 데 필수적이지 않습니다. AL 2와 AL 2.5의 차이점은 평가 결과를 공유하는 파트너에게 보이지 않습니다.

평가 수준 3(AL 3):

평가 수준 3에 해당하는 평가에서, 감사 제공자는 해당하는 요구 사항을 귀사에서 준수하는지 광범위하게 확인합니다. 감사관은 귀사의 자가 평가와 제출된 문서를 사용하여 평가를 준비합니다. 하지만 평가 수준 2와는 대조적으로 감사관이 모든 것을 확인합니다. 감사관은

- 문서와 증거를 살펴보고
- 프로세스 소유자들과 계획된 면접 조사를 실시하고
- 현지 상황을 관찰하고
- 프로세스 실행을 관찰하고
- 프로세스 참가자들과 계획되지 않은 면접 조사를 실시합니다.

참고:

이어지는 내용에서는 이 문서에서 나중에 설명할 몇 가지 개념에 대해 언급합니다.

AL 3의 경우 감사 제공자가 귀사의 위치까지 와야 합니다. 어떤 이유로든 일시적으로 이렇게 할 수 없거나 이렇게 하려면 합당하지 않게 많은 노력이 필요할 경우 감사 제공자는 비디오로 지원되는 원격 평가 방법을 사용하여 평가의 현장 활동을 수행할 수 있습니다.

> 감사 제공자는 이 사실을 TISAX 평가 보고서에 사소한 미준수로 기록해야 합니다. 감사 제공자가 귀사의 위치까지 올 수 있는 최대한 빠른 시간에 제공자는 이전에 불가능했던 현장 활동을 모두 포함하는 후속 평가를 실시해야 합니다. 또한 아직 다른 시정 조치를 완료하지 않은 경우에도 후속 평가 일정을 정해야 합니다.
>
> 감사 제공자가 현장 활동을 할 수 있을 때까지 기다리지 않고 이 접근방식을 사용하면 파트너와 임시 TISAX 레이블을 미리 공유할 수 있습니다.

평가 수준과 평가 방법

아래 표에는 각 평가 수준과 연관된 감사 방법의 간단한 개요가 제시되어 있습니다.

평가 방법	평가 수준 1 (AL 1)	평가 수준 2 (AL 2)	평가 수준 3 (AL 3)
자가 평가	예	예	예
증거	아니요	타당성 점검	철저한 확인
면접 조사	아니요	웹 회의를 통해[9]	대면, 현장에서
현장 점검	아니요	귀사의 요청 시	예

표 6. 평가 방법을 서로 다른 평가 수준에 적용할 수 있는지 여부

추가 정보:

- AL 2와 AL 3의 차이점
  두 접근방식은 계통적으로 약간 다릅니다. 평가 수준2에 해당하는 평가에서 감사관은 모든 것을 확인하지는 않습니다. 타당성만 점검합니다. 그러므로 감사 제공자는 평가 수준 2에 해당하는 평가의 결과를 평가 수준 3으로 업그레이드하는 근거로 사용할 수 없습니다. 평가 수준 3으로 업그레이드하기 위해 필요한 노력은 새로운 첫 평가에 필요한 노력과 근본적으로 같습니다.
- 타당성 점검과 확인 비교
  아주 간단하게 말하면, 타당성 점검은 무언가가 존재하고 정상으로 보이는지 점검하는 것입니다. 이에 반해, 확인은 무언가가 그것이 무엇이라고 주장하는 것이 맞는지 실제로 확인하는 것을 의미합니다.
- 정보 분류와 필요한 보호 수준
  정보 분류 등급(기밀 또는 비밀 등)을 필요한 보호 수준에 매핑하는 일은 여러 파트너에게 어려울 수 있습니다. 그러므로 여기서는 파트너의 정보 분류 등급이 필요한 보호 수준에 정확하게 매핑되는 간단한 표를 제시하고 싶어도 그럴 수 없습니다.
- 평가 수준만 알면 충분하지 않습니다.
  일부 파트너는 특정 평가 수준으로 TISAX 평가를 받을 것을 요청할 수 있습니다. 평가 수준만 알면 TISAX 프로세스를 시작하는 데 충분하지 않다는 점을 양해해 주십시오. 평가 수준은 ISA 기준 카탈로그 및 해당하는 필요한 보호 수준과 함께 생각해야만 합리적입니다. 일반적으로 파트너는 귀사에 TISAX 레이블(기준 카탈로그 + 필요한 보호 수준) 획득을 요청합니다. 하지만 필요한 보호 수준은 평가 수준과 1:1로 매핑되므로 기준 카탈로그와 평가 수준만 알아도 충분합니다.
- 평가 수준 계층구조
  더 높은 평가 수준에는 항상 더 낮은 평가 수준이 포함됩니다. 예를 들어 평가가 평가 수준 3 기반인 경우 평가 수준 2의 모든 요청 사항이 자동으로 충족됩니다.
- 평가 수준에 관한 권장 사항
  자체적인 판단에 따라 평가 목표를 선택(하고 따라서 해당하는 평가 수준도 암묵적으로 선택)해야 하는 경우, 평가 수준 3을 수반하는 평가 목표를 선택하는 것이 좋습니다. 평가 수준 3에 해당하는 TISAX 평가에 필요한 노력은 일반적으로 평가 수준 2에 필요한 노력보다 많지 않습니다.
  여러 파트너가 있는 공급업체는 종종 평가 수준 3을 수반하는 평가 목표를 선택합니다. 이 방법으로 공급업체는 향후의 모든 요청에 준비가 되고 다른 평가 수준에 신경 쓰지 않아도 됩니다.

- 상업적인 추가 고려 사항
  평가 수준과 관련하여, TISAX 평가의 총 비용은 내부 노력량과 평가 비용의 합으로 구성됩니다. 평가 수준 2에 해당하는 평가의 비용은 더 낮지만, 내부 노력량은 더 많을 수 있습니다. 평가 수준 2에 해당하는 평가에는 일반적으로 더 광범위한 자가 평가와 더 나은 내부 문서가 필요하다는 사실 때문에 그렇습니다. 평가 수준 3에 해당하는 평가에는 귀사에서 일하는 방법을 시연하고 기초 문서를 보여주면 감사관에게 충분한 증거가 되는 경우가 많습니다. 하지만 현장 점검을 하지 않으면 감사관이 정확한 문서를 요청합니다. 그러므로 평가 수준 2 대신 평가 수준 3을 선택하는 경우가 드물지 않습니다. 하지만 큰 회사보다 작은 회사가 이렇게 선택하는 경우가 많습니다.

4.3.3.6. 평가 목표와 자체 공급업체

TISAX에서는 귀사의 자체 공급업체에 모두 같은 요구 사항을 적용해야 한다고 요구하지 않을 수 있습니다. 평가 목표가 “필요한 보호 수준이 매우 높은 정보 보안” 인 경우, 귀사의 자체 공급업체들이 같은 평가 목표를 달성해야 함을 자동으로 의미하지는 않습니다. 공급업체에 TISAX 레이블이 있어야 함을 의미하지도 않습니다.

하지만 그래도 공급업체의 서비스를 사용하면 위험이 증가하거나 새로운 위협이 도입되는지 여부를 모든 공급업체에 대해 확인해야 합니다.

매우 간단한 예 두 개:

1. 귀사에는 매우 높은 데이터 보호 수준이 필요한 데이터에 일반 우편을 사용하면 안 된다는 방침이 있습니다. 그러므로 귀사의 이메일 제공업체는 필요한 보호 수준이 매우 높은 TISAX 레이블을 획득하지 않아도 됩니다. 귀사에서 암호화된 이메일만 보내고 이메일 제공업체가 필요한 데이터 보호 수준이 매우 높은 데이터를 볼 수 없는 경우에도 비슷한 결론에 도달할 수 있습니다.
2. 필요한 보호 수준이 매우 높은 인쇄된 데이터를 파쇄기에 폐기합니다. 이런 경우에는 물론 폐기물 처리 서비스 제공업체가 귀사와 동일한 요구 사항을 충족하지 않아도 됩니다.

하지만 위험 평가에서 귀사의 공급업체가 필요한 보호 수준이 매우 높은 데이터에 대한 요구 사항도 충족해야 하는 것으로 확인될 수 있습니다. 이 경우 TISAX 레이블은 귀사에 이를 적절히 입증하기 위한 선택 사항입니다.

4.3.4. 수수료

ENX 협회에서는 수수료를 징수합니다. ENX 협회의 가격 목록을 통해 귀사는 적용되는 수수료, 가능한 할인 및 지불 조건에 대해 알 수 있습니다.

가격 목록은 ENX 협회의 웹 사이트에서 다운로드할 수 있습니다. 주소:
enx.com/en-US/TISAX/downloads/
PDF 직접 다운로드:
enx.com/pricelist.pdf

등록을 준비하는 동안 청구서와 관련하여 고려해야 하는 몇 가지 측면이 있습니다.

- 청구서 주소 선택
  ENX 협회에서는 기본적으로 귀사의 참가자 위치로 제공된 주소로 청구서를 보냅니다. 하지만 청구서를 수신할 다른 주소를 제공할 수도 있습니다.

중요한 참고 사항:

청구서 주소가 정확한지 확인하십시오. 회계법에 따르면, 청구서에 기재된 주소는 귀사의 (청구서) 주소와 정확하게 일치해야 합니다. 법규 준수를 이유로, 청구서를 발행한 후에는 청구서 주소를 변경할 수 없습니다.

- 주문 참조 번호
  특정 구매 주문 번호와 그 외 유사한 정보를 청구서에서 확인할 수 있어야 하는 경우, ENX 협회에 주문 참조 번호를 제공할 수 있습니다.

- VAT 번호
  모든 청구 대금에는 독일 부가가치세(VAT)가 부과됩니다(해당하는 경우).
  이 번호는 EU에서 지불된 금액을 처리하는 데 필요합니다. 청구서 주소가 다음 국가 중 하나에 있는 경우 VAT 번호를 의무적으로 제공해야 합니다.
  오스트리아, 벨기에, 불가리아, 크로아티아, 키프로스(그리스 부분), 체코공화국, 덴마크, 에스토니아, 핀란드, 프랑스, 독일, 그리스, 헝가리, 아일랜드, 이탈리아, 라트비아, 리투아니아, 룩셈부르크, 몰타, 네덜란드, 폴란드, 포르투갈, 슬로바키아, 슬로베니아, 스페인, 스웨덴, 영국
- 공급업체 관리

중요한 참고 사항:

모든 TISAX 참가자 사이의 상호 관계로 인해, ENX 협회는 (일반 구매 약관, 행동 강령 같은) 추가 약관에 동의할 수 없음을 양해해 주십시오.

ENX 협회의 대금 청구 프로세스에 대한 추가 정보:

- ENX 협회는 개별적인 구매 약관에 동의할 수 없습니다.
- ENX 협회는 다음을 수락합니다.
  - 청구서에 명시된 은행 계좌로 자금 이체
  - 신용 카드 결제(등록 프로세스 도중에 ENX 협회의 결제 서비스 제공업체인 “Stripe”를 통해)
- ENX 협회의 청구서에는 귀사의 등록에 대한 다음과 같은 참조 정보가 포함됩니다.
  - 주 참가자 연락 담당자의 이름과 이메일 주소
  - 평가 범위 이름

  부록의 다음 섹션에서 청구서 예시를 확인할 수 있습니다. 섹션 7.1, “부록: 청구서 예시”.
- 귀사에서 청구서를 처리하는 데 필요한 대부분의 사실 정보가 청구서에 직접 포함됩니다. 이런 사실 정보와 더욱 많은 사실 정보를 ENX 협회의 “Information for Members and Business Partners(멤버와 비즈니스 파트너를 위한 정보)” 문서에서 확인할 수 있습니다. 이메일 주소를 보내주시면 최신 버전을 보내 드립니다.

참고:

회사의 내부 결제 승인 프로세스가 때로는 꽤 오래 걸릴 수 있음을 알고 있습니다. 그러므로 ENX 협회에서 지불금을 받지 않아도 TISAX 프로세스의 다음 단계로 진행하실 수 있습니다. 하지만 ENX 협회에서 지불금을 수령하지 못한 경우 평가 결과를 공유하실 수 없음을 양해해 주십시오.
이런 이유로 ENX 협회에서 청구서를 올바른 수신인에게 발송하고 청구서에 주문 참조 번호(해당하는 경우)가 포함되었는지 확인하는 것이 좋습니다. 사내에서 누군가가 청구서 대금을 지불했는지도 추적해야 합니다.

중요한 참고 사항:

ENX 협회에서는 수수료를 청구합니다. 이 수수료는 총 TISAX 평가 비용의 일부일 뿐입니다. TISAX 감사 제공자는 평가 비용을 청구합니다.

감사 제공자 관련 비용에 대한 자세한 내용은 다음을 참조하십시오. 섹션 5.3.4, “오퍼 평가”.

중요한 참고 사항:

수수료는 다음에 관계없이 지불해야 합니다.

- TISAX 프로세스를 계속 진행하는지 여부
- TISAX 평가 프로세스를 통과하여 합격하는지 여부

그러므로 첫 평가를 시작하기도 전에 청구서가 도착할 수 있습니다.

4.4. ENX 포털

다음 섹션에서는 이전 섹션에 설명된 대로 수집한 데이터를 모두 입력하는 온라인 등록 프로세스에 대해 설명합니다. 온라인 등록 프로세스를 시작하기 전에 ENX 포털의 목적과 이점에 대해 간단히 설명하겠습니다.

ENX 포털은 모든 TISAX 참가자의 데이터베이스를 유지관리하는 데 사용할 수 있고, 전체 TISAX 프로세스 내내 중요한 역할을 합니다. TISAX 등록 중에 귀사에서 입력하는 데이터를 사용하여, TISAX 감사 제공자는 (귀사에서 동의할 경우) 오퍼 금액을 계산하고 평가 절차를 계획할 수 있습니다. TISAX 평가 프로세스를 거친 후에는 ENX 포털의 교환 플랫폼을 사용하여 평가 결과를 파트너와 공유하게 됩니다.

포털의 이름이 “TISAX 포털”이 아니라 “ENX 포털”인 이유는 포털을 사용하여 다른 비즈니스 활동(ENX 네트워크 등)도 관리하기 때문입니다.

4.5. 온라인 등록 프로세스

위(섹션 4.3, “등록 준비”)의 조언에 따라 준비한 경우, 온라인 등록 프로세스를 시작할 준비가 됩니다.

4.5.1. 필요한 시간

소요 시간은 등록하는 범위와 위치의 수에 따라 크게 다릅니다. 범위가 하나이고 위치가 하나인 참가자로 처음 등록하면 시간이 최소 20분 이상 소요될 것이라고 예상할 수 있습니다.

등록을 한 번에 완료하는 것이 좋습니다. 현재 몇몇 단계는 나중에 계속 진행하기가 쉽지 않기 때문입니다. 그래도 등록을 잠시 멈춰야 하는 경우, 누락된 데이터를 요청하기 위해 연락 드립니다.

4.5.2. 여기서 시작

ENX 협회 웹 사이트에서 등록을 시작하십시오. 주소:
enx.com/en-us/Account/Login/Register?returnUrl=%2FTISAX%2Ftisax-initial-registration%2F

기본적으로 화면 지침을 따르기만 하면 됩니다. 그렇기는 하지만, 아래에서 프로세스를 간단히 설명하겠습니다.

4.5.3. 포털 계정

첫 단계에는 ENX 포털에서 계정을 만듭니다. 귀사의 “참가자 데이터”를 직접 관리할 수 있으려면 포털 계정이 필요합니다.

참고:

ENX 포털에서 이메일 주소가 이미 사용 중이라는 메시지가 나타나면 ENX 협회에 문의하십시오. 이 메시지는 해당 주소가 어떤 이유로든 ENX 협회의 시스템에 이미 저장되어 있음을 의미할 수 있습니다.

참고:

설명과 같이, 포털 계정은 평가 프로세스에서 능동적인 역할을 하는 “참가자 연락 담당자” 또는 “범위 연락 담당자”(아래 참조)가 아닐 수 있습니다.

그 반대도 마찬가지입니다. “참가자 연락 담당자” 또는 “범위 연락 담당자”는 포털 계정과 동일한 참가자 데이터 관리 권한을 자동으로 보유하지 않습니다. 즉, “참가자 연락 담당자” 또는 “범위 연락 담당자”로 지명된 동료가 ENX 포털에서 참가자 데이터에 자동으로 액세스할 수 있는 것은 아닙니다.

참가자 데이터 관리 권한을 ENX 포털에서 이미 만들었던 연락 담당자에게 할당하려면 (해당 담당자에게 역할을 배정했는지 여부에 관계없이) 해당 연락 담당자를 초대해야 합니다. 자세한 내용은 다음 섹션의 마지막 참고 사항을 참조하십시오. 섹션 4.5.5, “참가자 연락 담당자”.

4.5.4. 참가자 등록

두 번째 단계에는 귀사를 TISAX 참가자로 등록합니다. “TISAX 참가자”는 평가 결과를 다른 참가자와 교환하는 회사입니다.

4.5.5. 참가자 연락 담당자

귀사의 정보 보안 평가에 관한 모든 사안을 전반적으로 책임지는 사람입니다. 귀하이거나 회사의 다른 사람일 수 있습니다.

일반적으로 주 참가자 연락 담당자만 있으면 됩니다. ENX 협회와 TISAX 감사 제공자가 이 등록에 관해 보내는 모든 커뮤니케이션을 다른 사람도 수신하기를 원하면 참가자 연락 담당자를 더 추가하십시오.

중요한 참고 사항:

각 연락 담당자의 대체자를 하나 이상 지정하는 것이 좋습니다. 연락 담당자가 일시적으로 연락이 불가하거나 퇴사하는 경우, 대체자가 귀사의 참가자 데이터를 관리할 수 있습니다. 새 연락 담당자를 지정해야 하는 경우 (다른 유효한 담당자가 남아있지 않으면) 복잡한 프로세스를 거쳐야 합니다. ENX 협회의 프로세스는 회사를 법적으로 대표할 권한이 있다고 입증할 수 있는 사람만 새 주 연락 담당자 지정을 승인할 수 있도록 보장합니다.

참고:

나중에 (온라인 등록 프로세스를 완료한 후와 평가를 완료한 후에도) 언제든지 연락 담당자를 추가하거나 삭제할 수 있습니다.

참고:

그룹 이메일 주소(“info@acme.com” 또는 “IT@acme.com” 등)를 참가자 연락 담당자의 이메일 주소로 사용할 수 없습니다.

이 내용은 사용자 로그인에 관한 ISA 요구 사항에 따른 것입니다.

참고:

각 연락 담당자가 귀사의 참가자 데이터에 액세스할 수 있도록 할지 선택할 수 있습니다. 다음 방법 중에서 선택하십시오.

1. 간단히 연락 담당자를 추가합니다. 추가한 연락 담당자가 시스템에 저장되지만, 로그인하고 데이터를 관리할 수는 없습니다.
2. 또는 연락 담당자를 초대합니다. 그러면 ENX 포털에서 초대 이메일을 연락 담당자에게 보냅니다. 연락 담당자는 이메일에 있는 초대 링크를 따라가야 합니다. 연락 담당자가 자신의 ENX 포털 개인 계정을 만든 후에는 귀사의 참가자 데이터를 관리할 수 있게 됩니다.

새 연락 담당자를 만드는 방법: Sign in(로그인) > MY TISAX(내 TISAX) > ADMINISTRATORS(관리자) > Create new TISAX Administrator(새 TISAX 관리자 만들기)

연락 담당자를 초대하는 방법: Sign in(로그인) > MY TISAX(내 TISAX) > ADMINISTRATORS(관리자) > 표에서 연락 담당자가 있는 행 끝으로 이동하여 아래쪽 화살표가 있는 버튼 클릭 > Edit TISAX Administrator(TISAX 관리자 편집) > “ENX PORTAL ACCESS(ENX 포털 액세스)” 섹션으로 이동 > “INVITE THIS CONTACT(이 연락 담당자 초대)"를 “Yes(예)”로 설정 > “Save Contact(연락 담당자 저장)” 클릭

4.5.6. 일반 약관

세 번째 단계에는 “TISAX 참가 일반 약관”에 동의합니다.

다음 섹션에 있는 주석을 다시 참조하는 것이 좋습니다. 섹션 4.3.1, “법적 기초”.

4.5.7. 평가 범위 등록

네 번째 단계에는 정보 보안 평가의 평가 범위를 등록합니다.

다음이 요청됩니다.

1. 평가 범위 이름 지정.
   범위 이름은 주로 ENX 포털의 범위 요약 목록에서 범위를 쉽게 식별하기 위한 목적으로 사용됩니다.
   다음 섹션에 있는 주석을 다시 참조하는 것이 좋습니다. 섹션 4.3.2.6, “범위 이름”
2. 평가 범위 유형 선택.
   (표준, 맞춤)
   다음 섹션에 있는 주석을 다시 참조하는 것이 좋습니다. 섹션 4.3.2, “TISAX 평가 범위”.
3. 주 범위 연락 담당자 지정.
   이 담당자는 특정 범위의 평가에 대해 전반적으로 책임을 지는 사람입니다. 귀하이거나 회사의 다른 사람일 수 있습니다.
   일반적으로 주 범위 연락 담당자만 지정하면 됩니다. ENX 협회에서 이 특정 범위에 관해 보내는 모든 커뮤니케이션을 다른 사람도 수신하기를 원하면 참가자 연락 담당자를 더 추가하십시오.
4. 평가 목표를 선택합니다.
   다음 섹션에 있는 주석을 다시 참조하는 것이 좋습니다. 섹션 4.3.3, “평가 목표”.
5. 평가 범위 위치를 추가합니다.
   평가 범위에 포함되는 위치를 모두 지정해야 합니다.
   다음 섹션에 있는 주석을 다시 참조하는 것이 좋습니다. 섹션 4.3.2, “TISAX 평가 범위”.

참고:

새 위치를 만든 후에 편집할 수 없습니다. 사소한 변경 사항(회사 이름 변경, 거리 이름, 우편번호, 시 등의 오타)에 대해서는 ENX 협회에 문의하십시오. 대신 수정해 드립니다.

중요한 참고 사항:

이 참고 사항은 TISAX 레이블을 갱신하는 경우에만 관련이 있습니다.

이전 범위를 등록하는 도중에 만들고 사용했던 기존 위치 기록을 다시 사용하십시오. 새 위치 기록을 같은 주소로 만들지 마십시오.

이유: 일부 TISAX 참가자는 파트너의 평가 결과를 자동으로 처리합니다. 이런 참가자는 자체 시스템을 ENX 포털과 동기화합니다. 작은 차이만 있어도 동기화에 성공하지 못할 수 있습니다. 또한 불필요한 중복 때문에 참가자 데이터가 복잡해지지도 않습니다.

6. 게시 및 공유 수준을 선택합니다(선택 사항).
   평가 결과를 다른 TISAX 참가자를 위해 게시하고 평가 결과를 파트너(들)와 공유하기로 미리 결정할 수 있습니다. 일반적으로, 최소한 귀사가 참가자이고 TISAX 프로세스를 통과하여 합격했음을 ENX 협회가 표시할 수 있게 허용합니다.
   첫 등록 시에는 이 단계를 건너뛰어도 안전합니다. 귀사의 평가 결과에 대한 액세스 권한을 나중에 언제든지 정의할 수 있습니다.
   다음 섹션에 있는 주석을 다시 참조하는 것이 좋습니다. 섹션 4.3.2.8, “게시 및 공유”.

중요한 참고 사항:

게시 또는 공유 권한은 취소할 수 없습니다.
자세한 내용은 다음을 참조하십시오. 섹션 6.4, “교환된 결과의 영속성”.

7. 청구서를 누가 수신할지 지정합니다.
   청구서를 누가 수령할 것인지 지정해야 합니다.
   다음 섹션에 있는 주석을 다시 참조하는 것이 좋습니다. 섹션 4.3.4, “수수료”.

참고:

여기서 잘못될 수 있는 것은 많지 않습니다. 나중에 약간 다른 범위를 등록했어야 했다는 사실(위치를 하나 잊어버렸거나, 다른 평가 목표가 하나 더 있는 경우 등)을 알게 되어도 감사 제공자는 이에 관계없이 평가를 실시할 수 있습니다.

예: 감사관이 귀사에서 처음에 범위에 추가하지 않았던 추가 위치가 범위에 포함되어야 한다고 결정합니다. 감사관은 계속 진행한 후 나중에 ENX 포털에서 귀사의 평가 결과를 업로드하는 동안 귀사의 평가 범위를 업데이트합니다.

참고:

모든 평가 범위는 수명 주기를 거칩니다. 이 단계에 평가 범위의 상태는 “미완료”, “주문 대기 중” 또는 “ENX 승인 대기 중”입니다.

평가 범위의 상태에 대한 자세한 내용은 다음을 참조하십시오. 섹션 7.5.1, “개요: Assessment scope status(🇰🇷 평가 범위 상태)”.

참고:

위치가 여러 개인 대기업을 위해, TISAX는 간단 그룹 평가를 제공합니다. 다음과 같은 경우 이 평가를 고려할 수 있습니다.

- 범위에 위치가 세 개 이상 있고[10]
- 귀사의 정보 보안 관리 시스템이 최고 상태이고 중앙집중식으로 구성됨[11].

간단 그룹 평가에는 초기에 더 많은 노력이 필요합니다. 하지만 위치 수가 많을수록 더 효과적입니다.

“간단 그룹 평가”에 대한 자세한 내용은 “TISAX Simplified Group Assessment(TISAX 간단 그룹 평가)” 문서를 참조하십시오.

“TISAX Simplified Group Assessment(TISAX 간단 그룹 평가)” 문서는 ENX 협회 웹사이트에서 다운로드할 수 있습니다. 주소:
🇬🇧 enx.com/en-US/TISAX/downloads/

PDF 직접 다운로드:
enx.com/sga.pdf

참고:

평가 범위가 등록된 후에는 직접 변경할 수 없습니다.

“TISAX 범위 발췌 자료”를 감사 제공자에게 보내지 않았다고 신빙성 있게 확인해 주실 수 있는 경우, ENX 협회에 문의하십시오. 대신 변경해 드릴 수 있습니다.

“TISAX 범위 발췌 자료”를 감사 제공자에게 이미 보낸 경우, ENX 포털에서 새 위치를 만들고(해당하는 경우) 변경 사항에 대해 감사 제공자와 상의하기만 하면 됩니다. 감사 제공자는 변경 사항을 근거로 평가를 실시하고 ENX 포털에서 범위 정보를 업데이트합니다.

참고:

평가 범위를 ENX 포털에서 직접 삭제할 수 없습니다. 실수로 평가 범위를 만든 경우 ENX 협회에 문의하십시오. 대신 삭제해 드립니다.

4.5.8. 확인 이메일

위의 필수 단계를 모두 완료하면 ENX 협회에서 신청서를 확인합니다. 그런 다음 확인 이메일을 보내 드립니다.

이 이메일에는 중요한 요소가 두 개 있습니다.

- 모든 TISAX 감사 제공자의 연락처 목록
  귀사의 평가 범위를 평가하려면 ENX 협회의 TISAX 감사 제공자 중 하나를 선택해야 합니다. 연락처를 사용하여 오퍼를 요청할 수 있습니다.
  감사 제공자 선택에 대한 자세한 내용은 다음을 참조하십시오. 섹션 5.3, “감사 제공자 선택”.
- “TISAX Scope Excerpt(TISAX 범위 발췌 자료)” PDF 첨부 파일

  여기에는 다음이 포함됩니다.

  - ENX 협회의 데이터베이스에 저장된 정보
  - 귀사의 참가자 ID
    아래에서 다음을 참조하십시오. 섹션 4.5.8.1, “Participant ID (참가자 ID)”
  - 귀사의 범위 ID
    아래에서 다음을 참조하십시오. 섹션 4.5.8.2, “Scope ID (범위 ID)”

확인 이메일의 예는 다음을 참조하십시오. 섹션 7.2, “부록: 확인 이메일 예시”.

“TISAX 범위 발췌 자료”의 예는 다음을 참조하십시오. 섹션 7.3, “부록: TISAX 범위 발췌 자료 예시”.

확인 이메일은 일반적으로 삼 영업일 이내에 수신됩니다.

칠 영업일 이내에 ENX 협회의 연락을 받지 못할 경우 a) 모든 정보를 제공했고 b) 평가 범위 상태가 “ENX 승인 대기 중”인지 확인하십시오. 모든 것이 완료된 경우에만 ENX 협회에서 귀사의 등록을 처리합니다. 모든 것이 완료되었다고 생각되는데도 ENX 협회의 연락을 받지 못할 경우 ENX 협회에 문의하십시오.

확인 이메일을 주 참가자 연락 담당자에게 보내 드립니다.

참고:

모든 평가 범위는 수명 주기를 거칩니다. 이 단계에 평가 범위의 상태는 “ENX 승인 대기 중” 입니다.

평가 범위의 상태에 대한 자세한 내용은 다음을 참조하십시오. 섹션 7.5.5, “Assessment scope status “Awaiting your payment” (🇰🇷 평가 범위 상태 “지불 대기 중”)”.

이어지는 두 하위 섹션에서는 참가자 ID와 범위 ID의 목적에 대한 자세한 정보를 제시합니다.

4.5.8.1. Participant ID (🇰🇷 참가자 ID)

참가자 ID:

- TISAX 참가자를 식별합니다.
- 각 참가자마다 고유합니다.
- 등록 완료 시에 ENX 협회에서 지정합니다.
- TISAX 감사 제공자가 정보 보안 평가를 주문하기 위한 전제 조건입니다.
- 형식은 다음과 같습니다.

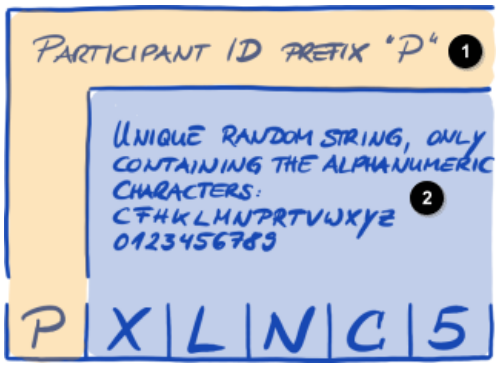


그림 7. 참가자 ID의 형식[12]

1. 참가자 ID 접두사 “P”
2. 영숫자만 포함하는 고유 임의 문자열:
   CFHKLMNPRTVWXYZ
   0123456789

참고:

다음 두 가지 방법으로 참가자 ID를 확인할 수 있습니다.

1. “TISAX 범위 발췌 자료” 를 확인합니다.
   위에서 다음을 참조하십시오. 섹션 4.5.8, “확인 이메일”
2. ENX 포털에 로그인하고, 주 탐색 모음으로 이동한 후 “DASHBOARD” (🇰🇷 “대시보드”)를 선택합니다. 거기에 귀사의 참가자 ID가 있습니다.

4.5.8.2. Scope ID (🇰🇷 범위 ID)

범위 ID:

- 평가 범위를 식별합니다.

- 각 평가 범위마다 고유합니다.
- 등록 완료 시에 ENX 협회에서 지정합니다.
- TISAX 감사 제공자가 정보 보안 평가를 주문할 수 있기 위한 전제 조건입니다.
- 형식은 다음과 같습니다.

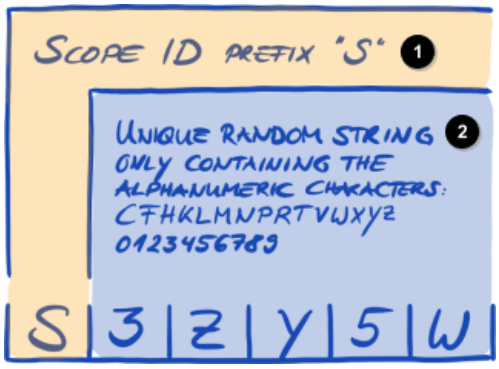


그림 8. 범위 ID의 형식

1. 범위 ID 접두사 “S”
2. 영숫자만 포함하는 고유 임의 문자열:
   CFHKLMNPRTVWXYZ
   0123456789

참고:

다음 두 가지 방법으로 범위 ID를 확인할 수 있습니다.

1. “TISAX 범위 발췌 자료”를 확인합니다.
   위에서 다음을 참조하십시오. 섹션 4.5.8, “확인 이메일”
2. ENX 포털에 로그인하고, 주 탐색 모음으로 이동한 후 “MY TISAX(내 TISAX)”를 선택한 다음 “SCOPES AND ASSESSMENTS(범위와 평가)”를 선택합니다. 거기에 범위 ID가 있습니다.

참고:

모든 평가 범위(범위 ID로 식별됨)는 수명 주기를 거칩니다.

평가 범위의 상태에 대한 자세한 내용은 다음을 참조하십시오. 섹션 7.5, “부록: Assessment scope status(🇰🇷 평가 범위 상태)”.

4.5.9. 상태 정보

이 단계에 TISAX 프로세스 진행 상황을 나타내기 위해 사용되는 다음과 같은 관련 상태가 두 개 있습니다.

1. 참가자 상태
2. 평가 범위 상태

다음은 특정 상태에 도달하기 위해 충족되어야 하는 조건을 설명하는 그림입니다.

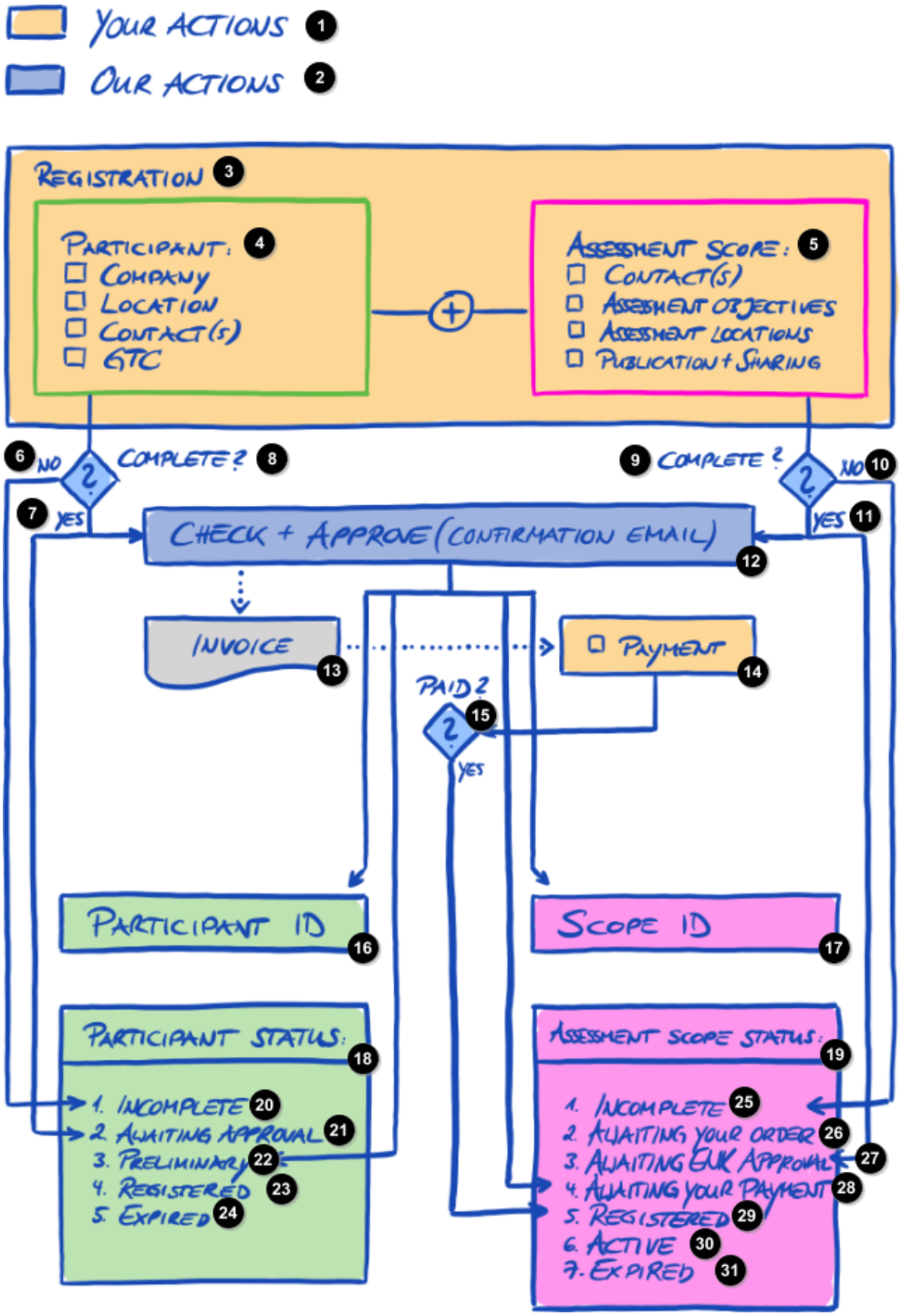


그림 9. 참가자 상태 및 평가 범위 상태에 도달하기 위한 조건

1. 귀사의 작업
2. ENX 협회의 작업
3. 등록

4 참가자:
[ ] 회사
[ ] 위치
[ ] 연락 담당자
[ ] GTC

5 평가 범위:
[ ] 연락 담당자
[ ] 평가 목표
[ ] 평가 위치
[ ] 게시 + 공유

6 아니요

7 예

8 완료?

9 완료?

10 아니요

11 예

12 확인 + 승인(확인 이메일)

13 청구서

14 [ ] 지불

15 지불 완료?

16 참가자 ID

17 범위 ID

18 참가자 상태:

19 평가 범위 상태:

20 1. 미완료

21 2. 승인 대기 중

22 3. 예비

23 등록됨

24 만료됨

25 1. 미완료

26 2. 주문 대기 중

27 3. ENX 승인 대기 중

28 4. 지불 대기 중

29 5. 등록됨

30 6. 활성

31 7. 만료됨

상태 정의와 다음 상태로 진행하기 위해 해야 할 일은 부록에서 확인할 수 있습니다.

자세한 내용은 다음을 참조하십시오.

- 참가자 상태 - 섹션 7.4, “부록: Participant status(🇰🇷 참가자 상태)” 참조.
- 평가 범위 상태 - 섹션 7.5, “부록: Assessment scope status(🇰🇷 평가 범위 상태)” 참조.

4.5.10. 등록 정보 변경

참고:

데이터 수명 주기에 관한 모든 답변은 다음을 참조하십시오. 섹션 7.9, “부록: 참가자 데이터 수명 주기 관리”. 여기에는 회사 이름이나 연락처 정보 같은 데이터를 변경하거나 업데이트하고 싶은 경우에 대한 설명이 수록되어 있습니다.

축하합니다. 이제 TISAX 참가자로 등록되었습니다. TISAX 프로세스의 다음 단계로 계속 진행할 준비가 되었습니다.

5. 평가(2 단계)

평가 섹션을 읽는 데 걸리는 예상 시간은 30~35분입니다.

5.1. 개요

TISAX 평가는 두 번째 단계입니다. 이 단계에 TISAX 평가를 받는 일을 대부분 하게 됩니다.

이어지는 내용에서는 평가를 진행하는 과정을 안내합니다.

1. 여기서는 ISA 자가 평가를 사용하여 TISAX 평가를 받을 준비가 되었는지 확인할 수 있는 방법에 대한 설명으로 시작합니다.
2. 이어서 TISAX 감사 제공자 중 하나를 선택하는 방법에 대해 설명합니다.
3. 그런 다음 평가 프로세스를 진행하는 과정에 대해 설명합니다..
4. 끝에서는 “처리 결과”(평가 결과와 관련 TISAX 레이블)에 대해 설명합니다.

5.2. ISA 기반 자가 평가

TISAX 평가를 받을 준비가 되려면 우선 정보 보안 관리 시스템(ISMS)의 상태가 최상이어야 합니다. ISMS가 기대되는 성숙도에 부합하는지 확인하려면 ISA를 기반으로 자가 평가를 실시해야 합니다.

“정보 보안 평가”(ISA)는 “독일 자동차 산업 협회”(Verband der Automobilindustrie e.V. - VDA)에서 발행하는 기준 카탈로그입니다. ISA는 정보 보안 평가에 대한 자동차 산업의 표준입니다.

이어지는 내용에서는 ISA를 기반으로 자가 평가를 실시하기 위한 실제 지침에 초점을 맞춥니다.

본 안내서에 수록된 설명 및 예와 스크린샷은 ISA 5 버전 기준입니다.

참고:

이전 ISA 버전과 다르게 변경된 사항에 대한 정보는 “Change history(변경 내역)” Excel 시트에서 확인할 수 있습니다.

참고:

VDA에서 새 ISA 버전을 발행하면 어느 ISA 버전이 귀사의 평가에 적용되는지에 대한 내용은 다음을 참조하십시오. 섹션 7.11, “부록: ISA 수명 주기 관리” .

5.2.1. ISA 문서 다운로드

ISA 문서를 다운로드하여 자가 평가를 시작하십시오.

이 문서는 ENX 협회 웹 사이트에서 다운로드할 수 있습니다. 주소:
enx.com/en-US/TISAX/downloads/

Excel 파일 직접 다운로드:
portal.enx.com/isa5-en.xlsx

ISA 문서는 독일어로도 제공됩니다.
enx.com/de-de/TISAX/downloads/

5.2.2. ISA 문서 이해

자가 평가를 시작하기 전에, 다음과 같은 설명을 참고하면 유용할 수 있습니다. 이런 설명은 ISA 문서에 수록된 공식 설명 및 정의와 별도로 제시되었지만, TISAX 평가의 용도에 초점을 맞춥니다.

5.2.2.1. 기준 카탈로그

ISA에는 현재 다음과 같은 세 가지 “기준 카탈로그”가 있습니다[13].

1.	정보 보안	Information Security
2.	프로토타입 보호	Prototype Protection
3.	데이터 보호	Data Protection

각 기준 카탈로그마다 다음과 같은 자체적인 Excel 시트가 있습니다.

그림 10. 스크린샷: ISA 기준 카탈로그 Excel 시트

어떤 기준 카탈로그가 귀사와 관련이 있을까요? 평가 목표에 따라 다릅니다.

각 평가 목표는 어느 기준 카탈로그의 어느 요구 사항이 적용되는지 정의합니다. 기준 카탈로그 하나의 요구 사항만 적용되는 평가 목표도 있고 하나보다 많은 기준 카탈로그의 요구 사항이 적용되는 목표도 있습니다.

앞에서 언급한 평가 목표는 다음과 같은 기준 카탈로그에 매핑됩니다.

번호	평가 목표(Assessment objective)	ISA 기준 카탈로그
1.	Info high	Information Security (정보 보안)
2.	Info very high	Information Security (정보 보안)
3.	Confidential	Information Security (정보 보안)
4.	Strictly confidential	Information Security (정보 보안)
5.	High availability	Information Security (정보 보안)
6.	Very high availability	Information Security (정보 보안)
7.	Proto parts	Prototype Protection (프로토타입 보호)
8.	Proto vehicles	Prototype Protection (프로토타입 보호)
9.	Test vehicles	Prototype Protection (프로토타입 보호)
10.	Proto events	Prototype Protection (프로토타입 보호)
11.	Data	Information Security (정보 보안) Data Protection (데이터 보호)
12.	Special data	Information Security (정보 보안) Data Protection (데이터 보호)

표 7. TISAX 평가 목표와 ISA 기준 카탈로그 매핑

예: “데이터 보호”를 평가 목표로 선택하면 “정보 보안” 및 “데이터 보호” 기준 카탈로그에 있는 문항에 답해야 합니다.

기준 카탈로그 하나에 평가 목표가 두 개 이상 있는 경우가 있습니다. 어느 요구 사항이 어느 평가 목표에 해당하는지 어떻게 알 수 있을까요?

아래 표에는 어느 요구 사항이 적용되는지 나와 있습니다.

번호	평가 목표(Assessment objective)	해당하는 요구 사항
1.	Info high	▪ 기준 카탈로그 “Information Security”(“정보 보안”) ◦ “Requirements (must)”(“요구 사항(필수)”) 열 ◦ “Requirements (should)”(“요구 사항(해당하는 경우 필수)”) 열 ◦ “Additional requirements for high protection needs”(“높은 보호 수준이 필요한 경우의 추가 요구 사항”) 열
2.	Info very high	▪ 기준 카탈로그 “Information Security”(“정보 보안”) ◦ “Requirements (must)”(“요구 사항(필수)”) 열 ◦ “Requirements (should)”(“요구 사항(해당하는 경우 필수)”) 열 ◦ “Additional requirements for high protection needs”(“높은 보호 수준이 필요한 경우의 추가 요구 사항”) 열 ◦ (“매우 높은 보호 수준이 필요한 경우의 추가 요구 사항”
3.	Confidential	▪ 기준 카탈로그 “Information Security”(“정보 보안”) ◦ “Requirements (must)”(“요구 사항(필수)”) 열 ◦ “Requirements (should)”(“요구 사항(해당하는 경우 필수)”) 열 ◦ “Additional requirements for high protection needs”(“높은 보호 수준이 필요한 경우의 추가 요구 사항”) 열 (하지만 Confidentiality(비밀 유지)를 의미하는 “C”로 표시된 것만)
4.	Strictly confidential	▪ 기준 카탈로그 “Information Security”(“정보 보안”) ◦ “Requirements (must)”(“요구 사항(필수)”) 열 ◦ “Requirements (should)”(“요구 사항(해당하는 경우 필수)”) 열 ◦ “Additional requirements for high protection needs”(“높은 보호 수준이 필요한 경우의 추가 요구 사항”) 열 (하지만 Confidentiality(비밀 유지)를 의미하는 “C”로 표시된 것만) ◦ (“매우 높은 보호 수준이 필요한 경우의 추가 요구 사항” (하지만 Confidentiality(비밀 유지)를 의미하는 “C”로 표시된 것만)

번호	평가 목표(Assessment objective)	해당하는 요구 사항
5.	High availability	▪ 기준 카탈로그 “Information Security”(“정보 보안”) ◦ “Requirements (must)”(“요구 사항(필수)”) 열 ◦ “Requirements (should)”(“요구 사항(해당하는 경우 필수)”) 열 ◦ “Additional requirements for high protection needs”(“높은 보호 수준이 필요한 경우의 추가 요구 사항”) 열 (하지만 Availability(가용성)을 의미하는 “A”로 표시된 것만)
6.	Very high availability	▪ 기준 카탈로그 “Information Security”(“정보 보안”) ◦ “Requirements (must)”(“요구 사항(필수)”) 열 ◦ “Requirements (should)”(“요구 사항(해당하는 경우 필수)”) 열 ◦ “Additional requirements for high protection needs”(“높은 보호 수준이 필요한 경우의 추가 요구 사항”) 열 (하지만 Availability(가용성)을 의미하는 “A”로 표시된 것만) ◦ (“매우 높은 보호 수준이 필요한 경우의 추가 요구 사항” (하지만 Availability(가용성)을 의미하는 “A”로 표시된 것만)
7.	Proto parts	▪ 기준 카탈로그 “Prototype Protection”(“프로토타입 보호”) 하지만 다음 장만: 8.1 Physical and Environmental Security (8.1 물리적 보안과 환경 보안) 8.2 Organizational Requirements (8.2 조직의 요구 사항) 8.3 Handling of vehicles, components and parts (8.3 차량, 구성 요소 및 부품 취급) ◦ “Requirements (must)”(“요구 사항(필수)”) 열 ◦ “Requirements (should)”(“요구 사항(해당하는 경우 필수)”) 열

번호	평가 목표(Assessment objective)	해당하는 요구 사항
8.	Proto vehicles	▪ 기준 카탈로그 “Prototype Protection”(“프로토타입 보호”) 하지만 다음 장만: 8.1 Physical and Environmental Security (8.1 물리적 보안과 환경 보안) 8.2 Organizational Requirements (8.2 조직의 요구 사항) 8.3 Handling of vehicles, components and parts (8.3 차량, 구성 요소 및 부품 취급) ◦ “Requirements (must)”(“요구 사항(필수)”) 열 ◦ “Requirements (should)”(“요구 사항(해당하는 경우 필수)”) 열 ◦ “Additional requirements for vehicles classified as requiring protection”(“보호할 필요가 있다고 분류된 차량에 추가로 요구되는 사항”) 열
9.	Test vehicles	▪ 기준 카탈로그 “Prototype Protection”(“프로토타입 보호”) 하지만 다음 장만: 8.2 Organizational Requirements (8.2 조직의 요구 사항) 8.3 Handling of vehicles, components and parts (8.3 차량, 구성 요소 및 부품 취급) 8.4 Requirements for trial vehicles (8.4 시험 차량에 요구되는 사항) ◦ “Requirements (must)”(“요구 사항(필수)”) 열 ◦ “Requirements (should)”(“요구 사항(해당하는 경우 필수)”) 열
10.	Proto events	▪ 기준 카탈로그 “Prototype Protection”(“프로토타입 보호”) 하지만 다음 장만: 8.2 Organizational Requirements (8.2 조직의 요구 사항) 8.3 Handling of vehicles, components and parts (8.3 차량, 구성 요소 및 부품 취급) 8.5 Requirements for events and shootings (8.5 이벤트와 촬영에 요구되는 사항) ◦ “Requirements (must)”(“요구 사항(필수)”) 열 ◦ “Requirements (should)”(“요구 사항(해당하는 경우 필수)”) 열

번호	평가 목표(Assessment objective)	해당하는 요구 사항
11.	Data	▪ 기준 카탈로그 “Information Security”(“정보 보안”) ◦ “Requirements (must)”(“요구 사항(필수)”) 열 ◦ “Requirements (should)”(“요구 사항(해당하는 경우 필수)”) 열 ◦ “Additional requirements for high protection needs”(“높은 보호 수준이 필요한 경우의 추가 요구 사항”) 열 (하지만 Confidentiality(비밀 유지)를 의미하는 “C”로 표시된 것만) ▪ 기준 카탈로그 “Data Protection”(“데이터 보호”) ◦ “Requirements (must)”(“요구 사항(필수)”) 열
12.	Special data	▪ 기준 카탈로그 “Information Security”(“정보 보안”) ◦ “Requirements (must)”(“요구 사항(필수)”) 열 ◦ “Requirements (should)”(“요구 사항(해당하는 경우 필수)”) 열 ◦ “Additional requirements for high protection needs”(“높은 보호 수준이 필요한 경우의 추가 요구 사항”) 열 (하지만 Confidentiality(비밀 유지)를 의미하는 “C”로 표시된 것만) ◦ ()“매우 높은 보호 수준이 필요한 경우의 추가 요구 사항” (하지만 Confidentiality(비밀 유지)를 의미하는 “C”로 표시된 것만) ▪ 기준 카탈로그 “Data Protection”(“데이터 보호”) ◦ “Requirements (must)”(“요구 사항(필수)”) 열

표 8. 평가 목표에 해당하는 요구 사항

참고:

“높은 보호 수준이 필요한 경우의 추가 요구 사항” 및 “매우 높은 보호 수준이 필요한 경우의 추가 요구 사항”이라는 두 개의 열에 있는 요구 사항에는 각각 Confidentiality(비밀 유지)를 의미하는 “C”, 또는 Integrity(무결성)을 의미하는 “I”, 또는 Availability(가용성)를 의미하는 “A”나 이 세 문자의 조합이 표시되어 있습니다.

위의 표에 따라 이 두 열에 있는 요구 사항이 앞에서 언급한 문자 중 하나로 표시된 것으로 좁혀지면 여기에는 항상 이 문자보다 많은 문자로 표시된 요구 사항도 포함됩니다.

예: “(C)”, “(C, I, A)” 또는 “(C, I)”로 표시된 모든 요구 사항은 위 표에 “C”가 명시된 경우(예: 평가 목표 “Special data”)에 해당합니다.

아래 스크린샷에는 “정보 보안” 기준 카탈로그에 있는 통제 문항의 주 요소가 나와 있습니다. (다른 기준 카탈로그에는 이런 요소의 부분 집합만 있습니다.) 모든 요소에 대해서는 더 아래에서 설명합니다.

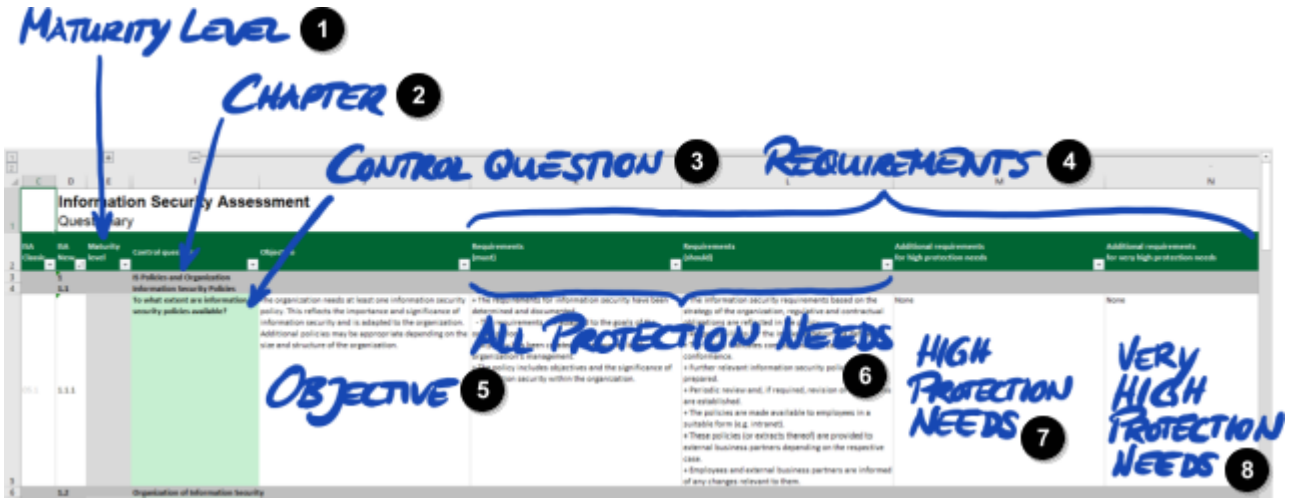


그림 11. 스크린샷: ISA 기준 카탈로그 “정보 보안”에 있는 문항의 주 요소

1. 성숙도
2. 장
3. 통제 문항
4. 요구 사항
5. 목표
6. 모든 필요한 보호 수준
7. 필요한 보호 수준 높음
8. 필요한 보호 수준 매우 높음

5.2.2.2. 장

각 기준 카탈로그에서는 문항 그룹을 장으로 나눕니다.

예: “2 인사(HR)”

그룹은 일반적인 사내 책임을 기준으로 나뉩니다. 이런 부서는 “Usual person responsible for process implementation(프로세스 이행을 일반적으로 책임지는 사람)” 열(위 예에서는 “HR”)에 명시됩니다.

5.2.2.3. 통제 문항

각 기준 카탈로그에 대한 문항은 해당하는 Excel 시트에 있습니다.

예: “4.1.2 사용자의 네트워크 서비스, IT 시스템 및 IT 애플리케이션 액세스는 어느 정도까지 보호됩니까?”

통제 문항을 “컨트롤”이라고도 합니다. 이 표현은 감사관이 사용합니다. ISA의 기초인 ISO 표준에서는 “컨트롤”이라는 용어를 사용합니다.

5.2.2.4. 자가 평가 양식 필드

“Maturity level”(🇰🇷 “성숙도”) 및 “Control question”(🇰🇷 “통제 문항”) 열 사이에는 자가 평가를 실시할 때 채워 넣어야 하는 양식 필드가 있습니다.

양식 필드	목적	필수?
Implementation description (🇰🇷 이행 설명) (F 열)	여기에는 귀사에서 이 통제 문항에 대응하기 위해 이행한 사항을 간략하게 서술해야 합니다.	예
Reference Documentation (🇰🇷 참조 문헌) (G 열)	여기에는 어느 문서에서 이행을 입증하는지 명시해야 합니다.	예
Findings/Result (🇰🇷 발견된 문제/결과) (H 열)	여기에는 목표와 현실 사이에 격차가 존재한다고 생각되는 감사 결과를 모두 적을 수 있습니다.	아니요

표 9. 자가 평가 양식 필드와 각 필드의 목적

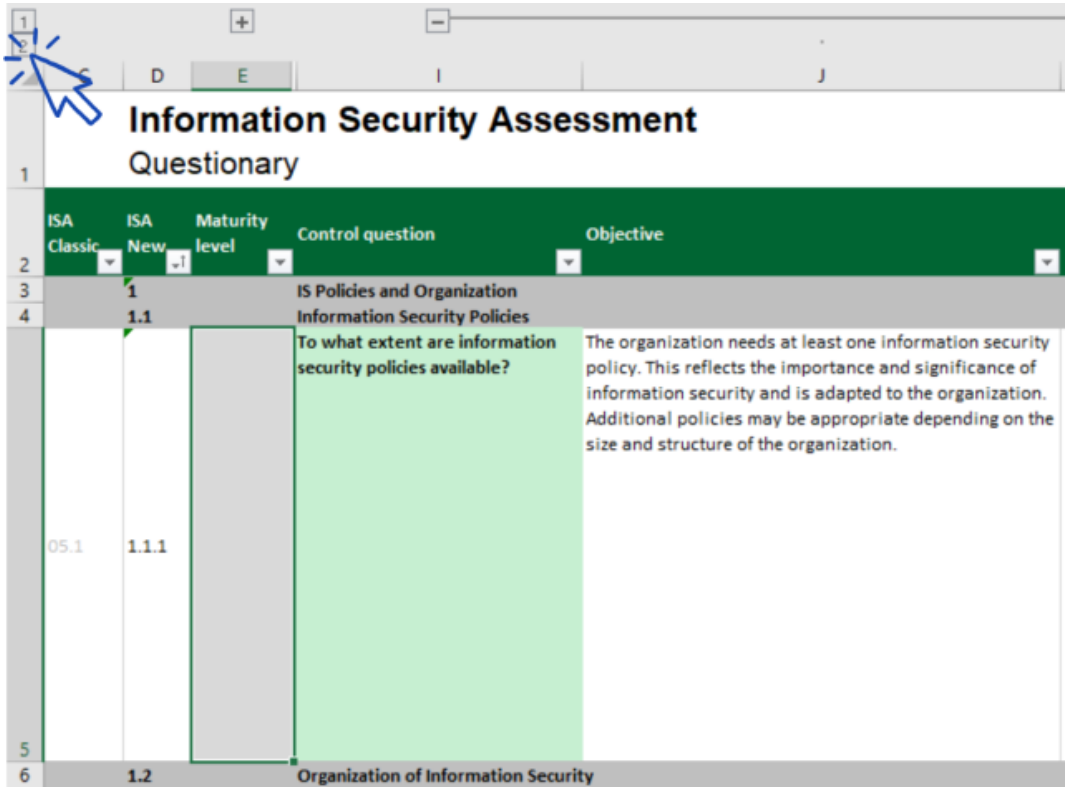
이행에 대한 간략한 설명과 귀사 문헌에 대한 참조만 필수입니다. 이 정보는 TISAX 감사 제공자가 귀사를 더 잘 이해하고 평가를 더 잘 준비하는 데 도움이 됩니다.

자가 평가에 도움이 되는 뒷받침하는 다음과 같은 선택적인 열이 더 있습니다.

- Measures/recommendations (🇰🇷 조치/권장 사항)(R 열)
- Date of assessment (🇰🇷 평가 날짜)(S 열)
- Date of completion (🇰🇷 완료 날짜)(T 열)
- Responsible department (🇰🇷 책임 부서)(U 열)
- Contact (🇰🇷 연락 담당자)(V 열)

중요한 참고 사항:

다운로드한 Excel 파일을 열고 기준 카탈로그 워크시트 중 하나(예: 정보 보안)를 선택하면 자가 평가 양식 필드가 즉시 보이지 않을 수 있습니다. 이런 필드를 표시하려면 수준 “2”에 해당하는 그룹화 버튼을 클릭해야 합니다[14]. 이 버튼은 C1 셀 위의 왼쪽에 있습니다. 이 버튼을 누르면 보기가 확장되어 자가 평가 양식 필드가 표시됩니다.



화살표 키를 사용하여 아래로 스크롤하는 방법도 권장됩니다. 셀 크기가 크기 때문에 스크롤 막대를 사용하여 스크롤하려면 미세 운동 기능이 뛰어나야 할 수 있습니다. 포인팅 장치의 스크롤 기능을 사용하면 큰 셀 몇 개를 실수로 건너뛸 수도 있습니다.

5.2.2.5. 목표

“통제 문항” 열 오른쪽에는 “목표” 열(J 열)이 있습니다. 이 열의 내용은 이 정보 보안 관리 측면에 관해 달성해야 하는 사항에 대해 설명합니다.

예(통제 문항 4.1.2번): “안전하게 식별된(인증된) 사용자만 IT 시스템에 액세스할 수 있어야 합니다. 이를 목적으로 사용자 신원이 적합한 절차를 통해 안전하게 확인됩니다.”

5.2.2.6. 요구 사항

요구 사항은 목표를 달성하기 위해 충족해야 한다고 기대되는 사항입니다.

요구 사항은 다음 네 열에 분산되어 있습니다.

1. Requirements (must) (🇰🇷 요구 사항(필수))(K 열)
2. Requirements (should) (🇰🇷 요구 사항(해당하는 경우 필수))(L 열)
3. Additional requirements for high protection needs (🇰🇷 높은 보호 수준이 필요한 경우의 추가 요구 사항)(M 열)

4. Additional requirements for very high protection needs (🇰🇷 매우 높은 보호 수준이 필요한 경우의 추가 요구 사항)(N 열)

(평가 목표에서 추론할 수 있는) 달성해야 하는 필요한 보호 수준까지의 모든 요구 사항을 충족해야 합니다.

몇몇 평가 목표에는 요구 사항의 일부만 해당합니다. 요구 사항의 해당 여부에 대한 자세한 내용은 섹션 5.2.2.1, “기준 카탈로그”의 표 8, “평가 목표에 해당하는 요구 사항”과 특히 이 섹션 끝에 있는 note를 참조하십시오.

“필수” 및 “해당하는 경우 필수” 요구 사항 수준의 ISA 정의에 대한 자세한 내용은 “정의” Excel 시트의 “주요 용어”를 참조하십시오.

중요한 참고 사항:

각 요구 사항을 목표의 맥락과 정신에 따라 해석해야 함을 이해하는 것이 중요합니다. 요구 사항을 문자 그대로 정확히 충족해도 감사 제공자가 요구 사항이 목표(J 열)의 맥락과 정신에 따라 충족되었다고 확인해 줄 것이라는 보장이 없습니다.

요구 사항과 그 표현의 기준은 규모를 알 수 없는 가상의 평균적인 회사에 의한 이론적인 이행입니다.

감사 제공자는 항상 목표를 귀사 고유의 이행과 비교하여 고려해야 합니다. 평균적인 회사에 적절한 것이 귀사의 특정한 상황에서는 충분하지 않을 수도 있습니다.

자세한 내용은 다음을 참조하십시오. 섹션 5.2.5, “자가 평가 결과의 문제 해결”.

5.2.2.7. 성숙도

ISA에서는 “maturity levels”(🇰🇷 “성숙도”)라는 개념을 정보 보안 관리 시스템의 모든 측면의 품질을 평가하는 데 사용합니다. 정보 보안 관리 시스템이 더 정교할수록 성숙도가 더 높을 것입니다.

ISA에서는 성숙도를 여섯 개로 구별합니다. 자세한 정의는 “Maturity levels”(🇰🇷 “성숙도”) Excel 시트에서 확인할 수 있습니다. 성숙도를 통합해서 보기 위해, 여기서는 ISA에 제시된 비공식적인 설명을 인용합니다.

Maturity level (🇰🇷 성숙도)	단어 하나로	설명
0	Incomplete (🇰🇷 미완료)	프로세스를 사용할 수 없거나, 따르지 않거나, 프로세스가 목표를 달성하는 데 적합하지 않습니다.
1	Performed (🇰🇷 수행됨)	문서화되지 않거나 문서화가 완료되지 않은 프로세스를 따르고, 프로세스가 그 목표를 달성함을 나타내는 지표가 존재합니다.
2	Managed (🇰🇷 관리됨)	목표를 달성하는 프로세스를 따릅니다. 프로세스 문헌과 프로세스 이행 증거가 있습니다.
3	Established (🇰🇷 확립됨)	전체 시스템에 통합된 표준 프로세스를 따릅니다. 다른 프로세스에 대한 종속성을 문서화하고 적합한 인터페이스를 만듭니다. 프로세스가 오랜 기간 동안 지속가능한 방법으로 활발하게 사용되어 왔다는 증거가 있습니다.
4	Predictable (🇰🇷 예측 가능)	확립된 프로세스를 따릅니다. 주요 수치를 수집하여 프로세스의 효과를 지속적으로 모니터링합니다. 프로세스가 충분히 효과적이지 않고 조정이 필요하다고 간주되는 한계 값을 정의합니다. (핵심 성과 지표)
5	Optimizing (🇰🇷 최적화 중)	지속적인 개선이 주요 목표인 예측 가능한 프로세스를 따릅니다. 개선 사항이 전담 리소스를 통해 적극적으로 진전됩니다.

표 10. 성숙도에 대한 비공식적인 설명

문항마다 정보 보안 관리 시스템의 성숙도를 평가해야 합니다. 성숙도를 “Maturity level”(🇰🇷 “성숙도”) 열(E

열)에 입력하십시오.

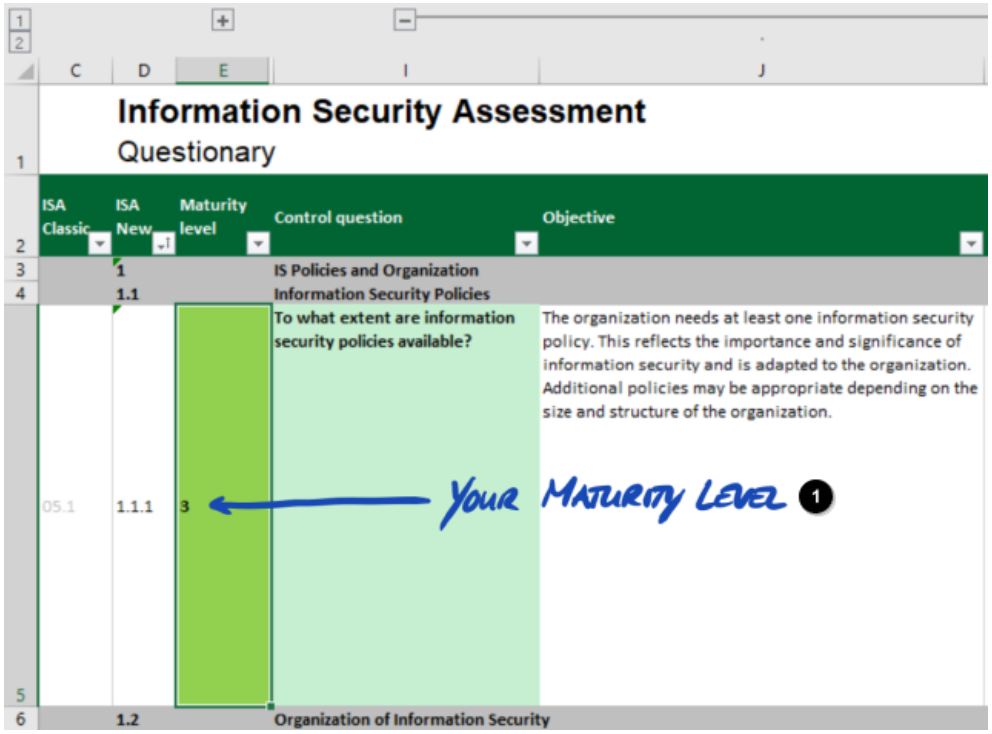


그림 12. 스크린샷: ISA 문서에서 성숙도를 선택하는 예(“정보 보안” Excel 시트)

1 귀사의 성숙도

목표 성숙도와 이 성숙도가 평가 결과에 미치는 영향에 대한 자세한 내용은 다음을 참조하십시오. 섹션 5.2.4, “자가 평가 결과 해석”.

이제 더 많은 것을 알게 되었으므로 자가 평가를 시작할 준비가 되었습니다.

5.2.3. 자가 평가 실시

Excel 파일을 열고 평가 목표에 해당하는 각 기준 카탈로그의 통제 문항에 모두 답하고 귀사 정보 보안 관리 시스템의 현 상태와 일치하는 성숙도를 결정하십시오. 이 작업은 최선의 판단에 따라 직접 수행해야 합니다. 이 단계에는 정답이나 오답이 없습니다.

자가 평가를 완료한 후에는 “결과(ISA5)” Excel 시트의 “결과” 열(H)이 숫자(0~5) 또는 “n.a.”(”해당 없음”)로 완전히 채워져야 합니다.

No.	Subject	Target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3
1.2.3	To what extent are information security requirements taken into account in projects?	3	3
1.2.4	To what extent are responsibilities between external IT service providers and the own organization defined?	3	3
1.3.1	To what extent are information assets identified and recorded?	3	3
1.3.2	To what extent are information assets classified and managed in terms of their protection needs?	3	3
1.3.3	To what extent is it ensured that only evaluated and approved external IT services are used for processing the organization's information assets?	3	3
1.4.1	To what extent are information security risks managed?	3	3
1.5.1	To what extent is compliance with information security ensured in procedures and processes?	3	3
1.5.2	To what extent is the ISMS reviewed by an independent entity?	3	3
1.6.1	To what extent are information security events processed?	3	3

1 GREEN = ✓

그림 13. 스크린샷: ISA 문서의 “결과(ISA5)” 시트 예

1 녹색

ISA에 관한 질문이 있는 경우 ENX 협회에 문의하십시오.

5.2.4. 자가 평가 결과 해석

이어지는 다섯 개의 하위 섹션에서는 자가 평가 결과를 분석 및 해석하는 방법에 대해 설명합니다. 분석을 통해 TISAX 평가 준비가 되었는지 아니면 아직 준비가 되지 않았는지 알 수 있습니다.

5.2.4.1. 분석

귀사의 결과 점수는 자가 평가 결과를 요약합니다.

결과 점수(“목표 성숙도로 삭감된 결과”)는 “결과(ISA5)” Excel 시트(D6 셀)에 있습니다. “삭감”에 대해서는 곧 설명하겠습니다.

Information Security Assessment Results

VDA Verband der Automobilindustrie

Result with cutback to target maturity level:	3,00	Maximum score:	3,00

Details: YOUR RESULT SCORE 1 MAXIMUM RESULT SCORE

No.	Subject	Target maturity level	Result 2
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

그림 14. 스크린샷: 결과 점수와 최고 결과 점수(“결과(ISA5)” Excel 시트, D6 및 G6 셀)

1. 귀사의 결과 점수
2. 최고 결과 점수

자가 평가 결과와 결과 점수를 이해한 후 해석하려면 다음과 같은 두 개의 분석 수준을 구별해야 합니다.

1. 문항 수준
   이 수준에는 모든 문항이 있습니다. 각 문항마다 목표 성숙도와 귀사의 성숙도가 있습니다.
2. 점수 수준
   이 수준에는 모든 문항의 결과를 요약하는 전체 결과가 있습니다. 최고 결과 점수와 귀사의 결과 점수가 있습니다.

아래 그림에는 분석 수준이 나와 있습니다.

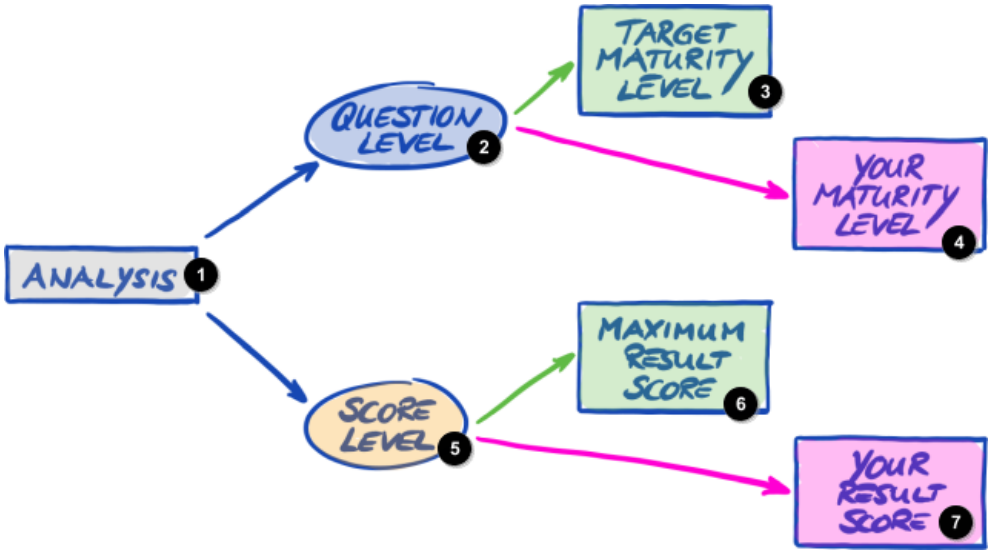


그림 15. 문항 수준과 점수 수준의 자가 평가 결과 분석

1. 분석
2. 문항 수준
3. 목표 성숙도
4. 귀사의 성숙도
5. 점수 수준
6. 최고 결과 점수
7. 귀사의 결과 점수

아래 그림에는 점수 수준의 결과와 문항 수준의 결과를 확인할 수 있는 위치가 나와 있습니다.

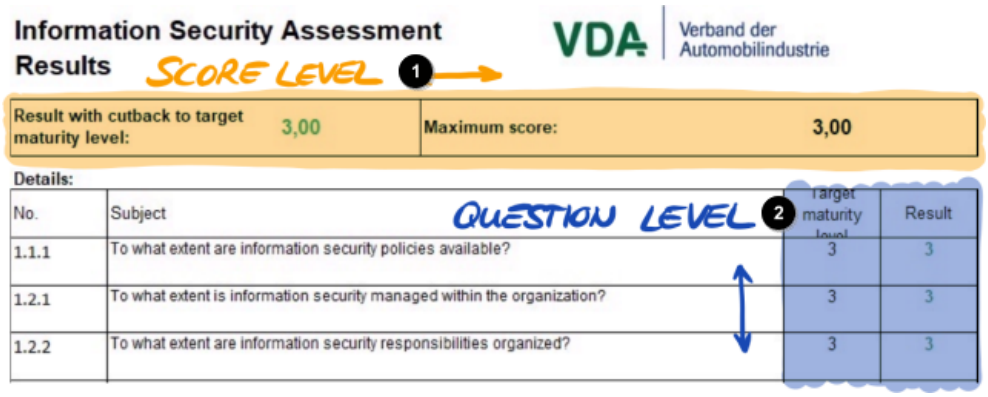


그림 16. “결과(ISA5)” Excel 시트의 점수 수준과 문항 수준

1. 점수 수준
2. 문항 수준

다음 그림에는 분석 수준, ISA 목표 정의 및 귀사의 자체 결과의 간단한 보기가 나와 있습니다.

그림 17. 문항 수준과 점수 수준의 목표와 귀사의 결과

1. 목표 성숙도

2. 귀사의 성숙도
3. 문항 수준
4. Q(문항)
5. TML(목표 성숙도)
6. YML(귀사의 성숙도)
7. 최고 결과 점수
8. 귀사의 결과 점수
9. 점수 수준

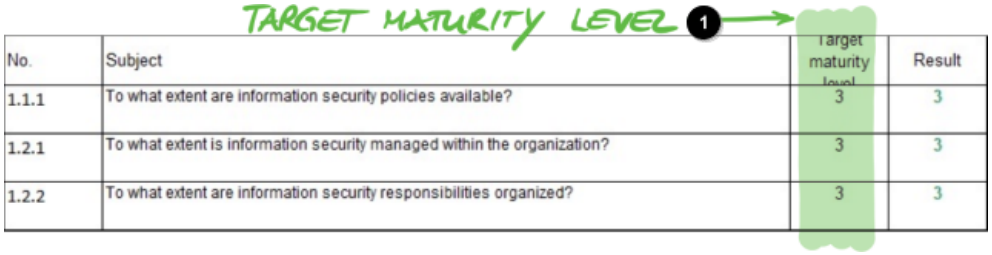
이어지는 내용에서는 결과와 결과의 분석에 대해 자세히 설명합니다.

5.2.4.2. 목표 성숙도(문항 수준)

ISA에서는 각 문항의 “목표 성숙도”를 3으로 정의합니다.

각 성숙도의 정의에 대한 자세한 내용은 다음을 참조하십시오. 섹션 5.2.2, “ISA 문서 이해”.

ISA에서는 목표 성숙도를 “결과(ISA5)” Excel 시트에서 정의합니다(G 열 22 행에서 시작. 아래 그림 참조).



No.	Subject	Target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

그림 18. “결과(ISA5)” Excel 시트의 목표 성숙도 정의

1. 목표 성숙도

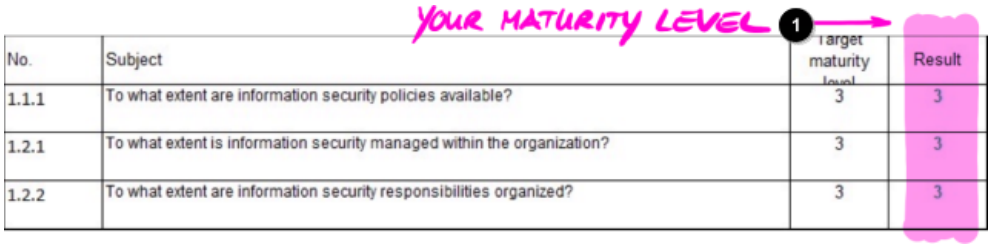
5.2.4.3. 귀사의 결과(문항 수준)

TISAX 레이블을 받기 위해서는 일반적으로 각 문항에 대한 귀사의 성숙도가 목표 성숙도와 같거나 그보다 높아야 합니다.

예: 문항 X에 대한 목표 성숙도가 “3” 인 경우, 해당 문항에 대한 귀사의 성숙도는 “3” 이상이어야 합니다. 해당 문항에 대한 귀사의 성숙도가 “3” 보다 낮으면 TISAX 레이블을 받지 못할 수 있습니다.

각 문항에 대한 귀사의 성숙도가 “3” 이상이어야 합니다. 두 문항에 대한 목표 성숙도가 “3” 인 경우, 문항 하나에 대한 귀사의 성숙도가 “2” 인 경우 성숙도가 “4” 인 다른 문항으로 보완할 수 없습니다.

ISA 문서에서는 귀사의 성숙도가 “정보 보안” Excel 시트(E 열)에서 “결과(ISA5)” Excel 시트(H 열 23번 행에서 시작)로 자동으로 이동됩니다.



No.	Subject	Target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

그림 19. “결과(ISA5)” Excel 시트의 귀사의 성숙도

1 귀사의 목표 성숙도

귀사의 성숙도에 계산이 적용된 후 계산된 값이 ISA 문서에서 귀사의 결과 점수에 요약됩니다. 근본적으로, 귀사의 성숙도가 목표 성숙도로 “삭감” 됩니다. 이렇게 하는 이유는 귀사의 성숙도가 목표 성숙도보다 높은 문항이 귀사의 성숙도가 목표 성숙도보다 낮은 문항을 보완하지 않도록 하기 위해서입니다.

ISA에서는 귀사의 결과를 문항 수준에서 다음과 같이 계산합니다.

- 귀사의 성숙도를 문항의 목표 성숙도에 비교합니다.
- 귀사의 성숙도가 목표 성숙도보다 높으면 목표 성숙도로 “삭감” 됩니다.
- 귀사의 성숙도가 목표 성숙도와 같거나 그보다 낮으면 이 문항에는 아무 일도 일어나지 않습니다.

예(아래 그림 참조): 목표 성숙도는 “3” 입니다. 귀사의 성숙도는 “4” 입니다. 이 문항에 대한 귀사의 “삭감된 결과” 는 “3” 이 됩니다.

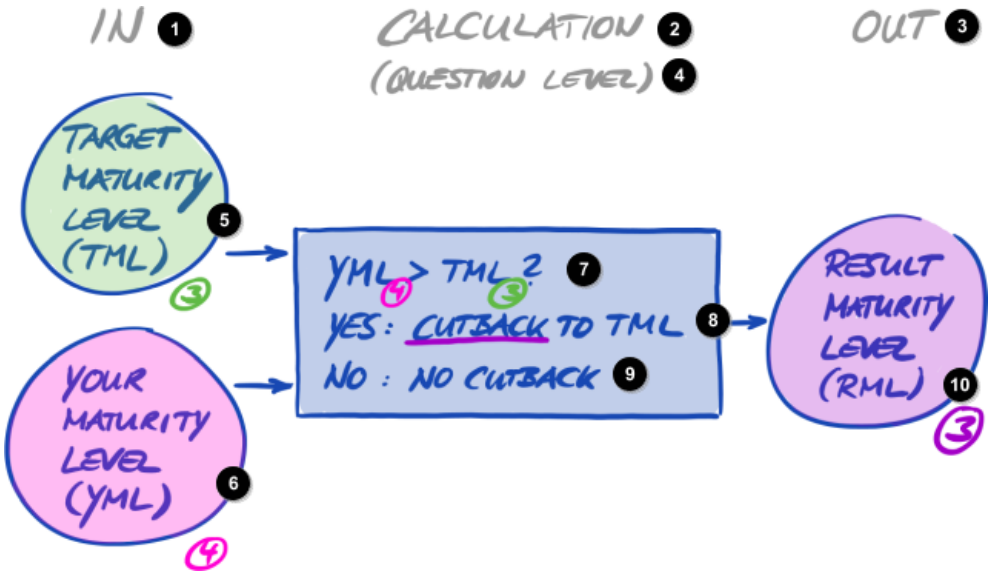


그림 20. 결과 성숙도 삭감 계산

1 입

2 계산

3 출

4 (문항 수준)

5 목표 성숙도(TML)

6. 귀사의 성숙도(YML)
7. YML > TML?
8. 예: TML로 삭감
9. 아니요: 삭감 없음
10. 결과 성숙도(RML)

아래 그림은 귀사의 성숙도가 목표 성숙도보다 높으면 ISA에서 귀사의 성숙도를 삭감함을 보여줍니다(녹색, 주황색, 빨간색이 “결과” 열에 사용된 색상과 일치함. 그림 19, “ “결과(ISA5)” Excel 시트의 귀사의 성숙도” 참조).

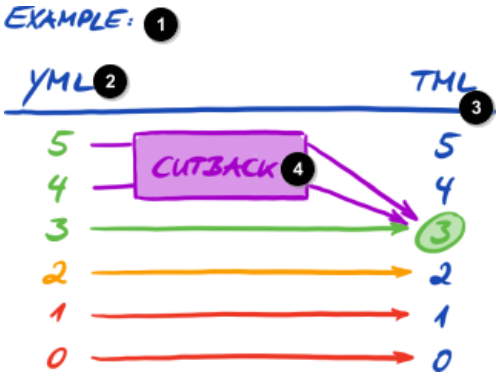


그림 21. “결과(ISA5)” Excel 시트에 사용되는 색상으로 삭감에 대해 설명한 그림

1. 예시:
2. YML
3. TML
4. 삭감

아래에는 성숙도를 문항 수준에서 보는 또 다른 방법이 나와 있습니다. 원의 색상은 목표 성숙도 또는 이 성숙도까지의 “간격”을 나타냅니다(예: 성숙도가 목표 성숙도 “-1” 이면 원이 주황색임). 체크 표시는 귀사의 성숙도를 나타냅니다.

그림 22. 문항 수준의 성숙도

1. 성숙도
2. 문항
3. 삭감
4. 목표 성숙도(TML)
5. TML보다 1 이상 높음
6. TML보다 1이 낮음
7. TML보다 2 이상 낮음
8. 귀사의 성숙도(YML)
9. TML로 삭감

참고:

모든 문항에 대해 목표 성숙도에 도달하지 않아도 TISAX 평가에 합격할 수 있습니다. 이런 경우에 중요한 문제는 귀사에 관련 위험이 있는지 여부입니다. 성숙도가 목표값보다 낮지만 위험이 없으면 이 성숙도로도 충분할 수 있습니다.

5.2.4.4. 목표(점수 수준)

ISA에서는 “이상적인” 전체 성숙도, 즉 “최고 결과 점수”(또는 “최고 점수”, G6 셀)를 정의합니다.

Information Security Assessment Results

VDA Verband der Automobilindustrie

Result with cutback to target maturity level:	3,00	Maximum score:	3,00

MAXIMUM RESULT SCORE

Details:

No.	Subject	Target maturity level	Result ❶
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

그림 23. 최고 결과 점수(“결과(ISA5)” Excel 시트)

❶ 최고 결과 점수

이론적으로, 이 전체 성숙도는 모든 목표 성숙도(문항 수준)의 평균입니다. 이 평균이 최고 결과 점수 “3.0” 이 됩니다.

하지만 모든 문항이 귀사의 상황에 해당하는 경우에만 “3.0” 입니다. 문항이 귀사의 상황에 해당하지 않으면 곧바로 평균이 바뀌고 최고 결과 점수가 “3.0” 보다 낮아집니다.

더 위에서 본 그림(그림 22, “문항 수준의 성숙도”)을 토대로, 아래에서 최고 결과 점수 평균에 무엇이 입력되었는지 확인할 수 있습니다.

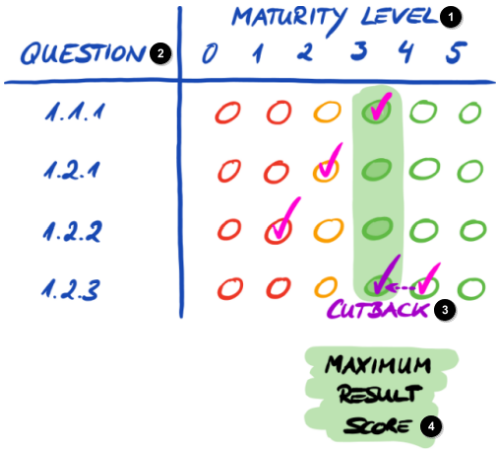


그림 24. 최고 결과 점수(점수 수준)

❶ 성숙도

❷ 문항

❸ 삭감

❹ 최고 결과 점수

5.2.4.5. 귀사의 결과(점수 수준)

귀사의 전체 결과 점수("목표 성숙도로 삭감된 결과” , D6 셀):

- 귀사 정보 보안 관리 시스템의 전체 성숙도를 요약합니다.

- 귀사의 모든 성숙도(문항 수준)의 평균입니다.
- 최고 평균 점수와 같거나 그보다 낮을 수 있습니다.
- 최고 결과 점수에 최대한 가까워야 합니다. 귀사의 결과 점수가 최고 결과 점수보다 더 낮을수록 TISAX 레이블을 받을 가능성이 낮습니다.

Information Security Assessment Results

VDA Verband der Automobilindustrie

Result with cutback to target maturity level:	3,00	Maximum score:	3,00

Details: YOUR RESULT SCORE ❶

No.	Subject	Target maturity level	Result
1.1.1	To what extent are information security policies available?	3	3
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3

그림 25. 귀사의 결과 점수(“결과(ISA5)” Excel 시트)

❶ 귀사의 결과 점수

더 위에서 본 그림(그림 22, “문항 수준의 성숙도”)을 다시 사용하여 아래의 결과 점수 평균에 무엇이 입력되었는지 확인할 수 있습니다.

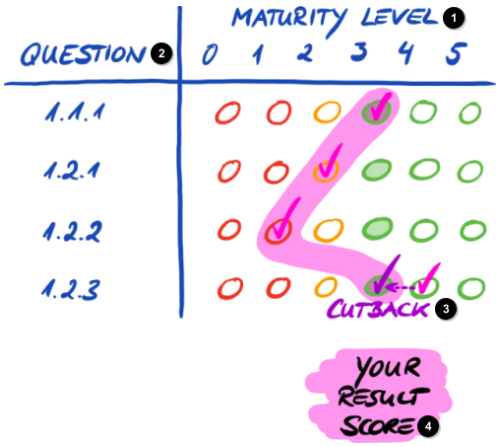


그림 26. 귀사의 결과 점수(점수 수준)

❶ 성숙도

❷ 문항

❸ 삭감

❹ 귀사의 결과 점수

결과 점수를 통해 다음을 알 수 있습니다.

- TISAX 평가를 받을 준비가 되었는지 여부
- TISAX 레이블을 받을 것이라 예상할 수 있는지 여부

귀사의 결과 점수(“목표 성숙도로 삭감된 결과”)가 “3.0”보다 낮으면 하나 이상의 문항에 대한 귀사의 성숙도가 목표 성숙도와 일치하지 않음을 의미합니다. 이 경우, TISAX 평가를 받을 준비가 되려면 정보 보안 관리 시스템을 먼저 개선해야 할 수 있습니다.

참고:

전체 점수의 경우, 귀사의 결과 점수와 최고 결과 점수(“목표 성숙도로 삭감된 결과”) 사이에 허용되는 “간격”의 공식 한도가 있습니다.

귀사의 결과 점수가

- 10% 넘게 더 낮으면 전체 평가 결과가 “사소한 미준수”가 됩니다.
- 30% 넘게 더 낮으면 전체 평가 결과가 “중대한 미준수”가 됩니다.

중요한 참고 사항:

결과 점수("목표 성숙도로 삭감된 결과”)가 “3”이면 합격을 불가능하게 하는 문제가 발견되지 않고 TISAX 평가에 합격할 것이라고 보장되지 않습니다. 감사 제공자가 특정 측면에 대해 귀사와 다르게 생각할 수 있음을 기억하십시오.

5.2.4.6. 준비되셨습니까?

위 분석의 목적은 TISAX 평가를 받을 준비가 되었는지 알아보기 위한 것입니다.

귀사의 결과 점수(“목표 성숙도로 삭감된 결과”)가 “3.0”이거나 이에 가까우면 TISAX 평가를 받을 준비가 확실히 되었음을 의미합니다. 이 경우, “결과” 열(H)의 모든 값이 녹색입니다(주황색 또는 빨간색 없음).

녹색이 아니면 자가 평가 결과의 문제를 해결해야 합니다(섹션 5.2.5, “자가 평가 결과의 문제 해결” 참조).

아래 그림에는 “결과(ISA5)” Excel 시트의 ISA 거미줄 다이어그램이 나와 있습니다. 녹색 선은 장별 목표 성숙도를 표시합니다. 귀사의 성숙도가 이 선에 있거나 그 위에 있으면 TISAX 평가를 받을 준비가 된 것입니다. 성숙도가 이 선 밑에 있으면 TISAX 레이블을 받기에 충분하지 않을 수 있습니다.

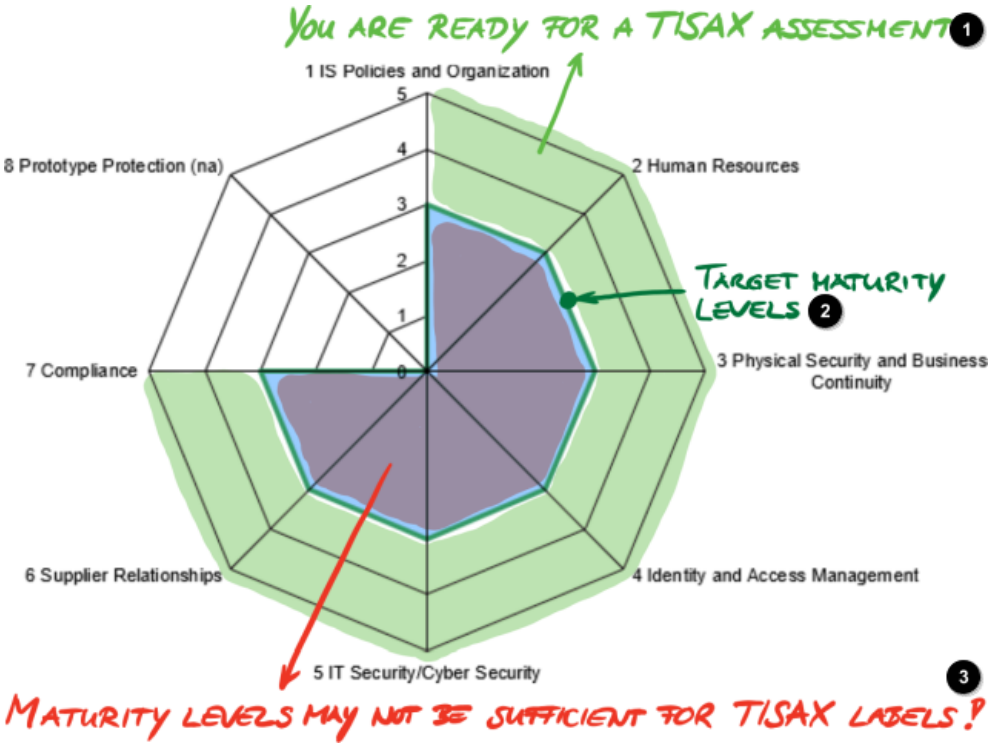


그림 27. 스크린샷: ISA 거미줄 다이어그램(“결과(ISA5)” Excel 시트)에서 목표 성숙도 충족

1. TISAX 평가를 받을 준비가 됨
2. 목표 성숙도
3. 성숙도가 TISAX 레이블을 받기에 충분하지 않을 수 있습니다!

ISA 거미줄을 문항 수준으로 “펼치면” 문항 수준에 대해서도 유사한 녹색/빨간색 보기를 다음과 같이 얻게 됩니다.

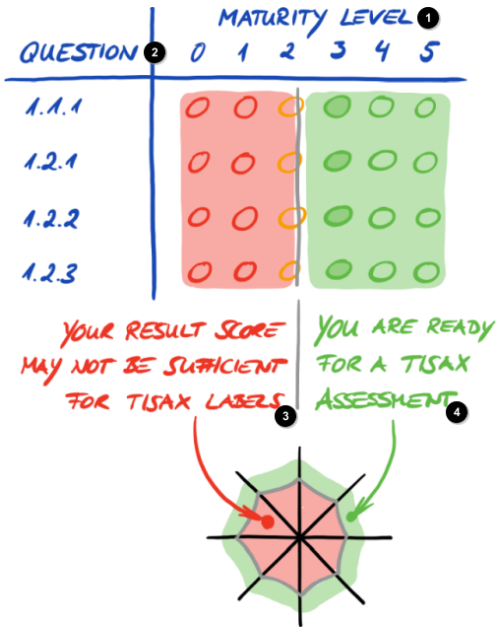


그림 28. ISA 거미줄 다이어그램 “펼치기”

1. 성숙도
2. 문항
3. 결과 점수가 TISAX 레이블을 받기에 충분하지 않을 수 있음
4. TISAX 평가를 받을 준비가 됨

5.2.5. 자가 평가 결과의 문제 해결

자가 평가 결과에 따르면 TISAX 레이블을 받을 준비가 되려면 정보 보안 관리 시스템을 먼저 개선해야 하는 것으로 나타날 수 있습니다.

귀사의 성숙도와 목표 성숙도의 격차 중 일부를 좁히는 방법은 이미 알고 계실 수 있습니다. 나머지 격차를 좁히려면 외부의 조언이 필요할 수 있습니다. 이 경우 TISAX 감사 제공자의 컨설팅 서비스를 요청할 수 있습니다. TISAX에서 이런 컨설팅은 허용되지만, 의무 사항은 아닙니다. 컨설팅하는 감사 제공자는 더 이상 귀사의 TISAX 평가를 실시할 수 없습니다.

중요한 참고 사항:

평가를 받기 전에 자가 평가 결과의 문제를 적절히 해결하지 않으면 여러 회사에 큰 걸림돌이 됩니다. 요구 사항에 따라 귀사의 정보 보안 관리 시스템을 준비하는 데 필요할 수 있는 노력을 과소 평가하지 마십시오. 여러 회사에서는 TISAX 평가를 준비하려면 큰 프로젝트를 공식적으로 계획해야 합니다.

참고:

TISAX 프로세스를 거치는 데 외부의 도움이 필요한 경우, 컨설팅 및 교육 서비스를 제공하는 다양한 회사를 찾을 수 있습니다. 이런 회사는 ENX 협회와 관련이 없습니다.

현재 ENX 협회에서는

- 공식 교육을 직접 제공하거나 제3자를 통해 제공하지 않습니다.
- 제3자 서비스의 질적 수준에 대해 어떤 진술도 하지 않으므로, 주의를 기울일 것을 권고합니다.

참고:

“사전 평가” 또는 “격차(gap) 분석” 같은 항목은 요청하거나 주문하지 않는 것이 좋습니다. 이런 방법으로 평가를 준비하고 싶을 수 있지만, 평가를 곧바로 시작하면 거의 모든 경우에 더 합리적입니다.

사전 평가가 권고되지 않은 이유에 대한 자세한 내용은 다음을 참조하십시오. 섹션 7.7, “부록: “사전 평가”와 “격차 분석”이 권장되지 않는 이유”.

5.3. 감사 제공자 선택

ENX 협회와 계약한 감사 제공자만 TISAX 평가를 실시할 수 있습니다[15]. TISAX 감사 제공자는 이전에 귀사와 컨설팅한 적이 없는 경우에만 귀사의 TISAX 평가를 실시할 수 있습니다.

협회의 모든 TISAX 감사 제공자는 등록된 TISAX 참가자인 회사의 TISAX 평가만 실시할 의무가 있습니다.

중요한 참고 사항:

TISAX 평가 범위를 등록한 후에는 감사 제공자들에게 연락하기 시작해야 합니다. 제공자가 감사를 실시할 수 있으려면 일정한 시간이 필요합니다. 준비를 마친 후에 제공자에게 연락하면 불필요한 지연이 더 발생할 수 있습니다.

참고:

모든 평가 범위는 수명 주기를 거칩니다. 이 단계에는 평가 범위의 상태가 “승인됨” 또는 “등록됨”이어야 합니다.

평가 범위의 상태에 대한 자세한 내용은 다음을 참조하십시오. 섹션 7.5.5, “Assessment scope status “Awaiting your payment” (평가 범위 상태 “지불 대기 중”)”.

5.3.1. 연락처 정보

TISAX 평가 범위를 등록한 후에는 모든 TISAX 감사 제공자에게 연락하고 오퍼를 요청할 수 있습니다. 제공자의 연락처 정보는 수신하신 등록 확인 이메일에 있습니다[16] (섹션 4.5.8, “확인 이메일” 참조).

참고:

등록된 후에만 TISAX 감사 제공자의 오퍼를 요청하십시오. 감사 제공자는 기존 등록이 있는지 여부를 확인합니다. 등록되어 있지 않으면 제공자가 요청을 거부해야 합니다.

그렇기 때문에 감사 제공자의 연락처 정보가 등록 확인 이메일에만 있고 ENX 협회의 공개 웹 사이트에는 없습니다.

5.3.2. 감사 가능 지역

현재 감사 제공자 연락처의 상당수가 독일에 있지만, ENX 협회의 모든 감사 제공자가 일반적으로 전세계에서 TISAX 평가를 실시할 수 있음을 아는 것이 중요합니다. 대부분은 여러 국가에 자체적인 직원을 두고 있기도 합니다.

ENX 협회의 웹 사이트에는 국가를 선택하면 현지에 영업 인력 및/또는 감사관을 보유하고 있는 감사 제공자를 확인할 수 있는 페이지가 있습니다(enx.com/en-US/TISAX/xap/).

5.3.3. 오퍼 요청

TISAX 감사 제공자가 예상되는 평가 노력을 정확하게 계산할 수 있도록 하기 위해, 항상 “TISAX 범위 발췌 자료”를 요청에 포함시켜야 합니다.

그림 29. 범위 발췌 자료 썸네일(첫 페이지)

자세한 내용은 다음을 참조하십시오. 섹션 4.5.8, “확인 이메일” .

참고:

중립성은 TISAX 감사 제공자의 핵심적인 특징입니다. 제공자는 이해 관계 상충이 존재하지 않도록 보장합니다. 제공자에게 연락할 때 이해 관계의 상충에 대해 고려하는 것이 좋습니다. 귀사가 감사 제공자와 어떻게든 관련이 있는 경우 해당 제공자에게 평가를 받을 수 없습니다.

5.3.4. 오퍼 평가

모든 TISAX 감사 제공자 중에서 자유롭게 선택할 수 있습니다. 모든 제공자는 같은 계약에 구속을 받습니다. 감사 제공자는 모두 같은 기준에 따라 같은 감사 방법으로 평가를 실시합니다. 감사 결과는 어떤 감사 제공자를 선택하든 차이가 없을 것입니다. 평가 결과는 모든 TISAX 참가자가 받아들입니다.

가격, 평판, 호감도 같은 자명한 요인 외에, 오퍼의 다음과 같은 측면을 고려할 수 있습니다.

- 가능한 시기:
  평가 프로세스를 얼마나 빨리 시작할 수 있습니까? TISAX 평가를 받는 것이 귀사에 긴급한 사항인 경우 중요할 수 있습니다.
- 현장 감사를 위한 출장 관련 비용:
  귀사와 같은 국가에 사무소가 있는 감사 제공자의 출장 관련 비용은 더 낮을 수 있습니다.
- 언어:
  귀하와 귀사의 다른 모든 면접 조사 대상자가 감사관과 모국어로 소통할 수 있습니까?
- 오퍼의 범위:
  어떤 평가가 포함됩니까?
  평가에 대한 자세한 내용은 다음을 참조하십시오. 섹션 5.4.3, “TISAX 평가 유형” .
  오퍼에는 일반적으로 첫 평가와 시정 조치 계획 평가가 포함됩니다. 후속 평가에 필요할 수 있는 노력의 양은 예측하기 힘들기 때문에 후속 평가는 일반적으로 다른 평가가 완료된 후에 제안됩니다.

궁극적으로는 신뢰가 가장 중요합니다. 감사 제공자는 귀사에 대해 많이 알게 될 것이므로, 감사 제공자와 신뢰 관계를 형성해야 합니다.

참고:

“사전 평가” 또는 “격차(gap) 분석” 같은 항목은 요청하거나 주문하지 않는 것이 좋습니다. 이런 방법으로 평가를 준비하고 싶을 수 있지만, 평가를 곧바로 시작하면 거의 모든 경우에 더 합리적입니다.

사전 평가가 권고되지 않은 이유에 대한 자세한 내용은 다음을 참조하십시오. 섹션 7.7, “부록: “사전 평가”와 “격차 분석”이 권장되지 않는 이유” .

참고:

당연히 감사 제공자가 평가에 대해 청구할 금액을 알려드리고 싶지만, 이 정보를 제공하기는 불가능하다는 점을 양해해 주시기 바랍니다. 비용을 좌우하는 요인이 너무 많기 때문입니다. 게다가 감사 제공자는 청구할 금액을 자유롭게 계산할 수 있습니다.

하지만 감사 제공자가 대금을 부과하는 기준이 될 노동량을 대략적으로 추정한 수치를 알려드릴 수는 있습니다. 위치가 한 개인 평균적인 소기업은 평가 수준 2에 해당하는 평가에 대해 3.5~4인일(man-day) 비용을 지불하고 평가 수준 3에 해당하는 평가에 대해 5-6인일 비용을 지불해야 한다고 귀사에 기대할 수 있습니다.

참고:

> 모든 평가는 수명 주기를 거칩니다.
>
> 평가의 상태에 대한 자세한 내용은 다음을 참조하십시오. 섹션 7.6, “부록: Assessment status(🇰🇷 평가 상태)” .

TISAX 감사 제공자 중 하나를 선택한 후에는 마침내 TISAX 평가 프로세스를 시작할 수 있습니다.

5.4. TISAX 평가 프로세스

5.4.1. 개요

TISAX 평가 프로세스는 몇 가지 유형의 평가로 구성됩니다. 대부분의 경우 평가를 두 번 이상 받게 됩니다.

평가 프로세스를 다음과 같은 서로 엮인 단계의 순서로 인식해야 합니다.

- 정보 보안 관리 시스템의 상태가 최상이 되도록 준비합니다.
- 감사 제공자가 귀사의 정보 보안 관리 시스템이 일련의 정해진 요구 사항을 충족하는지 확인합니다. 제공자가 격차를 발견할 수 있습니다.
- 그러면 귀사에서 격차를 정해진 기간 안에 해소해야 합니다.
- 그런 다음 감사 제공자가 격차가 해소되었는지 다시 확인합니다.

모든 격차가 해소될 때까지 이 두 단계를 번갈아 수행합니다.

평가 프로세스의 각 하위 단계를 귀사에서 시작한다는 사실을 이해하는 것이 중요합니다. 전체 평가 프로세스가 귀사의 통제 하에 있습니다. 그리고 물론 귀사에서 언제든지 원할 때 평가 프로세스를 중지하고 종료하기로 결정할 수 있습니다.[17]

TISAX 프로세스의 구조는 대체로 다음과 같습니다.

- 킥오프 회의
  귀사와 감사 제공자가 평가 프로세스의 세부 사항을 계획합니다.
- 평가 단계 1
  감사 제공자가 귀사의 자가 평가를 확인합니다.
- 평가 단계 2
  감사 제공자가 평가를 실시합니다.

5.4.2. 킥오프 회의

TISAX 평가 프로세스는 킥오프 회의로 시작됩니다. 이 회의에서 평가 프로세스의 세부 사항을 계획합니다. 킥오프 회의는 일반적으로 전화 회의로 진행됩니다. 감사 제공자가 회의를 이끕니다.

안건에 포함되는 주제는 다음과 같습니다.

- 회의 참가자는 누구인가?
- 어느 회사가 평가를 받는가?
- TISAX 평가 프로세스는 어떻게 진행되는가?
- 평가 범위는 무엇이고, 평가 범위가 적합한가?
- 이해 관계의 상충은 없는가?
- 좋은 자가 평가는 어떤 모습인가?

- 누가 무엇을 책임지는가?
- 서로 어떻게 소통하는가?
- 평가가 언제 진행되는가(그 외 다른 시간 계획)?
- 평가에 누가 참가해야 하는가?
- 불만 사항이 있으면 누구에게 연락할 수 있는가?

킥오프 회의가 끝난 후 일반적으로 1~3개월이 지나면 자가 평가가 실시됩니다. 하지만 6개월이 지나는 경우도 드물지 않습니다. 기간은 귀사의 준비 상태에 따라 다릅니다. TISAX는 이 기간을 제한하지 않습니다. 필요한 시간만큼 자가 평가를 준비하고 평가를 준비할 수 있습니다.

5.4.3. TISAX 평가 유형

TISAX 평가 프로세스는 다음과 같은 세 가지 유형의 TISAX 평가로 구성됩니다.

- 첫 평가(Initial assessment)
- 시정 조치 계획 평가(Corrective action plan assessment)
- 후속 평가(Follow-up assessment) [18]

첫 평가는 항상 실시됩니다. 나머지 두 가지 TISAX 평가도 실시될 수 있고, 몇 번 실시될 수 있습니다. 이런 평가는 다음과 같이 실시됩니다.

- 모든 격차가 해소될 때까지
- 또는 귀사에서 TISAX 평가 프로세스를 종료할 때까지
- 또는 첫 평가 종료 회의가 끝난 후 최대 기간인 9개월에 도달할 때까지(이 시점에 첫 평가를 한 번 더 실시해야 함)

이어지는 내용에서는 모든 TISAX 평가에 대해 설명합니다.

참고:

모든 평가는 수명 주기를 거칩니다.

평가의 상태에 대한 자세한 내용은 다음을 참조하십시오. 섹션 7.6, “부록: Assessment status(평가 상태)”.

5.4.4. TISAX 평가 요소

TISAX 평가는 각각 다음 요소로 구성됩니다.

- 공식 시작 회의[19][20]
  - 이 회의의 목표는 조직 차원의 주제를 모두 다루는 것입니다.
  - 실제 대면 회의가 아니어도 됩니다.
  - 주제를 모두 한 번에 다루거나 여러 번에 걸쳐 다룰 수 있습니다.
  - 이 회의는 조직의 평가 전 주제를 모두 담는 “논리적 컨테이너”입니다.
- 평가 절차
  - 감사 제공자가 모든 요구 사항을 확인합니다.
  - 평가 방법이 각 평가 수준에 따라 선택됩니다.

- 공식 종료 회의[21]
  - 이 회의는 TISAX 평가를 끝맺습니다.
  - 감사 제공자가 발견한 문제를 발표합니다.
  - 감사 제공자가 평가 결과를 발표합니다.
  - 실제 대면 회의가 아니어도 됩니다.
  - 이 회의는 조직의 모든 평가 후 주제를 담는 “논리적 컨테이너”입니다.

“종료 회의” 후에 감사 제공자가 업데이트된 “TISAX 평가 보고서” 초안을 작성하고 귀사로 보냅니다. 감사 제공자가 오해한 것이 있다고 생각되면 이의를 제기할 수 있습니다.[22] 그런 다음 감사 제공자가 최종 “TISAX 평가 보고서”를 발행합니다.

이런 요소에 대해서는 이어지는 섹션에서 모두 설명합니다.

5.4.5. 준수에 대한 설명

TISAX 프로세스에 대해 계속 설명하기 전에, 이어지는 섹션을 이해하는 데 필수적인 핵심 개념에 대해 설명하려고 합니다.

TISAX 평가의 목적은 귀사의 정보 보안 관리 시스템이 일련의 정해진 요구 사항을 충족하는지 여부를 결정하는 것입니다. 감사 제공자는 귀사의 정보 보안 관리 시스템이 요구 사항을 “준수”(“conforms”)하는지 여부를 확인합니다.

1 단계: 해당하는 각 요구 사항의 준수 여부를 개별적으로 확인합니다.

귀사의 접근방식이 모든 요구 사항을 “준수”하는 경우, 평가에 합격하고 귀사의 평가 목표에 해당하는 TISAX 레이블을 받습니다.

완전하거나 이상적인 준수에 미치지 못하는 모든 것을 발견된 문제(finding)라고 합니다. TISAX에서는 발견된 문제를 다음과 같은 네 가지 유형으로 나눕니다.

번호	유형	정의	대응	예시
1.	중대한 미준수(Major non-conformity)	중대한 미준수: ▪ 정보 보안에 상당하고 즉각적인 위험을 제기함 ▪ 또는 정보 보안 관리 시스템의 전체적인 효과에 관한 의구심이 들게 함	귀사에서 해야 하는 일: ▪ 적절한 보완 조치로 중대한 미준수 사항 즉시 해결 ▪ 지나친 지연 없이 시정 조치 이행	▪ 시스템 차원의 미준수 ▪ 비밀 정보의 보안에 중요한 위험을 제기하는 이행 문제 ▪ 적절한 시정 조치로 해결되지 않는 이행 문제
2.	사소한 미준수(Minor non-conformity)	사소한 미준수: ▪ 정보 보안에 상당하고 즉각적인 위험을 제기하지 않음 ▪ 그리고 정보 보안 관리 시스템의 전체적인 효과에 관한 의구심이 들게 하지 않음	귀사에서 해야 하는 일: ▪ 지나친 지연 없이 시정 조치 이행	▪ 단발적이거나 산발적인 실수 ▪ 요구 사항 또는 귀사 정책의 미준수 또는 이행 문제

번호	유형	정의	대응	예시
3.	관찰 사항(Observation)	관찰 사항은 귀사의 정보 보안에 즉각적인 위험을 제기하지 않지만 향후에 제기할 수 있는 요구 사항 또는 귀사 자체 정책의 미준수입니다.	귀사에서 해야 하는 일: ▪ 가능한 위험의 주의 깊은 조사, 모니터링 및 평가 ▪ 관찰 사항을 처리할 방법 결정	해당 없음
4.	개선 여지(Room for improvement)	앞에서 언급한 유형에 해당하지 않고 귀사의 정보 보안에 위험을 제기하지 않지만 분명한 개선의 여지가 있는 일탈.	이런 유형의 문제를 해결할지 여부 또는 해결할 방법을 직접 결정할 수 있습니다.	해당 없음

표 11. 네 가지 유형의 발견된 문제

2 단계: 이전의 “요구 사항별” 단계의 모든 결과가 전체 평가 결과에 병합됩니다.

가능한 전체 평가 결과는 다음과 같습니다.

a. 준수(Conform)
전체 평가 결과가 “준수” 입니다. 모든 요구 사항이 충족된 상태입니다.

b. 사소한 미준수(Minor non-conform)
요구 사항의 “사소한 미준수” 가 하나 이상 있는 경우 전체적인 평가 결과가 “사소한 미준수” 입니다.

c. 중대한 미준수(Major non-conform)
요구 사항의 “중대한 미준수” 가 하나 이상 있는 경우 전체적인 평가 결과가 “중대한 미준수” 입니다.
(승인된 시정 조치 계획이 없으면 모든 미준수 사항이 전체적인 평가 결과가 “중대한 미준수” 가 되는 원인이 됩니다.)

전체 평가 결과가

- “사소한 미준수” 인 경우 모든 미준수 사항이 해결될 때까지 임시 TISAX 레이블을 받을 수 있습니다.
- “중대한 미준수” 인 경우 문제를 각각 해결한 후에만 TISAX 레이블을 받을 수 있습니다.
  감사 제공자가 승인한 적절한 보완 조치와 시정 조치를 통해 전체 평가 결과를 “중대한 미준수” 에서 “사소한 미준수” 로 변경하여 임시 TISAX 레이블을 받을 수 있습니다.

전체 TISAX 평가 프로세스를 진행하는 동안 전체 평가 결과가 개선될 것임을 이해하는 것이 중요합니다.

다음과 같은 아주 간단한 예에 대해 생각해 보십시오. 첫 평가 후에 전체 평가 결과가 “중대한 미준수” 일 수 있습니다. 그 후 해당하는 위험을 완화합니다. 그러자 전체 평가 결과가 “중대한 미준수” 에서 “사소한 미준수” 로 변경됩니다. 그리고 위험을 제거한 후 최종 전체 평가 결과가 “준수” 가 됩니다.

이에 대해서는 아래에서 훨씬 더 자세히 설명할 것입니다. TISAX 레이블에 대해서는 더 아래에 있는 다음 섹션에서 자세히 확인할 수 있습니다. 섹션 5.4.14, “TISAX 레이블” .

5.4.6. 귀사의 TISAX 평가 프로세스 준비

감사 제공자는 귀사의 자가 평가를 토대로 평가를 준비하게 됩니다. 그러므로 귀사의 자가 평가 결과를 감사 제공자에게 미리 제공해야 함을 고려해 주십시오. 정확한 이행 마감 시한은 킥오프 회의에서 합의합니다.

감사 제공자가 준비를 잘 하면 평가에 필요한 시간이 단축됩니다. 자가 평가 외에, 감사 제공자는 평가 전에 관련 문서도 요청합니다. 자가 평가에서 참조한 문서와 감사 제공자가 관련이 있다고 간주하는 다른 문서를 요청할 수

있습니다.

이 정보를 토대로 감사 제공자가 평가 절차를 계획합니다.

5.4.7. 첫 평가

이 평가는 첫 TISAX 평가이며, TISAX 평가 프로세스의 공식적인 시작에 해당합니다.

중요한 참고 사항:

첫 평가는 두 중요한 기간의 시작에 해당합니다.

1. TISAX 레이블의 최대 유효 기간은 3년입니다.
2. 미준수 사항은 9개월 이내에 해결해야 합니다. 이 기간 내에 모든 미준수 사항을 해결하지 않으면 TISAX 레이블을 받지 못합니다. 하지만 이 마감 시한을 넘길 경우 곧바로 새로운 첫 평가로 계속 진행할 수 있습니다.

두 기간 모두 첫 평가의 종료 회의 날짜에 시작됩니다.

참고:

위에서 설명한 두 기간 외에 다른 시간 제약은 없습니다. 예를 들어 온라인 등록 프로세스를 완료하거나 감사 제공자에게 연락하거나 심지어는 킥오프 회의를 진행해도 마감 시한이 유발되지 않습니다. 첫 평가를 시작할지는 귀사에서 직접 결정합니다.

5.4.7.1. 첫 공식 시작 회의

모든 TISAX 평가와 마찬가지로, 첫 평가는 공식 시작 회의로 시작됩니다. 공식 시작 회의는 일반적으로 전화 회의나 웹 회의를 통해 진행됩니다. 다른 감사에서 경험을 어느 정도 얻었을 수 있는 작은 회사의 회의 시간은 길지 않습니다.

이 회의의 목적은 다음과 같습니다.

- 평가 전제 조건 확인
- 평가 프로젝트 리더와 평가 팀 소개
- 평가 계획

5.4.7.2. 평가 절차

준비된 계획에 따라 감사 제공자가 첫 평가를 실시합니다. 첫 평가가 구체적으로 어떻게 실시될 것인지는 평가 목표에 따라 다릅니다. 평가는 주로 전화 회의, 현장 면접 조사, 그리고 다양한 깊이의 현장 점검으로 구성됩니다[23].

감사 제공자가 첫 평가 도중에 발견한 문제를 모두 발표합니다.

5.4.7.3. 종료 회의

종료 회의에서 감사 제공자는 발견된 문제를 모두 다시 요약합니다.

5.4.7.4. TISAX 평가 보고서

종료 회의 후에 감사 제공자가 “TISAX 평가 보고서” 초안을 작성하고 귀사로 보냅니다. 감사 제공자가 오해한 것이 있다고 생각되면 이의를 제기할 수 있습니다.[24] 그런 다음 감사 제공자가 “TISAX 평가 보고서”를

발행합니다.

이 단계에 최신 전체 평가 결과는 다음 중 하나가 됩니다.

- 준수 또는
- 중대한 미준수
  해결되지 않은 (사소한) 미준수 사항이 있으면 항상 전체 평가 결과가 “중대한 미준수”가 됩니다. 미준수 사항을 해결할 조치를 이행할 작업을 정의한 후에만 전체 평가 결과가 “사소한 미준수”가 될 수 있습니다. 이렇게 할 수 있는 방법에 대한 자세한 내용은 다음을 참조하십시오. 섹션 5.4.9.4, “임시 TISAX 레이블”.

첫 평가 시점에 전체 평가 결과가 “준수”인 경우, 나머지 평가 섹션을 건너뛰고 결과 교환으로 계속 진행할 수 있습니다.

전체 평가 결과가 “중대한 미준수”인 경우, 다음에 할 일은 발견된 문제를 해결하는 방법과 감사 제공자가 발견한 격차를 해소하는 방법에 대한 계획을 세우는 것입니다. 이 계획을 공식적으로 “시정 조치 계획”(“corrective action plan”)이라고 합니다.

참고:

평가 시작 전에 미준수로 이어질 상황에 대해 알게 되고 평가 전에 이 상황을 해결할 수 없는 경우, 시정 조치(이행 날짜 포함)를 미리 계획하고 평가 도중에 감사 제공자에게 제시할 수 있습니다. 그러면 이론적으로는 전체 평가 결과가 “사소한 미준수”가 될 수 있습니다. 하지만 이런 상황은 드물 것입니다.

5.4.8. 시정 조치 계획 준비

“시정 조치 계획”(“corrective action plan”)은 첫 평가에서 발견된 문제를 어떻게 해결할 계획인지 정의합니다. 감사 제공자가 “시정 조치 계획”의 적절성을 평가할 것입니다(다음 섹션 참조).

“시정 조치 계획”을 세우려면 다음과 같은 요구 사항을 고려해야 합니다.

- 발견된 문제
  - 시정 조치가 해결하는 발견된 문제를 명시해야 합니다.
- 근본 원인
  - 발견된 문제의 근본 원인을 확인하고 명시해야 합니다.
- 시정 조치
  - 각각의 미준수 사항에 대해 미준수 사항을 해결하는 조치를 이행할 “시정 조치”를 하나 이상 정의해야 합니다.
- 이행 날짜
  - 각 시정 조치의 이행 날짜를 정의해야 합니다.
  - 이행 기간은 조치를 철저히 이행할 충분한 시간을 제공해야 합니다.
- 보완 조치
  - 중요한 위험을 제기할 수 있는 모든 미준수 사항에 대해, 시정 조치가 이행될 때까지 미준수 사항을 해결하는 보완 조치를 정의해야 합니다.
- 이행 기간
  - 이행하는 데 3개월보다 오래 걸리는 모든 시정 조치에 대해 긴 이행 기간을 해명해야 합니다.
  - 6개월보다 오래 걸리는 모든 시정 조치에 대해서는 더 빨리 이행할 수 없음을 입증하는 증거를 추가로 제시해야 합니다.

- 시정 조치의 이행 기간이 9개월보다 길면 안 됩니다.

시정 조치 계획이 완성되면 “시정 조치 계획 평가”를 요청할 수 있습니다.

중요한 참고 사항:

이행을 최대한 빨리 시작하는 것이 좋습니다. “시정 조치 계획 평가”의 결과를 기다릴 필요가 없습니다.
“시정 조치 계획 평가”는 일반적으로 시정 조치 계획을 감사 제공자에게 제출한 후에 행해집니다.

참고:

TISAX에는 내용에 관한 요구 사항만 있고 시정 조치 계획의 형식에 관한 요구 사항은 없습니다. 감사 제공자는 대부분 시정 조치 계획 템플릿을 제공합니다.

5.4.9. 시정 조치 계획 평가

“시정 조치 계획 평가”의 목적은 귀사의 “시정 조치 계획”(위 참조)이 TISAX 요구 사항을 충족하는지 확인하는 것입니다.

“시정 조치 계획”을 감사 제공자에게 제출합니다. 감사 제공자가 계획을 요구 사항에 따라 평가합니다(아래 참조). 계획이 요구 사항을 충족하는 경우, 감사 제공자가 업데이트된 “TISAX 평가 보고서”를 발행합니다.

이 평가는 일반적으로 오래 걸리지 않습니다. 대부분의 경우 이 평가는 전화 회의 또는 웹 회의로 진행됩니다. 때로는 이메일만으로 진행되기도 합니다.

5.4.9.1. 시정 조치 계획 평가의 이유

“시정 조치 계획 평가”의 이유는 다음과 같습니다.

- 다음 후에 미준수 사항이 남아 있음
  - 첫 평가
  - 후속 평가
  - 범위 확장 평가
- 이미 평가되었지만 요구 사항을 충족하지 않은 “시정 조치 계획”
- 시정 조치 계획 이행 기간을 계산하는 근거가 된 영향 요인이 변경됨

5.4.9.2. 첫 평가와 조합

“시정 조치 계획 평가”는 독립적인 이벤트가 아닐 수 있습니다. 첫 평가 종료 회의 도중에 “시정 조치 계획”을 미리 제시할 수 있습니다. 그러면 감사 제공자가 “시정 조치 계획 평가”를 곧바로 실시할 수 있습니다.

“시정 조치 계획 평가”를 첫 평가와 합칠 경우, “시정 조치 계획”이 요구 사항을 충족하면 감사 제공자와 “첫 평가 보고서”가 필요 없다고 합의할 수 있습니다. 그 대신 감사 제공자는 “시정 조치 계획 평가 보고서”만 작성합니다. 이 보고서를 사용하여 임시 TISAX 레이블을 직접 받을 수 있습니다.

5.4.9.3. 시정 조치 계획 요구 사항

감사 제공자는 다음 요구 사항을 기준으로 “시정 조치 계획”을 평가합니다.

- 조치가 적절함

- 감사 제공자는 시정 조치로 미준수의 근본 원인이 해결될지 여부를 기준으로 시정 조치의 적절성을 평가합니다.
- 중요 위험이 적절한 보완 조치로 완화됨[25]
- 이행 기간이 적절함
  - 이행 기간은 첫 평가가 끝난 날에 시작됩니다.
- 다음보다 더 긴 이행 기간이 없음:
  - 추가 해명이 없는 경우 3개월
  - 추가 해명 및 증거가 없는 경우 6개월
  - 9개월

5.4.9.4. 임시 TISAX 레이블

전체 평가 결과가 “사소한 미준수”인 경우, 임시 TISAX 레이블을 받습니다.

임시 TISAX 레이블은 나중에 귀사에서 영구 TISAX 레이블을 받는다는 조건 하에 파트너가 일반적으로 받아들인다는 이점이 있습니다. 이 레이블은 정보 보안 관리 시스템의 효과를 파트너에게 긴급하게 입증해야 하는 경우에 유용할 수 있습니다.

임시 TISAX 레이블을 받기 위한 전제 조건은 전체 평가 결과가 “사소한 미준수”인 시정 조치 계획 평가 보고서입니다.

임시 TISAX 레이블은 영구 TISAX 레이블과 동등합니다. 유일한 차이점은 임시 TISAX 레이블의 유효 기간이 더 짧다는 것뿐입니다.

임시 TISAX 레이블은 첫 평가 종료 회의 후 9개월까지 유효할 수 있습니다. 임시 TISAX 레이블의 유효 기간은 시정 조치의 가장 긴 이행 기간에 따라 결정됩니다.

예시:

- 미준수 사항이 하나만 있습니다. 정책 검토를 수행해야 합니다. 관련 이행 기간은 2개월입니다.
  그러면 임시 TISAX 레이블이 2개월 동안 유효합니다.
- 위에서 언급한 정책 검토 미준수 사항이 있습니다. 그 외에 새 외벽을 건립하는 시정 조치를 취해야 하는 미준수 사항이 있습니다. 지방 지자체의 필수 승인을 받는데 걸리는 시간 때문에 관련 이행 기간은 8개월입니다.
  그러면 임시 TISAX 레이블이 8개월 동안 유효합니다.

이행 기간에 관한 요구 사항에 대한 자세한 내용은 다음을 참조하십시오. 섹션 5.4.9.3, “시정 조치 계획 요구 사항”

참고:

“시정 조치 계획 평가”는 선택 사항입니다.

다음과 같은 경우 후속 평가로 곧바로 진행할 수 있습니다.

- 임시 TISAX 레이블이 필요없고
- 계획을 감사 제공자에게 승인받지 않아도 시정 조치를 이행하는 데 자신이 있음

모든 시정 조치를 완료한 후에는 “후속 평가”를 요청해야 합니다.

5.4.10. 후속 평가

“후속 평가”의 목적은 이전에 확인된 미준수 사항이 모두 해결되었는지 평가하는 것입니다. 일반적으로 모든 미준수 사항이 해결되었다고 확신하면 후속 평가를 요청합니다.

하지만 후속 평가를 필요한 만큼 많이 받을 수 있습니다. 후속 평가 도중에 감사 제공자가 기존 또는 새로운 미준수 사항이 아직도 있음을 입증할 경우, 간단히 시정 조치 계획을 업데이트하고 평가 프로세스의 이 부분을 다시 시작하기만 하면 됩니다.

이 평가는 직접 대면 회의나 전화 회의 또는 웹 회의로 진행할 수 있습니다.

5.4.10.1. 시기

감사 제공자는 첫 평가를 마친 후 최대 9개월 이내에 후속 평가를 실시할 수 있습니다[26].

5.4.10.2. 전제 조건

임시 TISAX 레이블이 필요하지 않으면 후속 평가를 곧바로 요청할 수 있습니다. 후속 평가 전에 “시정 조치 계획 평가”를 받지 않아도 됩니다.

5.4.10.3. 임시 TISAX 레이블 만료

임시 TISAX 레이블이 필요한 경우, 영구 TISAX 레이블을 받기 전에 공백이 발생하지 않도록 하고 싶을 수 있습니다. 그러므로 후속 평가를 가능한 가장 늦은 날짜보다 훨씬 더 빨리 요청하는 것이 좋습니다[27]. 그 이유는 후속 평가에서 확인된 사소한 문제를 해결할 수 있는 여유 시간을 충분히 확보해야 하기 때문입니다.

5.4.11. TISAX 평가 프로세스 다이어그램

이제 앞의 여러 섹션을 다음과 같은 프로세스 다이어그램과 같이 요약할 수 있습니다.

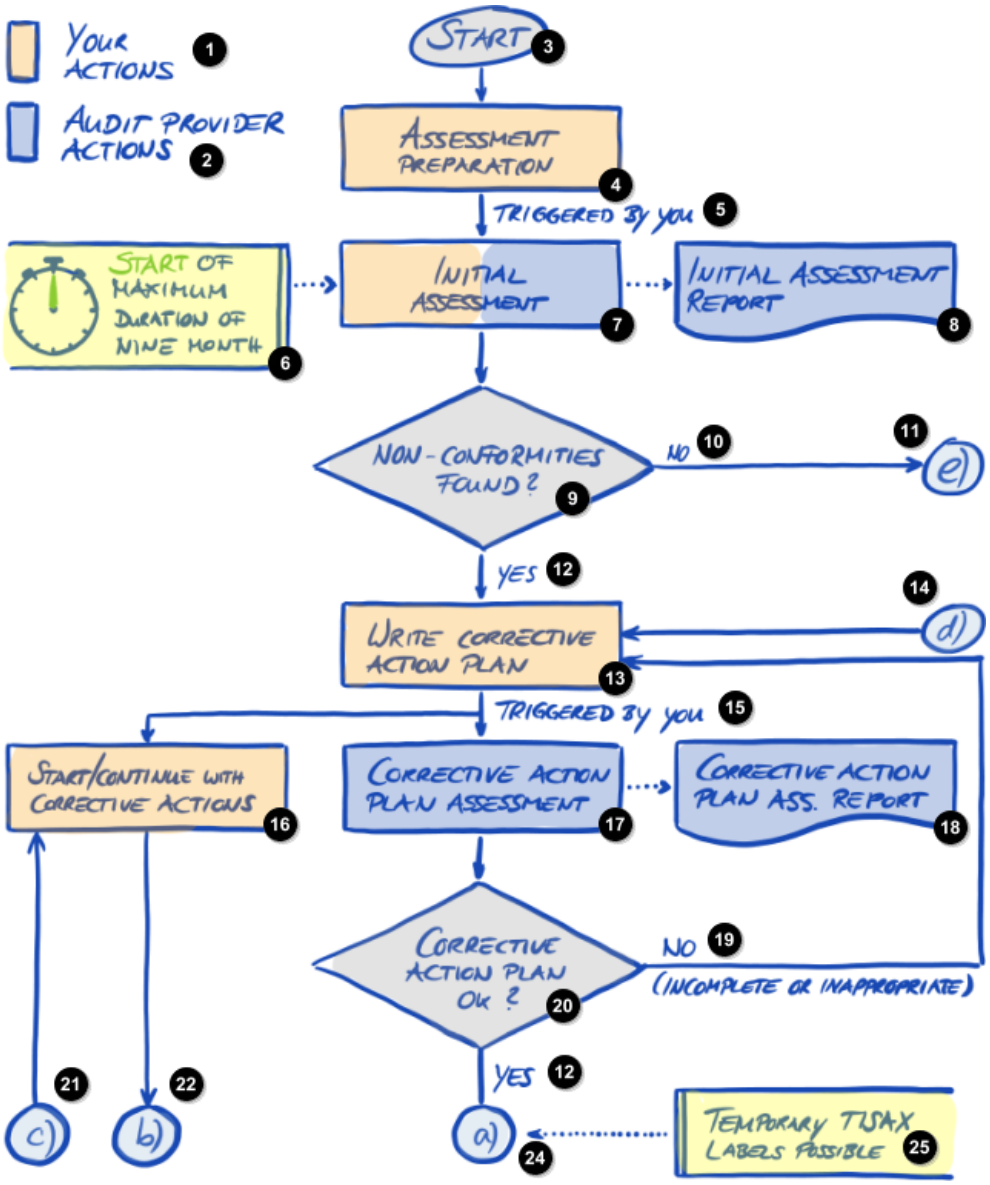


그림 30. TISAX 평가 프로세스 다이어그램(1/2부)

1. 귀사의 작업
2. 감사 제공자의 작업
3. 시작
4. 평가 준비
5. 귀사에 의해 유발됨
6. 최대 기간인 9개월 시작
7. 첫 평가
8. 첫 평가 보고서
9. 미준수 발견?

10 아니요

11 e)

12 예

13 시정 조치 계획 작성

14 d)

15 귀사에 의해 유발됨

16 시정 조치 시작/계속

17 시정 조치 계획 평가

18 시정 조치 계획 평가 보고서

19 아니요(미완료 또는 부적절)

20 시정 조치 계획 OK?

21 c)

22 b)

24 a)

25 임시 TISAX 레이블 가능

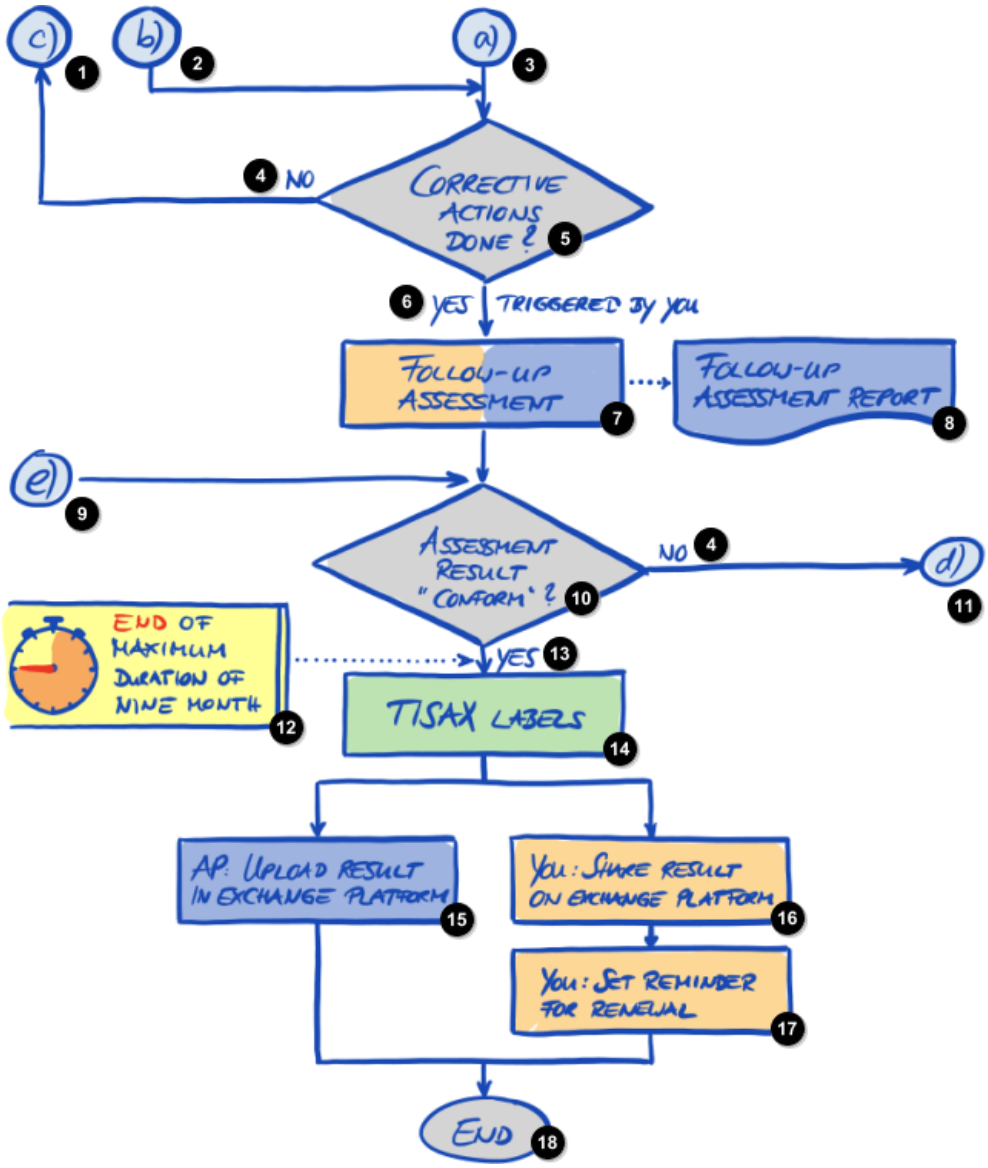


그림 31. TISAX 평가 프로세스 다이어그램(2/2부)

1. c)
2. b)
3. a)
4. 아니요
5. 시정 조치 완료?
6. 예, 귀사에 의해 유발됨
7. 후속 평가
8. 후속 평가 보고서
9. e)

10. 평가 결과 “준수”?
11. d)
12. 최대 기간인 9개월 끝
13. 예
14. TISAX 레이블
15. 감사 제공자: 교환 플랫폼에서 결과 업로드
16. 귀사: 교환 플랫폼에서 결과 공유
17. 귀사: 갱신에 대한 미리 알림 설정
18. 끝

5.4.12. Assessment ID (🇰🇷 평가 ID)

평가 범위의 각 TISAX 평가는 “평가 ID”로 식별됩니다. 이 ID는 평가 결과와 해당하는 TISAX 평가 보고서를 지칭합니다.

평가 ID의 형식은 다음과 같습니다.

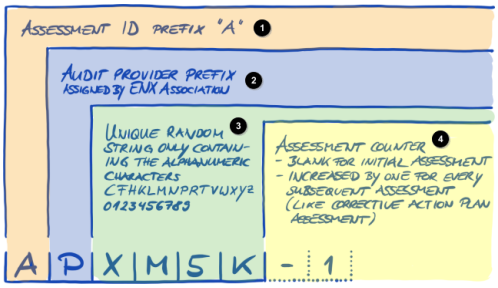


그림 32. 평가 ID의 형식

1. 평가 ID 접두사 “A”
2. ENX 협회에서 지정한 감사 제공자 접두사
3. 영숫자만 포함하는 고유 임의 문자열:
   CFHKLMNPRTVWXYZ
   0123456789
4. 평가 카운터
   - 첫 평가인 경우 비워 둠
   - 이후의 모든 평가(시정 조치 계획 평가 등)마다 일(1)씩 증가

평가 ID는 일반적으로 감사 제공자가 귀사와 소통할 때 사용됩니다.

5.4.13. TISAX 평가 보고서

“TISAX 평가 보고서”(🇬🇧 “TISAX assessment report”):

- 각각의 TISAX 평가 후에 (업데이트되고) 발행됩니다.

- 감사 제공자가 발견한 문제를 문서화합니다.
- 전체 평가 결과(준수, 사소한 미준수, 중대한 미준수)를 포함합니다.
- TISAX 평가와 관련된 다른 정보(평가 목표, 범위, 관련된 사람 및 위치 등)를 모두 포함합니다.

“TISAX 평가 보고서”의 유형은 (평가 유형에 따라) 다음과 같습니다.

- 첫 평가 보고서(Initial assessment report)
- 시정 조치 계획 평가 보고서(Corrective action plan assessment report)
- 후속 평가 보고서(Follow-up assessment report) [28]

“TISAX 평가 보고서”의 구조는 항상 같습니다[29]. 감사 제공자는 간단히 각 유형의 평가를 실시한 후에 보고서를 확장합니다. 따라서 TISAX 평가 보고서의 마지막 버전만 다루면 됩니다. 이 버전에 항상 이전 버전이 내용이 포함되어 있기 때문입니다.

최종적으로 파트너와 공유하는 것은 “TISAX 평가 보고서”의 첫 섹션 몇 개입니다.

TISAX 평가 보고서에서 파트너 또는 다른 참가자와 공유할 부분을 전적으로 직접 결정할 수 있다는 점은 TISAX의 핵심적인 특징 중 하나입니다. TISAX 평가 보고서는 이런 선택적인 공유가 가능한 구조로 되어 있습니다. 각 섹션은 세부 수준을 확장합니다.

“TISAX 평가 보고서”의 구조는 다음과 같습니다.

- A. 평가 관련 정보
  회사 이름, 평가 범위, 범위 ID, 평가 ID, 평가 수준, 평가 목표, 평가 날짜, 감사 제공자
  이 섹션에는 평가 결과가 포함되지 않습니다.
- B. 요약된 결과
  평가 결과(준수, 사소한 미준수, 중대한 미준수), 발견된 문제 수, 그 결과로 발생하는 위험의 추상적 분류의 전체 요약
- C. 평가 결과 요약
  평가 결과의 장별(예: “9 액세스 제어”) 및 기준 카탈로그별(예: “정보 보안”) 요약
- D. VDA ISA의 성숙도(결과 탭)
  각 요구 사항에 대한 성숙도
- E. 상세 평가 결과
  모든 발견된 문제, 해당하는 위험 평가 결과, 요구되는 조치, 이행 기간에 대한 자세한 설명

“교환” 단계(자세한 설명은 아래 참조)에 귀사의 TISAX 평가 보고서 내용에 파트너가 액세스할 수 있는 최고 액세스 수준을 직접 결정합니다.

5.4.14. TISAX 레이블

이 주제에 관해서는 등록 준비 섹션에서 간단히 알아보았습니다. 이 섹션에 설명되어 있듯이, 전에는 평가 목표라고 했던 것이 이제는 TISAX 레이블이 되었습니다.

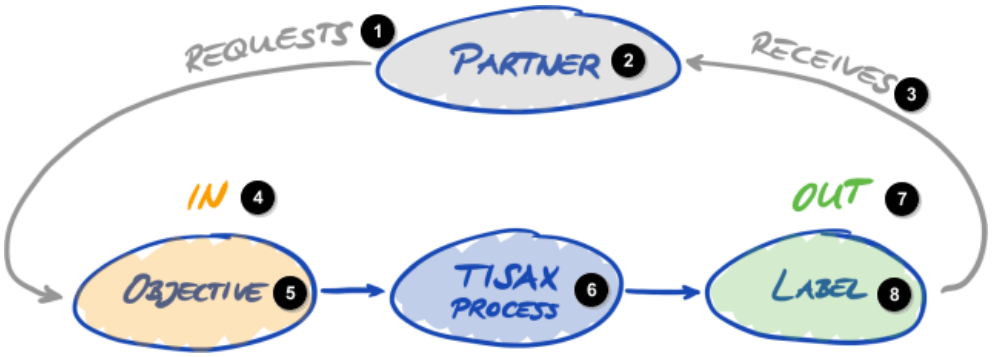


그림 33. 평가 목표와 TISAX 레이블

1. 요청
2. 파트너
3. 수령
4. 입
5. 목표
6. TISAX 프로세스
7. 출
8. 레이블

TISAX 레이블은

- TISAX 평가 프로세스의 결과물입니다.
- 평가 결과를 요약합니다.
- 정보 보안 관리 시스템이 일련의 정해진 요구 사항을 충족한다는 진술입니다.

TISAX 레이블을 사용하면 파트너 및 TISAX 감사 제공자와 TISAX에 관해 더 쉽게 소통할 수 있습니다. 레이블에서 TISAX 평가 프로세스의 정의된 산출물에 대해 언급하기 때문입니다.

5.4.14.1. TISAX 레이블 계층 구조

평가 목표와 해당하는 TISAX 레이블은 서로 간단하게 매핑됩니다. 하지만 몇몇 TISAX 레이블은 계층적으로 연결되어 있다는 중요한 측면이 하나 더 있습니다. 즉, 특정 TISAX 레이블을 받으면 이 레이블 "아래"의 TISAX 레이블도 자동으로 받게 됩니다.

예: 평가 목표가 "Very high availability"였을 경우, 이에 해당하는 TISAX 레이블인 "Very high availability"도 받습니다. 하지만 "Very high availability" 평가 목표는 "High availability"의 확대 집합이기 때문에 "High availability" TISAX 레이블도 자동으로 받습니다.

이 계층 구조는 현재 다음과 같은 레이블에 대해 존재합니다.

- "Info high"는 "Confidential" 및 "High availability"의 확대 집합임.
- "Info very high"는 "Strictly confidential" 및 "Very high availability"의 확대 집합임.
- "Strictly confidential"은 "Confidential"의 확대 집합임.

- “Very high availability” 는 “High availability” 의 확대 집합임.
- “Special data” 는 “Data” 의 확대 집합임.

참고:

TISAX 레이블을 소급적으로 받을 수도 있습니다. 이미 받은 TISAX 레이블 중 하나의 부분 집합인 새 레이블이 도입되면 이 새 레이블을 자동으로 받습니다.

예: “High availability” TISAX 레이블이 아직 존재하지 않았을 때 “Info high” 레이블을 받았습니다. High availability 레이블이 도입될 때 시스템이 이 레이블을 자동으로 귀사에 할당했습니다.

다음 그림에 나와 있는 해당하는 요구 사항을 비교하여 이런 계층적 관계를 추론할 수 있습니다. 표 8, “평가 목표에 해당하는 요구 사항” .

이 관계가 모든 참가자에게 중요하다고 생각되지 않을 수 있습니다. 하지만 한 파트너가 “Very high availability” TISAX 레이블을 보여줄 것을 요청하고 다른 파트너가 “High availability” TISAX 레이블을 요청하는 경우를 상상해 보십시오. 이 경우 두 TISAX 레이블이 모두 있으면 모두에게 더 편리합니다. 아무도 “High availability” 가 “Very high availability” 의 부분 집합이라는 것을 알 필요가 없기 때문입니다. 파트너가 다소 엄격한 구매 프로세스 때문에 특정 TISAX 레이블을 갖고 있어야 하는 경우 더욱 편리할 수 있습니다. 당연히 “Very high availability” 가 “High availability” 보다 “더 낫다” 고 설명하고 싶지는 않을 것이기 때문입니다. 귀사의 TISAX 레이블을 모두 보여주기만 하면 평가하는 사람이 간단히 “’ High availability’ TISAX 레이블이 있어야 한다” 는 요구 사항이 충족되었다고 평가할 수 있습니다.

5.4.14.2. TISAX 레이블의 유효 기간

TISAX 레이블은 일반적으로 3년 동안 유효합니다. 유효 기간은 평가 프로세스 끝에 (TISAX 평가 보고서가 발행되기도 전에) 시작합니다.

TISAX 범위와 관련된 중요한 사항이 변경되는 경우 유효 기간이 더 짧아질 수 있습니다.

예: 귀사의 위치 이전, 새 위치. (이런 경우에 해야 할 일에 대한 설명은 다음을 참조하십시오. 섹션 7.9.3.2, “위치 변경을 요청하는 방법” , 섹션 7.9.3.4, “위치를 더 추가하는 방법” .)

참고:

TISAX 레이블은 ENX 포털에서만 확인할 수 있습니다. TISAX 평가 보고서에는 기록되지 않습니다.

5.4.14.3. TISAX 레이블 갱신

TISAX 레이블을 오래 유지하려면 3년마다 갱신[30]해야 합니다.

갱신하려면 근본적으로 TISAX 프로세스를 다시 거쳐야 합니다(평가 범위를 등록하고, TISAX 평가를 다시 받고, 평가 결과 공유). 회사를 TISAX 참가자로 다시 만들지 않아도 되므로 등록하기는 조금 더 쉽습니다. 그리고 물론 TISAX 데이터베이스에 이미 저장되어 있는 모든 연락처와 위치를 다시 사용할 수도 있습니다.

중요한 참고 사항:

감사 제공자에게 연락하기 전에 새 범위를 등록하십시오. 새 범위 ID를 제공할 수 있어야만 감사 제공자가 새 평가 프로세스를 시작할 수 있습니다.

대부분의 경우 새 범위를 등록하기는 쉽습니다. 새 범위 이름을 지정하고, 연락처를 추가하고, 평가 목표를 선택하고, 위치를 추가하기만 하면 됩니다. 시스템에 이미 있는 이전에 등록된

범위의 연락처와 위치를 다시 사용할 수 있습니다.

중요한 참고 사항:

이전 범위를 등록하는 도중에 만들고 사용했던 기존 위치 기록을 다시 사용하십시오. 새 위치 기록을 같은 주소로 만들지 마십시오.

이유: 일부 TISAX 참가자는 파트너의 평가 결과를 자동으로 처리합니다. 이런 참가자는 자체 시스템을 ENX 포털과 동기화합니다. 작은 차이만 있어도 동기화에 성공하지 못할 수 있습니다. 또한 불필요한 중복 때문에 참가자 데이터가 복잡해지지도 않습니다.

중요한 참고 사항:

파트너와 관계를 유지하는 동안 유효한 TISAX 레이블을 보유해야 한다고 요구되는 경우, 필요한 갱신 프로세스를 시작해야 한다는 미리 알림을 일정에 추가하도록 적극 권장됩니다.

늦어도 TISAX 레이블이 만료되기 1년 전에 갱신을 시작하는 것이 좋습니다.

이제 TISAX 레이블을 받았으므로 마지막 단계로 진행하여 레이블을 파트너와 공유할 수 있습니다.

6. 교환(3 단계)

교환 섹션을 읽는 데 걸리는 예상 시간은 7분입니다.

지금까지 TISAX 프로세스를 진행했지만, 파트너는 아직 귀사의 정보 보안 관리 시스템이 자신의 비밀 데이터를 보호할 수 있다는 어떤 “증거” 도 보지 못했습니다. 이어지는 내용에서는 이제 평가 결과를 파트너와 공유하고 요청된 증거를 제시하는 방법에 대해 설명합니다.

6.1. 전제

평가 결과를 직접 완전히 통제할 수 있다는 것은 TISAX의 핵심적인 특징 중 하나입니다. 명시적인 허가 없이는 평가에 관한 모든 정보가 누구하고도 공유되지 않습니다.

6.2. 교환 플랫폼

ENX 포털은 교환 플랫폼을 제공합니다.

감사 제공자는 귀사의 TISAX 평가 보고서의 첫 두 섹션(A 및 B)을 업로드합니다. 이 단계에는 정보가 귀사를 제외하고 누구에게도 제공되지 않습니다.

등록하는 동안 만들었던 계정을 사용하여 포털에 액세스하고 교환 플랫폼을 사용할 수 있습니다.

다음 주소에서 포털에 액세스할 수 있습니다.
enx.com/en-US/SignIn

6.3. 일반적인 전제 조건

다음과 같은 전제 조건 두 개가 충족되어야만 평가 결과를 파트너와 공유할 수 있습니다.

1. 감사 제공자가 평가 결과를 교환 플랫폼에 제출했어야 합니다.
   평가 결과는 일반적으로 TISAX 평가 보고서 발행 후 5 ~10영업일 뒤에 교환 플랫폼에서 확인할 수 있습니다.
2. 납부하신 수수료를 ENX 협회에서 수령했어야 합니다(해당하는 경우).

두 전제 조건이 모두 충족되면 평가 범위의 상태가 “활성” 이 됩니다.

참고:

모든 평가 범위는 수명 주기를 거칩니다. 이 단계에는 평가 범위의 상태가 “활성” 이어야 합니다.

평가 범위의 상태에 대한 자세한 내용은 다음을 참조하십시오. 섹션 7.5.5, “Assessment scope status “Awaiting your payment” (평가 범위 상태 “지불 대기 중”)”.

평가 결과를 공유할 준비가 되었는지(평가 범위 상태 = 활성) 확인하려면 다음 절차를 따르십시오.

1. ENX 포털에 로그인합니다.
2. 주 탐색 모음으로 이동한 후 “MY TISAX”(“내 TISAX”)를 선택합니다.
3. 드롭다운 메뉴에서 “SCOPES AND ASSESSMENTS”(“범위와 평가”)를 선택합니다.
4. 표로 이동한 후 평가 범위가 있는 행을 표에서 찾습니다.
5. 평가 범위의 평가 범위 상태가 “Active”(“활성”)인지 확인합니다(“Scope Status”(“범위 상태”) 열).

6.4. 교환된 결과의 영속성

중요한 참고 사항:

게시 또는 공유 권한은 취소할 수 없습니다.

그 이유는 모든 수동적 참가자가 받은 모든 평가 결과에 계속 액세스할 수 있도록 하기 위해서입니다. 그렇지 않으면 평가 결과를 참가자가 직접 관리하고 보관해야 할 것이기 때문입니다.

이 권한은 TISAX 평가의 전체 유효 기간 동안 계속 유효합니다.

게시 또는 공유 권한을 실수로 만든 경우 즉시 ENX 협회에 문의하십시오.

6.5. 공유 수준

공유 수준은 TISAX 평가 보고서의 주요 섹션인 A~E에 1:1 매핑됩니다.

	TISAX 평가 보고서의 주요 섹션	교환 플랫폼의 공유 수준
1	A. 평가 관련 정보(Assessment Related Information)	
2	B. 요약된 결과(Summarized Results)	
3	C. 평가 결과 요약(Assessment result summary)	
4	D. VDA ISA의 성숙도(결과 탭) (Maturity Levels of VDA ISA (Result Tab))	
5	E. 상세 평가 결과(Detailed Assessment Results)	

표 12. TISAX 평가 보고서의 주요 섹션과 교환 플랫폼의 공유 수준

공유 수준이 높을수록 각 참가자가 TISAX 평가에 대한 세부 정보에 더 많이 액세스할 수 있습니다.

각 TISAX 평가 보고서 섹션의 내용에 대해 자세히 알아보려면 다음을 참조하십시오. 섹션 5.4.7.4, “TISAX 평가 보고서”.

6.6. 교환 플랫폼에 평가 결과 게시

평가 결과를 교환 플랫폼에 게시하여 다른 모든 TISAX 참가자와 공유할 수 있습니다. 그러면 다른 모든 TISAX 참가자가 부여받은 최고 공유 수준까지 평가 결과에 액세스할 수 있습니다.

전체 평가 결과가 “준수”인 경우에만 평가 결과를 게시할 수 있습니다.

교환 플랫폼에 게시하는 평가 결과에 대해 선택할 수 있는 공유 수준은 다음으로 제한됩니다.

- Do not publish (Default) (게시 금지(기본))
- A. Assessment Related Information (A. 평가 관련 정보)
- A + Labels (A + 레이블)
- A + Labels + B. Summarized Results (A + 레이블 + B. 요약된 결과)

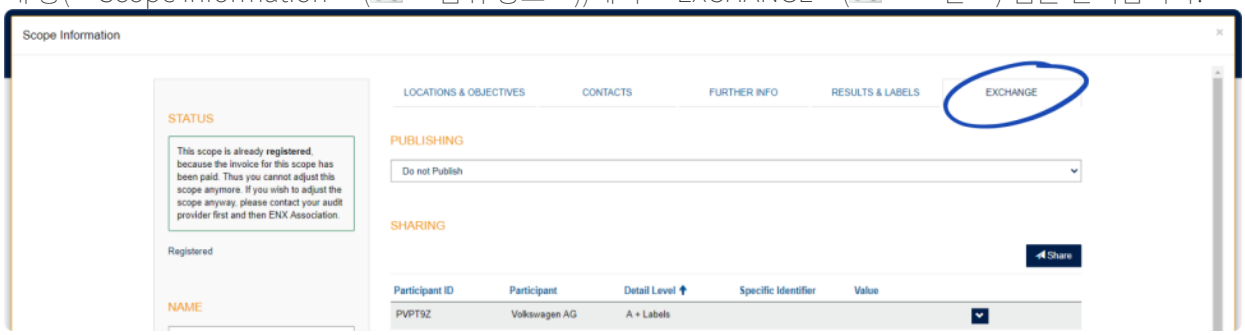
이 일반적인 게시 유형에는 “A + Labels”(“A + 레이블”)이 권장됩니다.

중요한 참고 사항:

> 다음에 서술된 전제 조건이 충족된 경우에만 평가 결과를 게시할 수 있습니다. 섹션 6.3, “일반적인 전제 조건”

평가 결과를 교환 플랫폼에 게시하려면 다음 절차를 따르십시오.

1. ENX 포털에 로그인합니다.
2. 주 탐색 모음으로 이동한 후 “MY TISAX”(🇰🇷 “내 TISAX”)를 선택합니다.
3. 드롭다운 메뉴에서 “SCOPES AND ASSESSMENTS”(🇰🇷 “범위와 평가”)를 선택합니다.
4. 표로 이동한 후 평가 범위가 있는 행을 표에서 찾습니다.
5. 평가 범위의 평가 범위 상태가 “Active”(🇰🇷 “활성”)인지 확인합니다(“Scope Status”(🇰🇷 “범위 상태”) 열).
6. 표에서 평가 범위가 있는 행 끝으로 이동하여 아래쪽 화살표가 있는 버튼을 클릭합니다.
7. “Scope Information”(🇰🇷 “범위 정보”)을 선택합니다.
8. 새 창(“Scope Information”(🇰🇷 “범위 정보”))에서 “EXCHANGE”(🇰🇷 “교환”) 탭을 선택합니다.



9. “PUBLISHING”(🇰🇷 “게시”) 섹션으로 이동하고, 드롭다운 메뉴를 열고, 원하는 공유 수준을 선택합니다(위 권장 사항 참조).

> 참고:
>
> 평가 결과는 교환 플랫폼에만 게시됩니다. 다른 TISAX 참가자만 평가 결과에 액세스할 수 있습니다. 모든 TISAX 참가자의 공개 목록은 없습니다. 순 TISAX 참가자 수만 공개 TISAX 웹 사이트에서 언급될 수 있습니다.

6.7. 특정 참가자와 평가 결과 공유

TISAX 평가 결과를 교환 플랫폼에 게시하는 앞에서 언급한 방법 외에, 공유 수준이 높은 특정 TISAX 참가자를 선택하여 평가 결과를 공유할 수도 있습니다.

앞에서 언급한 게시 방법과 달리, 전체 평가 결과가 (중대한/사소한) 미준수인 경우에도 평가 결과를 공유할 수 있습니다.

평가 결과 공유는 TISAX의 중요한 일부분입니다. 정보 보안 관리 시스템을 한 번만 평가받았지만, 이제 평가 결과를 원하는 수의 파트너와 공유할 수 있습니다.

평가 결과를 교환 플랫폼에서 공유할 때 선택할 수 있는 옵션은 다음과 같습니다.

1. A: Assessment Related Information (🇰🇷 A: 평가 관련 정보)
2. A + Labels (🇰🇷 A + 레이블)
3. A + Labels + B: Assessment Summary (🇰🇷 A + 레이블 + B: 평가 요약)

4. A + Labels + B + C: Summarized Results (A + 레이블 + B + C: 요약된 결과)
5. A + Labels + B + C + D: Detailed Assessment Results (A + 레이블 + B + C + D: 상세 평가 결과)
6. A + Labels + B + C + D + E: Maturity Levels according to ISA (A + 레이블 + B + C + D + E: ISA에 따른 성숙도)

공유에는 “A + Labels”(“A + 레이블”) 공유 수준이 권장됩니다. 대부분의 파트너에는 이 공유 수준으로 충분합니다. 나중에 언제든지 더 높은 공유 수준을 선택할 수 있습니다.

참고:

몇몇 TISAX 참가자는 파트너의 평가 결과를 자동으로 처리합니다. 이런 참가자는 자체 시스템을 ENX 포털과 동기화합니다. 이 참가자와 특별히 공유되는 평가 결과만 동기화됩니다. 섹션 6.6, “교환 플랫폼에 평가 결과 게시” 에 설명된 대로, 게시하기만 하면 인정되지 않습니다.

TISAX를 사용하는 OEM 중에서는 BMW를 예로 들 수 있습니다. BMW의 파트너인 경우 평가 결과를 게시하는 데 그치지 않고 공유하기도 해야 합니다.

6.7.1. 전제 조건

평가 결과를 파트너(또는 다른 TISAX 참가자)와 공유하기 위한 전제 조건이 있습니다.

- TISAX 평가 결과는 다른 TISAX 참가자하고만 공유할 수 있습니다.
- 파트너는 TISAX 참가자여야 합니다.
- 파트너의 참가자 ID가 필요합니다.[31]
- 수수료를 납부해야 합니다(해당하는 경우).

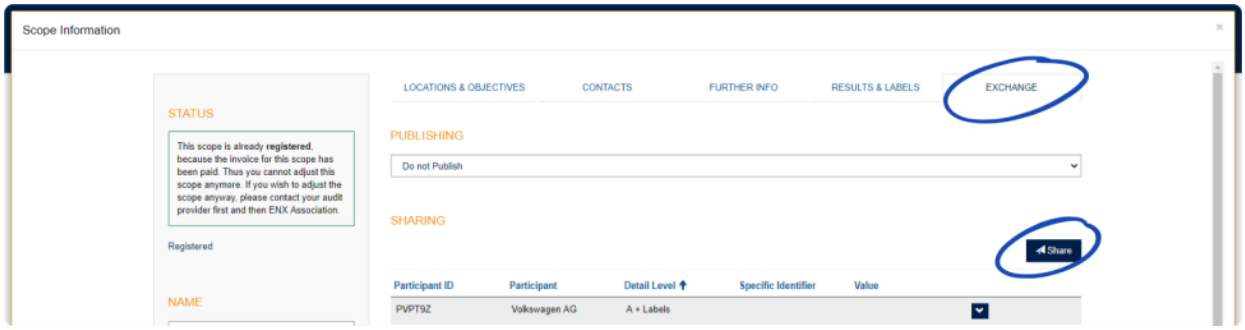
중요한 참고 사항:

다음에 서술된 전제 조건이 충족된 경우에만 평가 결과를 공유할 수 있습니다. 섹션 6.3, “일반적인 전제 조건”

6.7.2. 공유 권한을 만드는 방법

평가 결과를 다른 TISAX 참가자와 공유하려면 다음 절차를 따르십시오.

1. ENX 포털에 로그인합니다.
2. 주 탐색 모음으로 이동한 후 “MY TISAX”(“내 TISAX”)를 선택합니다.
3. 드롭다운 메뉴에서 “SCOPES AND ASSESSMENTS”(“범위와 평가”)를 선택합니다.
4. 표로 이동하여 평가 범위가 있는 행을 표에서 찾습니다.
5. 평가 범위의 평가 범위 상태가 “Active”(“활성”)인지 확인합니다(“Scope Status”(“범위 상태”) 열).
6. 표에서 평가 범위가 있는 행 끝으로 이동하여 아래쪽 화살표가 있는 버튼을 클릭합니다.
7. “Scope Information”(“범위 정보”)을 선택합니다.
8. 새 창(“Scope Information”(“범위 정보”))에서 “EXCHANGE”(“교환”) 탭을 선택합니다.



9. “SHARING”(“공유”) 섹션으로 이동한 후 “Share”(“공유”) 버튼을 클릭합니다.
10. 새 창(“SHARE THIS SCOPE”(“이 범위 공유”))에서 파트너의 참가자 ID를 입력(하거나 인접한 검색 상자의 참가자 목록에서 파트너를 선택)합니다.
11. 원하는 공유 수준을 선택합니다.
12. “Next”(“다음”) 버튼을 클릭합니다.
13. 공유 권한의 영속성에 관한 지침을 읽고 이해하십시오.
14. “confirm”(“확인”) 확인란 두 개를 선택합니다.
15. “Submit”(“제출”) 버튼을 클릭합니다.

나머지는 교환 플랫폼에서 모두 자동으로 수행됩니다. 공유 수준 A, B에 해당하는 정보는 교환 플랫폼에서 확인할 수 있습니다. 파트너는 이제 ENX 포털에 로그인하여 귀사에서 공유한 평가 결과를 확인할 수 있습니다[32].

공유 수준이 더 높은 경우(C~E), 교환 플랫폼에서 감사 제공자에게 알립니다. 그러면 감사 제공자가 (선택된 공유 수준과 일치하는) 해당 정보를 파트너의 주 참가자 연락 담당자에게 보냅니다.

6.8. TISAX 밖에서 평가 결과 공유

규칙[33]에 따르면, TISAX 교환 플랫폼만 사용하여 다른 TISAX 참가자들에게 귀사의 평가 결과를 알릴 수 있습니다.

6.8.1. 교환 메커니즘을 엄격하게 관리하는 이유

TISAX에서는 표준화된 평가 결과 교환 메커니즘을 제공합니다. 따라서 교환이 다양한 방법으로 이루어지고 교환 시에 전체적인 그림을 파악하는 데 필요한 모든 정보가 항상 포함되지는 않는 다른 인증(예: ISO) 결과보다 교환을 통해 더 많은 가치를 얻을 수 있습니다.

OEM들은 특히 이 표준화의 가치를 높이 평가합니다. 하지만 분명하게 정의된 절차는 다른 회사에도 이익이 됩니다.

6.8.2. TISAX에 대한 공개적인 글 작성에 관한 가이드

평가 결과에 대한 공개적인 글을 쓰면 안 되지만, 귀사의 TISAX 노력에 대해 언급할 수는 있습니다. ENX 포털에서, ENX 협회는 공개적인 글을 쓰는 방법에 대해 조언합니다. 귀사에서 사용할 수 있는 TISAX 로고도 제공합니다.

ENX 포털에 로그인한 후 다음 웹 페이지에서 정보를 확인할 수 있습니다.
enx.com/en-US/myenxportal/marketing/
ZIP 압축 파일 직접 다운로드(문서 및 로고):
enx.com/en-US/myenxportal/marketing/TISAX-Trademark-and-Logos-Terms-and-Conditions.zip

벽에 걸 수 있는 인증서가 있는지 궁금한 경우:
위에 언급된 표준화된 교환 프로세스 때문에 ENX 협회에서는 이런 인증서를 제공하지 않습니다.

6.8.3. 아직 TISAX 참가자가 아닌 파트너와 공유하기

TISAX 평가 결과를 a) 아직 TISAX 참가자가 아니고 b) 아직 (평가 프로세스를 거쳐서) TISAX 레이블을 받지 않은 특정 파트너와 공유하려면 다음 절차를 따르십시오.

1. 파트너에게 TISAX 참가자로 등록하라고 알립니다.
   파트너는 TISAX 참가자로 등록하기만 하면 됩니다. 평가 범위 등록으로 계속 진행하지는 않아도 됩니다.
2. 파트너에게 ENX 협회에 연락하라고 알립니다.
   일반적으로, ENX 협회는 회사가 평가 범위도 등록하는 경우에만 신규 등록을 처리합니다. 파트너가 요청할 경우, ENX 협회에서 파트너의 등록을 처리합니다. 따라서 파트너가 TISAX 참가자가 됩니다. 파트너는 이제 귀사의 TISAX 평가 결과를 일반적인 교환 프로세스를 통해 받을 수 있습니다.

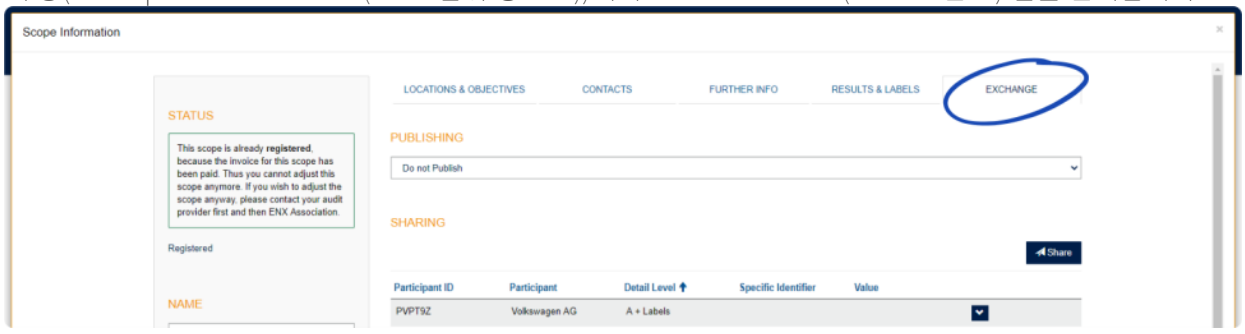
이렇게 접근하는 목적은 파트너가 TISAX 평가 결과 교환에 적용되는 “TISAX 참가 일반 약관” 준수에 동의하도록 보장하기 위해서입니다.

평가 범위 등록에 대한 비용만 발생합니다. TISAX 참가자로 등록하는 비용은 무료이므로 파트너가 귀사의 평가 결과를 무료로 받을 수 있습니다. 하지만 자체 평가 결과가 없으면 파트너가 평가 결과를 최대 5개까지만 받을 수 있고 게시물은 볼 수 없습니다.

6.8.4. ENX 포털에 직접 액세스할 수 없는 파트너의 직원과 공유하기

ENX 포털 계정이 있는 파트너의 직원만 귀사의 평가 결과를 직접 볼 수 있습니다. 포털에 액세스할 수 없는 파트너의 직원에게 TISAX 레이블을 증명해야 하는 경우, 특별 PDF 문서를 이 용도로 사용할 수 있습니다. 이 문서를 받으려면 다음 절차를 따르십시오.

1. 다음 섹션에 설명된 대로 평가 결과를 파트너와 공유합니다. 섹션 6.7, “특정 참가자와 평가 결과 공유” .
2. ENX 포털에 로그인합니다.
3. 주 탐색 모음으로 이동한 후 “MY TISAX”(“내 TISAX”)를 선택합니다.
4. 드롭다운 메뉴에서 “SCOPES AND ASSESSMENTS”(“범위와 평가”)를 선택합니다.
5. 표로 이동한 후 평가 범위가 있는 행을 표에서 찾습니다.
6. 평가 범위의 평가 범위 상태가 “Active”(“활성”)인지 확인합니다(“Scope Status”(“범위 상태”) 열).
7. 표에서 평가 범위가 있는 행 끝으로 이동하여 아래쪽 화살표가 있는 버튼을 클릭합니다.
8. “Scope Information”(“범위 정보”)을 선택합니다.
9. 새 창(“Scope Information”(“범위 정보”))에서 “EXCHANGE”(“교환”) 탭을 선택합니다.



10. “SHARING”(“공유”) 섹션으로 이동하여 (1 단계에 만들었던) 공유 권한이 있는 행을 표에서 찾습니다.
11. 표에서 공유 권한이 있는 행 끝으로 이동하여 아래쪽 화살표가 있는 버튼을 클릭합니다.
12. “Edit”(“편집”)을 선택합니다.
13. 새 창(“SHARE THIS SCOPE”(“이 범위 공유”))에서 맨 아래로 스크롤하여 “Request Shared Information as PDF”(“공유된 정보를 PDF로 요청”)를 선택합니다.

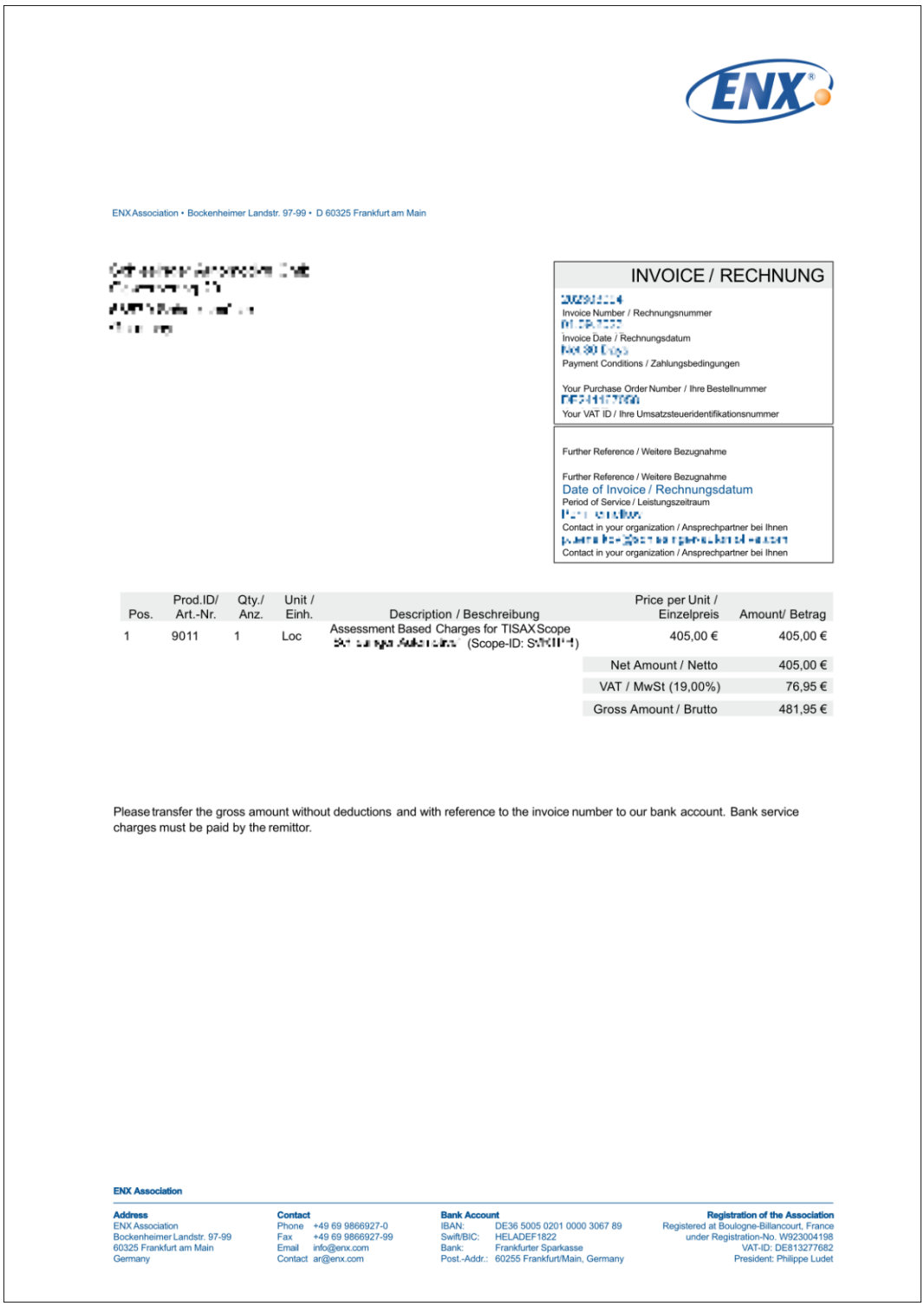
14. 문서가 생성될 때까지 잠시 기다립니다.
15. 문서(“Copy of information shared with ACME.pdf (66.84 KB)” (🇰🇷 “ACME와 공유된 정보의 복사본.pdf(66.84 KB)”))를 다운로드합니다.

7. 부록

7.1. 부록: 청구서 예시

다음은 ENX 협회에서 보내는 청구서의 예입니다.

자세한 내용은 다음을 참조하십시오. 섹션 4.3.4, “수수료” .



ENX Association • Bockenheimer Landstr. 97-99 • D 60325 Frankfurt am Main

[redacted]

INVOICE / RECHNUNG

[redacted]
Invoice Number / Rechnungsnummer
[redacted]
Invoice Date / Rechnungsdatum
[redacted]
Payment Conditions / Zahlungsbedingungen

Your Purchase Order Number / Ihre Bestellnummer
[redacted]
Your VAT ID / Ihre Umsatzsteueridentifikationsnummer

Further Reference / Weitere Bezugnahme

Further Reference / Weitere Bezugnahme
Date of Invoice / Rechnungsdatum
Period of Service / Leistungszeitraum
[redacted]
Contact in your organization / Ansprechpartner bei Ihnen
[redacted]
Contact in your organization / Ansprechpartner bei Ihnen

Pos.	Prod.ID/ Art.-Nr.	Qty./ Anz.	Unit / Einh.	Description / Beschreibung	Price per Unit / Einzelpreis	Amount/ Betrag
1	9011	1	Loc	Assessment Based Charges for TISAX Scope [redacted] (Scope-ID: [redacted])	405,00 €	405,00 €
					Net Amount / Netto	405,00 €
					VAT / MwSt (19,00%)	76,95 €
					Gross Amount / Brutto	481,95 €

Please transfer the gross amount without deductions and with reference to the invoice number to our bank account. Bank service charges must be paid by the remittor.

ENX Association

Address
ENX Association
Bockenheimer Landstr. 97-99
60325 Frankfurt am Main
Germany

Contact
Phone +49 69 9866927-0
Fax +49 69 9866927-99
Email info@enx.com
Contact ar@enx.com

Bank Account
IBAN: DE36 5005 0201 0000 3067 89
Swift/BIC: HELADEF1822
Bank: Frankfurter Sparkasse
Post.-Addr.: 60255 Frankfurt/Main, Germany

Registration of the Association
Registered at Boulogne-Billancourt, France
under Registration-No. W923004198
VAT-ID: DE813277682
President: Philippe Ludet

7.2. 부록: 확인 이메일 예시

온라인 등록 프로세스를 진행하는 동안 필수 단계를 모두 완료하면 ENX 협회에서 확인 이메일을 보내 드립니다.

이 확인 이메일을 보내는 시기에 대한 자세한 내용은 다음을 참조하십시오. 섹션 4.5.8, “확인 이메일”.

제목: [TISAX] 범위 S3ZY5V 승인됨

존 도우님께,

TISAX 평가 범위를 등록해 주셔서 감사합니다. 저는 귀사의 범위 등록을 진행하고 범위를 승인하였습니다. 모든 범위 정보와 최신 TISAX 감사 제공자 목록을 포함한 TISAX 범위 발췌 자료를 첨부해 드렸습니다.

다음 단계

첨부해 드린 TISAX 범위 발췌 자료를 사용하여 이제 모든 TISAX 감사 제공자에게 범위에 대한 견적을 요청하실 수 있습니다.

도움이 필요하십니까?

TISAX에 관해 궁금한 사항이 더 있는 경우, TISAX FAQ나 TISAX 참가자 안내서를 읽어 주십시오. TISAX에 관해 도움이 더 필요한 경우, 언제든지 TISAX 핫라인에 이메일(tisax@enx.com) 또는 전화(+49 69 986692-777)로 문의해 주십시오.

감사합니다.

TISAX 팀 배상

7.3. 부록: TISAX 범위 발췌 자료 예시

확인 이메일에 첨부된 “TISAX 범위 발췌 자료”를 수신합니다.

자세한 내용은 다음을 참조하십시오. 섹션 4.5.8, “확인 이메일”.

TISAX Scope Excerpt S[illegible]
Participant: [illegible]

Scope: [illegible]	S[illegible]

Standard Scope 2.0

The TISAX Scope defines the scope of the assessment. The assessment includes all processes, procedures and resources under responsibility of the assessed organization that are relevant to the security of the protection objects and their protection goals as defined in the listed assessment objectives at the listed locations. The assessment is conducted at least in the highest Assessment Level listed in any of the listed Assessment Objectives. All assessment criteria listed in the listed assessment objectives are subject to the assessment.

Assessment Objectives	**AL**	**Locations**
Information with High Protection Needs	2	1

Maturity of ISMS	**Certified on**	**Certified in**
Established ISMS (already experienced, but not yet certified)		

Complexity of ISMS	**Justification (only if simple ISMS)**
Complex ISMS (very large number of methods/ processes)	

Use of Consulting Firm for ISMS	**Name of Consulting Firm**
No Support by consultancy provider	none

Earliest Kickoff-Meeting	**Labels needed until**	**External Requirement**
[illegible]	[illegible]	No

Location: [illegible]

Company Name and Address	**Location-ID**	**DUNS**
[illegible]	L[illegible]	[illegible]
	Type	
	Campus owned and exclusively used by company	
	Passive Site Protection	**Employees**
	Yes	Overall: 1.001-5.000
	Industry	IT: 1-10
		IT-Security: 1-10
		Location Security: 4-10

2023[illegible]

Page **1** of **1**

7.4. 부록: Participant status(🇰🇷 참가자 상태)

7.4.1. 개요: Participant status(🇰🇷 참가자 상태)

“참가자 상태”는 (회사로서) 귀사의 TISAX 프로세스 진행 상태를 나타냅니다.

가능한 “참가자 상태”는 다음과 같습니다.

1. Incomplete (🇰🇷 미완료)
2. Awaiting approval (🇰🇷 승인 대기 중)
3. Preliminary (🇰🇷 예비)
4. Registered (🇰🇷 등록됨)
5. Expired (🇰🇷 만료됨)

아래의 각 상태에 대한 섹션에 있는 표에서는 다음에 대해 설명합니다.

- 귀사의 상황
  (이 상태인 시점에 해당하는 내용)
- 귀사의 다음 작업
  (다음 상태로 진행하기 위해 해야 할 일(해당하는 경우))
- ENX 협회의 다음 작업
  (귀사의 상태를 격상시키기 위해 ENX 협회에서 해야 할 일(해당하는 경우))
- 다음 상태
  (해당하는 경우)

아래 그림에는 한 상태에서 다음 상태로 진행하기 위해 수행하는 작업이 나와 있습니다.

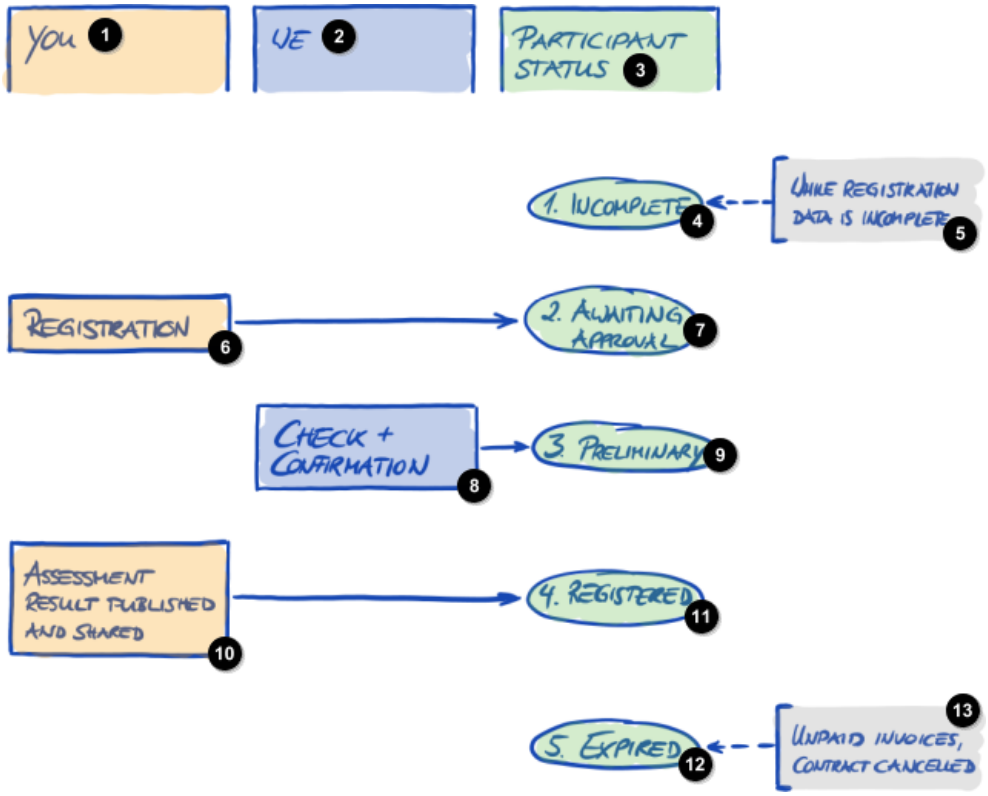


그림 34. 참가자 상태 개요

1. 귀사
2. ENX 협회
3. 참가자 상태
4. 1. 미완료
5. 등록 데이터가 불완전한 상태
6. 등록
7. 2. 승인 대기 중
8. 점검 + 확인
9. 3. 예비
10. 평가 결과 게시 및 공유됨
11. 4. 등록됨
12. 5. 만료됨
13. 미지불 청구서, 계약 취소됨

7.4.2. Participant status “Incomplete” (참가자 상태 “미완료”)

상태	상황	귀사의 다음 작업	ENX 협회의 다음 작업	다음 상태
미완료	TISAX 등록을 완료하지 않았습니다. 일반 약관에 동의하지 않았거나, 주 참가자 위치를 지정하지 않았거나, 주 참가자 연락 담당자를 지정하지 않았거나, ENX 협회에서 요구하는 다른 정보가 누락되었습니다.	다음 링크에서 계속: enx.com/en-US/SignIn	이메일로 미리 알림을 (일반적으로 며칠 내에) 보내 드립니다.	승인 대기 중

7.4.3. Participant status “Awaiting approval” (🇰🇷 참가자 상태 “승인 대기 중”)

상태	상황	귀사의 다음 작업	ENX 협회의 다음 작업	다음 상태
승인 대기 중	TISAX 등록이 완료되었습니다. 평가 범위를 등록했거나 아직 등록하지 않았을 수 있습니다.	ENX 협회가 다음 작업을 수행할 때까지 기다립니다.	ENX 협회에서 귀사의 신청을 확인하고 일반적으로 승인합니다. 하지만 일반적으로 귀사에서 평가 범위를 등록하여 ENX 협회에서 확인하도록 유발하기도 합니다. ENX 협회에서 참가자 ID와 범위 ID를 할당합니다. 확인 이메일을 보내드립니다. 첨부되는 “TISAX 범위 발췌 자료” (PDF)에는 ENX 협회의 데이터베이스에 있는 정보가 요약됩니다.	예비

7.4.4. Participant status “Preliminary” (🇰🇷 참가자 상태 “예비”)

상태	상황	귀사의 다음 작업	ENX 협회의 다음 작업	다음 상태
예비	TISAX 등록 프로세스를 성공적으로 완료했습니다.	수수료를 지불합니다(해당하는 경우). TISAX 평가 프로세스를 거칩니다. 평가 결과를 게시하고 공유합니다.	없음	등록됨

7.4.5. Participant status “Registered” (참가자 상태 “등록됨”)

상태	상황	귀사의 다음 작업	ENX 협회의 다음 작업	다음 상태
등록됨	성공적으로 TISAX 평가 프로세스를 완료하고 TISAX 레이블을 받았습니다. 평가 결과를 게시하고 공유했습니다. TISAX 평가 프로세스를 통과하여 합격해야만 TISAX 레이블을 받습니다. ENX 포털에서 이 사실은 평가 범위 상태가 “활성”인 평가 범위로 나타납니다.	없음	없음	(만료됨)

참고:

파트너의 평가 결과에 액세스하려는 경우:

다른 참가자의 평가 결과를 수신할 수 있기 위한 개념적인 전제 조건은 다음 중 하나입니다.

- 귀사의 자체 평가 결과를 공유합니다(그러면 귀사가 진지한 TISAX 참가자이고 자동차 커뮤니티의 구성원임이 “입증”됨).
- 자동차 산업에서 귀사가 갖고 있는 평판을 근거로 ENX 협회에서 귀사를 인정합니다(OEM, 1급 공급업체 등).
- 다른 참가자의 평가 결과를 받아야 하는 정당한 이해 관계가 있음을 증명합니다. ENX 협회에서는 복잡한 프로세스를 통해 이를 확인해야 하므로 상당한 수수료가 발생할 수 있습니다. 더 자세한 사항은 ENX 협회에 문의하십시오.

7.4.6. Participant status “Expired” (참가자 상태 “만료됨”)

상태	상황	귀사의 다음 작업	ENX 협회의 다음 작업	다음 상태
만료됨	수수료를 납부하지 않았습니다. 또는 귀사 또는 ENX 협회에서 양측의 상호 계약(GTC)을 취소했습니다.	없음	없음	해당 없음

7.5. 부록: Assessment scope status(평가 범위 상태)

7.5.1. 개요: Assessment scope status(🇰🇷 평가 범위 상태)

“평가 범위 상태”는 평가 범위가 수명 주기의 어디에 있는지 정의합니다.

“평가 범위 상태”는 “평가 상태”와 다르다는 점에 유의하십시오. “평가 상태”에 대한 자세한 내용은 다음을 참조하십시오. 섹션 7.6, “부록: Assessment status(🇰🇷 평가 상태)”.

귀사의 “평가 범위 상태”는 다음 중 하나일 수 있습니다.

1. Incomplete (🇰🇷 미완료)
2. Awaiting your order (🇰🇷 주문 대기 중)
3. Awaiting ENX approval (🇰🇷 ENX 승인 대기 중)
4. Awaiting your payment (🇰🇷 지불 대기 중)
5. Registered (🇰🇷 등록됨)
6. Active (🇰🇷 활성)
7. Expired (🇰🇷 만료됨)

아래의 각 상태에 대한 섹션에 있는 표에서는 다음에 대해 설명합니다.

- 귀사의 상황
  (이 상태인 시점에 해당하는 내용)
- 귀사의 다음 작업
  (다음 상태로 진행하기 위해 해야 할 일(해당하는 경우))
- ENX 협회의 다음 작업
  (귀사의 상태를 격상시키기 위해 ENX 협회에서 해야 할 일(해당하는 경우))
- 다음 상태
  (해당하는 경우)

아래 그림에는 한 상태에서 다음 상태로 진행하기 위해 수행하는 작업이 나와 있습니다.

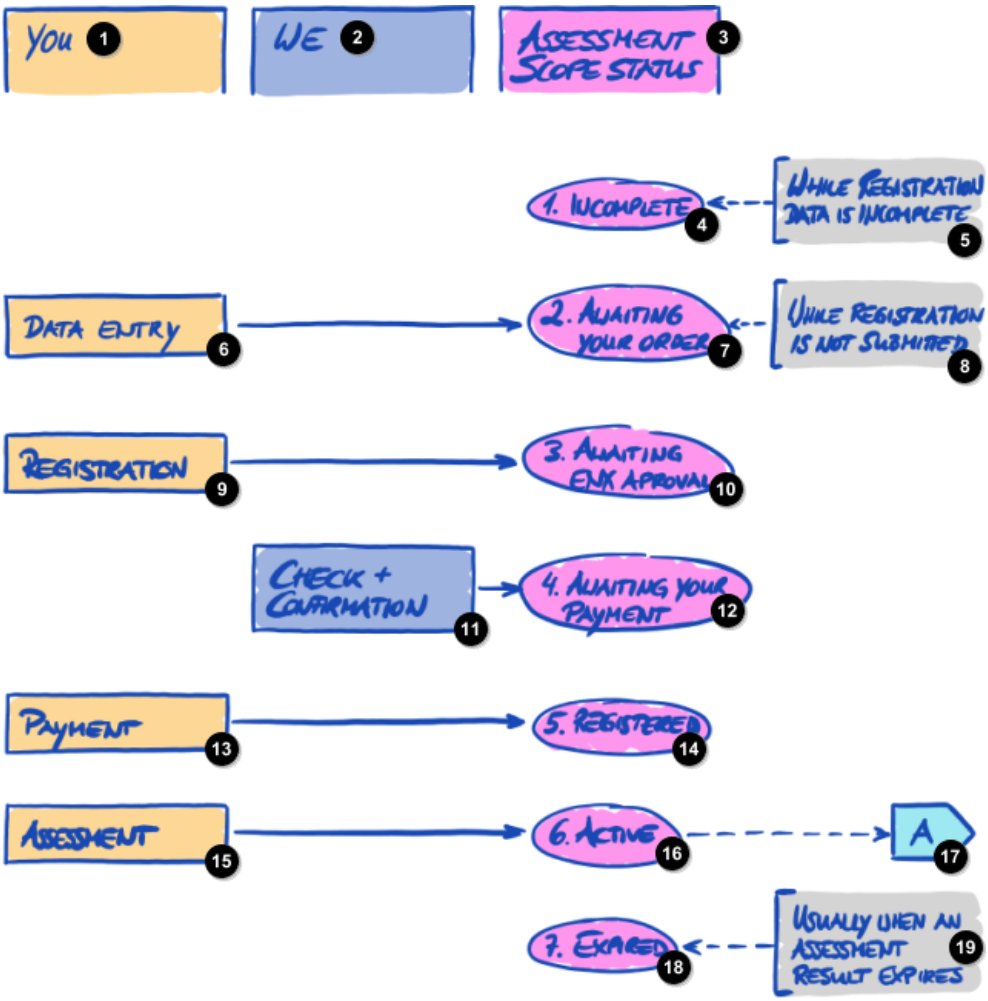


그림 35. 평가 범위 상태 개요

1. 귀사
2. ENX 협회
3. 평가 범위 상태
4. 1. 미완료
5. 등록 데이터가 불완전한 상태
6. 데이터 입력
7. 2. 주문 대기 중
8. 등록이 제출되지 않은 상태
9. 등록
10. 3. ENX 승인 대기 중
11. 점검 + 확인
12. 4. 지불 대기 중

13 지불

14 5. 등록됨

15 평가

16 6. 활성

17 A

18 7. 만료됨

19 일반적으로 평가 결과 만료 시

위 그림에서 다른 페이지 참조인 “A” 는 “활성” 평가 범위 상태를 “평가 상태” 와 연결합니다. “평가 상태” 에 대한 자세한 내용은 다음을 참조하십시오. 섹션 7.6, “부록: Assessment status(🇰🇷 평가 상태)” .

7.5.2. Assessment scope status “Incomplete” (🇰🇷 평가 범위 상태 “미완료”)

상태	상황	귀사의 다음 작업	ENX 협회의 다음 작업	다음 상태
미완료	평가 범위 등록을 완료하지 않았거나, 필수 정보를 모두 제공하지 않았습니다.	다음 링크에서 계속: 🇬🇧 enx.com/en-US/SignIn	이메일로 미리 알림을 (일반적으로 며칠 내에) 보내 드립니다.	주문 대기 중

이 상태가 어디서 역할을 하는지에 대한 자세한 내용은 다음을 참조하십시오. 섹션 4.5.7, “평가 범위 등록” .

7.5.3. Assessment scope status “Awaiting your order” (🇰🇷 평가 범위 상태 “주문 대기 중”)

상태	상황	귀사의 다음 작업	ENX 협회의 다음 작업	다음 상태
주문 대기 중	범위 등록을 마치지 않았습니다.	다음 링크에서 계속: 🇬🇧 enx.com/en-US/SignIn	이메일로 미리 알림을 (일반적으로 며칠 내에) 보내 드립니다.	ENX 승인 대기 중

이 상태가 어디서 역할을 하는지에 대한 자세한 내용은 다음을 참조하십시오. 섹션 4.5.7, “평가 범위 등록” .

7.5.4. Assessment scope status “Awaiting ENX approval” (🇰🇷 평가 범위 상태 “ENX 승인 대기 중”)

상태	상황	귀사의 다음 작업	ENX 협회의 다음 작업	다음 상태
ENX 승인 대기 중	평가 범위 등록이 완료되었습니다.	ENX 협회가 다음 작업을 수행할 때까지 기다립니다.	ENX 협회에서 귀사의 신청을 확인하고 일반적으로 승인합니다. ENX 협회에서 범위 ID를 할당합니다. ENX 협회에서 확인 이메일을 보냅니다. 첨부되는 “TISAX 범위 발췌 자료”(PDF)에는 ENX 협회의 데이터베이스에 있는 정보가 요약됩니다.	지불 대기 중

이 상태가 어디서 역할을 하는지에 대한 자세한 내용은 다음을 참조하십시오. 섹션 4.5.7, “평가 범위 등록”.

7.5.5. Assessment scope status “Awaiting your payment” (🇰🇷 평가 범위 상태 “지불 대기 중”)

상태	상황	귀사의 다음 작업	ENX 협회의 다음 작업	다음 상태
지불 대기 중	평가 범위 등록이 완료 및 승인됩니다. 귀사에서 ENX 협회의 확인 이메일과 “TISAX 범위 발췌 자료”를 수신했습니다.	수수료를 지불합니다(해당하는 경우). TISAX 감사 제공자에게 오퍼를 요청합니다. “지불 대기 중” 상태 이후에 귀사는 ▪ 일부 평가 관련 정보를 파트너와 공유하기 시작할 수 있습니다.[34] ▪ 평가 결과 게시를 미리 설정할 수 있습니다. (이 설정은 평가 범위 상태가 “활성”으로 변경된 후에만 적용됩니다.	귀사의 대금 지불을 기다립니다.	등록됨

이 상태가 어디서 역할을 하는지에 대한 자세한 내용은 다음을 참조하십시오. 섹션 4.5.8, “확인 이메일”.

7.5.6. Assessment scope status “Registered” (🇰🇷 평가 범위 상태 “등록됨”)

상태	상황	귀사의 다음 작업	ENX 협회의 다음 작업	다음 상태
등록됨	평가 범위가 등록된 상태입니다. ENX 협회에서 귀사의 지불금을 전액 수령했거나, 귀사의 상업적 상태가 다른 상황으로 인해 “녹색” 입니다.	TISAX 평가 프로세스를 거칩니다.	없음	활성

7.5.7. Assessment scope status “Active” (🇰🇷 평가 범위 상태 “활성”)

상태	상황	귀사의 다음 작업	ENX 협회의 다음 작업	다음 상태
활성	성공적으로 TISAX 평가 프로세스를 완료하고 TISAX 레이블을 받았습니다.	평가 결과를 게시하고 공유합니다. 더 낮은 상태에서 미리 설정한 게시 및 공유 권한이 이제 적용됩니다.	없음	만료됨

게시 및 공유에 대한 자세한 내용은 다음을 참조하십시오. 섹션 6, “교환(3 단계)” .

7.5.8. Assessment scope status “Expired” (🇰🇷 평가 범위 상태 “만료됨”)

상태	상황	귀사의 다음 작업	ENX 협회의 다음 작업	다음 상태
만료됨	다음 중 하나 이상: ▪ 평가 범위 등록을 90일 이내에 완료하지 않았거나,	새 평가 범위 등록을 시작합니다.	없음	미완료 또는 주문 대기 중 또는 ENX 승인 대기 중
	• 수수료 지불이 지나치게 지연되었거나,			
	• TISAX 프로세스를 중간에 종료했거나,			
	• 평가 결과 유효 기간(3년)이 만료되었거나,			
	• 평가 범위에 중대한 변화가 있었습니다(예: 평가 범위에 포함된 모든 위치가 더 이상 귀사의 위치가 아님).			

7.6. 부록: Assessment status(🇰🇷 평가 상태)

7.6.1. 개요: Assessment status(🇰🇷 평가 상태)

“평가 상태” 는 귀사가 평가 프로세스의 어디에 있는지 정의합니다. 한 평가 유형에서 다음 평가 유형으로 진행(예: “첫 평가” 에서 “시정 조치 계획 평가” 로)하면 상태가 바뀝니다.

“평가 상태” 는 “평가 범위 상태” 와 다르다는 점에 유의하십시오. “평가 범위 상태” 에 대한 자세한 내용은 다음을 참조하십시오. 섹션 7.5, “부록: Assessment scope status(🇰🇷 평가 범위 상태)” .

귀사의 "평가 상태"는 다음 중 하나일 수 있습니다.

1. Initial assessment ordered (🇰🇷 첫 평가 주문됨)
2. Initial assessment ongoing (🇰🇷 첫 평가 진행 중)
3. Waiting for corrective action plan assessment (🇰🇷 시정 조치 계획 평가 대기 중)
4. Waiting for follow-up (🇰🇷 후속 평가 대기 중)
5. Finished (🇰🇷 마침)

아래의 각 상태에 대한 섹션에 있는 표에서는 다음에 대해 설명합니다.

- 귀사의 상황
  (이 상태인 시점에 해당하는 내용)
- 귀사의 다음 작업
  (다음 상태로 진행하기 위해 해야 할 일(해당하는 경우))
- ENX 협회의 다음 작업
  (귀사의 상태를 격상시키기 위해 ENX 협회에서 해야 할 일(해당하는 경우))
- 다음 상태
  (해당하는 경우)

아래 그림에는 한 상태에서 다음 상태로 진행하기 위해 수행하는 작업이 나와 있습니다.

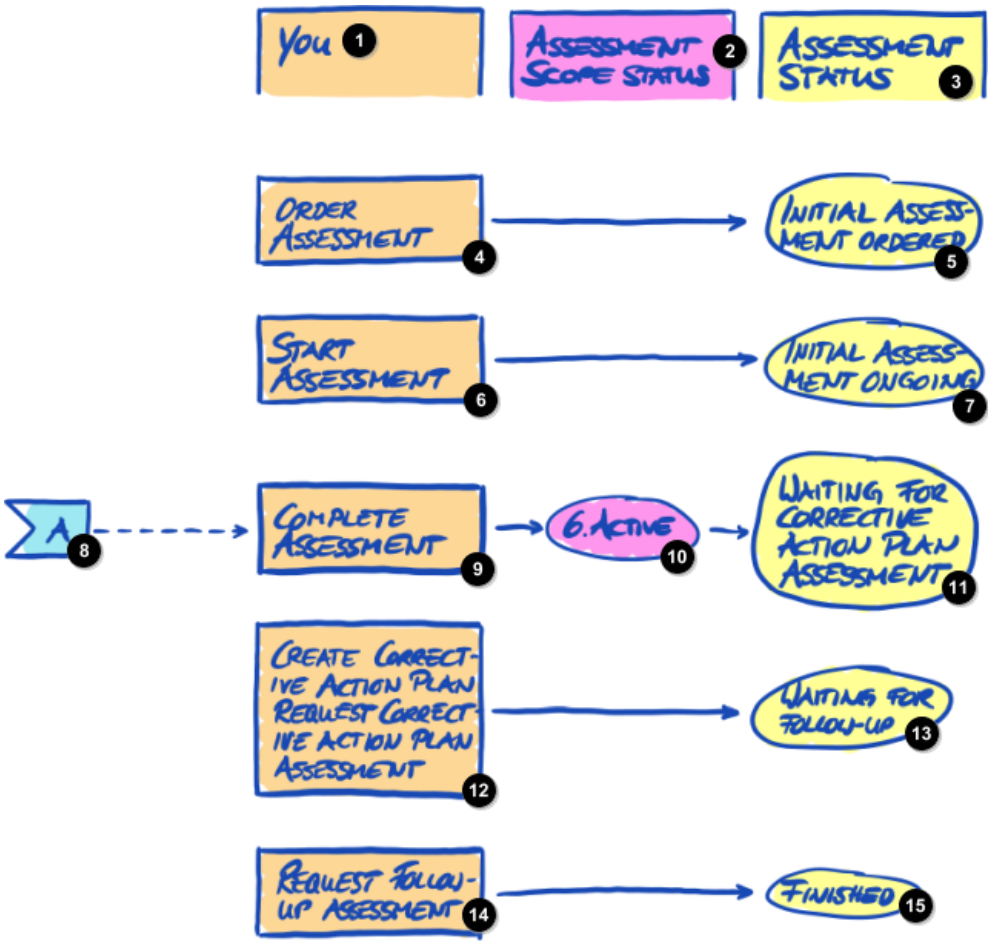


그림 36. 평가 상태 개요

1. 귀사
2. 평가 범위 상태
3. 평가 상태
4. 평가 주문
5. 첫 평가 주문됨
6. 평가 시작
7. 첫 평가 진행 중
8. A
9. 평가 완료
10. 6. 활성
11. 시정 조치 계획 평가 대기 중
12. 시정 조치 계획 수립
    시정 조치 계획 평가 요청
13. 후속 평가 대기 중
14. 후속 평가 요청
15. 마침

위 그림에서 다른 페이지 참조인 “A”는 “활성” 평가 범위 상태를 “시정 조치 계획 평가 대기 중” 평가 상태와 연결합니다. “평가 범위 상태”에 대한 자세한 내용은 다음을 참조하십시오. 섹션 7.5, “부록: Assessment scope status(🇰🇷 평가 범위 상태)”.

7.6.2. Assessment status “Initial assessment ordered” (🇰🇷 평가 상태 “첫 평가 주문됨”)

상태	상황	귀사의 다음 작업	ENX 협회의 다음 작업	다음 상태
첫 평가 주문됨	TISAX 감사 제공자 중 하나를 선택하고 첫 평가를 주문했습니다.	TISAX 평가 프로세스를 계속 진행합니다.	없음	첫 평가 진행 중

7.6.3. Assessment status “Initial assessment ongoing” (🇰🇷 평가 상태 “첫 평가 진행 중”)

상태	상황	귀사의 다음 작업	ENX 협회의 다음 작업	다음 상태
첫 평가 진행 중	첫 평가가 ▪ 시작되었거나, ▪ 완료되었지만 감사 제공자가 아직 TISAX 평가 보고서를 제출하지 않았습니다.	없음	없음	시정 조치 계획 평가 대기 중(해당하는 경우)

7.6.4. Assessment status “Waiting for corrective action plan assessment” (평가 상태 “시정 조치 계획 평가 대기 중”)

상태	상황	귀사의 다음 작업	ENX 협회의 다음 작업	다음 상태
시정 조치 계획 평가 대기 중	감사 제공자가 첫 평가를 실시했습니다. 감사 제공자가 TISAX 평가 보고서를 ENX 협회에 제출했습니다. 평가 결과가 (중대한/사소한) 미준수입니다.	시정 조치 계획을 수립합니다. 시정 조치를 시작합니다. 시정 조치 계획 평가를 요청합니다.	없음	후속 평가 대기 중(해당하는 경우)

“시정 조치 계획 평가 대기 중” 평가 상태는 9개월로 제한됩니다. 자세한 내용은 다음을 참조하십시오. 섹션 5.4.9.3, “시정 조치 계획 요구 사항”.

7.6.5. Assessment status “Waiting for follow-up” (“후속 평가 대기 중” 평가 상태)

상태	상황	귀사의 다음 작업	ENX 협회의 다음 작업	다음 상태
후속 평가 대기 중	감사 제공자가 시정 조치 계획을 승인했습니다. 시정 조치를 이행했습니다.	후속 평가를 요청합니다.	없음	마침

“후속 평가 대기 중” 평가 상태는 9개월로 제한됩니다. 자세한 내용은 다음을 참조하십시오. 섹션 5.4.9.3, “시정 조치 계획 요구 사항”.

7.6.6. Assessment status “Finished” (평가 상태 “마침”)

상태	상황	귀사의 다음 작업	ENX 협회의 다음 작업	다음 상태
마침	감사 제공자가 후속 평가를 실시했습니다. 평가 결과에 미준수 사항이 없습니다. 감사 제공자가 TISAX 평가 보고서를 ENX 협회에 제출했습니다.	평가 결과를 게시하고 공유합니다.	없음	해당 없음

7.7. 부록: “사전 평가”와 “격차 분석”이 권장되지 않는 이유

일반적으로, 감사 제공자에게 “사전 평가” 또는 “격차(gap) 분석”을 해 달라고 요청하는 것은 권장되지 않습니다. 대부분의 경우에는 TISAX 평가 프로세스를 곧바로 시작하면 더 합리적입니다.

이어지는 내용에서는 가장 일반적인 우려 사항에 답합니다.

사전 평가를 고려하는 이유는 무엇입니까?

1. 고객이 잠재적으로 불리한 평가 결과를 볼 수 있다고 우려하십니까?

   귀사의 평가 결과를 누가 볼 수 있는지에 대한 전적인 결정권은 귀사에 있습니다. 감사 제공자가 ENX 포털에 무언가를 업로드할 수 있는지도 귀사에서 결정합니다. 아무도 보면 안 되는 것은 (물론 작성자를 제외하고) 아무도 보지 않습니다.

   게다가 감사 제공자는 항상 TISAX 평가 보고서의 첫 두 섹션만 업로드하고 상세 평가 결과는 어차피 업로드하지 않습니다.

2. 사전 평가를 하면 비용이 절약될 수 있다고 생각하십니까?
   - 사전 평가를 할 경우:
     - 사전 평가 비용 지불
     - 미준수 사항을 해결하기 위한 내부 비용이 발생할 수 있음
     - 전체 TISAX 평가(“첫 평가”) 비용 지불

     발견되는 문제가 없어도 두 차례의 전체 평가 비용은 항상 지불합니다.

   - TISAX 평가부터 시작할 경우:
     - “첫 평가” 비용 지불
     - 발견된 문제를 해결하기 위한 내부 비용이 발생할 수 있음
     - 감사관이 첫 평가의 미준수 사항이 해결되었는지 여부에만 집중하는 소위 “후속 평가”에 대해 지불하는 비용이 (첫 평가보다) 훨씬 더 적을 수 있음

     발견된 문제가 있어도 전체 평가와 짧은 후속 평가 비용만 지불

3. 평가에 불합격하여 영구적인 영향이 있을 수 있다고 생각하십니까?

   평가를 원하는 횟수만큼 받을 수 있기 때문에 영구적으로 불합격할 수는 없습니다. 평가 결과가 기대를 충족하지 않거나, 시정 조치를 통해 미준수 사항을 해결해야 하는 기간인 구 개월 이내에 해결하지 못할 경우, 간단히 실패한 시도를 사전 평가라고 간주하고 새로 시작하면 됩니다. 그리고 첫 번째 시도의 결과는 아무도

보지 않아도 됩니다. 합격한 평가의 평가 결과만 공유하면 됩니다.

추가로 고려할 사항:

- 평가 결과가 예상보다 더 좋으면 임시 TISAX 레이블을 받을 수 있습니다. 이 레이블을 파트너와 직접 공유할 수 있습니다. 사전 평가의 경우 이렇게 할 수 없습니다.
- 사전 평가를 실시하는 감사 제공자가 TISAX 평가도 실시해야 하는 경우, 이 제공자는 귀사에 컨설팅 서비스를 제공할 수 없습니다. 그렇지 않으면 TISAX 평가를 실시할 다른 감사 제공자를 선택해야 합니다.

감사를 받은 대부분의 회사에는 사전 평가가 이득이 되지 않지만, 사전 평가는 다음과 같은 장점도 있습니다.

감사관은

- 귀사에서 자신 없어 하는 ISMS의 중요한 측면에 집중할 수 있습니다.
- 일반적인 경우보다 더 많은 시간을 들여서 더 많은 통찰력을 얻을 수 있습니다.
- 발견된 문제를 다르게 문서화할 수 있습니다.

TISAX 평가 프로세스에 대한 섹션을 읽고 나면 위에 언급된 이유를 더욱 쉽게 이해할 수 있을 것입니다.

7.8. 부록: 맞춤 범위

거의 모든 TISAX 참가자가 표준 범위를 선택합니다. 하지만 특정한 드문 상황에는 맞춤 범위를 선택해야 할 수 있습니다.

두 가지 유형의 맞춤 범위가 있습니다.

7.8.1. 맞춤 확장 범위

범위를 직접 확장할 수 있습니다. 맞춤 확장 범위에는 표준 범위보다 더 많은 것이 포함됩니다. 감사 제공자가 더 많은 점검을 수행합니다.

목적: 맞춤 확장 범위는 TISAX 평가를 내부 용도로 사용하거나 자동차 산업 밖에서 사용하려는 경우에 관련이 있을 수 있습니다.

TISAX 레이블과 결과 공유: 맞춤 확장 범위에는 항상 표준 범위가 포함됩니다. 그러므로 맞춤 확장 범위는 TISAX 레이블을 받게 됩니다[35]. 그래도 다른 TISAX 참가자들은 평가 결과를 받아들일 것입니다.

설명: 표준 범위에는 미리 정의된 설명이 있지만, 맞춤 확장 범위가 필요한 경우 범위 설명을 직접 작성해야 합니다.

7.8.2. 전체 맞춤 범위

귀사에서 자체 범위를 완전히 정의할 수 있습니다.

목적: 귀사에 다른 평가 범위에 속하고 특정 현장(데이터 센터 등)에서 서비스를 사용하는 위치가 있는 경우, 해당 서비스에 대해 전체 맞춤 범위를 사용할 수 있습니다. 따라서 TISAX 감사 제공자는 서비스의 전체 맞춤 범위에 대한 평가 결과를 쉽게 다시 사용할 수 있습니다.

예: 귀사에 (다른 범위의 일부일 수 있는) 여러 위치가 있고, 이런 위치 중 하나에 중앙 IT 부서가 있습니다. IT 부서에 대해서만 전체 맞춤 범위를 정의하면 평가 결과를 각각 다른 범위에 다시 사용하기가 더 쉬워질 수 있습니다.

TISAX 레이블과 결과 공유: 전체 맞춤 범위에 대한 TISAX 레이블은 수여되지 않습니다. 평가 결과는 ENX 포털에 날짜, 유효 기간, 그리고 전체 평가 결과가 준수인지 미준수인지 여부와 함께 기록됩니다. 이런 평가 결과를 공유할 수 있습니다. 하지만 TISAX 레이블 없이 평가 결과를 공유하면 대부분의 수신인에게 평가에 “불합격” 한 것처럼 보일 수 있습니다. 다른 TISAX 참가자들은 일반적으로 전체 맞춤 범위의 평가 결과를 받아들이지 않습니다.

설명: 맞춤 확장 범위와 마찬가지로, 전체 맞춤 범위가 필요한 경우 범위 설명을 직접 작성해야 합니다.

중요한 참고 사항:

전체 맞춤 범위가 얼마나 드물게 사용되는지 강조하기 위해 설명하면, 감사 제공자가 전체 맞춤 범위를 표준 범위로 되돌릴 확률은 98%에 이릅니다. 감사 제공자의 조언을 받지 않고 전체 맞춤 범위를 선택하여 성공한 참가자는 없습니다.

전체 맞춤 범위를 사용한 평가에는 TISAX 레이블이 수여되지 않습니다. 그러므로 ENX 협회에서는 일반적으로 전체 맞춤 범위를 선택하지 않을 것을 권장하며, 주된 이유는 다른 참가자들이 일반적으로 전체 맞춤 범위를 사용한 평가 결과를 받아들이지 않기 때문입니다. 파트너가 결과를 받아들일 것이고 특정 범위 설명에 동의했음을 분명히 확인하지 않고 전체 맞춤 범위를 선택하지 마십시오.

7.9. 부록: 참가자 데이터 수명 주기 관리

이어지는 내용에서는 참가자 데이터에 관련된 사항이 변경될 경우에 해야 할 일에 대해 설명합니다.

7.9.1. 참가자 데이터에 액세스할 수 없게 됨(ENX 포털)

귀사에 ENX 포털에 액세스할 권한이 있는 사람이 없어서 참가자 데이터가 방치되는 경우 ENX 협회에 문의하십시오. 귀사의 참가자 데이터에 다시 액세스할 수 있게 도와 드릴 수 있게 노력하겠습니다.

7.9.2. 연락 담당자 관리

포털 계정이 있는 귀사의 주 참가자 연락 담당자와 그 외 모든 “관리 책임자”는 언제든지 ENX 포털로 이동하여 다음 작업을 수행할 수 있습니다.

- 새 연락 담당자 추가
- 기존 연락 담당자 삭제
- 기존 연락 담당자의 연락 담당자 세부 정보 변경

7.9.2.1. 새 연락 담당자를 추가하는 방법

새 연락 담당자를 추가하려면 다음 절차를 따르십시오.

1. ENX 포털에 로그인합니다.
2. 주 탐색 모음으로 이동한 후 “MY TISAX”(“내 TISAX”)를 선택합니다.
3. 드롭다운 메뉴에서 “ADMINISTRATORS”(“관리자”)를 선택합니다.
4. “Create new TISAX Administrator”(“새 TISAX 관리자 만들기”) 버튼을 클릭합니다.
5. 연락 담당자의 데이터를 입력합니다.
6. “Save Contact”(“연락 담당자 저장”) 버튼을 클릭합니다.
7. 표로 이동하여 연락 담당자가 있는 행을 표에서 찾습니다.
8. 표에서 연락 담당자가 있는 행 끝으로 이동하여 아래쪽 화살표가 있는 버튼을 클릭합니다 .
9. “Edit TISAX Administrator”(“TISAX 관리자 편집”)를 선택합니다.
10. 새 창(“Edit TISAX Contact”(“TISAX 연락 담당자 편집”))에서 “ENX PORTAL ACCESS”(“ENX 포털 액세스”) 섹션까지 아래로 스크롤합니다.
11. “Yes”(“예”)를 선택합니다.

12. “WEB ROLES”(“웹 역할”) 섹션이 나타나면 “Add Role”(“역할 추가”) 버튼을 클릭합니다.
13. 할당할 역할(예: “TISAX Administrator”(“TISAX 관리자”))을 선택합니다.
14. “Add Role(역할 추가)” 버튼을 클릭합니다.
15. “Save Contact(연락 담당자 저장)” 버튼을 클릭합니다.

7.9.2.2. 기존 연락 담당자를 삭제하는 방법

기존 연락 담당자를 삭제하려면 다음 절차를 따르십시오.

1. ENX 포털에 로그인합니다.
2. 주 탐색 모음으로 이동한 후 “MY TISAX”(“내 TISAX”)를 선택합니다.
3. 드롭다운 메뉴에서 “ADMINISTRATORS”(“관리자”)를 선택합니다.
4. 표로 이동하여 연락 담당자가 있는 행을 표에서 찾습니다.
5. 표에서 연락 담당자가 있는 행 끝으로 이동하여 아래쪽 화살표가 있는 버튼을 클릭합니다.
6. “Delete TISAX Administrator”(“TISAX 관리자 삭제”)를 선택합니다.
7. 확인 요청이 표시되면 “Delete”(“삭제”) 버튼을 클릭합니다.

7.9.2.3. 기존 연락 담당자 세부 정보를 업데이트하는 방법

기존 연락 담당자의 세부 정보를 업데이트하려면 다음 절차를 따르십시오.

1. ENX 포털에 로그인합니다.
2. 주 탐색 모음으로 이동한 후 “MY TISAX”(“내 TISAX”)를 선택합니다.
3. 드롭다운 메뉴에서 “ADMINISTRATORS”(“관리자”)를 선택합니다.
4. 표로 이동하여 연락 담당자가 있는 행을 표에서 찾습니다.
5. 표에서 연락 담당자가 있는 행 끝으로 이동하여 아래쪽 화살표가 있는 버튼을 클릭합니다 .
6. “Edit TISAX Administrator”(“TISAX 관리자 편집”)를 선택합니다.
7. 세부 정보를 업데이트합니다.
8. “Save Contact”(“연락 담당자 저장”) 버튼을 클릭합니다.

7.9.3. 위치 관리

포털 계정이 있는 귀사의 주 참가자 연락 담당자와 그 외 모든 “관리 책임자”는 언제든지 ENX 포털로 이동하여 다음을 요청할 수 있습니다.

- 회사 이름 변경
- 위치 변경(이동/이전)
- 거리 이름 변경
- 새 위치 추가

이어지는 내용에서는 필요한 단계에 대해 설명합니다.

참고:

- TISAX에서는 회사 이름과 주소의 조합으로 “위치”를 정의합니다.
- 각 위치마다 “위치 ID”가 있습니다. (위치 ID는 항상 “L”로 시작하고, 길이는

6자입니다. 예: L1L3XY)

- 회사가 현재 주소에서 새 주소로 이전하면 이전 위치가 더 이상 유효하지 않습니다.

중요한 참고 사항:

ENX 포털에서 “Save Location(위치 저장)” 버튼을 클릭한 후에는 위치를 더 이상 직접 변경할 수 없습니다. 아래에 서술된 상황에는 변경을 요청할 수 있습니다.

7.9.3.1. 회사 이름 변경을 요청하는 방법

상황:	귀사의 이름이 변경되었습니다.
예시:	이전 회사 이름은 “ACME Tires Corporation” 입니다. 새 회사 이름은 “ACME Corporation” 입니다.

회사 이름 변경을 요청하려면 다음 절차를 따르십시오.

1. ENX 포털에 로그인합니다.
2. 주 탐색 모음으로 이동한 후 “MY TISAX”(“내 TISAX”)를 선택합니다.
3. 드롭다운 메뉴에서 “LOCATIONS”(“위치”)를 선택합니다.
4. 표로 이동하여 위치가 있는 행을 표에서 찾습니다.
5. 표에서 위치가 있는 행 끝으로 이동하여 아래쪽 화살표가 있는 버튼을 클릭합니다.
6. “Request Change”(“변경 요청”)를 선택합니다.
7. 새 창(“Request Change”(“변경 요청”))에서 “Subject of the change”(“변경 대상”) 양식 필드로 이동한 후 드롭다운 메뉴를 열고 “Company Name”(“회사 이름”)을 선택합니다.
8. 양식을 계속 작성합니다.
9. 양식을 제출합니다.

ENX 협회에서 요청 사항을 확인하고, 가능한 경우 회사 이름 변경 요청을 수락하고, 변경되면 귀사에 알립니다.

7.9.3.2. 위치 변경을 요청하는 방법

상황:	회사가 새 위치로 이전했습니다.
예시:	이전 위치는 “ACME Corporation, Bockenheimer Landstraße 97-99, 60325 Frankfurt, Germany” 입니다. 새 위치는 “ACME Corporation, Behrenstraße 35, 10117 Berlin, Germany” 입니다.

중요한 참고 사항:

공식 정부 기관에서 위치의 거리명을 변경하는 경우, 섹션 7.9.3.3, “거리 이름 변경을 요청하는 방법”에서 자세한 내용을 참조하십시오.

위치 중 하나가 새 주소로 이전되는 경우, 다음 절차를 따르십시오.

1. 새 위치 만들기:
   a. ENX 포털에 로그인합니다.
   b. 주 탐색 모음으로 이동한 후 “MY TISAX”(“내 TISAX”)를 선택합니다.
   c. 드롭다운 메뉴에서 “Locations”(“위치”)를 선택합니다.

d. “Create TISAX Location”(“TISAX 위치 만들기”) 버튼을 클릭합니다.

e. 새 창(“CREATE TISAX LOCATION”(“TISAX 위치 만들기”))에서 새 위치의 세부 정보를 양식에 입력합니다.

f. “Save Location”(“위치 저장”) 버튼을 클릭합니다.

2. 새로 만든 “Location ID”(“위치 ID”)를 기억합니다. “MY LOCATIONS”(“내 위치”) 표의 첫 번째 열에서 “위치 ID”를 확인할 수 있습니다. 감사 제공자가 ENX 포털에서 귀사의 평가 범위를 업데이트하려면 “위치 ID”가 필요합니다.

3. 감사 제공자에게 위치 이전에 대해 알립니다(이전 위치와 새 위치의 “위치 ID” 제공). 평가를 이미 완료하셨습니까?

a. 아직 완료하지 않은 경우, 위치 변경에 관해 수행해야 하는 다른 작업은 없습니다.

b. 완료한 경우, 감사 제공자에게 “범위 확장 평가”(“scope extension assessment”)를 요청해야 합니다. 자세한 내용은 다음을 참조하십시오. 섹션 7.10, “부록: 범위 확장 평가”.

감사 제공자가 ENX 포털에서 요청을 확인하고 귀사의 평가 범위를 업데이트합니다.

참고:

감사 제공자는 귀사에서 이미 해당 감사 제공자에게 평가를 주문한 경우에만 평가 범위를 업데이트할 수 있습니다.

7.9.3.3. 거리 이름 변경을 요청하는 방법

상황:	위치의 거리 이름이 변경되었습니다. 귀사는 아직도 같은 물리적 장소에 있습니다.
예시:	이전 위치는 “ACME Corporation, Bockenheimer Landstraße 97-99, 60325 Frankfurt, Germany” 입니다. 새 위치는 “ACME Corporation, Behrenstraße 97-99, 60325 Frankfurt, Germany” 입니다.

공식 정부 기관에서 위치의 거리명을 변경하는 경우, 다음 절차를 따르십시오.

1. ENX 포털에 로그인합니다.
2. 주 탐색 모음으로 이동한 후 “MY TISAX”(“내 TISAX”)를 선택합니다.
3. 드롭다운 메뉴에서 “Locations”(“위치”)를 선택합니다.
4. 표로 이동하여 위치가 있는 행을 표에서 찾습니다.
5. 표에서 위치가 있는 행 끝으로 이동하여 아래쪽 화살표가 있는 버튼을 클릭합니다.
6. “Request Change”(“변경 요청”)를 선택합니다.
7. 새 창(“Request Change”(“변경 요청”))에서 “Subject of the change”(“변경 대상”) 양식 필드로 이동한 후 드롭다운 메뉴를 열고 “Address”(“주소”)를 선택합니다.
8. 양식을 계속 작성합니다.
9. 양식을 제출합니다.

ENX 협회에서 요청 사항을 확인하고, 가능한 경우 거리 이름 변경 요청을 수락하고, 변경되면 귀사에 알립니다.

중요한 참고 사항:

이 절차는 귀사가 아직 같은 물리적 장소에 있지만 공식 정부 기관에서 거리 이름을 변경한 경우에만 해당합니다.
새 위치로 이동한 경우, 자세한 내용은 다음을 참조하십시오. 섹션 7.9.3.2, “위치 변경을

요청하는 방법”

7.9.3.4. 위치를 더 추가하는 방법

기존 TISAX 레이블의 유효 기간 도중에 위치를 추가할 경우 “범위 확장 평가”(“scope extension assessment”)를 감사 제공자에게 요청할 수 있습니다.

자세한 내용은 다음을 참조하십시오. 섹션 7.10, “부록: 범위 확장 평가” .

7.10. 부록: 범위 확장 평가

섹션 5.4.3, “TISAX 평가 유형”에서 설명한 표준 평가 유형 외에, “범위 확장 평가”(“scope extension assessment”) 라는 다른 특별 평가 유형이 하나 더 있습니다.

다음을 하나 이상 추가하려면 기존 TISAX 평가 범위를 확장할 수 있습니다.

- 평가 목표, 또는
- 위치.

“범위 확장 평가”를 실시할 다른 감사 제공자를 선택할 수 없습니다. 이 평가는 표준 평가 유형과 유사합니다. 하지만 감사 제공자는 이전 평가의 해당하는 결과를 다시 사용하는 방법을 고려할 가능성이 큽니다.

범위 확장 평가가 미준수 사항 없이 끝나면 감사 제공자가 다음 작업을 수행합니다.

- ENX 포털에서 귀사의 평가 범위를 업데이트합니다.
- 범위 확장 평가 보고서를 발행합니다.

범위 확장 평가는 기존 TISAX 레이블의 원래 유효 기간을 연장하지 않습니다.

참고:

범위 확장 평가의 이유가 위치 이전 또는 위치 추가인 경우, ENX 포털에서 새 위치를 만들어야 합니다. “위치 발췌 자료” 나 최소한 “위치 ID” 를 감사 제공자에게 제공하십시오.
각 위치마다 “위치 ID” 가 있습니다. (위치 ID는 항상 “L” 로 시작하고, 길이는 6자입니다. 예: L1L3XY) 감사 제공자가 ENX 포털에서 귀사의 평가 결과를 업데이트하려면 위치 ID가 필요합니다.

7.11. 부록: ISA 수명 주기 관리

ENX 워킹그룹이 ISA를 유지관리하고 있습니다.

다음과 같은 사실을 알면 유용할 수 있습니다.

- VDA에서 새 버전을 공식 발행합니다.
- 감사 제공자는 귀사에서 첫 평가를 주문할 때 유효한 ISA 버전을 사용합니다.
- 상호 합의에 따라, 주문 후 첫 평가를 시작하기 전에 더 새로운 ISA 버전이 발행될 경우 이 버전을 사용할 수 있습니다.
- 특정 ISA 버전의 발행 날짜를 “표지” Excel 시트에서 확인할 수 있습니다.
  - 예시:
    버전: 5.0 | 4차 개정판 | 2021-04-16

7.12. 부록: 유용한 문서

이 섹션에는 ENX 협회에서 유용하다고 간주하는 문서가 나열되어 있습니다.

- 백서 “Harmonization of classification levels(비밀 등급의 조화)”

  “이 백서에서는 비밀 보호(권한이 없는 사람, 조직 또는 프로세스가 정보에 액세스할 수 없게 하는 것을 의미) 목표에 초점을 맞춘 계획의 결정에 대한 정보 보안 워킹그룹의 제안에 대해 설명합니다. 또한, 이 백서에서는 가용성, 무결성 및 신뢰성 같은 보호 목표에 초점을 맞추지 않습니다.

  발행: Verband der Automobilindustrie e.V.(“독일 자동차 산업 협회”)

  제공 언어: 영어, 독일어

  https://www.vda.de/en/news/publications/publication/harmonization-of-classification-levels
  https://www.vda.de/de/aktuelles/publikationen/publication/whitepaper--harmonisierung-der-klassifizierungsstufen-

- 백서 “Information Security Risk Management(정보 보안 위험 관리)”

  “이 백서의 목표는 자동차 산업의 회사에 위험 지향적인 정보 보안 관리에 관해 알리고 이런 회사가 효과적인 정보 보안 위험 관리를 확립할 수 있도록 지원하는 것입니다. 이 백서는 VDA ISA 통제 문항 1.4.1의 요구 사항을 충족하기 위해 TISAX 평가를 준비하거나 실시하는 조직을 지원하기 위해 작성되었습니다. 이 백서의 내용은 필수 요구 사항이 아닌 이행 권장 사항으로 간주해야 합니다.

  발행: Verband der Automobilindustrie e.V.(“독일 자동차 산업 협회”)

  제공 언어: 영어, 독일어

  https://www.vda.de/en/news/publications/publication/white-paper--information-security-risk-management-
  https://www.vda.de/de/aktuelles/publikationen/publication/whitepaper--risikomanagement-in-der-informationssicherheit-

7.13. 부록: 불만 사항 관리

7.13.1. 불만의 원인

ENX 협회에서는 불만 사항을 다음과 같이 둘로 나눠서 관리합니다.

1. ENX 협회⊠—⊠TISAX를 관리하는 조직
2. 감사 제공자⊠—⊠TISAX 평가를 실시하는 조직

7.13.1.1. ENX 협회에 대한 불만 사항

ENX 협회에 대한 불만 사항이 있는 경우, “근무 중인 TISAX 관리자”에게 문의하십시오(아래의 상세 연락처 참조).

7.13.1.2. 감사 제공자에 대한 불만 사항

첫째, 감사관과 직접 문제를 해결하려고 해야 합니다.

다음 단계는 감사 제공자의 TISAX 책임자와 함께 진행해야 합니다.

그 후의 다음 연락 담당자는 감사 제공자의 품질 관리 책임자가 될 것입니다.

그래도 문제가 해결되지 않으면 ENX 협회의 “근무 중인 TISAX 관리자”에게 문의해야 합니다(아래의 상세 연락처 참조).

“근무 중인 TISAX 관리자”의 상급자에게 문의하는 방법도 선택할 수 있습니다. 이런 경우에는 ENX 협회의 상무이사와 상의합니다.

VDA는 불만 사항을 관리하는 어떤 역할도 하지 않습니다.

참고:

감사 제공자는 킥오프 회의 중에 불만 사항을 접수할 권리에 대해 귀사에 알려야 합니다. 알리지 않으면 그 자체로 불만 사항을 접수할 이유가 됩니다.

7.13.1.3. 불만 사항 접수를 위한 요구 사항

ENX 협회의 관여를 원하는 경우, 다음과 같은 정보가 필요합니다.

- 누가 불만을 접수하려고 합니까?
  - 회사 이름
  - TISAX 참가자 ID
  - 연락 담당자(이름, 이메일 주소, 전화번호)
- 어느 평가에 해당합니까?
  - 평가 ID
  - 평가가 아직 ENX 포털에 기록되지 않은 경우: 범위 ID
- 감사 제공자가 누구입니까?
  - 감사 제공자 회사 이름
  - 감사관(들)의 이름
- 불만 사항이 무엇에 대한 것입니까?
  1. 감사 제공자의 업무 수행에 대한 일반적인 불만 사항
  2. 감사관의 접근방식에 대한 불만 사항
  3. 평가의 내용에 관한 불만 사항
- 평가의 내용에 관한 불만 사항의 경우: 어느 발견된 문제에 반대하십니까?
  - 통제(예: 1.6.1 "정보 보안 사건이 어느 정보까지 처리됩니까?")
  - 발견된 문제(전문)
  - 이의 제기 대상:
    - 컨트롤의 해석
    - 내용 관련 확인(사용 가능한 증거가 올바르게 평가되지 않음)
    - 위험 평가(적절성이 고려되지 않음)
  - 귀사에서 결과를 다르게 평가하는 근거

7.13.2. 불만 사항 관련 연락 담당자

“근무 중인 TISAX 관리자”에게 문의하십시오.

이메일 주소: tisax-complaints@enx.com

전화번호: +49 69 9866927-79

독일의 일반 영업 시간 중에 연락할 수 있습니다(UTC+01:00).

영어와 독일어로 문의할 수 있습니다.

8. 문서 수정 내역

2.7 버전

- 4개 국어(일본어, 포르투갈어(브라질), 이탈리아어, 한국어)가 더 추가됨
- HTML 버전에 언어 전환 기능 추가됨(오른쪽 상단 모서리)
- PDF 버전 레이아웃 개선됨
- 여러 섹션이 두 개의 새로운 비밀유지 평가 목표로 업데이트됨
- “평가 목표 목록” 섹션 업데이트됨(평가 목표 “Special data”의 표현이 수정되고 레이블 전환에 관한 참고 사항 추가됨)
- 오타 수정됨

2.6 버전

- 이 버전에 추가된 평가 목표와 레이블에 관한 일반적인 참고 사항: 이전 버전에서는 평가 목표와 레이블에 긴 “공식 이름”과 “짧은 이름”(예: “필요한 보호 수준이 높은 정보의 처리”와 “Info high”)이 있었습니다. 사람들이 대부분 짧은 이름만 사용했기 때문에 이제 짧은 이름이 “공식 이름”이 되었습니다. 이전의 긴 이름을 이제 “설명”이라고 합니다. 또한 ENX 포털과 TISAX 참가자 안내서의 모든 번역본에서는 영문 공식 이름만 사용됩니다.
- “평가 목표 목록” 섹션이 “높은 가용성”과 “매우 높은 가용성”이라는 두 평가 목표를 포함하도록 업데이트되고 “그림 6. TISAX 평가 목표(표 표시, 길고 짧은 형식)” 제거됨
- “평가 목표와 ISA” 섹션이 정보 보안 기준 카탈로그의 부분 집합만 “높은 가용성”과 “매우 높은 가용성”이라는 두 평가 목표에 해당한다는 사실을 반영하여 업데이트됨
- “평가 목표 및 각각의 종속성” 섹션 제거됨
- “평가 목표 선택” 섹션이 두 개의 평가 목표인 “높은 가용성”과 “매우 높은 가용성”을 포함하도록 업데이트됨
- “필요한 보호 수준과 평가 수준” 섹션이 “높은 가용성”과 “매우 높은 가용성”이라는 두 평가 목표를 포함하도록 업데이트되고 “표 5. ISA 기준 카탈로그 및 필요한 보호 수준과 TISAX 평가 목표 매핑” 제거됨
- “기준 카탈로그” 섹션이 “높은 가용성”과 “매우 높은 가용성”이라는 두 평가 목표를 포함하도록 업데이트됨
- “요구 사항” 섹션이 정보 보안 기준 카탈로그의 부분 집합만 “높은 가용성”과 “매우 높은 가용성”이라는 두 평가 목표에 해당한다는 사실을 반영하여 업데이트됨
- “TISAX 레이블 계층 구조” 섹션이 이제는 계층 구조가 존재하는 경우가 적다는 사실을 반영하여 업데이트되고 “그림 36. TISAX 평가 목표와 TISAX 레이블(종속성과 계층 구조)” 제거됨
- “부록: 유용한 문서” 섹션이 링크 변경을 반영하여 업데이트됨
- 여러 부수적인 자세한 설명과 작은 수정 사항
- 오타 수정됨

2.5 1 버전

- 깨진 링크 수정됨

2.5 버전

- “위치 관리” 섹션 추가됨

- “부록: 유용한 문서” 섹션이 링크 변경을 반영하여 업데이트됨

2.4 버전

- TISAX 평가 프로세스의 최대 기간에 관한 부정확한 내용이 섹션 3.1, “개요”에서 제거됨
- “TISAX 보고서”의 이름이 “TISAX 평가 보고서”로 변경됨
- ISO 27001과 TISAX의 차이점에 관한 참고 사항 업데이트됨
- “범위 설명” 섹션이 업데이트되고, 맞춤 범위 섹션이 부록으로 이동됨
- “표준 범위 설명”이 2.0 버전으로 업데이트됨
- “게시 및 공유” 섹션이 평가 상태 공유에 대한 참고 사항을 포함하도록 업데이트됨
- “필요한 보호 수준과 평가 수준” 섹션이 “평가 수준 2.5”, “비디오로 지원되는 원격 평가 방법”, AL 2와 AL 3의 차이점, 타당성 점검과 확인 비교에 대한 내용을 포함하도록 업데이트됨
- 등록 프로세스 시작으로 연결되는 링크가 업데이트됨
- “포털 계정” 섹션이 변경된 초대 프로세스를 반영하여 업데이트됨
- ISA 문서 다운로드 링크 변경됨(이제 enx.com에서도 다운로드 가능)
- “오퍼 평가” 섹션이 비용 추산 근거를 포함하도록 업데이트됨
- “킥오프 회의” 섹션 추가됨(“첫 공식 시작 회의” 섹션에서 여기로 이동된 내용 포함)
- “준수에 대한 설명” 섹션이 네 가지 유형의 발견된 문제에 대한 새로운 표를 포함하도록 업데이트됨
- “첫 평가” 섹션이 시간 제한에 관한 참고 사항을 포함하도록 업데이트됨
- “TISAX 평가 보고서” 섹션이 예방적 시정 조치 계획에 관한 참고 사항을 포함하도록 업데이트됨
- “시정 조치 계획 준비” 섹션이 “발견된 문제” 및 “근본 원인” 요구 사항과 시정 조치 계획 템플릿에 관한 참고 사항을 포함하도록 업데이트됨
- “시정 조치 계획 평가” 섹션이 유일한 커뮤니케이션 수단으로 사용되는 이메일에 관한 비고를 포함하도록 업데이트됨
- “시정 조치 계획 평가를 위한 전제 조건” 섹션의 이름이 “시정 조치 계획 평가의 이유”로 변경되고 이유가 두 개 추가됨
- “임시 TISAX 레이블” 섹션이 유효 기간에 관한 예와 자세한 설명을 포함하도록 업데이트됨
- “TISAX 보고서” 섹션의 이름이 “TISAX 평가 보고서”로 변경됨
- “TISAX 레이블 갱신” 섹션이 ENX 포털에서 위치 기록을 재사용하는 것에 관한 참고 사항을 포함하도록 업데이트됨
- “부록: “사전 평가”와 “격차 분석”이 권장되지 않는 이유” 섹션이 추가됨
- “부록: 맞춤 범위” 섹션 추가됨(“확장 범위”와 “좁힌 범위”가 “고객 확장 범위”와 “전체 맞춤 범위”로 대체됨
- “부록: 범위 확장 평가” 섹션이 위치 기록을 참가자의 ENX 포털 계정에 추가하는 이유와 관련 참고 사항을 포함하도록 업데이트됨
- “부록: ISA 수명 주기 관리” 섹션이 현재 상황을 반영하여 업데이트됨
- “부록: 유용한 문서” 섹션이 링크 변경을 반영하여 업데이트됨
- “부록: 불만 사항 관리” 섹션 추가됨
- 이제 전화번호를 클릭할 수 있음
- 여러 부수적인 자세한 설명과 작은 수정 사항
- 오타 수정됨

- TISAX 감사 제공자를 위한 참고 사항: 이 업데이트는 ENX 문서 ID 612, 2.1 버전 기준입니다.

2.3 버전

- 부제 표현 수정
- 안내서의 주 형식을 Word/PDF에서 HTML로 변경
- 추가 번역본 사용 가능(중국어와 프랑스어, 다음 항목 참조)
- “TISAX 참가자 안내서의 다른 언어 및 형식” 섹션 추가됨
- ENX 홈페이지로 연결되는 모든 링크가 "https://portal.enx.com"에서 "https://enx.com"으로 변경됨(이전 링크 계속 사용 가능)
- “VDA ISA”가 “ISA”가 됨
- 섹션 5.2, “ISA 기반 자가 평가” 섹션이 ISA 5 버전에 도입된 변경 사항을 반영하여 업데이트됨
- 평가 목표를 나열하는 모든 표의 행 순서가 ISA 5에서 변경된 기준 카탈로그 순서와 일치하도록 변경됨
- 평가 목표를 나열한 그림이 기준 카탈로그 ISA 5의 변경된 순서와 일치하도록 업데이트됨
- “범위 맞춤 조정” 섹션 업데이트됨(그림 6, 오타 수정, 평가 목표 업데이트)
- “수수료” 섹션이 신용 카드 결제에 대한 정보를 포함하도록 업데이트됨
- “TISAX 평가 프로세스 다이어그램” 섹션 업데이트됨(그림 34, 관리되는 서비스 제공자에 대한 언급 제거됨)
- “부록: 유용한 문서” 섹션 업데이트됨(“Information Security Risk Management(정보 보안 위험 관리)” 백서 추가됨)

2.2 1 버전

- 오타 수정됨

2.2 버전

- 표지 인쇄 문제 수정됨
- 모든 ENX 협회 홈페이지 및 다운로드 링크 변경됨
- 이제 이탈리아어도 지원됨
- “맞춤 범위” 섹션 확장됨
- “범위 위치” 섹션 업데이트됨
- 평가 목표 “제3자에 연결” 제거됨. 그림 7, 9, 38 업데이트됨. 표 4, 5, 6, 8 업데이트됨
- “with assessment level(평가 수준 ~이(가) 포함됨)”이라는 표현이 “in assessment level(평가 수준 ~에 해당하는)”로 변경됨
- “필요한 보호 수준과 평가 수준” 섹션에서 “TISAX 활성화 목록”에 대한 언급 제거됨 (더 이상 해당되지 않음)
- “평가 목표와 자체 공급업체” 섹션 추가됨
- “참가자 연락 담당자” 섹션이 그룹 이메일 주소와 ENX 포털에서 참가자 데이터를 관리할 수 있게 연락 담당자를 초대하는 것에 관한 정보를 포함하도록 업데이트됨
- “평가 범위 등록” 섹션이 평가 범위 변경에 대한 정보를 포함하도록 업데이트됨
- “상태 정보” 섹션 업데이트됨(그림 12)
- “자가 평가 결과의 문제 해결” 섹션이 제3자의 외부 지원에 관한 정보를 포함하도록 업데이트됨

- “감사 가능 지역” 섹션이 감사 제공자 감사 가능 지역 표로 연결되는 링크를 포함하도록 업데이트됨
- “오퍼 요청” 섹션 업데이트됨
- “오퍼 평가” 섹션이 “사전 평가”에 관한 정보를 포함하도록 업데이트됨
- “TISAX 레이블 갱신” 섹션이 새 범위를 등록해야 하는 필요성에 관한 정보를 포함하도록 업데이트됨
- “교환(3 단계)” 섹션의 여러 하위 섹션이 ENX 포털의 인터페이스 변경 사항을 반영하여 업데이트됨
- “특정 참가자와 평가 결과 공유” 섹션이 공유 수준에 관한 권장 사항과 공유된 평가 결과의 자동 처리에 관한 참고 사항을 포함하도록 업데이트됨
- “TISAX 밖에서 평가 결과 공유” 섹션 추가됨
- “ISA 수명 주기 관리” 섹션 추가됨
- “부록: 평가 범위 상태” 섹션 업데이트됨(새 상태 “주문 대기 중”, “승인 대기 중” 상태의 이름이 “ENX 승인 대기 중”으로 변경됨, “승인됨” 상태의 이름이 “지불 대기 중”으로 변경됨, 그림 40)
- “부록: 확인 이메일 예시” 섹션 업데이트됨
- “부록: TISAX 범위 발췌 자료 예시” 섹션 업데이트됨
- “부록: 평가 상태” 섹션 업데이트됨(새 상태 “첫 평가 진행 중”, “후속 평가 대기 중” 상태의 이름이 “후속 평가 대기 중”으로 변경됨, 그림 41)
- “부록: Volkswagen 레거시 평가” 섹션(과 그에 대한 참조) 제거됨(더 이상 관련 없음)

2.1 2 버전

- “귀사의 결과 점수”와 “최고 결과 점수” “간격”의 공식 한도가 25%에서 30%로 수정됨

2.1 1 버전

- 오타 수정됨

2.1 버전

- “관리되는 서비스 제공자” 섹션 제거됨
- 새 TISAX 평가 목표/레이블(GDPR에 따른 데이터 보호 레이블, 프로토타입 레이블 두 개 대신 네 개, 이름 변경: 보호 수준 대신 필요한 보호 수준, 선택에 관한 조언 업데이트됨)
- ISA의 변경(4.0 → 4.1 버전)으로 인한 업데이트
- 새 문서 “TISAX Simplified Group Assessment(TISAX 간단 그룹 평가)”(본 안내서의 부록) 참조
- 위치 이름 및 범위 이름 지정에 대한 제안 추가됨
- “등록 수수료”의 이름이 “수수료”로 변경됨
- 부 연락 담당자에 대한 권장 사항 추가됨
- 수수료 부과 모델 선택 제거됨

맨 위로 돌아가기.

[1] TISAX 프로세스를 선제 조치로서 미리 거치는 방법을 고려해 볼 수 있습니다. 준비를 더 잘 하기 위해 이렇게 하는 회사들도 있습니다. 이미 TISAX 평가를 받았으면 온보딩 기간이 훨씬 짧아져서 TISAX 평가를 아직 받지 않은 경쟁업체보다 유리할 수 있습니다.

[2] “TISAX 레이블”은 평가 결과를 요약하는 개념이며, TISAX 프로세스의 결과물입니다. 자세한 내용은 섹션 5.4.14, “TISAX 레이블”을 참조하십시오.

[3] 등록 단계는 대부분 TISAX 참가자로 시작할 때 한 번만 거치면 됩니다. 평가 결과를 갱신하는 경우 등록 데이터를 업데이트하고 확인하기만 하면 됩니다.

[4] ENX 협회는 GTC에 적용된 변경 사항을 ENX 포털에 게시하고 등록된 연락 담당자에게 알립니다.

[5] 이 내용은 다른 모든 추가 계약(예: 행동 강령)에도 적용됩니다.

[6] 파트너에게는 현재 새로운 권한에 대해 자동으로 알리지 않습니다. 파트너가 평가 결과를 확인할 수 있게 된 후에 파트너에게 알리는 것이 좋습니다.

[7] 이 목록에 포함되려면 ENX 협회에 문의하십시오.

[8] 증거란 특정 요구 사항을 충족한다는 귀사의 주장을 뒷받침하는 것을 의미합니다. 증거는 대부분 문서입니다. 귀사에서는 분명 내부 문서를 증거로 사용할 것입니다.

[9] 평가 수준 2가 포함된 평가를 위한 면접 조사는 일반적으로 웹 회의를 통해 실시합니다. 귀사에서 요청할 경우 면접 조사를 현장에서 실시할 수 있습니다.

[10] 간단 그룹 평가를 위한 이론적인 최소 위치 수는 세 개입니다.

[11] 정보 보안 관리 시스템을 개선해야 할 것임을 이미 알고 있는 경우, 권장되는 최소 위치 수는 12개 이상입니다.

[12] 숫자와 문자가 혼동될 가능성을 방지하기 위해, 특정 문자(8과 B 등)는 참가자 ID에 사용할 수 없습니다. 하지만 오래된 참가자 ID에는 “G” 자가 포함되어 있을 수 있습니다.

[13] ISA에서는 기준 카탈로그를 “모듈”이라고도 합니다.

[14] 기초를 이루는 Excel 기능은 “데이터” 리본의 “개요” 섹션에 있습니다.

[15] 귀사를 위해 유사한 평가(ISO 27001 등)를 실시하는 감사 제공자 중에 TISAX 평가도 실시하는 데 관심이 있는 제공자가 있습니까? 있다면 본 안내서를 제공자와 공유하고 ENX 협회에 연락하여 TISAX 감사 제공자가 되기 위해 요구되는 사항에 대해 알아보라고 하십시오.

[16] ENX 협회의 목록에 포함되어 있지 않은 감사 제공자는 TISAX 평가를 실시할 수 없습니다.

[17] 평가 프로세스를 종료하면 TISAX 레이블을 받을 수 없습니다.

[18] 실제로 네 번째 유형인 “범위 확장 평가”가 있습니다. 이 평가는 특별한 경우에 해당하므로 부록의 다음 섹션에서 이 평가에 대해 자세히 설명합니다. 섹션 7.10, “부록: 범위 확장 평가”.

[19] 첫 평가의 공식 시작 회의에 대해서만 자세히 설명합니다. 나머지 TISAX 평가에 대해서는 감사 제공자가 이런 회의의 일정을 정하고 회의를 준비합니다.

[20] 감사 제공자에 따라 “킥오프 회의”와 “공식 시작 회의”를 동의어로 사용할 수도 있습니다.

[21] 첫 평가의 공식 종료 회의에 대해서만 자세히 설명합니다. 나머지 TISAX 평가에 대해서는 감사 제공자가 이런 회의의 일정을 정하고 회의를 준비합니다.

[22] 분쟁을 해결할 수 없는 경우 문제를 에스컬레이션할 수 있습니다. 자세히 알아보려면 섹션 7.13, “부록: 불만 사항 관리”에서 세부 정보를 더 확인하십시오.

[23] 감사 방법과 강도에 대한 자세한 내용은 다음을 참조하십시오. 섹션 4.3.3.5, “필요한 보호 수준과 평가 수준”.

[24] 분쟁을 해결할 수 없는 경우 문제를 에스컬레이션할 수 있습니다. 자세한 내용은 ENX 협회에 문의하십시오.

[25] 적절한 시정 조치를 정의한 경우에도 전체 평가 결과가 계속 “중대한 미준수”일 수 있습니다. 조치가 즉시 적용되지 않는/적용될 수 없는 경우에 그렇습니다.

[26] 이 내용은 물론 미준수 사항이 확인된 첫 평가에만 해당합니다. 첫 평가의 평가 결과가 “준수”인 경우 후속 평가는 불필요합니다.

[27] 이론적으로 이 날짜는 첫 평가가 끝난 후 9개월 뒤일 수 있습니다.

[28] 사실은 네 번째 유형인 “범위 확장 평가 보고서”도 있습니다. 이 유형은 특별한 경우에 해당하므로 다음 섹션에서 자세히 설명합니다. 섹션 7.10, “부록: 범위 확장 평가”.

[29] “TISAX 평가 보고서”는 모든 TISAX 감사 제공자가 사용해야 할 의무가 있는 템플릿을 기반으로 작성됩니다.

[30] ”갱신”이라는 단어는 오해의 소지가 있을 수 있습니다. TISAX 레이블을 3년 넘게 유지하려면 TISAX 프로세스를 다시 거쳐야 합니다. 이 프로세스는 새 평가 범위를 등록하는 것으로 시작됩니다.

[31] ENX 협회에서는 참가자 ID의 “TISAX 공개” 목록을 유지관리하지 않습니다. 그 이유는 비슷한 회사 이름이나 다른 “인적 오류” 때문에 잘못 공유될 가능성을 방지하기 위해서입니다. 그러므로 파트너에게 직접 연락하여 파트너의 참가자 ID를 확인해야 합니다.

[32] 파트너가 포털에 로그인하여 귀사에서 공유한 평가 결과를 능동적으로 조회해야 합니다. 파트너는 새로 공유된 평가 결과에 대한 자동 알림을 받지 않습니다.

[33] 이 규칙은 “TISAX 참가 일반 약관”(https://enx.com/tisaxgtcen.pdf)에 정의되어 있습니다.

[34] 평가 범위 상태가 “지불 대기 중”이거나 “등록됨”인 동안에는 “평가 관련 정보”에 평가 범위 위치, 평가 범위 상태 및 평가 목표가 포함됩니다. 평가 결과 또는 TISAX 레이블은 포함되지 않습니다.

[35] “TISAX 레이블”은 평가 결과를 요약하는 개념이며, TISAX 프로세스의 결과물입니다. 자세한 내용은 섹션 5.4.14, “TISAX 레이블”을 참조하십시오.