《TISAX 参与者手册》

目录

助您完成 TISAX 评估流程，并与合作伙伴共享评估结果

出版方

ENX Association
一家根据法国法律（1901 年）成立的协会。
注册地：Sous-préfecture de Boulogne-Billancourt，France；注册编号：w923004198

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

作者

Florian Gleich

联系方式

tisax@enx.com
+49 69 9866927-77

版本信息

日期: 2021-01-06
版本: 2.3 beta
类别: 公开
ENX doc ID: 602-CN

版权声明

1. 总述

1.1. 目的

欢迎了解 TISAX（Trusted Information Security Assessment Exchange，即“可信信息安全评估交换”）认证体系。

您的某个合作伙伴可能要求您证明，您的信息安全管理体系符合“VDA[1] ISA（德国汽车工业协会信息安全评估标准）”特定等级的要求，并且您亦希望了解如何达到这一要求。

本手册的目的，便是要帮助您满足合作伙伴的要求，甚至是在合作伙伴提出此类要求之前，即可做好万全的应对准备。

本手册介绍了您需要采取的相关步骤，来确保顺利完成 TISAX 评估流程，并与合作伙伴共享评估结果。

建立并维持一套“信息安全管理体系（ISMS）”本身已是一项繁杂的工作，而向您的合作伙伴证明，自己的信息安全管理体系能够胜任工作要求，更是繁上加繁。本手册并不会帮助您管理自己的信息安全体系，而是旨在尽可能减少相关的工作量，从而方便您向合作伙伴证明自己的工作成效。

1.2. 范围

本手册适用于您参与的所有 TISAX 流程。

它包含您需要了解的所有相关知识，来确保顺利完成 TISAX 评估流程。

本手册从评估的核心环节出发，针对如何满足信息安全要求，提出了相关建议。但是总的来说，它并不会具体告诉您应该如何去做，才能通过信息安全评估。

1.3. 受众

本手册的主要受众是，需要或希望证明自身的信息安全管理体系符合“VDA ISA（德国汽车工业协会信息安全评估标准）”特定等级要求的所有公司。

一旦您积极参与 TISAX 评估流程，您将从本手册提供的信息中受益。

而同时，要求供应商证明其信息安全管理体系符合特定等级要求的公司亦将从中受益。本手册有助于公司了解其供应商为了满足特定要求，需要具体做哪些工作。

1.4. 结构

首先，我们将简要介绍 TISAX；之后，立即展开详述具体步骤。您将了解到完成评估流程所需要的一切信息 — 按照合理的先后顺序。

阅读本文档预计需要 75-90 分钟。

1.5. 如何使用本文档

对于本文档中所述的大部分信息，您或许早晚有用上的一天。为了妥善准备有关工作，我们建议您通篇阅读本手册。

我们以 TISAX 评估流程三大主要步骤为线索，来编排本手册的章节结构，从而方便您查阅自己需要的章节内容，以及之后浏览其余内容。

本手册使用插图来帮助您理解，插图中的颜色通常具有特殊含义。因此，我们建议您通过电脑屏幕或彩印副本来阅读本文档。

我们重视您的反馈。如果您认为本手册中有内容缺失或难于理解之处，请立即联系我们。我们与本手册未来的广大读者一道，将感谢您所给出的反馈意见。

如果您使用过较早版本的《 参与者手册》，本手册末尾的备注可能会对您有所帮助，请参见章节 8, “文档历史”。

1.6. 联系我们

我们的宗旨是指导您顺利完成 TISAX 评估流程，并为您解答可能遇到的任何问题。我们的联系方式如下：

电邮： tisax@enx.com

电话： +49 69 9866927-77

您可在德国正常营业时间（UTC+01:00 (https://www.worldtimeserver.com/current_time_in_DE.aspx)）内联系我们。

我们所有人均提供 英语和 德语服务。此外，有两名同事可提供 意大利语母语服务。

1.7. 《TISAX 参与者手册》其他语言版本和格式

《TISAX 参与者手册》已推出下列语言版本和格式：

语言	版本	格式	链接	大小
英语	2.4	联机	https://www.enx.com/handbook/tisax-participant-handbook.html (https://www.enx.com/handbook/tisax-participant-handbook.html)	不适用
		脱机	https://www.enx.com/handbook/tisax-participant-handbook-offline.html (https://www.enx.com/handbook/tisax-participant-handbook-offline.html)	6.4 MB
		PDF	https://www.enx.com/handbook/TISAX%20Participant%20Handbook.pdf (https://www.enx.com/handbook/TISAX%20Participant%20Handbook.pdf)	6.4 MB

语言	版本	格式	链接	大小
德语	2.4	联机	https://www.enx.com/handbook/tisax-teilnehmerhandbuch.html (https://www.enx.com/handbook/tisax-teilnehmerhandbuch.html)	不适用
		脱机	https://www.enx.com/handbook/tisax-teilnehmerhandbuch-offline.html (https://www.enx.com/handbook/tisax-teilnehmerhandbuch-offline.html)	6,4 MB
		PDF	https://www.enx.com/handbook/TISAX-Teilnehmerhandbuch.pdf (https://www.enx.com/handbook/TISAX-Teilnehmerhandbuch.pdf)	5,0 MB
法语	2.3 beta	联机	https://www.enx.com/handbook/tph-fr.html (https://www.enx.com/handbook/tph-fr.html)	不适用
		脱机	https://www.enx.com/handbook/tph-fr-offline.html (https://www.enx.com/handbook/tph-fr-offline.html)	7,0 MB
		PDF	https://www.enx.com/handbook/tph-fr.pdf (https://www.enx.com/handbook/tph-fr.pdf)	7,0 MB
中文	2.3 beta	联机	https://www.enx.com/handbook/tph-cn.html (https://www.enx.com/handbook/tph-cn.html)	不适用
		脱机	https://www.enx.com/handbook/tph-cn-offline.html (https://www.enx.com/handbook/tph-cn-offline.html)	7,0 MB
		PDF	https://www.enx.com/handbook/tph-cn.pdf (https://www.enx.com/handbook/tph-cn.pdf)	7,0 MB

重要提示：

英语版本为第一版本，
其他所有语言版本均为英语版本的译文。
若有疑问，请以英语版本为主。

1.7.1. 关于中文译本

本《TISAX 参与者手册》是英文版本的译文。

所有 TISAX 相关文档（例如，所有合约以及针对 TISAX 审计服务提供商的要求）均以英文起草，因此，您的合作伙伴或审计服务提供商可能会使用某些英文 TISAX 术语。

为了便于您参照，我们在中文版《TISAX 参与者手册》里采取了保留英文 TISAX 术语，或在中文译文后加括号标注等做法。

1.7.2. 关于联机格式

每一章节都有唯一的 ID 编号（格式为：ID1234）。
一个 ID 总是指代一个特定的章节，与语言版本无关。
如希望链接至某个章节，您可以：

- 右键单击章节标题并复制链接，或者
- 单击章节标题，并从浏览器地址栏中复制链接。

大多数插图的尺寸要大于此处的默认显示尺寸，单击插图后可使其放大显示。

1.7.3. 关于脱机格式

脱机格式保留了联机格式的大多数特性，其中一个最显著的特点是，插图嵌入在 HTML 文件中。您只需要一个文件，便可使用脱机格式。

与联机格式相比，脱机格式中：

- 图片无法放大显示
- 联机格式的原始字体不可用
  您浏览器的默认设置将定义显示字体。

1.7.4. 关于 PDF 格式

PDF 格式是基于联机格式生成的。通常，我们使用浏览器将联机格式保存为 PDF。

如果在电脑上使用 PDF 格式，那么您仍然可以单击所有的引用链接。但是如果将 PDF 版本打印出来，由于没有页码等参照物，您需要自行查找链接内容的位置。

2. 简介

以下章节将介绍 TISAX 这一概念。

如果您时间紧迫，可跳过这部分内容，直接开始阅读 章节 4.3, “注册准备”。

2.1. 为什么选择 TISAX?

换句话说，您阅读本手册的目的是什么?

为了回答这个问题，我们首先大致思考一下商业交易的规则，尤其是涉及到信息保护这方面。

想象您有一个合作伙伴，他手握机密信息，并希望与供应商，也就是您进行共享。您与这名合作伙伴之间的合作可以创造价值，而该合作伙伴与您共享信息，则是价值创造中的一个重要环节。所以，他想要采取适当的保护措施，并希望您本人也以同样谨慎的态度来处理保密信息。

然而，他如何能保证可以放心地将自己的信息交于他人？他总不可能盲目地去“相信”您。作为合作伙伴，需要眼见为实，方可证明对方有这个能力。

那么问题来了，由谁来定义信息处理的“安全”标准？以及如何证明自己符合标准要求?

2.2. 谁来定义"安全"标准?

第一次面对此类问题的，并非只有您与您的合作伙伴，几乎所有人都得努力寻求答案，而大多数答案都具有相似性。

针对一个常见的问题，与其每次都从头开始研究解决方案，不如制定出一套应对标准，从而实现化繁为简。确定一套标准虽然工作量巨大，但确是一劳永逸、造福后来者之举。

诚然，就保护信息而言，何为正确手段，人们众说纷纭；然而，从上述造福后来者的角度出发，大多数公司都倾向于制定标准，因为标准本身便是由那些已被前人证明、历经时间考验，且针对特定挑战的最佳实践所凝聚而成的精华。

就您的情况而言，遵循并实施 ISO/IEC 27001（关于信息安全管理体系，简称“ISMS”）等标准，将有助于建立最先进的防护体系，从而确保以安全的方式来处理保密信息。此类标准可为您省去许多不必要的重复性工作，更重要的是，有了标准后，当两家公司需要彼此交换保密信息时，便可在同等基础上开展这一工作。

2.3. 汽车业内标准的由来

从性质上来看，非行业标准更像是“一刀切”式的解决方案，无法满足汽车公司的特殊需求。

很久以前，汽车行业内部便成立了很多协会，它们的主要目标是，针对自身特殊需求，精准制定并优化相关标准。“德国汽车工业协会（VDA）”便是其中之一。当时，汽车行业的数位成员建立了信息安全工作小组，并最终一致认为，由于彼此间需求相似，因而有必要对现有的信息安全管理标准进行量身调整。

在各方的共同努力下，一份调查问卷应运而生，其中涵盖了汽车行业内普遍接受的信息安全要求，而该问卷便是“VDA ISA（德国汽车工业协会信息安全评估标准）”。

随着 ISA 面世，“谁来定义‘安全’标准？”这个问题也随之有了答案：由 VDA 来定，也就是说，由汽车行业自己来向其成员提供这一问题的答案。

2.4. 如何以高效的方式证明符合安全标准?

有些公司仅在内部使用 ISA，而有些公司则利用 ISA 来对其供应商的信息安全管理体系成熟度进行评估。一般情况下，为建立业务关系，进行自我评估便足矣；然而，在某些情况下，公司会对其供应商的信息安全管理体系进行全面评估（包括现场审计）。

随着人们对信息安全管理需求意识的普遍提高，以及 ISA 作为信息安全评估工具得到广泛应用，越来越多的供应商正面临着来自不同合作伙伴的类似要求。

但是，这些合作伙伴采用的标准依然各不相同，对于如何解释标准也是说法不一。而供应商需要证明的事情则基本上是一样的，只是途径有别而已。

所以，一方面是合作伙伴不断督促供应商证明自己的信息安全管理体系符合特定等级要求，而另一方面，是供应商面对无休止的重复性劳动而怨声载道。毕竟，不停地给一个又一个审计人员展示相同的信息安全管理措施，绝非是高效的工作方式。

那么，该如何提高这一步骤的效率？如果一名审计人员的报告可以被不同的合作伙伴重复使用，是否会有助于改善情况?

负责 ISA 维护的 VDA 工作小组中的 OEM（原始设备制造商）与供应商在听取了各家供应商的不满和抱怨后，现在，针对“如何证明符合安全标准？”这个问题，为汽车行业的广大供应商及相关企业给出了如下答案。

这个答案便是 TISAX，全称为 “Trusted Information Security Assessment Exchange”（可信信息安全评估交换）。

3. TISAX 流程

3.1. 总述

TISAX 流程启动的标志通常[2]是，您的某个合作伙伴要求您证明，自己的信息安全管理体系符合“VDA ISA（德国汽车工业协会信息安全评估标准）”特定等级的要求。为了满足该要求，您需要完成 TISAX 流程三大步骤。本章将为您简要介绍这些步骤。

TISAX 流程三大步骤包括：

插图 1. TISAX 流程概述

1. 第 1 步
   注册
2. 第 2 步
   评估
3. 第 3 步
   交换

1. 注册
   我们采集您公司以及评估过程所需要的信息。
2. 评估
   您参与评估流程，评估工作由我方指定的一名 TISAX 审计服务提供商执行。
3. 交换
   您与合作伙伴共享评估结果。

每一步都包含若干子步骤，这些内容将在以下篇幅中分成三节进行讲解，每一节均详细描述其中一个步骤。

请注意：

虽然我们很想告诉您，多久以后可以拿到 TISAX 评估结果，但我们自己亦无法做出准确预测，因此，恳请您理解。TISAX 流程的总体耗时取决于许许多多的因素：由于公司规模、评估对象，外加信息安全管理体系的建立情况等千差万别，因而无法预测所需时间。

然而，TISAX 规定，整个 TISAX 评估流程用时最长不超过 9 个月。

3.2. 注册

注册是参与 TISAX 评估的第一步。

TISAX 注册的主要目的，是采集关于您公司的信息。我们使用在线注册流程，来帮助您向我们提供该信息。

注册是所有后续步骤的先决条件，并需要缴纳费用。

在线注册过程中：

- 我们会要求您提供联系方式与地址信息。
- 您须接受我们的条款和条件。
- 您可以自定义信息安全评估的范围。

若要直接开始该步骤，请参见章节 4, “注册（第 一步）”。

在线注册流程详见章节 4.5, “在线注册流程”。 若想即刻开始，请前往 enx.com/en-US/TISAX/。

3.3. 评估

第二步是完成信息安全评估。

其中，包含四个子步骤：

a. 评估准备
   您需要针对评估工作进行准备，其程度视您的信息安全管理体系目前的成熟度而定。准备工作应基于 ISA 目录进行。

b. 选择审计服务提供商
在准备好接受评估后，您需要选择一名由我方指定的 TISAX 审计服务提供商。

c. 信息安全评估
您选定的审计服务提供商将从满足合作伙伴的要求出发，依照评估范围来相应开展评估工作。评估流程将包括预审计这一基本步骤。
如果您的公司未能立即通过评估，则评估流程可能需要增加额外的步骤。

d. 评估结果
一旦您的公司通过评估，您的审计服务提供商将向您提供正式的 TISAX 报告。您的评估结果亦将印上“TISAX 标签”。[3]

有关该步骤的更多信息，请参见 章节 5, “评估（第 二步）”。

3.4. 交换

第三步，也就是最后一步，是与您的合作伙伴共享自己的评估结果。TISAX 报告的内容按照等级进行划分，您可自行决定合作伙伴有权查看哪一级别的内容。

评估结果的有效期为三年，假设届时您仍是合作伙伴的供应商，那么您需要再次完成上述三大步骤。[4]

有关该步骤的更多信息，请参见章节 6, “交换（第 三步）”。

至此，您已基本了解什么是 TISAX 流程；在后续章节中，您将进一步了解如何完成各个步骤。

4. 注册（第一步）

阅读“注册”章节预计需要 30-40 分钟。

4.1. 总述

注册是完成 TISAX 流程的第一步。注册是所有后续步骤的先决条件，

以下章节内容将带您完成注册这一步：

1. 首先，我们为您解释一个重要的新术语
2. 之后，我们就如何针对在线注册流程进行准备，向您提出建议
3. 接下来，我们引导您完成在线注册流程

4.2. 您的 TISAX 参与者身份

首先，我们为您介绍一个有必要理解的新术语。到目前为止，您的身份一直是“供应商”，阅读本手册的目的，是为了满足您的“客户”所提出的要求。然而，TISAX 本身并不区分这两种角色。对于 TISAX 而言，每一位注册人员都是“参与者”，也就是说，您与合作伙伴“参与”了信息安全评估结果的交换过程。

插图 2. 注册成为 TISAX 参与者

1 您的公司
2 TISAX 注册

3 TISAX 参与者

为了从一开始便区分这两个角色，我们将您（供应商）称作“主动参与者（active participant）”，将您的合作伙伴称作“被动参与者（passive participant）”。作为“主动参与者”，您接受 TISAX 评估，并与其他参与者共享自己的评估结果。“被动参与者”是要求您接受 TISAX 评估的人，也是您的评估结果的接收人。

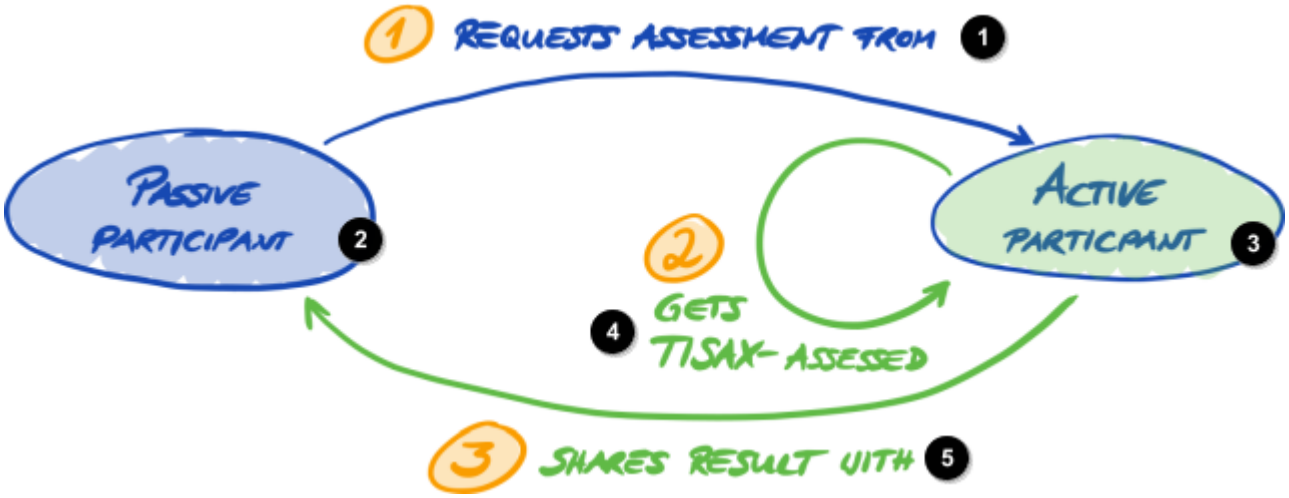


插图 3. “被动参与者”与“主动参与者”

1 1 要求对方接受评估
2 被动参与者
3 主动参与者
4 2 接受 TISAX 评估
5 3 与对方共享评估结果

每一家公司都可以扮演两种角色：您可能在与合作伙伴共享评估结果的同时，也要求自己的供应商接受 TISAX 评估。

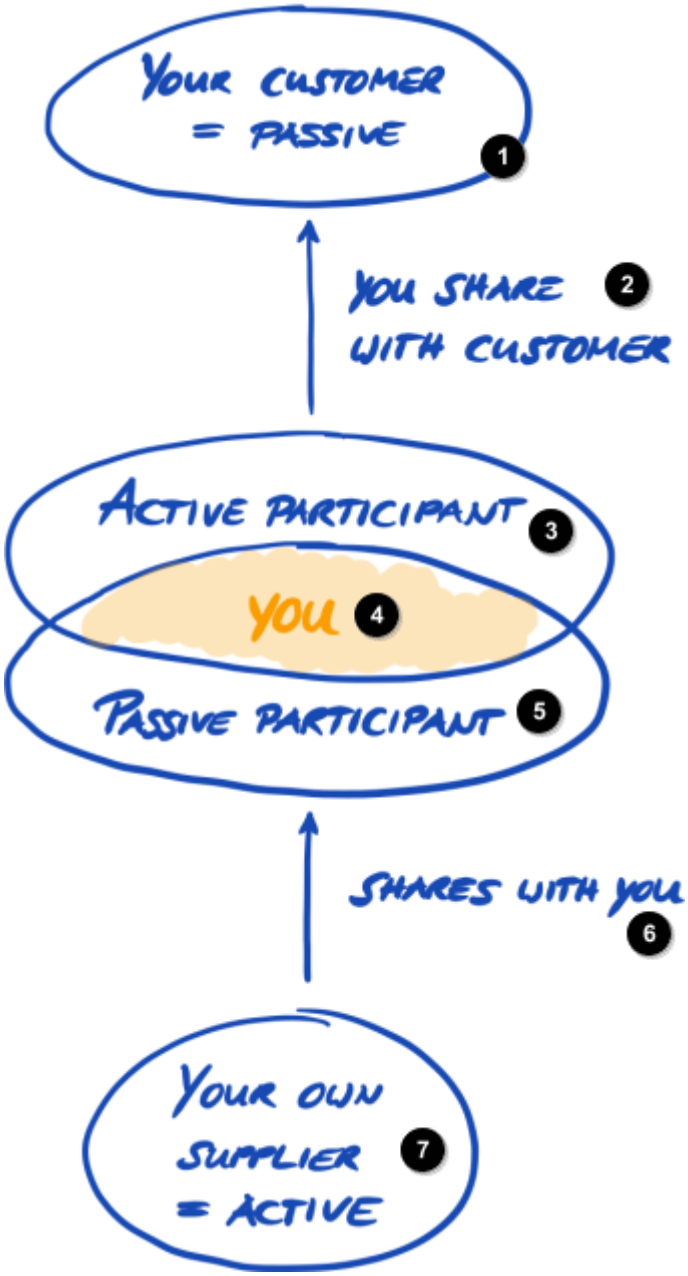


插图 4. TISAX 参与者可以同时为“主动”和“被动”参与者

1. 您的客户
   == 被动方
2. 您与客户共享结果
3. 主动参与者
4. 您
5. 被动参与者
6. 与您共享结果
7. 您的供应商
   == 主动方

如果您自己的供应商亦会接触您合作伙伴的保密信息，那么强烈建议其也接受 TISAX 评估。

4.3. 注册准备

在本节中，我们将就如何针对注册流程进行*准备*，来为您提供相关建议。更多关于注册流程本身的信息，请参见章节 4.5, “在线注册流程”。

在开始在线注册之前，我们强烈建议您：

- 提前收集信息
- 针对某些事宜作出决定。

4.3.1. 法律基础

一般来说，您需要签订两份合约，第一份合约的签订人是您与 ENX 协会：即“ TISAX 参与一般条款和条件”（TISAX 参与者 GTC）；第二份合约的签订人是您与一名由我方指定的 TISAX 审计服务提供商。注册流程仅会用到第一份合约。

“TISAX 参与者 GTC”确立了我们相互间的关系，以及您与其他 TISAX 参与者之间的关系，并规定了所有各方的权利和义务。除了大多数合同中常见的条款外，该合约还详细规定了在 TISAX 流程期间，交换和获得的信息如何进行处理。这些规定的一个关键目的，是确保 TISAX 评估结果保密。由于所有 TISAX 参与者都受相同规则的制约，因而您可以期待，您的合作伙伴（以“被动参与者”的身份）亦会为您的 TISAX 评估结果提供适当的保护。

我们将于在线注册流程开始时，便要求您接受“TISAX 参与者 GTC”。由于这是一份真正意义上的合同，我们因此建议您在开始在线注册流程之前，首先认真阅读“TISAX 参与者 GTC”。其中一个原因是，您可能需要从公司内部或外部律师那里获得许可函，这取决于您在公司里的角色。

您可登录我们的网站，下载“TISAX 参与一般条款和条件”：[5]
enx.com/en-US/TISAX/downloads/

下载 PDF：
enx.com/tisaxgtcen.pdf

在线注册过程中，我们将要求您选中两个复选框（必选）：

❏ We accept the TISAX Participation General Terms and Conditions
我方接受“TISAX 参与一般条款和条件”

❏ 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;
我方确认已知晓，根据“TISAX 参与一般条款和条件”IX.5 和 X.3 部分有关规定，申请者将解除针对审计服务提供商的职业保密义务；

我们设置第二个复选框的原因是，我方的 TISAX 审计服务提供商中，有些是注册会计师，他们对职业保密有特殊的要求。在选中此框之前，您可能需要仔细了解相关条款。

如果您通常要求与处理保密信息的一方之间签订保密协议（NDA），则请查看我们 GTC 的有关章节，其中的内容应该能够解答您的疑惑。

最后，我们希望您理解，整个体系本身的基础是“人人接受相同规则的约束”，因此，我们不会接受其他任何一般性条款和条件。[6]

4.3.2. TISAX 评估范围

在 TISAX 流程的第二步中，我方的一名 TISAX 审计服务提供商将执行信息安全评估工作，他需要知道从哪里开始以及在哪里结束。这就是为什么您需要指定一个“评估范围”。

“评估范围”描述的是信息安全评估工作的范围，简单来说，在您的公司里，只要涉及到处理合作伙伴保密信息的环节，则均属于评估范围。您可以将其视为审计服务提供商的主要任务描述，它规定了审计服务提供商需要评估的内容。

评估范围之所以重要，有两个原因：

a. 对于您公司里负责处理合作伙伴信息的各个环节，只有当相应的评估范围涵盖所有此类环节时，评估结果才能够满足合作伙伴的要求。

b. 对于我方的 TISAX 审计服务提供商，精确定义评估范围是合理计算成本的必要前提条件。

重要提示：

如果您的公司拥有 ISO/IEC 27001 认证：“TISAX 评估范围”的定义与 ISO/IEC 27001 认证所需要的“范围”定义是相似的。区别在于，在 TISAX 中，范围是预先定义好的。

4.3.2.1. 范围描述

范围描述规定了评估工作的范围。您需要从以下两种范围类型中选择一种：

1. Standard scope （标准范围）
2. Custom scope （自定义范围）
   a. Extended scope （扩展型范围）
   b. Narrowed scope （缩减型范围）

4.3.2.2. 标准范围

标准范围是开展 TISAX 评估的基础，其他 TISAX 参与者也仅接受基于标准范围描述的评估结果。

标准范围是预先定义好的，无法更改。如果您希望使用自定义范围，则可以为您的评估选择“扩展型范围”或“缩减型范围”。

使用标准范围的好处是，您无需自己定义范围。

以下是标准范围的描述：[7]

The standard scope comprises all processes and involved resources at the sites defined below that are subject to security requirements from partners in the automotive industry. Involved processes and resources include collection of information, storage of information and processing of information.

Examples for involved resources: Work equipment, employees, IT systems including cloud services such as infrastructure/ platform/software as a service, physical sites, relevant contractors

Examples for sites: Office sites, development sites, production sites, data centres

标准范围包括：与以下场地有关的所有流程和资源，其应当符合汽车行业合作伙伴的安全性要求。相关流程和资源包括信息的收集、存储和处理。

涉及资源示例：工作设备、员工、IT 系统（包括云服务，如基础设施/平台/软件即服务）、物理场地、相关承包商

场地示例：办公场地、研发场地、生产场地、数据中心

我们强烈建议选择标准范围，因为所有 TISAX 参与者都接受基于标准范围作出的信息安全评估结果。

4.3.2.3. 范围界定

在确定了范围类型后，下一个任务便是决定哪些公司地点属于评估范围。

如果您的公司规模不大（仅一处地点），那便好办，您只需将公司地点添加到评估范围即可。

如果您的公司规模较大，则应考虑注册一个以上的评估范围。

您可以注册一个囊括所有公司地点的单一范围，这样做的好处是：

- 评估报告、评估结果及其有效期的数量都只有一个（份）。
- 评估费用更低，因为 TISAX 审计服务提供商只会一次性评估您的核心流程、程序和相关资源。

然而，单一范围也有缺点，比如：

- 只有在 TISAX 审计服务提供商对所有地点完成评估后，才会出具评估结果。如果您急需评估结果，那么这一点就比较麻烦。
- 最终评估结果的好坏，取决于是否所有地点均通过了评估。就算只有一处地点未通过，都会影响到整体评估结果。[8]

4.3.2.4. 范围调整

是选择一个范围还是选择多个范围，这个问题只能留给您自己。然而，通过回答下图中的问题，可有助于您做出决定。

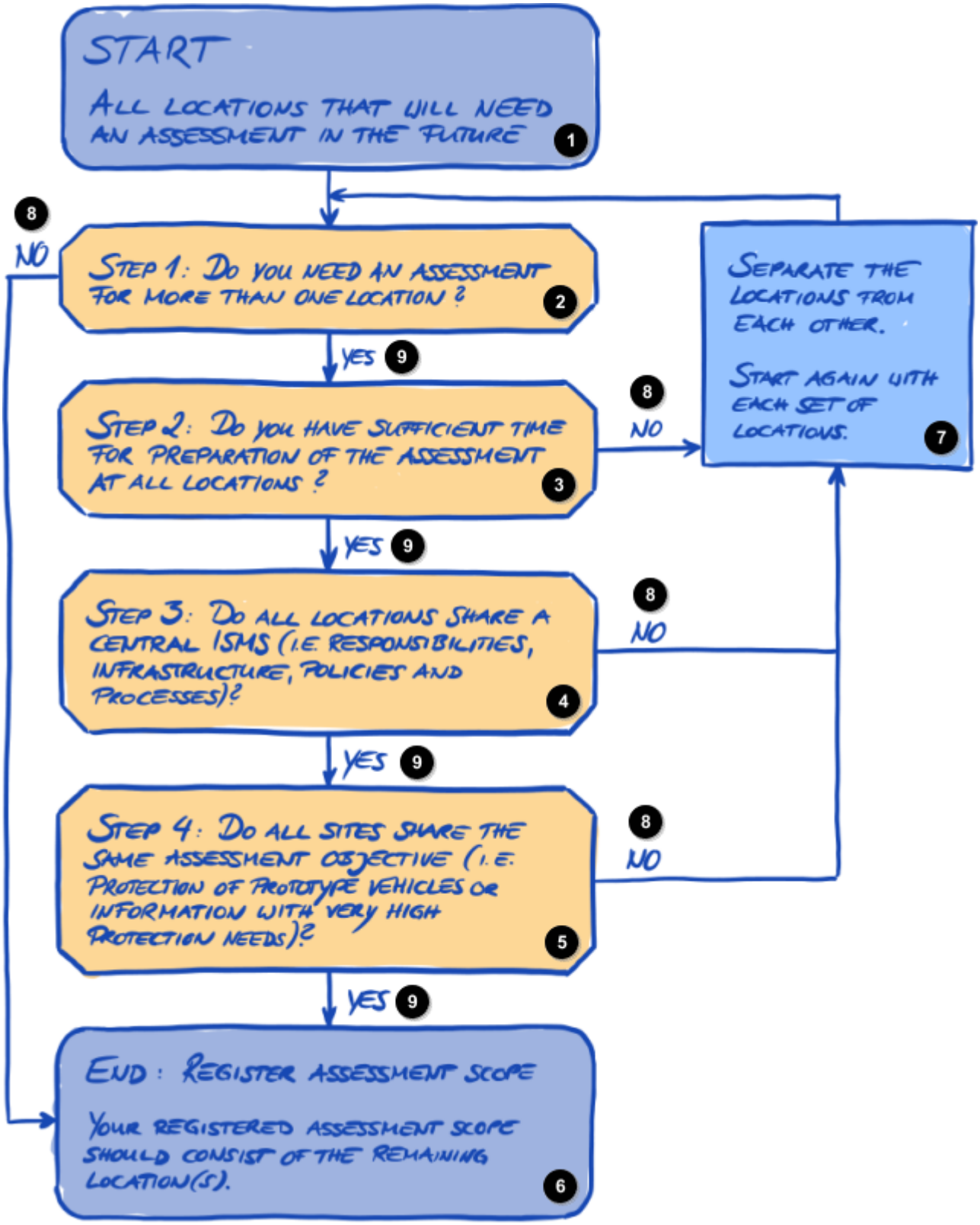


插图 5. 范围调整决策树

1. 开始
   针对今后需要评估的所有地点
2. 第一步：您是否需要对一个以上的地点进行评估?
3. 第二步：您是否有足够的时间去准备所有地点的评估工作?
4. 第三步：是否所有地点都有统一的 ISMS 体系（例如在职责、基础设施、政策和流程方面）？
5. 第四步：所有场地是否有相同的评估对象 - 例如，“原型车辆或信息（保护需求极高）的保护”?

6. 结束：注册评估范围
   您注册的评估范围应囊括其余的地点。
7. 将各个地点拆分开。
   重新分组并从头开始上述步骤。
8. 否
9. 是

请注意：

面对这一决策过程，您无需胆怯。只要审计服务提供商还未最终完成评估，您便可随时更改评估范围。

例如，在评估准备过程中，您可能会发现评估范围并不合适，因而相应做出调整。或者，您的审计服务提供商可能会建议您，在评估早期阶段就变更范围。

请注意：添加范围内容会导致费用增加，而从范围中移除地点，则不会退款。

4.3.2.5. 范围地点信息

现在，您已经确定哪些地点属于评估范围，接下来，您可以着手收集与地点相关的信息。

对于每一处地点，我们都要求提供相应的信息，如公司名称和地址。另外，我们还需要您提供一些附加信息，以便我方的 TISAX 审计服务提供商能够更好地了解您公司的结构。您提供的信息将是其开展评估工作的基础。

针对您公司的各个地点，请准备好提供以下信息（红色星号 *表示在线流程中的必填信息）：

字段	**选择项**
地点名称 *	不适用
D&B D-U-N-S 编号 (https://en.wikipedia.org/wiki/Data_Universal_Numbering_System)	不适用
地点类型 *	公司自有建筑（仅由公司使用） 公司租用建筑 公司租用楼层/办公室（在共用建筑中） 与其他公司共用办公室 自有数据中心 共享数据中心
被动场地保护 *	是 否
行业 *（可多选）*	信息技术 ❑ IT 服务 ❑ 电信服务 ❑ 软件开发 管理 ❑ 咨询

字段	选择项
	媒体 ❑ 营销 ❑ 代理 ❑ 打印服务 ❑ 摄影 ❑ 翻译服务 研发 ❑ 车辆测试 ❑ 车辆模拟 ❑ 原型构造 ❑ 微型汽车模型 ❑ 开发服务 ❑ CAx 开发服务 生产 ❑ 生产服务 ❑ 签约制造 ❑ 车间 ❑ 物流 销售及售后 ❑ 进口，NSC ❑ 经销 ❑ 金融服务 ❑ 保险 ❑ 理赔 其他行业 *（请输入）*
地点雇用员工数：总计 *	0 1-10 11-100 101-1000 1.001-5000 5000 以上

字段	选择项
地点雇用员工数：IT *	0 1-10 11-25 26-50 50 以上
地点雇用员工数：IT 安全 *	0 兼职 1-5 6-25 25 以上
地点雇用员工数：地点安全 *	0 兼职 1-3 4-10 10 以上
该地点所获认证	ISO 27001 其他 *（请输入）* ISAE 3402 SOC2

表格 1. 地点相关信息

请注意：

关于“行业”：请尽量根据您的了解来选择。以上选项无对错之分，如果找不到与您的业务类型相匹配的选项，您只需在“其他”中输入相应的选项。

对于每个地点，您必须指定一个“location name” (地点名称)。地点名称的作用是，在将地点分配给评估范围时，更容易对其进行引用。

我们建议，根据以下格式来指定地点名称：

格式： [地理位置引用]

示例： 针对虚构公司“ACME”

- 法兰克福
  （以德国**城市**法兰克福来作为地点名称）

4.3.2.6. 范围名称

对于每个范围，您必须指定一个“scope name” (范围名称)。范围名称的作用是，在进行与 TISAX 相关的交流（例如，与您的 TISAX 审计服务提供商）时，能够更容易引用有关范围。

您可以指定任意范围名称，但不要为一个以上的范围分配相同的范围名称。

如果以后想要更新 TISAX 评估，您到时要创建一个新范围（可能与当前范围完全相同）。因此，我们建议将评估年份添加到范围名称中。

我们建议，根据以下格式来分配范围名称：

格式： [地理位置或*功能信息*引用] [评估年份]

示例： 针对虚构公司“ACME”

- 2020
  （如果您公司只有一处地点，则无需地理位置）
- 法兰克福 2020
  （针对若干处地点位于德国**城市**法兰克福的范围）
- 下萨克森 2020
  （针对所有地点位于德国**联邦州**下萨克森的范围）
- 德国 2020
  （针对所有地点位于**德国**境内的范围）
- EMEA 2020
  （针对所有地点位于 EMEA **地区**（“欧洲、中东、亚洲”）的范围）
- 原型开发 2020
  （*功能信息*引用，针对所有地点均涉及原型开发的范围）

4.3.2.7. 联系人

为了与您保持沟通，我们会收集您公司的联系人信息。

我们通常要求您公司至少要指定一名联系人来作为 TISAX 参与者，并为每一个评估范围相应指定一名联系人。另外，您还可以添加其他联系人。

在注册准备期间，您应当决定自己公司的联系人人选。

我们需要以下联系人信息：

	联系人信息	是否必须提供?	示例
1.	称呼	是	女士、先生
2.	学位		Dr.、Ph.D. 或其他
3.	名	是	John
4.	姓	是	Doe
5.	职位	是	IT 主管
6.	部门	是	信息技术
7.	常用联系电话	是	+49 69 986692777
8.	备用联系电话		
9.	电子邮件	是	john.doe@acme.com
10.	首选交流语言	是	英语（默认）
11.	其他交流语言		德语、法语

	联系人信息	是否必须提供?	示例
12.	个人地址标识符		HPC 1234
13.	街道地址	是	Bockenheimer Landstraße 97-99
14.	邮编	是	60325
15.	城市	是	法兰克福
16.	州/省份		
17.	国家	是	德国

表格 2. 联系人信息

重要提示：

我们建议，为每个联系人指定至少一名代理人。一旦联系人暂时联络不上或不在公司，则可由他人代为管理您公司的参与者信息。+ 否则，如果要新指定一名联系人（非其他现有的有效联系人）的话，相关流程会比较复杂，因为我们的流程旨在确保，只有公司的合法代言人才有资格批准新指定一名主要联系人。

4.3.2.8. 发布与共享

TISAX 的主要目的，是向其他 TISAX 参与者发布您的评估结果，并与您的合作伙伴共享评估结果。

您可在注册过程中或以后的任何时候决定是否发布和共享您的评估结果。

如果您想从“占据先手”这一角度出发来参与 TISAX 流程，那么您已经可以决定将评估结果向其他 TISAX 参与者发布。否则，您无需针对该阶段进行准备。

如果您的合作伙伴要求您完成 TISAX 评估流程，那么，您迟早要共享评估结果。在注册期间，您已经可以与合作伙伴共享状态信息。一旦您拿到了评估结果，合作伙伴将自动拥有访问权限。[9]

若要共享状态信息，您需要两项信息：

1. 合作伙伴的 TISAX 参与者 ID

   TISAX 参与者 ID 是合作伙伴作为 TISAX 参与者的一个标识。

   通常，您的合作伙伴应向您提供其 TISAX 参与者 ID。

   为了便于您查找，我们的注册表单为一些经常接收共享评估结果的公司提供一份“参与者 ID”下拉列表。[10]

   但是，如果您的合作伙伴是一家大型原始设备制造商（OEM），有时公司部门虽下达了要接受 TISAX 评估的要求，但却不清楚自己公司的参与者 ID 是什么。这种情况下，您可以联系我们。 我们可为您提供合作伙伴的“参与者 ID”。

2. 所需共享级别

   共享级别规定了您的合作伙伴可以访问哪个层次的评估结果信息。

   您的合作伙伴可以请求获取某个共享级别，您自己亦可以决定为合作伙伴授予何种级别的访问权限。

   有关共享级别的详细信息，请参阅章节 6.5, “共享级别”。

因此，您可能希望确保自己已掌握上述信息。

请注意：

- 您可以决定以后再发布您的评估结果。
- 您可以在以后的某个时间为合作伙伴创建共享权限。

重要提示：

如果您不发布或不共享评估结果，则他人将无法看到。

重要提示：

发布或共享操作无法撤销。

更多信息，请参阅章节 6.4, “交换结果操作的不可逆性”。

有关发布和共享评估结果的详细信息，请参阅 章节 6, “交换（第 三步）”。

4.3.3. 评估对象

注册过程期间，您需要定义评估对象。评估对象(assessment objective)规定了您的信息安全管理体系（ISMS）应当满足的有关要求。评估对象的确定，完全是基于您代表合作伙伴参与处理的数据类型。

在以下章节中，我们将描述评估对象，并就如何选择正确的评估对象提供建议。

由于评估对象代表了已定义好的 TISAX 评估流程输入，因此，在与合作伙伴以及我们的 TISAX 审计服务提供商进行有关 TISAX 的沟通时，使用评估对象会有利于开展相关工作。

请注意：

某些合作伙伴可能会要求您接受 TISAX 特定“评估级别（Assessment Level，简称 AL）”的评估，而不会指定评估对象。有关评估级别的更多信息，请参阅 章节 4.3.3.6, “保护需求与评估级别”（子章节“其他信息”）。

4.3.3.1. 评估对象列表

目前，有八大 TISAX 评估对象。您需要选择至少一个评估对象，也可以选择多个。

请将评估对象视为对您的信息安全管理体系进行评估的基准，因为评估对象是 TISAX 流程的关键输入。所有 TISAX 审计服务提供商的评估策略都主要基于评估对象。

目前，TISAX 评估对象如下所示：

序号	评估对象 (Assessment objective)	缩写
1.	保护需求较高的信息 Handling of information with high protection needs	信息——高保护需求（Info high）
2.	保护需求 极高的信息 Handling of information with very high protection needs	信息——极高保护需求（Info very high）
3.	原型零部件保护 Protection of prototype parts and components	原型零件（Proto parts）

序号	评估对象 (Assessment objective)	缩写
4.	原型车保护 Protection of prototype vehicles	原型车（Proto vehicles）
5.	试验车处理 Handling of test vehicles	试验车（Test vehicles）
6.	原型保护——活动及录制、拍摄期间 Protection of prototypes during events and film or photo shoots	活动 + 拍摄（Events + Shootings）
7.	数据保护 依据欧洲《通用数据保护条例》（GDPR）第 28 条“Processor”（“处理人”） Data protection According to Article 28 (“Processor”) of the European General Data Protection Regulation (GDPR)	数据（Data）
8.	数据保护——针对 特殊类个人信息 依据欧洲《通用数据保护条例》（GDPR）第 28 条“Processor”（“处理人”），以及第 9 条中关于特殊类个人信息的规定 Data protection with special categories of personal data According to Article 28 (“Processor”) with special categories of personal data as specified in Article 9 of the European General Data Protection Regulation (GDPR)	特殊数据（Special data）

表格 3. 目前的 TISAX 评估对象

示例：如果您正在公路上进行试驾，那么序号 7“试验车处理（Handling of test vehicles）”便是您的评估对象之一。

在下方的插图中，我们将使用图表形式，来展示 TISAX 八大评估对象。此外，我们将使用缩略语，来实现更直观的视觉效果。

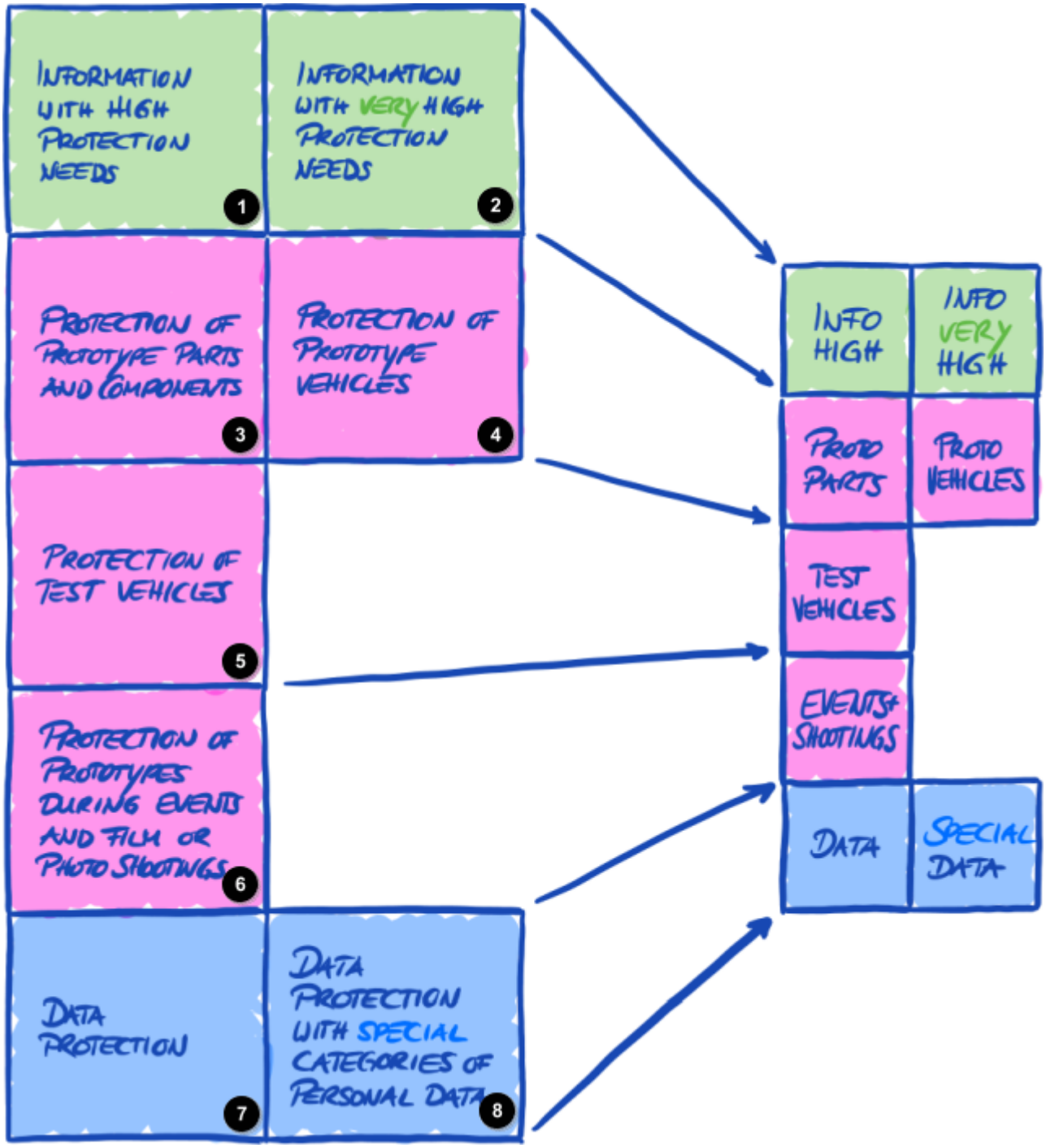


插图 6. TISAX 评估对象（图表展示、全称及简称）

1. 保护需求较高的信息
2. 保护需求 极高的信息
3. 原型零部件保护
4. 原型车保护
5. 试验车处理
6. 原型保护——活动及录制、拍摄期间
7. 数据保护
8. 数据保护——针对 特殊类个人信息

重要提示：

在 TISAX 中，“评估对象”通常是过程的输入项。但是，某些合作伙伴可能会要求您接受 TISAX 特定“评估级别”（AL）的评估。

有关保护需求与评估级别之间关系的更多信息，请参阅 章节 4.3.3.6, “保护需求与评估级别”。

4.3.3.2. 评估对象和 ISA

每个评估对象都对应了 ISA 目录中的某个标准。

例如：对于具有较高或极高保护需求的“信息”评估对象，其对应的均是 ISA 目录中的“信息安全”标准。这两个评估对象的 Excel 表也是相同的。您可以根据对每项要求（在相应副标题“关于（极）高保护需求情形的其他信息”）的描述，来相应区分（高、极高）这两个保护需求；请见章节 5.2.2, “看懂 ISA 文件”。

要进一步了解 TISAX 评估对象与 ISA 标准目录和评估级别之间的关系，请参阅 章节 5.2.2, “看懂 ISA 文件”。

4.3.3.3. 评估对象和 TISAX 标签

您的合作伙伴可能会提起“TISAX 标签”，而“评估对象”和“TISAX 标签”基本上是一回事。不同点在于，评估过程刚开始时会有“评估对象”，如果通过了评估，则您会收到相应的“TISAX 标签”。

示例：您的合作伙伴要求您获得 TISAX标签“保护需求较高的信息（保护需求较高的信息）”。然后，您选择“保护需求较高的信息（保护需求较高的信息）”作为评估对象。

下图为您展示了 TISAX 流程的输入和输出：

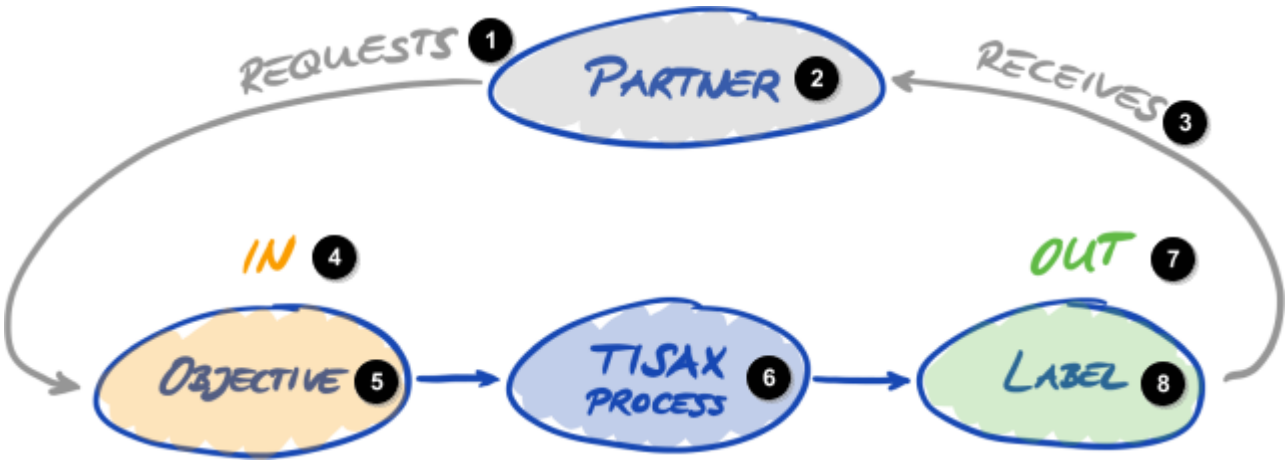


插图 7. 评估对象和 TISAX 标签

1. 请求
2. 合作伙伴
3. 接收
4. 输入
5. 对象
6. TISAX 流程
7. 输出
8. 标签

有关 TISAX 标签的更多信息，请参阅 章节 5.4.13, “TISAX 标签”。

4.3.3.4. 评估对象及其依存关系

评估对象“保护需求较高的信息（保护需求较高的信息）”是 TISAX 评估的必选项。在此基础上，其他评估对象为可选项。然而，根据您所处理的信息性质，您可能需要添加其他评估对象。在下文中，您将进一步了解自己可能需要哪些评估对象。

有些评估对象与其他对象之间有依存关系：比如，评估对象“保护需求较高的信息（保护需求较高的信息）”或“保护需求极高的信息（保护需求极高的信息）”是其他所有评估对象的基础。

示例：如果您需要评估对象“原型零部件保护（原型零部件）”达标，那么您需确保基础评估对象“保护需求较高的信息（保护需求较高的信息）”亦同时达标。在下文中，您将进一步了解这种依存关系。

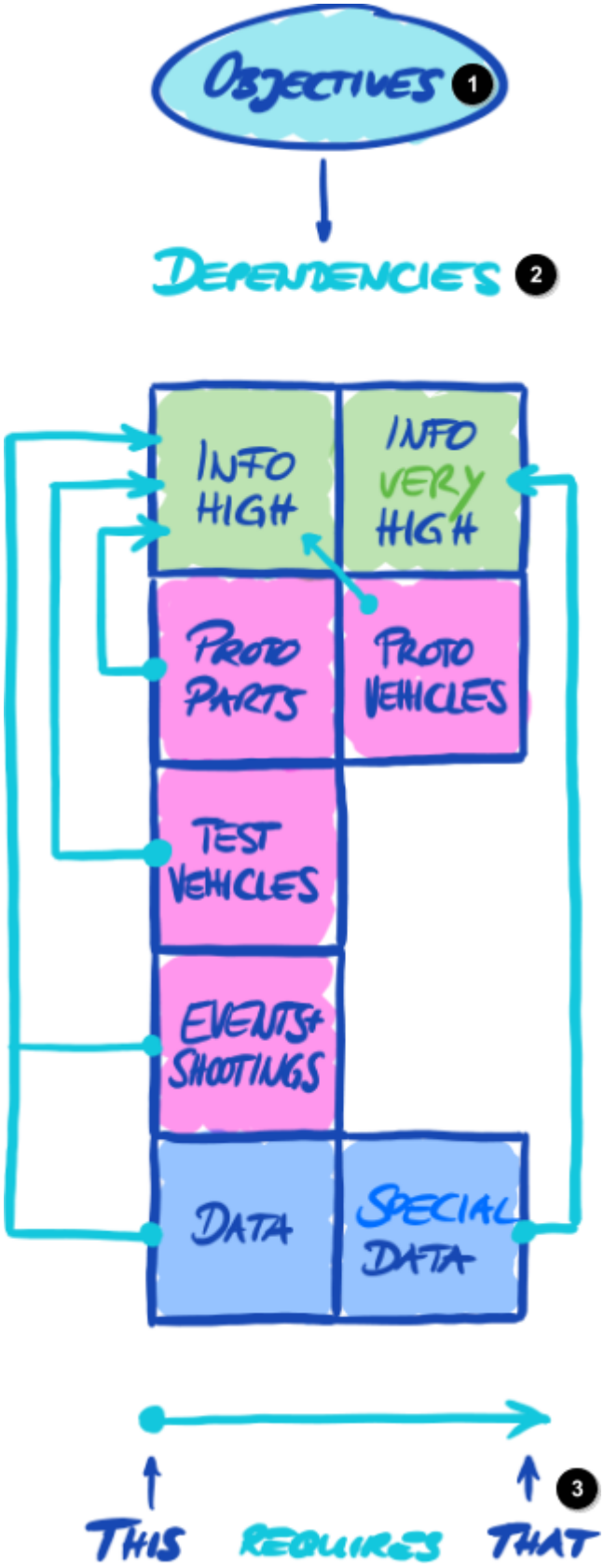


插图 8. 评估对象及其依存关系

1. 评估对象
2. 依存关系
3. 前者需要后者

4.3.3.5. 评估对象选择

理想情况下，您的合作伙伴会准确地告诉您哪些评估对象必须达标。

在下列情况下，您应根据自己的判断来选择评估对象：

a. 您希望在合作伙伴要求之前主动接受 TISAX 评估，或者

b. 您的合作伙伴并未告诉您哪些评估对象应当达标。

重要提示：

如遇到上述情况，我们强烈建议您亦考虑其他合作伙伴的要求，也就是说，在您现有的合作伙伴中，是否有些伙伴有相同或更高的要求？您估计，未来的合作伙伴会否提出更高的要求？

这样一来，您可能希望考虑选择保护需求更高的评估对象，因为该做法可以防止出现问题，比如一旦遇到其他合作伙伴提出更高要求的情况。

如果您需要根据自己的判断来选择评估对象，以下建议可能会对您有所帮助：

序号	评估对象	建议信息
1.	保护需求较高的信息 （信息——高保护需求（Info high））	您可以通过合作伙伴的文档分类标准，来相应推断出保护需求（高、极高）。
2.	保护需求极高的信息 （信息——极高保护需求（Info very high））	
3.	原型零部件保护 （原型零件（Proto parts））	针对制造、储存或使用客户提供的组件或零件的所有公司，这些组件或零件被归类为需要在其所处地点受到保护。 物理安全、周边区域安全要求、组织要求以及原型处理相关要求等，均是这项评估的一部分。
4.	原型车保护 （原型车（Proto vehicles））	针对制造、储存或使用客户提供的车辆的所有公司，这些车辆被归类为需要在其所处地点受到保护。 物理安全、周边区域安全要求（包括是否存在受保护车库及车间区域）、组织要求以及原型处理相关要求等，均是这项评估的一部分。 成功通过评估后，您将自动获得 TISAX 标签“原型零部件保护”。
5.	试验车处理 （试验车（Test vehicles））	针对利用客户提供的车辆进行测试和试驾（例如，在公路或试车跑道上进行试驾）的所有公司，此类车辆被归类为需要保护。 组织要求、原型处理相关要求（包括在公路和试车跑道上进行试驾期间，对车辆采用的伪装遮蔽层和处理措施）是这项评估的一部分。 而物理安全、周边区域安全要求却未必是评估的一部分。如果您的评估地点配备了相应的设施，我们建议您也选择评估对象“原型车保护”。

序号	评估对象	建议信息
6.	原型保护——活动及录制、拍摄期间（活动 + 拍摄（Events + Shootings））	针对利用客户提供的车辆、部件或零件进行展示或开展活动（例如，市场调查、活动、营销活动），以及进行录制和拍摄的所有公司，此类车辆、部件或零件被归类为需要保护。 组织要求、原型处理相关要求（包括与在受保护的房间和公共场合进行展示、开展活动，以及进行录制和拍摄相关的要求）是这项评估的一部分。 而物理安全、周边区域安全要求却未必是评估的一部分。如果您的评估地点配备了相应的设施，我们建议您也选择评估对象“原型车保护”。
7.	数据保护（数据（Data））	根据《通用数据保护条例》（GDPR）第 28 条，如果您以“处理人”的身份来处理个人数据，则可能需要选择“（数据保护）”这一对象。
8.	数据保护——针对 特殊类个人信息（特殊数据（Special data））	根据《通用数据保护条例》（GDPR）第 28 条，如果您以“处理人”的身份来处理特殊类个人信息（如健康或宗教），则可能需要选择“（数据保护——针对 特殊类个人信息）”这一对象。

表格 4. 评估对象选择建议

补充说明：

- 如果您的合作伙伴明确给出了相关要求，则您通常无需再与其商讨评估对象一事；但是，如果合作伙伴未明确给出相关要求，则我们强烈建议您在启动评估流程之前，向您的合作伙伴咨询有关事宜。
- ISA 标准通过“高（high）”和“极高（very high）”这两大保护需求（如有），来相应描述各项要求在执行上的差异。更多相关信息，请见 插图 13, “截图：ISA 标准目录中相关问题的主要元素”。

4.3.3.6. 保护需求与评估级别

您的合作伙伴拥有不同类型的信息，有些信息的保护级别可能需要高于其他信息。为了应对这种情况，ISA 标准定义了三大“保护需求”(Protection needs)：正常（normal）、高（high）和极高（very high），来对信息进行区分。您的合作伙伴可通过对自己的信息进行分类，从而相应确定保护需求。

TISAX 评估对象与 ISA 标准目录在“高（high）”或“极高（very high）”这两个保护需求上是一一对应的。

序号	ISA 标准目录	保护需求	TISAX 评估对象
1.	信息安全（Information security)	高	保护需求较高的信息 Handling of information with high protection needs
2.	信息安全（Information security)	极高	保护需求 极高的信息 Handling of information with very high protection needs
3.	原型保护（Prototype protection)	高	原型零部件保护 Protection of prototype parts and components

序号	ISA 标准目录	保护需求	TISAX 评估对象
4.	原型保护（Prototype protection）	高	原型车保护 Protection of prototype vehicles
5.	原型保护（Prototype protection）	高	试验车处理 Handling of test vehicles
6.	原型保护（Prototype protection）	高	原型保护——活动及录制、拍摄期间 Protection of prototypes during events and film or photo shoots
7.	数据保护（Data protection）	高	数据保护 依据欧洲《通用数据保护条例》（GDPR）第 28 条“Processor”（“处理人”） Data protection According to Article 28 (“Processor”) of the European General Data Protection Regulation (GDPR)
8.	数据保护（Data protection）	极高	数据保护——针对 特殊类个人信息 依据欧洲《通用数据保护条例》（GDPR）第 28 条“Processor”（“处理人”），以及第 9 条中关于特殊类个人信息的规定 Data protection with special categories of personal data According to Article 28 (“Processor”) with special categories of personal data as specified in Article 9 of the European General Data Protection Regulation (GDPR)

表格 5. ISA 标准目录和保护需求与 TISAX 评估对象的对照

保护需求越高，您的合作伙伴就越希望确保能够放心地让您处理他们的信息。因此，TISAX 定义了三大“评估级别（Assessment Level，简称 AL）”。评估级别规定了我们的 TISAX 审计服务提供商所执行的审核深度，以及其使用的审计方法。简单来说，评估级别越高，相应的评估强度就越高，使用的评估方法也就越高级。

序号	TISAX 评估对象	评估级别（AL）
1.	保护需求较高的信息 Handling of information with high protection needs	AL 2
2.	保护需求 极高的信息 Handling of information with very high protection needs	AL 3
3.	原型零部件保护 Protection of prototype parts and components	AL 3
4.	原型车保护 Protection of prototype vehicles	AL 3
5.	试验车处理 Handling of test vehicles	AL 3

序号	TISAX 评估对象	评估级别（AL）
6.	原型保护——活动及录制、拍摄期间 Protection of prototypes during events and film or photo shoots	AL 3
7.	数据保护 依据欧洲《通用数据保护条例》（GDPR）第 28 条“Processor”（“处理人”） Data protection According to Article 28 (“Processor”) of the European General Data Protection Regulation (GDPR)	AL 2
8.	数据保护——针对 特殊类个人信息 依据欧洲《通用数据保护条例》（GDPR）第 28 条“Processor”（“处理人”），以及第 9 条中关于特殊类个人信息的规定 Data protection with special categories of personal data According to Article 28 (“Processor”) with special categories of personal data as specified in Article 9 of the European General Data Protection Regulation (GDPR)	AL 3

表格 6. TISAX 评估对象与评估级别对照

评估级别 1（AL 1）：

评估级别 1 主要针对公司内部用途，是真正意义上的自我评估(self-assessment)。

为确认是否符合该级别（级别 1），审计人员只会检查是否存在完整的自我评估结果，但不会对自我评估的内容进行评估，甚至也不会要求提供进一步的证据。

该级别（级别 1）的评估结果可信度低，因而不被 TISAX 采纳。但是，您的合作伙伴仍然完全有可能会要求您在 TISAX 评估的框架之外，额外完成这样一份自我评估。

评估级别 2（AL 2）：

为确认是否符合该级别（级别 2），审计服务提供商会对您的自我评估结果（针对评估范围内的所有地点）执行合理性检查。此外，审计服务提供商还会检查相关的证据[11]，并约您以及其他同事谈话。

审计服务提供商通常以电话会议的形式完成谈话过程，您亦可要求其与您进行面对面谈话。

该评估级别（级别 2）一般不包含现场检查。但如果您选择了其中一个“原型”评估对象，则评估过程将总是包含一次现场检查。

如果某些证据材料不方便寄给审计服务提供商，则可要求其进行现场检查。这样一来，审计服务提供商依然可对这类“仅供内部使用”的证据执行检查。

评估级别 3（AL 3）：

为确认是否符合该级别（级别 3），审计服务提供商会执行评估级别 2 所要求的所有检查，只不过，相关检查的范围会更广，并且审计服务提供商将通过深入开展现场检查以及面对面谈话等形式，来全面核查您的自我评估结果。

下表中简要列出了与各评估级别相对应的审计方法：

评估方法	评估级别 1 （AL 1）	评估级别 2 （AL 2）	评估级别 3 （AL 3）

评估方法	评估级别 1 (AL 1)	评估级别 2 (AL 2)	评估级别 3 (AL 3)
自我评估	是	是	是
证据	否	合理性检查	全面核查
谈话	否	通过电话会议[12]	面对面、现场
现场检查	否	根据您的要求	是

表格 7. 评估方法的适用性——针对不同的评估级别

补充信息：

- 信息分类与保护需求
  对于不同的合作伙伴来说，信息分类（如“保密级”、“绝密级”）与保护需求之间的对应关系可能亦有差别。因此，即使我们愿意，我们也无法做到以简洁明了的表格形式，为您——列出合作伙伴的信息分级体系与保护需求之间严格的对应关系。
- 仅仅知道评估级别是不够的
  某些合作伙伴可能会要求您接受 TISAX 特定“评估级别”的评估。您需要明白，仅仅知道评估级别，是不足以启动 TISAX 流程的。因为，只有在与某个 ISA 标准目录及其相应的保护需求结合使用时，评估级别才有意义。通常，合作伙伴会要求您获得 TISAX 标签（即“标准目录 + 保护需求”）。然而，由于保护需求同评估级别之间是 1:1 的对应关系，因此，您只需知道“标准目录 + 评估级别”即可。
- 评估级别的上下级关系
  高评估等级总是包含低评估等级。例如，如果您的评估是基于评估等级 3，那么它将自动满足评估等级 2 的所有要求。
- 我们关于评估级别选择的建议
  如果您需要根据自己的判断来选择评估对象（并指明相应的评估级别），我们建议为评估对象指定“评估级别 3”。在 TISAX 体系中，评估级别 3 所对应的评估工作力度并不总是高于评估级别 2。
  但是，有多个合作伙伴的供应商通常都会为评估对象选择“评估级别 3”。这样一来，便可充分准备好应对未来的一切要求，而无需费时费力去指定不同的评估级别。
- 其他经济考量
  关于评估级别，一次 TISAX 评估的总成本包括您公司内部相关工作的成本，外加上评估本身的成本。虽然评估级别 2 对应的评估成本更低，但由此带来的您公司内部相关工作的成本可能会更高。原因是，评估级别 2 通常要求进行更全面的自我评估，以及提供更完整的内部相关文件。而对于评估级别 3，通常只需要为审计人员介绍整体情况，并提供一些基本文件即可。但是，若无现场检查这一环节的话，审计人员会要求提供更多相关文件。所以说，选择评估级别 3 而非评估级别 2 这一做法并不罕见，只不过，做出这一选择的通常是规模较小，而非规模较大的企业。

4.3.3.7. 评估对象与您供应商之间的关系

选择 TISAX 并不一定意味着，您所有的供应商都要满足同样的要求。如果您的评估对象为“信息安全——保护需求*极高*”，那么这并不是说，您的供应商都要在相同的评估对象方面达标，更不是说他们都需要获得 TISAX 标签。

只不过，您仍需自行审核并判断，使用供应商所提供的服务是否会增加风险，或带来新风险。

两个非常简化的示例：

1. 您公司有一项规定，普通的电子邮件不能用于发送保护需求极高的信息。那么，您的电子邮件服务商便无需获得 TISAX 标签（极高保护需求）。
   同样，如果您只发送加密邮件的话，邮件服务商甚至都看不到“保护需求极高”的信息，上述结论也一样成立。
2. 您将已打印出的“保护需求极高”的信息放入碎纸机中进行处理。这种情况下，废物处理服务提供商自然也无需满足与您一样的要求。

然而，经过风险评估后，有可能出现您的供应商亦需满足针对“极高保护需求”的要求这一情况。此时，TISAX 标签便是一种可为您提供相应证明的可选方案。

4.3.4. 费用

我们收取评估费用。您可浏览我们的价目表，了解相关费用、折扣以及付款条件等信息。

价目表可登录我们的网站下载：
enx.com/en-US/TISAX/downloads/
下载 PDF：
enx.com/tisaxgtcen.pdf

在注册准备期间，有一些与账单相关的问题需要您考虑清楚：

- 账单地址选择
  默认情况下，我们会将账单发送至您作为参与者所提供的地址，但您也可以提供其他地址来用于接收账单。
  请认真检查账单地址。根据会计法要求，账单上的地址需要与您公司的（账单）地址保持一致。
- 更改账单地址
  与您提供的其他信息不同，您一旦在流程中选定了账单地址，我们将无法进行更改。如果您需要通过另一个地址来接收账单，请联系我们。
  请注意：如果您在选择账单地址之前，暂停并随后回到注册流程，那么您将无法再执行地址选择操作。我们将与您联系，告知您账单地址缺失一事，并请您提供该信息，从而为您录入系统中。
- 订单参考编号
  如果您需要在账单上显示某个特定的采购订单号或类似内容，那么您可以向我们提供一个订单参考编号。
- 增值税编号
  我们的一切收费均包含德国增值税（如适用）。
  我们需要该编号来处理欧盟内部的付款。如果您的账单地址属于以下国家之一，那么必须提供增值税编号：
  奥地利、比利时、保加利亚、克罗地亚、塞浦路斯（希腊部分）、捷克共和国、丹麦、爱沙尼亚、芬兰、法国、德国、希腊、匈牙利、爱尔兰、意大利、拉脱维亚、立陶宛、卢森堡、马耳他、荷兰、波兰、葡萄牙、斯洛伐克、斯洛文尼亚、西班牙、瑞典、英国
- 供应商管理

重要提示：

请您理解，鉴于所有 TISAX 参与者之间的对等关系，我们不接受其他任何类型的条款（如一般采购条款、行为准则）。

关于我们账单流程的其他信息：

- 我们不接受个人采购条款
- 我们接受：
  - 转账汇款至账单上指定的银行账户
  - 信用卡付款（注册期间，通过我们的付款服务提供商“Stripe” (https://stripe.com)）
- 我们的账单将包含以下有关您的注册信息：
  - 您的主要参与者联系人的姓名和电子邮件地址
  - 评估范围名称

  账单样式请见附录章节 7.1, “附录：账单示例”。

- 我们提供的大多数账单信息都是您在处理账单时通常所需要的，更多相关信息可参见我们的文档“成员与业务伙伴信息（Information for Members and Business Partners）”。如需要最新版本，请邮件联系我们。

请注意：

我们知道，有时公司的内部付款审核流程相当繁琐。因此，您在 TISAX 流程中完成下一步骤本身并不受我们是否收到付款的影响。但请注意，如果我们未收到付款的话，您将无法共享评估结果。
鉴于此，我们建议您确保，我们能够将账单发送给合适的接收人，并且账单中包含订单参考编号（如适用）。毕竟，您可能也希望在公司内部跟踪账单的付款状态。

重要提示：

我们—ENX 协会—将收取一定的费用，该费用只是 TISAX 评估总费用的一部分。您的 TISAX 审计服务提供商将收取评估费用。

更多关于审计服务提供商相关费用的信息，可参见章节 5.3.4, “评估执行人选择依据”。

重要提示：

无论是以下哪种情况，您均需缴纳费用：

- 继续 TISAX 流程与否。
- 是否成功通过 TISAX 评估流程。

因此，账单可能在您启动预评估之前便已经到达。

4.4. ENX 门户

以下章节将讲述在线注册流程，在这一流程中，你需要输入前述章节中建议您收集的所有信息。在开始在线注册流程之前，我们来简要介绍一下 ENX 门户的作用与好处。

ENX 门户允许我们维护一个包含所有 TISAX 参与者的数据库，它在整个 TISAX 流程期间扮演着重要的角色。在 TISAX 注册期间，您输入的信息将随后被 TISAX 审计服务提供商使用（如果您同意），来相应计算报价并制定评估程序计划。完成 TISAX 评估流程后，您将使用 ENX 门户上的交换平台，来与您的合作伙伴共享评估结果。

该门户叫做“ENX 门户”而非“TISAX 门户”，是因为我们还利用门户来管理其他业务活动（如 ENX network (https://enx.com/enxnetwork/)）。

4.5. 在线注册流程

如果您根据我们的上述建议（章节 4.3, “注册准备”）进行了准备，那么您便可启动在线注册流程了。

4.5.1. 所需时间

注册所需时间很大程度上取决于您注册的范围和地点数量。作为参与者，如果打算注册一个范围和一处地点，那么预计至少需要 20 分钟的时间来完成注册。

我们建议，在单次对话中一次性完成注册，否则跟上后面步骤的节奏会比较吃力。若您确实需要中止注册，那么我们会联系您，并要求您提供缺失的信息。

4.5.2. 此处开始

您可登录我们的网站进行注册：
enx.com/en-us/Account/Login/Register?returnUrl=%2FTISAX%2Ftisax-initial-registration%2F

您只需按照屏幕提示操作即可。以下是关于注册流程的简要介绍。

4.5.3. 门户账号

注册的第一步，是在 ENX 门户中为自己创建一个账号。这一步是例行公事，因为您正是需要利用门户账号，才能够管理您公司的“参与者信息”。

创建账号后，您并不会自动成为您公司的正式 TISAX 联系人。[13] 到目前为止，您仅仅是在填写在线注册表。您可在注册流程的后续环节确定“参与者联系人”和“范围联系人”，并将此角色分配给合适的人选。

请注意：

如果 ENX 门户提示您，您的邮件地址已被使用，请联系我们。 该提示信息可能表明，由于某些其他原因，您的信息已录入我们的系统中。

请注意：

如上所述，创建门户账号并不意味着已成为“参与者联系人”或“范围联系人”（见下文），可以积极参与评估流程。

反之亦然，“参与者联系人”或“范围联系人”也不会自动获得门户账号中参与者信息的管理权限。也就是说，被指定为“参与者联系人”或“范围联系人”的同事不会自动获得 ENX 门户中参与者信息的访问权限。

如果您希望将管理参与者信息的权限授予一名您已在 ENX 门户中创建的联系人（不管您是否为其分配了角色），请联系我们。 我们将向该联系人发送邀请邮件，邮件中包含链接，可引导其创建自己的门户账号。

在请求我们分配该权限之前，请确保您已经创建了新的联系人。

4.5.4. 参与者注册

第二步，是将您的公司注册为“TISAX 参与者”。“TISAX 参与者”是指与其他参与者交换评估结果的公司。

4.5.5. 参与者联系人

我们会要求您指定主要的参与者联系人。

主要联系人通常负责与您公司的信息安全评估有关的一切事宜。其可以是您，也可以是您公司里的其他人。

通常，我们只需要您指定主要联系人。若您希望，其他人亦可以看到由我们和我方的 TISAX 审计服务提供商所发送的所有注册流程交流信息，则请添加“备选参与者联系人”。

重要提示：

我们建议，为每个联系人指定至少一名代理人。一旦联系人暂时联络不上或不在公司，则可由他人代为管理您公司的参与者信息。+ 否则，如果要新指定一名联系人（非其他现有的有效联系人）的话，相关流程会比较复杂，因为我们的流程旨在确保，只有公司的合法代言人才有资格批准新指定一名主要联系人。

请注意：

您可在后续流程中（甚至是在完成在线注册流程，或完成评估之后），随时添加或删除联系人。

请注意：

参与者联系人不可使用公共邮箱（例如“info@acme.com” 或 “IT@acme.com”）作为电子邮件地址。

这一规定也符合 ISA 关于用户登录的规定。

请注意：

对于每一位联系人，您可以选择是否为其授予访问您公司参与者信息的权限。具体做法如下：

1. 您只是添加联系人，该联系人的信息录入我们系统，但其没有登录或管理信息的权限。
2. 或者，您邀请联系人。ENX 门户将向该联系人发送邀请邮件，联系人须按照其中邀请链接的内容提示进行操作。在创建了自己的 ENX 门户账号后，该联系人便可管理您公司的参与者信息。

4.5.6. 一般条款和条件

第三步，是接受“TISAX 参与一般条款和条件”。

相关注解，可参见上述 章节 4.3.1, “法律基础”。

4.5.7. 评估范围注册

第四步，是为您的信息安全评估注册评估范围。

您需要做的是：

- 指定评估范围名称。
  我们将在下文中使用“范围名称”来代指该范围。
- 选择评估范围类型。
  （标准、自定义）
  相关注解，可参见上述章节 4.3.2, “TISAX 评估范围”。
- 指定主要范围联系人。
  该联系人通常负责特定范围的评估事宜，其可以是您，也可以是您公司里的其他人。
  通常，我们只需要您指定主要范围联系人。若您希望，其他人亦可以看到由我们和我方的 TISAX 审计服务提供商所发送的、与该特定范围相关的所有交流信息，您可添加“备选参与者联系人”。
- 选择评估对象。
  相关注解，可参见上述章节 4.3.3, “评估对象”。
- 添加评估范围地点
  我们会要求您指定从属于评估范围的所有相关地点。
  相关注解，可参见上述章节 4.3.2, “TISAX 评估范围”。
- 选择发布与共享级别（可选）
  在此阶段，您便已经可以决定，是否向其他 TISAX 参与者发布您的评估结果，并与您的合作伙伴共享评估结果。通常，该操作步骤会授权我们至少显示以下信息：您的公司是一名参与者，且已成功通过 TISAX 评估流程。
  在最初注册时，您可选择跳过此步骤，并于之后的某个时间再设定您评估结果的访问权限。
  相关注解，可参见上述章节 4.3.2.8, “发布与共享”。

  重要提示：

  发布或共享权限一旦设定，将无法撤销。
  更多信息，请参阅章节 6.4, “交换结果操作的不可逆性”。
- 指定账单接收人。
  我们会要求您指定账单的接收人。
  相关注解，可参见上述章节 4.3.4, “费用”。

请注意：

每一项评估范围都会经历一个工作周期。在目前阶段，您的评估范围的状态可能为“未完成（Incomplete）”、“等待您的指令（Awaiting your order）”或者“等待 ENX 批准（Awaiting ENX approval）”。

关于评估范围状态的更多信息，请参见章节 7.5.1, “概述： 评估范围状态”。

请注意：

对于有许多地点的大型企业，TISAX 提供“快捷群体评估”服务。如果您满足下列条件，则可以考虑选择该服务：

- 您的评估范围中至少有三处地点[14]，并且
- 您的信息安全管理体系运作良好，且集中管理。[15]

对于“快捷群体评估”而言，初期工作量会比较大。但是，您的评估地点越多，您越能从这一服务中受益。

有关“快捷群体评估”的更多信息，请参见文档“TISAX 快捷群体评估（TISAX Simplified Group Assessment）”。

您可登录我们的网站，下载文档“TISAX 快捷群体评估（TISAX Simplified Group Assessment）”：
enx.com/en-US/TISAX/downloads/

下载 PDF：
enx.com/sga.pdf

请注意：

一旦我们注册了您的评估范围，您将无法自行更改。

如果您能以可靠的方式向我们保证，还未将您的“TISAX 范围摘要（TISAX scope excerpt）”发给我方的审计服务提供商，则请联系我们， 由我们为您更改。

如果您已经将“TISAX 范围摘要（TISAX scope excerpt）”发给了我方（其中一个）审计服务提供商，则您只需在 ENX 门户中创建新地点（如适用），并与您的审计服务提供商讨论相关变更事宜即可，后者将基于变更内容来执行评估工作。之后，您的审计服务提供商将会把与评估范围相关的必要变更信息，连同评估结果一道告知我们。

请注意：

一旦您创建了一个新地点，您将无法自行编辑。若要做微小的改动（如更改公司名称，以及街道名称、邮编、城市等信息中的输入错误），请联系我们， 由我们来为您更正。

请注意：

在 ENX 门户中，您无法删除评估范围。若因不小心错误创建了评估范围，请联系我们， 由我们来为您删除。

4.5.8. 确认邮件

在您完成上述所有强制性步骤后，我们将对您的申请进行审核，并向您发送确认邮件。

该邮件包含两项重要信息：

- 所有 TISAX 审计服务提供商的联系人列表
  为针对您的评估范围来相应执行评估工作，您必须选择我方其中一家 TISAX 审计服务提供商。您可以通过联系人来咨询评估事宜。
  有关审计服务提供商选择的更多信息，请参见章节 5.3, “选择审计服务提供商”。
- 以 PDF 附件形式提供的“TISAX 范围摘要（TISAX Scope Excerpt）”

  该文件包含：
  - 我们数据库中储存的信息
  - 您的参与者 ID
    请参见下文章节 4.5.8.1, “Participant ID（参与者 ID）”
  - 您的范围 ID
    请参见下文章节 4.5.8.2, “Scope ID（范围 ID）”

关于确认邮件的样式，请参见章节 7.2, “附录：确认邮件示例”。

关于“TISAX 范围摘要（TISAX Scope Excerpt）”的示例，请参见章节 7.3, “附录：TISAX 范围摘要示例”。

通常，您将在 3 个工作日内收到我们的确认邮件。

如果 7 个工作日内未收到我们的通知，请检查自己所提供的信息是否完整。只有在信息完整的情况下，我们才会启动注册处理流程。如果您认为，所提供的信息是完整的，而我们却没有联系您，那么请您与我们联系。

我们会将确认邮件发送给“主要参与者联系人”以及所有的“备选参与者联系人”。

请注意：

每一项评估范围都会经历一个工作周期。在目前阶段，您的评估范围的状态为“已批准（Approved）”。

关于评估范围状态的更多信息，请参见章节 7.5.5, “Assessment scope status “Awaiting your payment”（评估范围状态“等待您的付款”）”。

以下两个子章节将详细介绍“参与者 ID”与“范围 ID”的作用。

4.5.8.1. Participant ID（参与者 ID）

参与者 ID 的特点：

- 标识某个 TISAX 参与者。
- 对每个参与者来说是唯一的。
- 在完成注册后，由我们进行分配。
- 是我方所有 TISAX 审计服务提供商执行信息安全评估工作的前提条件。
- 参与者 ID 示例：

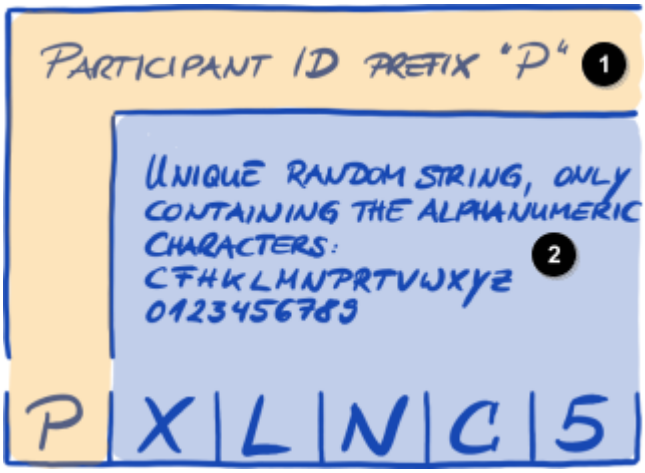


插图 9. 参与者 ID 的格式[16]

1. 参与者 ID 的前缀是“P”
2. 为唯一、任意字符串，只包含字母和数字：
   CFHKLMNPRTVWXYZ
   0123456789

请注意：

查找您的参与者 ID 有两种方法：

1. 查看您的“TISAX 范围摘要（TISAX Scope Excerpt）”。
   请参见上文 章节 4.5.8, “确认邮件”
   如果您手头上没有“TISAX 范围摘要”，请联系我们获取。
2. 登录 ENX 门户 (https://enx.com/)，前往主导航栏，选择 “DASHBOARD” (仪表板)。您在此处便可看到您的参与者 ID。

4.5.8.2. Scope ID（范围 ID）

范围 ID 的特点：

- 标识某个评估范围。
- 对每个评估范围来说是唯一的。
- 在完成注册后，由我们进行分配。
- 是允许我方所有 TISAX 审计服务提供商执行信息安全评估工作的前提条件。
- 参与者 ID 示例：

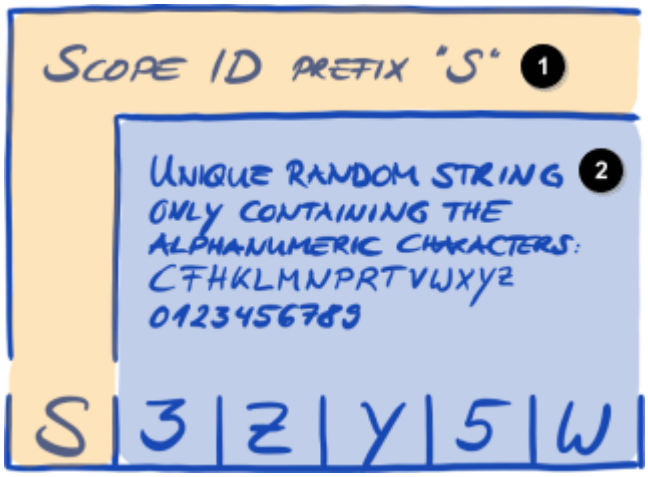


插图 10. 范围 ID 的格式

1. 范围 ID 的前缀是“S”
2. 为唯一、任意字符串，只包含字母和数字：
   CFHKLMNPRTVWXYZ
   0123456789

请注意：

查找您的范围 ID 有两种方法：

1. 查看您的“TISAX 范围摘要（TISAX Scope Excerpt）”。
   请参见上文 章节 4.5.8, “确认邮件”
   如果您手头上没有“TISAX 范围摘要”，请联系我们获取。
2. 登录 ENX 门户，前往主导航栏，选择“我的 TISAX（MY TISAX）”，然后选择“范围和评估（SCOPES AND ASSESSMENTS）”。您在此处便可看到您的范围 ID。

请注意：

每一项评估范围（由范围 ID 标识）都会经历一个工作周期。

关于评估范围状态的更多信息，请参见 章节 7.5, “附录：Assessment scope status（ 评估范围状态）”。

4.5.9. 状态信息

在当前阶段，我们使用以下两种状态，来描述您在 TISAX 流程中所处的位置：

1.参与者状态
2.评估范围状态

下图中说明了，为达到某个状态所必需满足的条件：

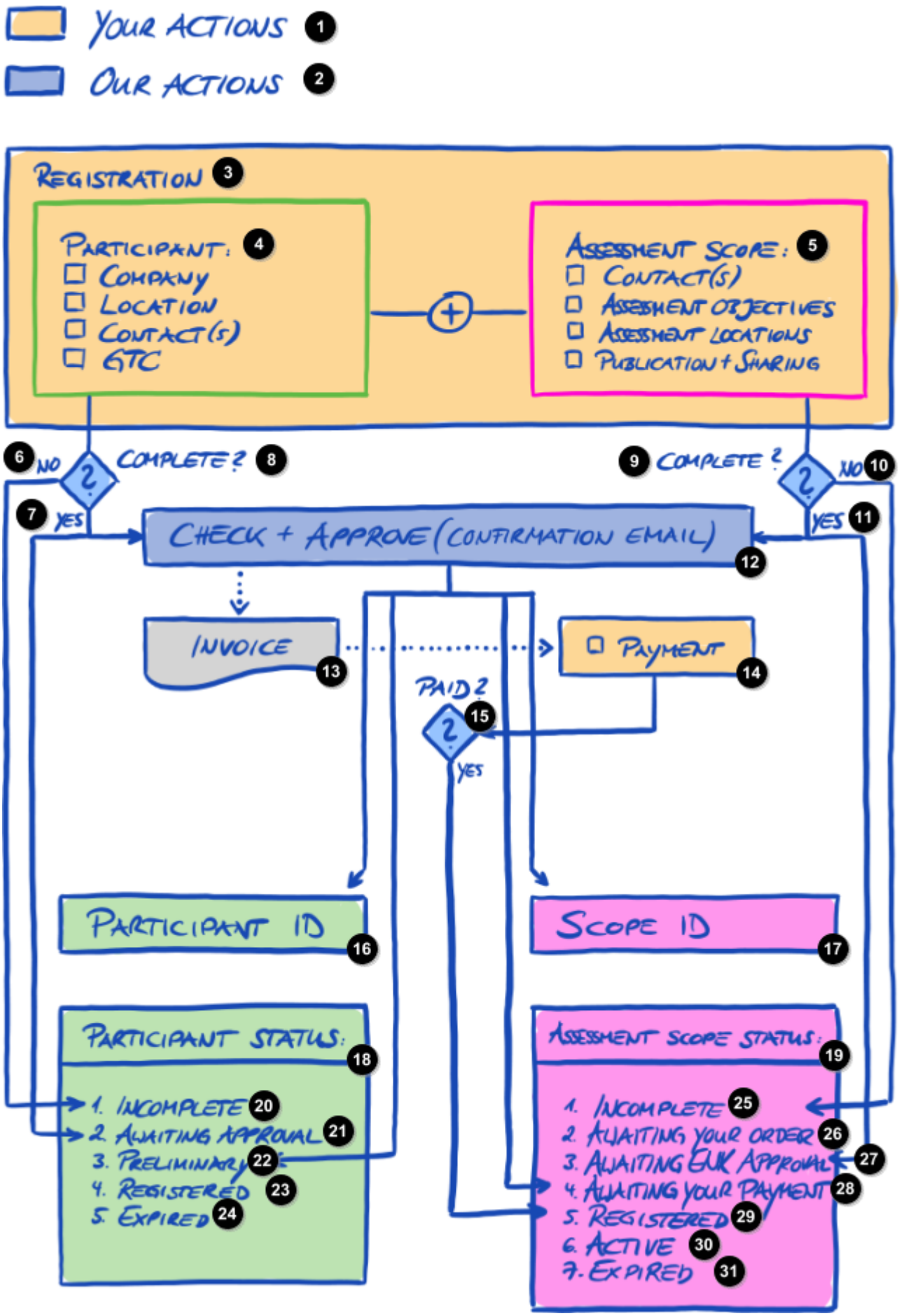


插图 11. “参与者状态”和“评估范围状态”的满足条件

1 您的行动

2. 我们的行动
3. 注册
4. 参与者：
   [ ] 公司
   [ ] 地点
   [ ] 联系人
   [ ] 一般条款和条件（GTC）
5. 评估范围：
   [ ] 联系人
   [ ] 评估对象
   [ ] 评估地点
   [ ] 发布 + 共享
6. 否
7. 是
8. 完成?
9. 完成?
10. 否
11. 是
12. 审核 + 批准（确认邮件）
13. 账单
14. [ ] 付款
15. 已付款?
16. 参与者 ID
17. 范围 ID
18. 参与者状态：
19. 评估范围状态：
20. 1.未完成
21. 2.等待批准
22. 3.初步完成
23. 已完成注册
24. 已失效
25. 1.未完成
26. 2.等待您的指示
27. 3.等待 ENX 批准
28. 4.等待您的付款
29. 5.已完成注册
30. 6.已通过评估
31. 7.已失效

关于状态的含义，以及您如何顺利过渡到下一个状态，请参见附录。

要进一步了解：

- 参与者状态，请见章节 7.4, “附录：Participant status（参与者状态）”。
- 评估范围状态，请见 章节 7.5, “附录：Assessment scope status（评估范围状态）”。

4.5.10. 更改注册信息

请注意：

有关信息工作周期的所有解答，请参见章节 7.8, “附录：参与者信息工作周期管理”. 该章节为您讲述如何更改或更新相关数据，如您的公司名称或联系人信息。

恭喜！现在，您已是一名 TISAX 注册参与者，可以前往 TISAX 流程的下一步骤。

5. 评估（第二步）

阅读“评估”章节预计需要 30-35 分钟。

5.1. 总述

评估是 TISAX 流程的第二步，也是完成 TISAX 评估最主要的一个环节。

以下章节内容将带您完成评估这一步：

1. 首先，我们将介绍如何利用ISA 自我评估来确定，您是否已准备好接受 TISAX 评估。
2. 之后，我们将就如何选择TISAX 审计服务提供商，来相应给出建议。
3. 接下来，我们为您具体讲述评估流程。
4. 最后，我们将阐述“流程结果”：即您的评估结果以及相关的TISAX 标签。

5.2. 基于 ISA 的自我评估

为了准备接受 TISAX 评估，首先，您需要将自己的信息安全管理体系（ISMS）调整到最佳状态。为了确认您的 ISMS 是否达到预期的成熟度等级，您应依据 ISA 标准来做一次自我评估。

“信息安全评估”（Information Security Assessment，简称 ISA）是一套标准目录，由“德国汽车工业协会”（Verband der Automobilindustrie e.V.——简称 VDA）发布，是汽车行业执行信息安全评估的通用标准。

以下章节主要以实例形式，来讲解如何完成基于 ISA 的自我评估。

本手册中的阐释、示例和截图依据的是 ISA 文件（版本：5.0.3）。

请注意：

欲了解与以往的 ISA 版本相比出现了哪些变化，可参见其 Excel 表“变更历史（Change history）”，来获得相关信息。

请注意：

当 VDA 发布 ISA 新版本时，哪一套 ISA 版本适合作您评估之用？相关信息，请参见 章节 7.9, “附录：ISA 工作周期管理”。

5.2.1. 下载 ISA 文件

开始自我评估之前，请先下载 ISA 文件。

您可从 VDA 网站下载：
portal.enx.com/isa5-en.xlsx

ISA 德语版请见：
portal.enx.com/isa5-de.xlsx

5.2.2. 看懂 ISA 文件

在开始自我评估之前，建议您阅读以下说明信息，这可能会有助于您完成相关工作。除了提供 ISA 文件中的官方阐释和定义外，我们还提供这些说明信息是为了重点讲述在 TISAX 评估中的应用。

5.2.2.1. 标准目录

当前，ISA 有三大“标准目录”[17]：

1.	信息安全	Information Security
2.	原型保护	Prototype Protection
3.	数据保护	Data Protection

每一个标准目录都有对应的 Excel 表：

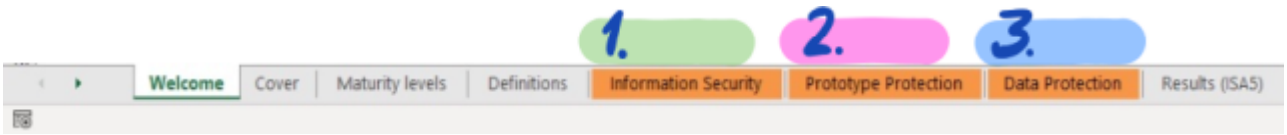


插图 12. 截图：ISA 标准目录（Excel 表）

ISA 的核心是“信息安全”这个标准目录。无论是哪一次 TISAX 评估，这个标准目录中的问题总是必选项。

而另外两大标准目录则为可选项，其是否适用于评估，取决于您的评估对象。

前述提到的评估对象与这些标准目录呈对应关系：

序号	评估对象(Assessment objective)	ISA 标准目录
1.	保护需求较高的信息 Handling of information with high protection needs	Information Security (信息安全)
2.	保护需求 极高的信息 Handling of information with very high protection needs	Information Security (信息安全)
3.	原型零部件保护 Protection of prototype parts and components	Prototype Protection (原型保护)
4.	原型车保护 Protection of prototype vehicles	Prototype Protection (原型保护)
5.	试验车处理 Handling of test vehicles	Prototype Protection (原型保护)

序号	评估对象(Assessment objective)	ISA 标准目录
6.	原型保护——活动及录制、拍摄期间 Protection of prototypes during events and film or photo shoots	Prototype Protection (原型保护)
7.	数据保护 依据欧洲《通用数据保护条例》（GDPR）第 28 条“Processor”（“处理人”） Data protection According to Article 28 (“Processor”) of the European General Data Protection Regulation (GDPR)	Data Protection (数据保护)
8.	数据保护——针对 特殊类个人信息 依据欧洲《通用数据保护条例》（GDPR）第 28 条“Processor”（“处理人”），以及第 9 条中关于特殊类个人信息的规定 Data protection with special categories of personal data According to Article 28 (“Processor”) with special categories of personal data as specified in Article 9 of the European General Data Protection Regulation (GDPR)	Data Protection (数据保护)

表格 8. TISAX 评估对象与 ISA 标准目录之间的对应关系

示例：如果您选择了评估对象“数据保护”，则必须回答“信息安全”和“数据保护”这两个标准目录中的问题。

您可能注意到了，每个标准目录所对应的评估对象不止一个。那么，如何知道哪些要求适用于哪个评估对象？

下表将为您展示所适用的要求：

序号	评估对象 (Assessment objective)	适用要求
1.	保护需求较高的信息 Handling of information with high protection needs	▪ 标准目录“Information Security” (信息安全) (“Requirements (must)” (要求 (必须)) 和 “Requirements (should)” (要求 (应当)) 列) 中的所有要求 ▪ 外加“Additional requirements for high protection needs” (针对“高”保护需求的其他要求) (如适用) 列中的其他要求
2.	保护需求 极高的信息 Handling of information with very high protection needs	▪ 标准目录“Information Security” (信息安全) (“Requirements (must)” (要求 (必须)) 和 “Requirements (should)” (要求 (应当)) 列) 中的所有要求 ▪ 外加“Additional requirements for very high protection needs” (针对 极高保护需求的其他要求) (如适用) 列中的其他要求

序号	评估对象 (Assessment objective)	适用要求
3.	原型零部件保护 Protection of prototype parts and components	▪ 适用于评估对象“保护需求较高的信息”的所有要求 ▪ 外加标准目录“Prototype Protection” (原型保护) 以下章节中的要求: ▪ 8.1 Physical and Environmental Security (物理和环境安全) ▪ 8.2 Organizational Requirements (组织要求) ▪ 8.3 Handling of vehicles, components and parts (车辆、零部件的处理)
4.	原型车保护 Protection of prototype vehicles	▪ 适用于评估对象“保护需求较高的信息”的所有要求 ▪ 外加标准目录“Prototype Protection” (原型保护) 以下章节中的要求: ▪ 8.1 Physical and Environmental Security (物理和环境安全) ▪ 8.2 Organizational Requirements (组织要求) ▪ 8.3 Handling of vehicles, components and parts (车辆、零部件的处理) ▪ 外加“Additional requirements for vehicles classified as requiring protection” (针对“被列为需要保护的车辆”的其他要求) (如适用) 列中的其他要求
5.	试验车处理 Handling of test vehicles	▪ 适用于评估对象“保护需求较高的信息”的所有要求 ▪ 外加标准目录“Prototype Protection” (原型保护) 以下章节中的要求: ▪ 8.2 Organizational Requirements (组织要求) ▪ 8.3 Handling of vehicles, components and parts (车辆、零部件的处理) ▪ 8.4 Requirements for trial vehicles (试验车辆要求)
6.	原型保护——活动及录制、拍摄期间 Protection of prototypes during events and film or photo shoots	▪ 适用于评估对象“保护需求较高的信息”的所有要求 ▪ 外加标准目录“Prototype Protection” (原型保护) 以下章节中的要求: ▪ 8.2 Organizational Requirements (组织要求) ▪ 8.3 Handling of vehicles, components and parts (车辆、零部件的处理) ▪ 8.5 Requirements for events and shootings (活动和拍摄要求)
7.	数据保护 Data protection	▪ 适用于评估对象“保护需求较高的信息”的所有要求 ▪ 标准目录“Data Protection” (数据保护) 中的所有要求

序号	评估对象 (Assessment objective)	适用要求
8.	数据保护——针对 特殊类个人信息 Data protection with special categories of personal data	▪ 适用于评估对象“保护需求 极高的信息”的所有要求 ▪ 标准目录“Data Protection” (数据保护) 中的所有要求

表格 9. 要求是否适用于评估对象

以下截图展示了每个标准目录中相关问题的主要元素。我们将在下文中逐一解释这些元素。

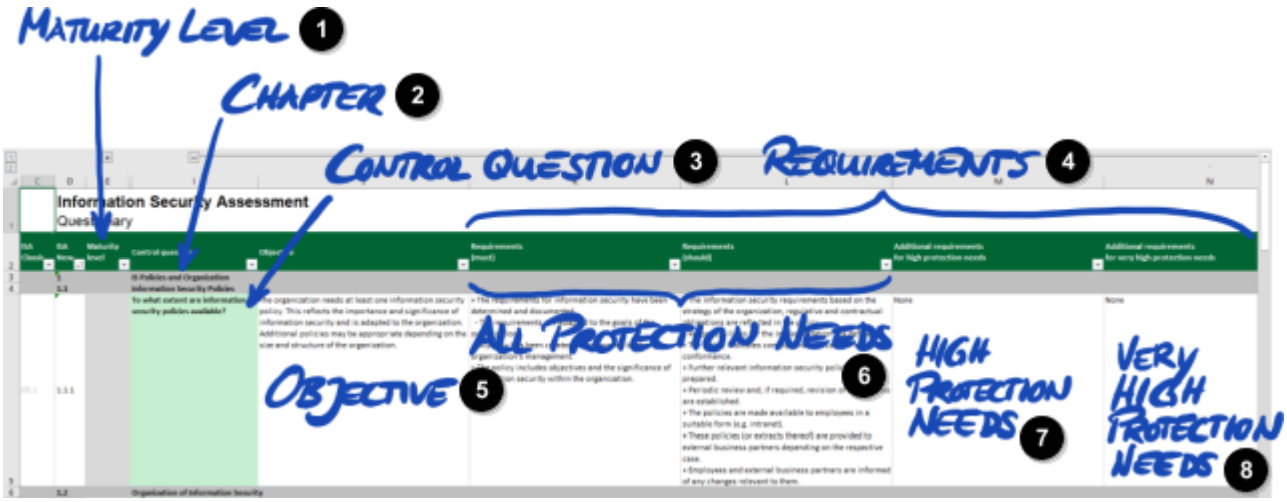


插图 13. 截图：ISA 标准目录中相关问题的主要元素

1. 成熟度等级
2. 章节
3. “控制”问题
4. 要求
5. 对象
6. 所有保护需求
7. “高”保护需求
8. “极高”保护需求

5.2.2.2. 章节

每个标准目录都以章节形式对问题进行分组。

例如：“4 身份识别与访问管理”

分组依据的是信息安全管理体系的多个方面。

5.2.2.3. “控制”问题

针对每一个标准目录，您可在相应的 Excel 表中看到该问题。

例如：“4.1.2 用户在访问网络服务、IT 系统及 IT 应用时，其安全性保障程度如何？”

“控制”问题亦称作“控制点”，是“审计人员行话”。ISA 所依据的 ISO 标准使用“控制”一词。

5.2.2.4. 自我评估表单字段

在“Maturity level” (成熟度等级) 列和 “Control question” (控制问题) 列之间，是您在进行自我评估时需要填写的表单字段：

表单字段	用途	是否必须填写?
Implementation description (实施描述) (F 列)	您应在此处简要说明，为了在您公司应对提到的“控制”问题，您都做了哪些工作。	是
Reference Documentation (参考文件) (G 列)	您应在此处说明，哪个（些）文件可以证明您所做的工作。	是
Findings/Result (发现/结果) (H 列)	如果您认为理想情况与实际情况不符，那么您可在此处填写相关发现。	否

表格 10. 自我评估表单字段及其用途

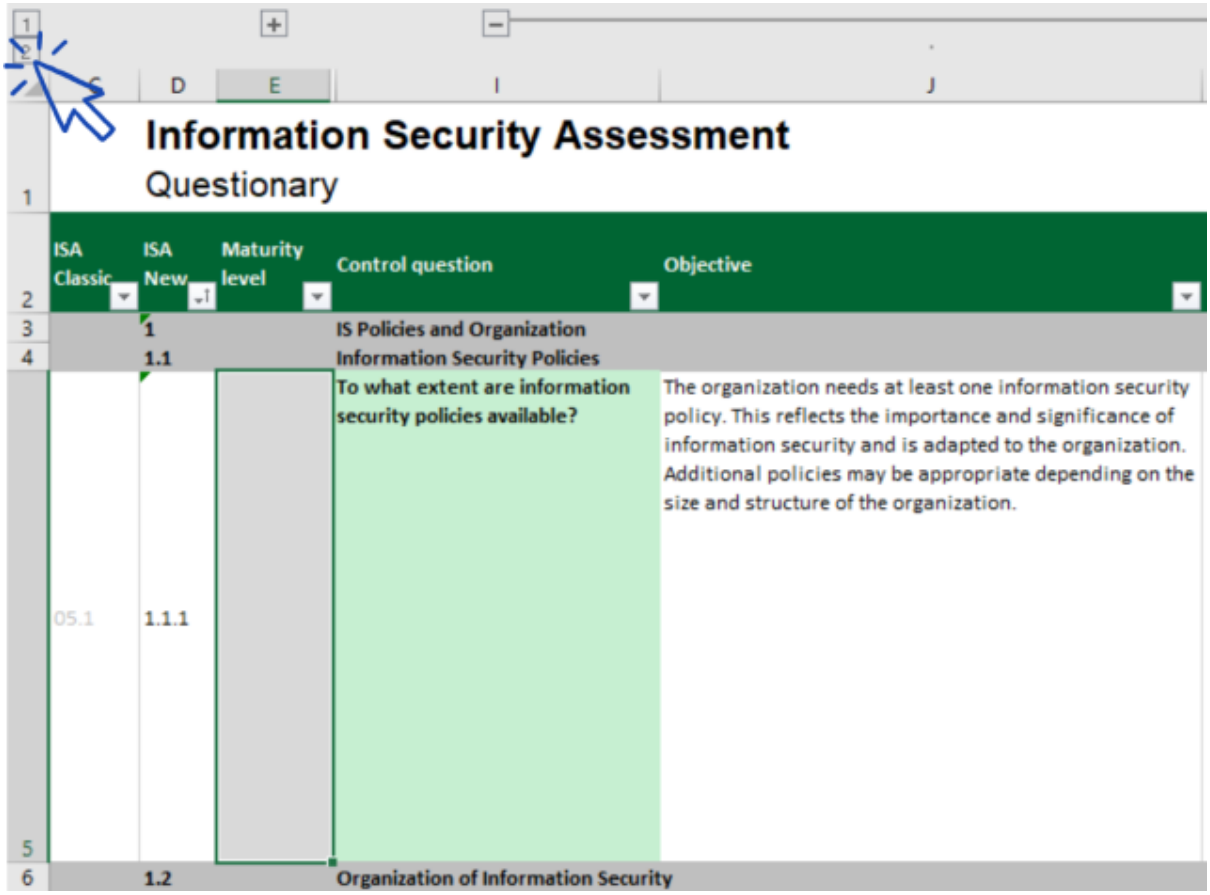
只有“实施描述”和“参考文件”为必填项。上述信息将有助于我们的 TISAX 审计服务提供商更好地了解您的公司，从而更有针对性地准备评估工作。

为了支持您开展自我评估，以下几列信息可供您参考：

- Measures/recommendations (措施/建议) (R 列)
- Date of assessment (评估日期) (S 列)
- Date of completion (完成日期) (T 列)
- Responsible department (负责部门) (U 列)
- Contact (联系人) (V 列)

重要提示：

如果您打开下载后的 Excel 文件，并选择其中一个标准目录工作表（如“信息安全”），那么您可能不会立即看到自我评估表单字段。为了令其显示，您需要点击“2”级分组按钮。[18] 该按钮位于 C1 单元格左上方，点击后将扩展视图，从而显示自我评估表单字段。



另一个方法是，按住箭头向下滚动。由于单元格中的信息量庞大，因而在拖动滚动条时，需要精确掌握好滑移位置。如果您利用指针设备的滚动功能来实现这一点，那么您可能会不经意间跳过某些内容较多的单元格。

5.2.2.5. 目标

“控制问题（Control question）”列的右侧是“目标（Objective）”列（J 列）。该栏内容描述了，为了在所提到的方面使您的信息安全管理符合要求，您需要具体做什么。

示例（针对控制问题 4.1.2）：“只有经过安全识别（验证）的用户才能访问 IT 系统。鉴于此，将通过适当的流程来确认用户的身份，从而确保访问安全。”

5.2.2.6. 要求

要求是指为了实现目标而需要满足的条件。

相关要求分布在以下四列中：

1. Requirements (must) (要求 (必须)) (K 列)
2. Requirements (should) (要求 (应当)) (L 列)
3. Additional requirements for high protection needs (针对“高”保护需求的附加要求) (M 列)
4. Additional requirements for very high protection needs (针对“极高”保护需求的附加要求) (N 列)

根据您需要达到的保护需求（可参考您的评估对象），您应当相应满足所有的要求。

欲进一步了解 ISA 对要求等级“必须（must）”和“应当（should）”的定义，请参见 Excel 表“定义（Definitions）”中的“关键术语（Key terms）”。

重要提示：

您应当明白一点：即使满足了所有要求，也不能想当然地认为审计人员就一定会向您保证，并确认您已达标。这一点十分重要。

关于文中的要求及其措辞表述，其依据对象是一家虚构的、规模不详的普通公司，且在理论条件下实施有关工作。

而审计人员则需要根据您公司的实际执行情况，来相应对目标进行权衡判断。对于普通公司合情合理的情况，对于您的公司未必符合要求。

如有疑问，请咨询我们的 TISAX 审计服务提供商。

更多相关信息，请参见 章节 5.2.5, “分析并总结自我评估结果”。

5.2.2.7. 成熟度等级

针对您的信息安全管理体系，ISA 使用“maturity levels” (🇨🇳 成熟度等级) 这个概念来对其各个方面的质量水平进行评级。您的信息安全管理体系越复杂，其成熟度等级就越高。

ISA 区分六种不同的成熟度等级，您可在 Excel 表“Maturity levels” (🇨🇳 成熟度等级) 中查看详细定义。为了以直观的方式了解各个成熟度等级，我们在此引用 ISA 中给出的非正式描述：

Maturity level (🇨🇳 成熟度等级)	名称	描述
0	Incomplete (🇨🇳 不完整)	流程缺失、未得到遵守，或者不适合用于实现目标。
1	Performed (🇨🇳 基本可行)	遵循了流程，但流程无书面记录或记录不完整。然而，有证据表明，借助它可以实现目标。
2	Managed (🇨🇳 组织有序)	遵循了流程，且借助流程可以实现目标；流程文档以及流程执行证据齐全。
3	Established (🇨🇳 健全完善)	遵循了标准流程，且该流程贯穿整个体系；与其他流程之间的依存关系有书面记录，且已创建合适的衔接标准。有证据表明，在相当长的一段时间内，所述流程的使用频率和受重视程度均较高。
4	Predictable (🇨🇳 查缺补漏)	遵循了健全完善的流程。通过收集关键数据，对流程的有效性进行持续监控。针对流程被认为不够有效且需要调整的地方，相应定义了极限值。(关键绩效指标“KPI”)
5	Optimizing (🇨🇳 持续优化)	遵循了经过查缺补漏且以持续改进作为主要目标的流程。通过集中相关资源，来积极推动改进。

表格 11. 成熟度等级的非正式描述

您应当按照各个问题，来对您信息安全管理体系的成熟度等级进行评估。在“Maturity level” (成熟度等级) (E 列) 这一列中输入您的成熟度等级。

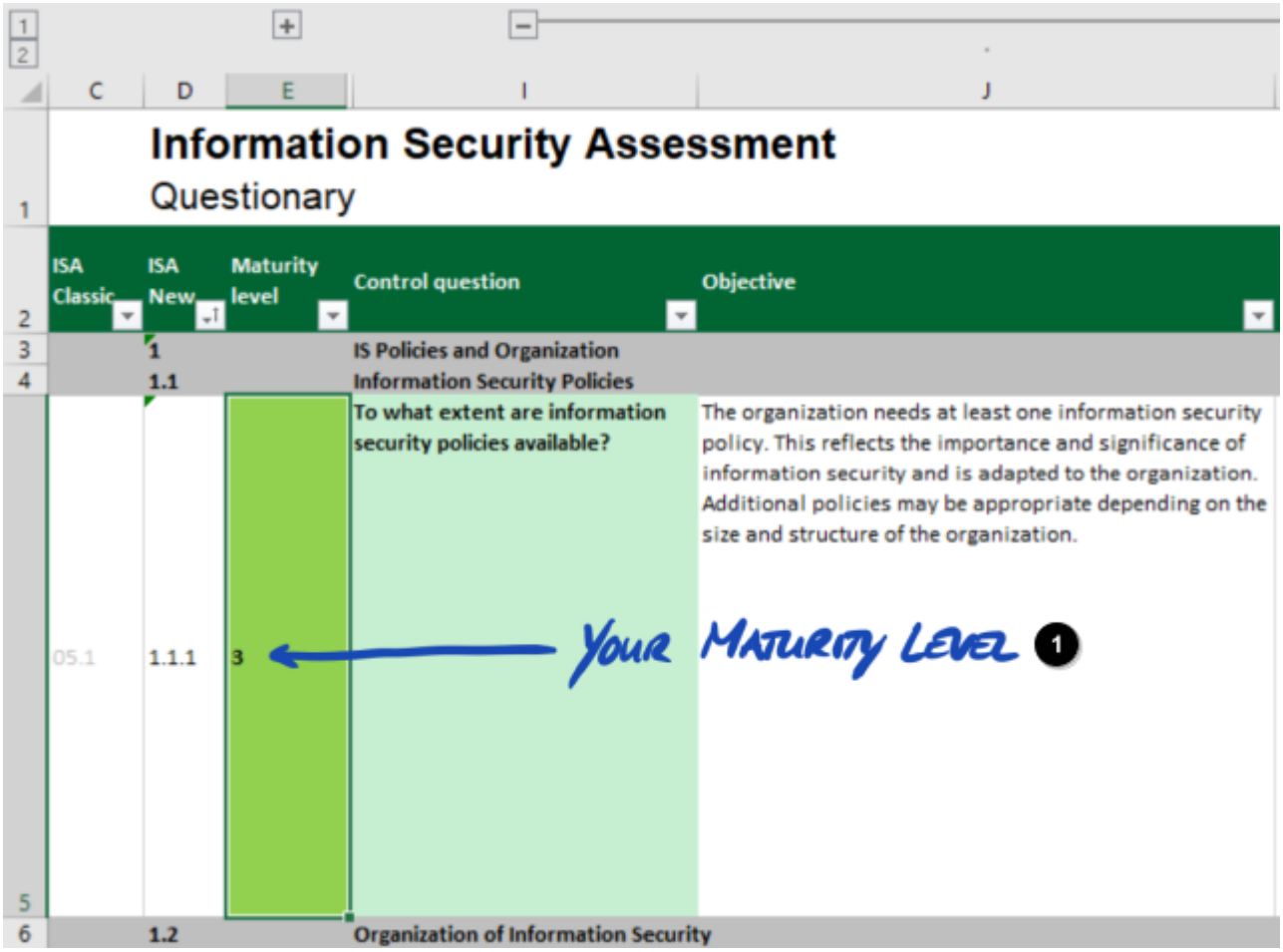


插图 14. 截图：ISA 文件中成熟度等级选择示例（Excel 表“信息安全”）

1 您的成熟度等级

欲进一步了解目标成熟度等级，及其对您评估结果的影响，请参见章节 5.2.4, “解读自我评估结果”.

有了进一步的了解之后，您便可准备开始进行自我评估了。

5.2.3. 执行自我评估

打开 Excel 文件，检查各个标准目录（适用于您的评估对象）中的所有“控制”问题，并确定与您信息安全管理体系的当前状态相匹配的成熟度等级。请依据您自己的最佳判断来完成这一步——在该阶段，并无对与错之说。

在您完成自我评估后，应完整填写 Excel 表“结果”（Results，ISA5）中的“结果（Result）”列（H），可填写数字（0-5），或“n.a.”（即表示“不适用”）。

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

插图 15. 截图：ISA 文件中“结果”（Results，ISA5）表示例

1 绿色

如有关于 ISA 的问题，请联系我们

5.2.4. 解读自我评估结果

在以下五个子章节中，我们将阐述如何分析并解读您的自我评估结果。通过分析，您将明白自己是否已为 TISAX 评估做好准备。

5.2.4.1. 分析

您的结果得分是对自我评估结果的总结。

您可在 Excel 表“结果”（Results，ISA5）（D6 单元格）中查看结果得分（“回归至目标成熟度等级的结果”）。我们将稍后解释什么是“回归”。

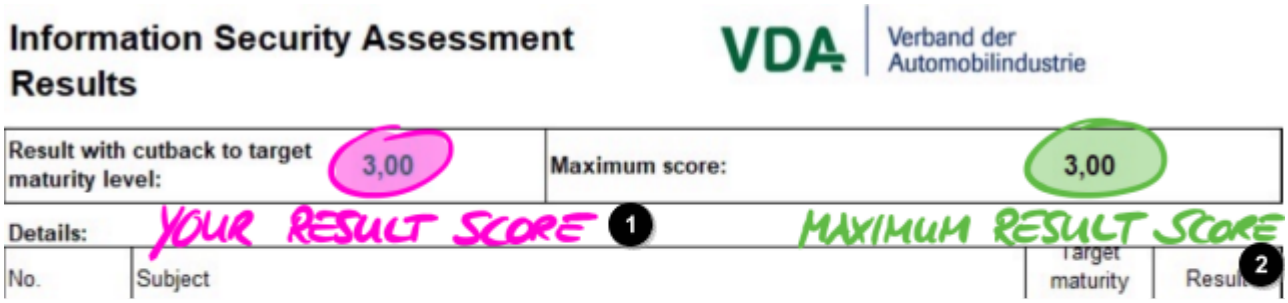


插图 16. 截图：您的结果得分和最高结果得分——Excel 表“结果”（Results，ISA5） (D6 和 G6 单元格)

1. 您的结果得分
2. 最高结果得分

为了理解并随后对您的自我评估结果和结果得分进行解读，您需要区分两种类型的分析级别：

1. 问题级
   该级别涉及所有的问题，每个问题均对应一个目标成熟度等级和您的成熟度等级。
2. 分数级
   在该级别有一个总体结果，它是所有问题结果的总结。相应地，也有一个最高结果得分以及您的结果得分。

下图中展示了这两个分析级别：

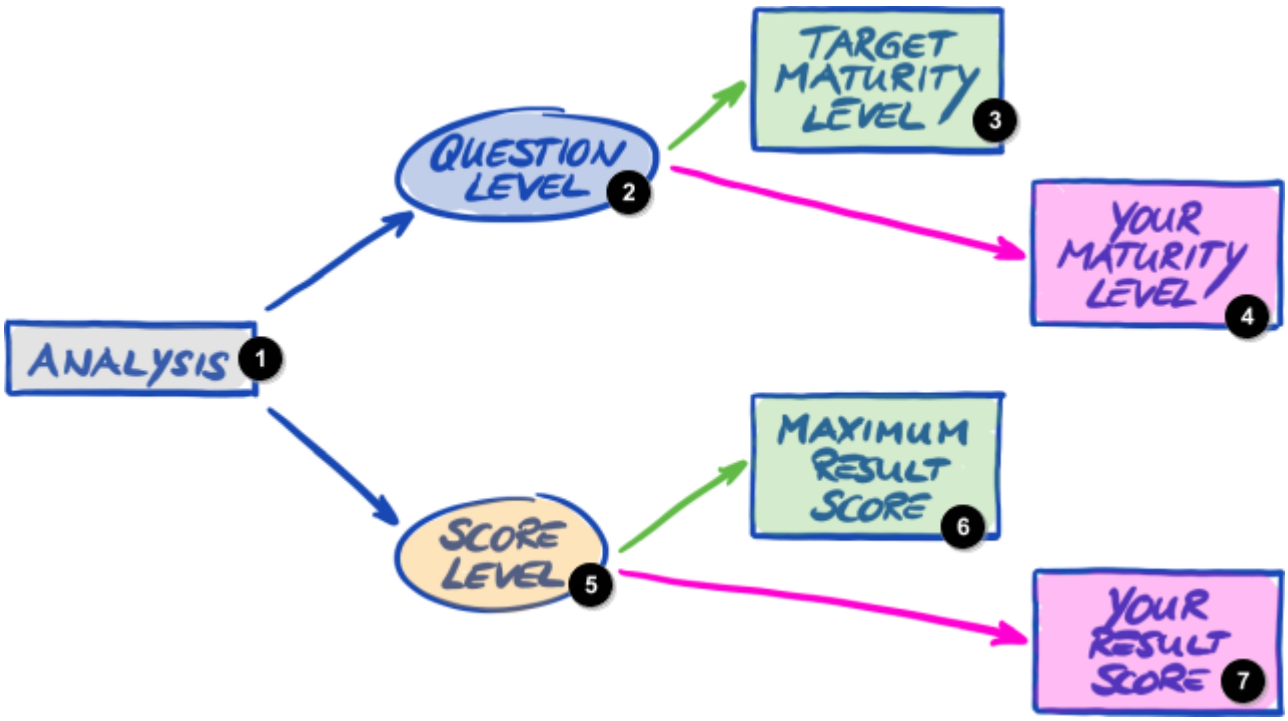


插图 17. 自我评估结果分析——问题级和分数级

1. 分析
2. 问题级
3. 目标成熟度等级

4. 您的成熟度等级
5. 分数级
6. 最高结果得分
7. 您的结果得分

下图展示了在何处可以看到 分数级和 问题级的结果。

插图 18. Excel 表“结果”（Results，ISA5）中的分数级和问题级

1. 分数级
2. 问题级

下图直观展示了分析级别、 ISA 目标定义以及 您本人的结果:

插图 19. 目标值以及您的结果值——问题级和分数级

1. 目标成熟度等级
2. 您的成熟度等级
3. 问题级
4. Q（问题）
5. TML（目标成熟度等级）
6. YML（您的成熟度等级）
7. 最高结果得分
8. 您的结果得分
9. 分数级

以下章节对结果及其分析进行了详细的阐述。

5.2.4.2. 目标成熟度等级（问题级）

ISA 为每个问题所规定的“目标成熟度等级”为 3。

欲进一步了解各个成熟度等级的定义，请参见章节 5.2.2, “看懂 ISA 文件”。

ISA 在 Excel 表“结果”（Results，ISA5）中（从 G 列、第 22 行开始，见下图）对目标成熟度等级进行了定义。

插图 20. Excel 表“结果”（Results，ISA5）中的目标成熟度等级定义

1 目标成熟度等级

5.2.4.3. 您的结果（问题级）

为了获得 TISAX 标签，您通常需要使每个问题的成熟度等级等于或者高于目标成熟度等级。

示例：如果问题 X 的目标成熟度等级为“3”，则您针对该问题的成熟度等级也应当为“3”或者更高。但是，如果您的成熟度等级在“3”以下，那么就有可能无法获得 TISAX 标签。

这一点只适用于单个问题，比如说，如果两个问题的目标成熟度等级都是“3”，而您针对其中一个问题的成熟度等级是“2”，另一个为“4”，那么，您不能采用“取高补低”的做法，让两个成熟度等级都达到“3”。

ISA 文件会自动将您的成熟度等级从 Excel 表“信息安全”（E 列）转移到 Excel 表“结果”（Results，ISA5）（从 H 列、第 23 行开始）中：

插图 21. Excel 表“结果”（Results，ISA5）中您的成熟度等级

1 您的目标成熟度等级

在 ISA 文件总结您的成熟度等级，并将之体现在得分结果中之前，会对其进行计算。一个基本原则是，您的成熟度等级会“回归”到目标成熟度等级。这样做是为了防止一旦您针对某些问题的成熟度等级*高于*目标成熟度等级，而针对另一些则*低于*目标成熟度等级，从而出现两者之间“取高补低”的情况。

以下是 ISA 计算结果（问题级）的方式：

- 取您的成熟度等级，并将其与问题的目标成熟度等级进行比较。
- 如果您的成熟度等级高于目标成熟度等级，则其将“回归”到目标成熟度等级。
- 如果您的成熟度等级低于或等于目标成熟度等级，则针对该问题将不采取行动。

示例（见下图）： 目标成熟度等级为“3”，而 您的成熟度等级为“4”。因此，针对该问题，您的“回归结果”将为“3”。

插图 22. 结果成熟度等级的“回归”计算

1 输入
2 计算
3 输出
4 （问题级）
5 目标成熟度等级（TML）
6 您的成熟度等级（YML）
7 YML > TML?
8 是：回归至 TML

9 否：不执行回归

10 结果成熟度等级（RML）

在下图中可以看到，如果您的成熟度等级高于目标成熟度等级，ISA 将执行回归操作（图中的绿色、橙色和红色对应了“结果”列中使用的颜色，请见插图 21, “Excel 表“结果”（Results，ISA5）中您的成熟度等级”）。

插图 23. 回归图解——配 Excel 表“结果”（Results，ISA5）中使用的颜色

1 示例：

2 YML

3 TML

4 回归

以下是另一种查看成熟度等级（问题级）的方式。圆圈的颜色代表目标成熟度等级，或与它之间的“距离”（例如，如果成熟度等级比目标成熟度等级低“1”级，则用橙色圆圈表示）。对勾则代表您的成熟度等级。

插图 24. 成熟度等级（问题级）

1 成熟度等级

2 问题

3 回归

4 目标成熟度等级（TML）

5 比 TML 高一级或一级以上

6 比 TML 低一级

7 比 TML 低两级或两级以上

8 您的成熟度等级（YML）

9 回归至 TML

请注意：

即使您在所有问题上都没有达到目标成熟度等级，您依然有可能通过 TISAX 评估。在这种情况下，主要问题在于您是否存在关联风险。如果您的成熟度等级低于目标值，但您自身并无风险，那么依然可能满足通过条件。

5.2.4.4. 目标值（分数级）

ISA 定义了一个“理想”的总体成熟度等级——即“最高结果得分”（或“最高得分”，G6 单元格）。

插图 25. 最高结果得分——Excel 表“结果”（Results，ISA5）

1 最高结果得分

理论上来说，该总体成熟度等级是所有目标成熟度等级（问题级）的平均值，也就是最高结果得分为“3.0”。

然而，该值为“3.0”的前提条件是，所有问题均适用于您的具体情况。一旦某个问题不适用于您的情况，那么平均值就会发生变化，最高结果得分将低于“3.0”。

根据上图（插图 24, “成熟度等级（问题级）”）所示，再参照下图，您可以看到最高结果得分平均值的变动轨迹：

插图 26. 最高结果得分（分数级）

1. 成熟度等级
2. 问题
3. 回归
4. 最高结果得分

5.2.4.5. 您的结果得分（分数级）

您的总体结果得分（“回归至目标成熟度等级的结果”，D6 单元格）：

- 对您信息安全管理体系的总体成熟度等级进行了总结。
- 是您所有成熟度等级（问题级）的平均值。
- 可能低于或等于最高结果得分。
- 应当尽可能接近最高结果得分。您的结果得分与最高结果得分之间的差距越大，您获得 TISAX 标签的可能性就越小。

插图 27. 您的结果得分——Excel 表“结果”（Results，ISA5）

1. 您的结果得分

同样，根据上图（插图 24, “成熟度等级（问题级）”）所示，再参照下图，您可以看到结果得分平均值的变动轨迹：

插图 28. 您的结果得分（分数级）

1. 成熟度等级
2. 问题
3. 回归
4. 您的结果得分

通过结果得分，您可以看到：

- 自己是否已准备好接受 TISAX 评估。
- 自己是否有望获得 TISAX 标签。

如果您的结果得分（“回归至目标成熟度等级的结果”）在“3.0”以下，则说明至少在一个问题上，您的成熟度等级未达到目标成熟度等级。在这种情况下，为做好接受 TISAX 评估的准备，您或许应首先对自己的信息安全管理体系进行改进。

请注意：

关于总体得分，您的结果得分与最高结果得分（“回归至目标成熟度等级的结果”）之间可以存在一个合理的“差距”，也就是官方限值。

如果您的结果得分低于最高结果得分的幅度：

- 大于 10%，则总体评估结果将为“轻微不符合”。
- 大于 30%，则总体评估结果将为“重大不符合”。

重要提示：

结果得分（“回归至目标成熟度等级的结果”）为“3”并不能保证您一定会顺利通过 TISAX 评估，且无任何不利于您的发现。请记住，审计人员看待某些问题的方式可能与您不同。

5.2.4.6. 您准备好了吗?

上述分析的目的是让您了解自己是否已准备好接受 TISAX 评估。

如果您的结果得分（“回归至目标成熟度等级的结果”）为（接近于）“3.0”，那么毫无疑问，您已具备接受 TISAX 评估的资格。在这种情况下，“结果”列（H）中的所有值均为绿色（无橙色或红色）。

如果不是绿色，那么您需要对自我评估结果进行分析总结（请参见 章节 5.2.5, “分析并总结自我评估结果”）。

下图中展示了 Excel 表“结果”（Results，ISA5）中的 ISA 蜘蛛网图。 绿线表示每一章对应的目标成熟度等级。如果您的成熟度等级 恰好达到或超过该线，则表明您已经可以接受 TISAX 评估了。反之，如果在该线 以下，则说明您的条件还不足以获得 TISAX 标签。

插图 29. 截图：ISA 蜘蛛网图中的目标成熟度等级实现——Excel 表“结果”（Results，ISA5）

1. 您已准备好接受 TISAX 评估
2. 目标成熟度等级
3. 满足成熟度等级要求并不意味着一定有资格获得 TISAX 标签！

如果您将 ISA 蜘蛛网图“展开”到问题级，则会获得类似的 绿色/红色视图（问题级）：

插图 30. “展开”ISA 蜘蛛网图

1. 成熟度等级
2. 问题
3. 您的结果得分可能不足以获得 TISAX 标签
4. 您已准备好接受 TISAX 评估

5.2.5. 分析并总结自我评估结果

您的自我评估结果可能表明，在具备获得 TISAX 标签的资格之前，您需要对自己的信息安全管理体系进行改进。

对于您的成熟度等级与目标成熟度等级之间的差距，您或许已知道如何进行弥补。对于其他事宜，您可能需要咨询外部人士。在这种情况下，您可以请求我们的 TISAX 审计服务提供商为您提供咨询服务。TISAX 允许其提供咨询，但不作要求。请注意，无论是哪一家审计服务提供商，只要为您提供过咨询服务，便不能再为您进行 TISAX 评估。

重要提示：

对于许多公司而言，在接受正式评估*之前*，*没有*对自我评估结果进行适当的分析和总结是阻碍其通过评估的主要绊脚石。请不要低估这项工作——根据要求去调整改进您的信息安全管理体系，在这方面付出的时间和精力都是值得的。许多公司为了准备 TISAX 评估，甚至需要为此专门立项，且工作量巨大。

请注意：

当您为通过 TISAX 评估流程而寻求外部帮助时，您会发现有不少公司提供这方面的咨询和培训服务。这些公司当中没有任何一家与我们有关联。

目前，我们：

- 不提供官方培训，包括直接提供或通过第三方提供。
- 不对第三方的服务质量进行评论，亦不会就此给出相关建议或注意事项。

5.3. 选择审计服务提供商

只有我们的签约审计服务提供商才有资格执行 TISAX 评估工作。[19]。 TISAX 审计服务提供商有资格为您执行 TISAX 评估，但前提是，他们此前从未向您提供过任何形式的咨询服务。

我们所有的 TISAX 审计服务提供商将仅为那些成为 TISAX 注册参与者的公司提供 TISAX 评估服务。

请注意：

每一项评估范围都会经历一个工作周期。在目前阶段，您的评估范围的状态应当为“已批准（Approved）”或“已完成注册（Registered）”。

关于评估范围状态的更多信息，请参见 章节 7.5.5, “Assessment scope status “Awaiting your payment”（ 评估范围状态“等待您的付款”）”。

5.3.1. 联系人信息

完成注册后，您可以联系所有的 TISAX 审计服务提供商并请求报价。后者的联系人信息会随注册确认邮件一并发送给您[20]（请参见 章节 4.5.8, “确认邮件”）。

请注意：

请确保仅在注册完成后，才向 TISAX 审计服务提供商请求报价。审计服务提供商将相应检查是否有注册记录，如无，则会拒绝您的请求。

这也是为什么您仅在注册确认邮件中才会收到审计服务提供商的联系人信息，而不是通过我们的公共网站获得。

5.3.2. 地域限制

目前，虽然许多审计服务提供商的联系人都常驻德国办公，但您需要明白的是，我们所有的审计服务提供商原则上都能够在全球各地执行 TISAX 评估任务。其中，大多数甚至已在多个国家雇用本地员工开展业务。

在我们的网站上，我们设立了专门页面来供您选择国家，从而了解哪一家审计服务提供商在本地安排了销售人员和/或审计人员（ enx.com/en-US/TISAX/xap/）。

5.3.3. 请求报价

为了让我们的 TISAX 审计服务提供商能够针对预期评估工作量进行精确计算，您应确保提供“TISAX 范围摘要（TISAX Scope Excerpt）”。

插图 31. “范围摘要”缩略图（第一页）

更多相关信息，请参见章节 4.5.8, “确认邮件”。

请注意：

公正性是 TISAX 审计服务提供商工作中的一个关键要素，旨在确保不会出现利益冲突。您在联系服务提供商的时候，应当考虑到这一点。如果您的公司与审计服务提供商有某种程度的关系，则其将无法为您提供评估服务。

5.3.4. 评估执行人选择依据

您可以自由选择 TISAX 审计服务提供商，因为他们均受相同合同的约束，且均基于相同的标准和审计方法来执行评估工作。就评估结果而言，无论您选择哪一家审计服务提供商，都不会给结果带来影响——您的评估结果是被所有 TISAX 参与者承认的。

除了价格、声誉和喜好等外在因素，您还应当考虑以下方面：

- 时效性：评估流程需要多久才能启动？如果您急需通过 TISAX 评估，则应重点考虑该方面。
- 与现场审计相关的差旅成本：审计服务提供商如在您的国家设有办事处，则可相应降低差旅成本。
- 语言：您和您公司里的每一位受约谈话人是否能够用自己的母语与审计人员交流？
- 具体包括哪些评估内容？
  更多评估相关信息，请参见章节 5.4.2, “TISAX 评估类型与要素”。
  通常，评估内容包括“初始评估”以及“纠正行动计划评估”。由于后续评估工作量难以预测，因而通常等到其他评估工作完结后才相应提供。

最后要考虑的便是信任。由于审计服务提供商会深入了解您公司的情况，因而您需要与其结成一种充满互信的合作关系。

请注意：

我们不建议您订购或要求我们提供类似于“预评估”的服务。虽然我们理解您的用心：您旨在通过此方式来为正式评估进行准备。然而，在几乎所有情况下，马上开始正式评估才是更加明智之举。而且，就价格而言，“预评估”与实际正式评估之间并无多少差别。此外，对于后者而言，您总是有机会通过纠正行动来针对评估发现进行整改。在读完下一章节后，您会有一个更清晰的认识。

请注意：

每一项评估都会经历一个工作周期。

关于评估状态的更多信息，请参见章节 7.6, “附录：Assessment status（ 评估状态）”。

您在选择了其中一家 TISAX 审计服务提供商后，便可正式启动 TISAX 评估流程。

5.4. TISAX 评估流程

5.4.1. 总述

TISAX 评估流程包含多项不同类型的评估。大多数情况下，评估数量都会在一项以上。

您应将整个评估流程视为一个相互交织的步骤序列，其中：

- 您针对自己的信息安全管理体系进行准备，确保其运作良好。
- 审计服务提供商负责检查您的信息安全管理体系，看其是否符合特定的要求，且有可能发现漏洞。
- 您需要在规定的期限内消除漏洞。
- 之后，审计服务提供商将再次检查您是否已消除了漏洞。

上述步骤将交替进行，直到消除所有漏洞为止。

您需要明白的是，负责启动评估流程中每一个步骤的，正是*您本人*。整个评估流程是在您的掌控之下。当然，是否随时终止并退出评估流程，也取决于您自己。[21]

5.4.2. TISAX 评估类型与要素

TISAX 评估流程由三大评估类型组成：

- 初始评估(Initial assessment)
- 纠正行动计划评估 (Corrective action plan assessment)
- 后续工作评估 (Follow-up assessment)[22]

“初始评估”标志着 TISAX 评估流程的开始。

另外两项 TISAX 评估可能在出现下列情形前反复进行多次：

- 您消除了所有漏洞
- 您退出了 TISAX 评估流程
- 或者，九个月的最长评估期限到了（此时需要重新进行初始评估）

在以下章节中，我们将为您讲述所有类型的 TISAX 评估。

请注意：

每一项评估都会经历一个工作周期。

关于评估状态的更多信息，请参见 章节 7.6, “附录：Assessment status（评估状态）”。

5.4.3. TISAX 评估要素

每一项 TISAX 评估均包含以下要素：

- 正式立项会议（Formal opening meeting）[23][24]
  - 旨在讨论所有组织安排事宜。
  - 会议无需以面对面形式进行。
  - 相关事宜可一次性、或分多次讨论完毕。
  - 是所有评估*初期*组织安排事宜的“指挥图”。
- 评估程序（Assessment procedure）
  - 您的审计服务提供商负责检查所有要求。
  - 依据相应的评估级别来选择评估方法。
- 正式结项会议（Formal closing meeting）[25]
  - 对 TISAX 评估进行总结。

- 审计服务提供商介绍评估发现。
- 审计服务提供商宣布评估结果。
- 会议无需以面对面形式进行。
- 是所有评估*后期*组织安排事宜的“指挥图”。

在“结项会议”之后，审计服务提供商会准备好更新后的“TISAX 报告”（草稿版）并发送给您。如果您认为，审计服务提供商在某些事项上存在误解，则您可以提出异议。[26]之后，审计服务提供商将签发最终版的“TISAX 报告”。

以上所有要素将在下文章节中进行阐述。

5.4.4. 关于符合性

在继续讲述 TISAX 评估流程之前，我们想为您解释一个重要概念，它对于理解接下来章节的内容至关重要。

TISAX 评估的目的，是确定您的信息安全管理体系是否符合特定的要求。审计服务提供商将检查您的信息安全管理体系，看其是否“符合”(to conform)相关的要求。

第一步：针对每一项适用要求进行检查。

如果您的体系方法“符合”所有要求，那么您便可以通过评估，并获得与您的评估对象相匹配的 TISAX 标签。

如果您的体系方法*不*符合特定要求，则审计服务提供商会区分以下两种“不符合项”(non-conformity)：

a. *轻微*不符合项(*Minor* non-conformity)
   该结论的适用情况是：不符合项既不会影响到您信息安全管理体系的整体有效性，也不会造成重大信息安全风险。
   示例：孤立的、偶尔出现的错误，执行不足

b. *重大*不符合项(*Major* non-conformity)
   该结论的适用情况是：不符合项影响到您信息安全管理体系的整体有效性，或者造成重大信息安全风险。
   示例：系统性出现的不符合事项、执行不足等，给保密信息的安全性带来重大风险；执行不足之处未通过适当的纠正行为进行矫正

> 请注意：
>
> 对于评估结果来说，以下各项（完全或较好符合要求）被称作“评估发现”。TISAX 共有四种类型的评估发现：
>
> - 观察意见(Observation)
> - 改进建议(Room for improvement)
> - 轻微不符合项(Minor non-conformity)
> - 重大不符合项(Major non-conformity)
>
> 只有两种不符合项关系到评估结果。

第二步：将前述“对照要求”步骤的所有评估结果纳入整体评估结果。

整体评估结果有以下几种情形：

a. 符合(Conform)
   整体评估结果为“符合”，即满足所有要求。

b. 轻微不符合(Minor non-conform)
针对某项要求，如果您至少有一处“轻微不符合项”，则整体评估结果为“轻微不符合”。

c. 重大不符合(Major non-conform)
针对某项要求，如果您至少有一处“重大不符合项”，则整体评估结果为“重大不符合”。
（如果没有相应的纠正行动计划，每一个“轻微不符合项”都会导致整体评估结果成为“重大不符合”。）

如果您的整体评估结果为：

- “轻微不符合”，那么您可以获得 TISAX *临时*标签，直到所有的轻微不符合问题得到解决为止。
- “重大不符合”，那么您只有在解决了有关问题之后，才能获得 TISAX 标签。
  如果有合适的、经过审计服务提供商批准的整改措施和纠正行动计划，则您有可能将整体评估结果从“重大不符合”改为“轻微不符合”，因而获得 TISAX 临时标签。

您需要明白的是，在整个 TISAX 评估流程期间，您的整体评估结果是可以改进的。

简单举例说明：在初始评估之后，您获得“重大不符合”这一整体评估结果。之后，您采取措施缓解了有关风险。这一行动会将您的整体评估结果由“重大不符合”提升至“轻微不符合”，在彻底消除风险后，您的整体评估结果将变成“符合”。

相关内容将在下文中作详细阐述。有关 TISAX 标签的更多信息，请参考下文 章节 5.4.13, “TISAX 标签”。

5.4.5. TISAX 评估流程准备工作

审计服务提供商将基于您的自我评估结果来相应准备评估工作。因此，建议您提前将自我评估结果提供给审计服务提供商。相应的文件交付截止日期可在“正式立项会议”上进行商议。

审计服务提供商在做好充分准备的情况下，可有助于减少评估所需要的时间。除了自我评估文件以外，审计服务提供商在开始评估之前，还会要求您提供其他相关文件，比如您在自我评估中引用的文件，以及审计服务提供商认为相关的其他文件。

基于这些信息，审计服务提供商将相应制定评估程序计划。

5.4.6. 初始评估

这是首项 TISAX 评估，它标志着 TISAX 评估流程正式开始。

重要提示：

“初始评估”标志着两个重要时间段的开始：

1. TISAX 标签的最长有效期（三年）
2. 整个 TISAX 评估流程的最长持续时间（九个月）
   这一时间段始于初始评估，并止于最后一次后续工作评估。
   该期限为硬性规定。如果您未能在此期限内成功完成评估流程，则无法获得 TISAX 标签。

以上两个期限均始于结项会议之日。

5.4.6.1. 首次正式立项会议

与所有 TISAX 评估一样，初始评估开始的标志是召开正式立项会议。与其他 TISAX 评估类型不同的是，该会议期间所讨论的事宜最为全面，因为这也是首次与您的审计服务提供商进行互动。正式立项会议通常以电话或视频会议的形式进行。

会议的目的是：

- 检查评估前提条件
- 介绍评估项目负责人以及评估团队

- 制定评估计划

待检查的评估前提条件有：

- 您是否有 TISAX 注册记录？
- 您与审计服务提供商之间是否已签合同？

评估计划包括：

- 评估范围确认
  - 您的评估范围是否已注册，是否合适？[27]
- 评估对象检查
  - 评估对象与您自己和/或您合作伙伴的要求是否匹配？
- 己方约谈人员
  - 在您公司，除了负责 ISMS 的人员，谁还必须接受约谈（以电话，或现场评估期间以面对面形式）？
- 您与审计服务提供商之间的交流
  - 您将如何交换保密信息？您将保密文件交给审计服务提供商，后者将为您提供评估报告（保密）。
  - 参与交流过程的人员都有哪些？
  - 如适用：您将如何组织评估约谈专项电话和视频会议？
- 关键评估事宜
  - 基于您的自我评估，审计服务提供商将提出其认为重要的评估事宜。
- 时间规划
  - 文件提交截止日期。文件包括您基于 ISA 的自我评估以及其他相关文件（如还未提交）
  - 约谈和现场检查（如适用）时间安排
  - 评估报告（草稿版和最终版）截止日期

5.4.6.2. 评估程序

审计服务提供商将依据准备工作计划，来相应执行初始评估。具体评估过程将视您的评估对象而定。评估形式主要包括电话会议、现场约谈以及现场检查，其所涉及的评估深度各不相同。[28]。

在初始评估期间，审计服务提供商将介绍所有的评估发现。

5.4.6.3. 结项会议

在结项会议上，审计服务提供商将再次总结所有的评估发现。

5.4.6.4. TISAX 报告

在结项会议之后，审计服务提供商会准备并向您发送“TISAX 报告”（草稿版）。如果您认为，审计服务提供商在某些事项上存在误解，则您可以提出异议。[29]之后，审计服务提供商将正式签发“TISAX 报告”。

在此阶段，整体评估结果的状态有可能是：

- 符合，或者

- 重大不符合
  如果“（轻微）不符合项”未得到处理，则会导致整体评估结果成为“重大不符合”。然而，若您相应制定了行动计划，并采取措施来纠正不符合项，那么您的整体评估结果可确保转为“轻微不符合”。
  关于如何实现这一点，更多信息请见章节 5.4.8.4, “TISAX 临时标签”。

如果在初始评估阶段，您的整体评估结果就已经为“符合”，那么您可跳过其余评估环节，直接前往评估结果“交换”这一步。

如果您的整体评估结果为“重大不符合”，那么您接下来的任务便是相应制定计划，对照评估发现进行纠错整改，并消除审计服务提供商所发现的漏洞。这项计划被正式称为“纠正行动计划”(“corrective action plan”).

5.4.7. 纠正行动计划准备

您的“纠正行动计划”(“corrective action plan”)将确定您如何相应制定计划，来针对初始评估发现中的问题进行整改。审计服务提供商将对“纠正行动计划”的合适性进行评估（见以下章节）。

为创建“纠正行动计划”，您应当考虑下列要求：

- 纠正行动
  - 针对每一个不符合项，您需要制定一项或多项“纠正行动”，以确保能够采取措施来消除不符合项。
- 实施日期
  - 您需要为每一项纠正行动确定一个实施日期。
  - 具体实施期限应确保为全面落实措施留出充足的时间。
- 整改措施
  - 对于所有带来重大风险的不符合项，您需要相应制定整改措施，来消除不符合项，直到纠正行动得到落实为止。
- 落实期限
  - 对于所有落实期限超过三个月的纠正行动，您需要就该期限给出合理的解释。
  - 对于所有落实期限超过六个月的纠正行动，您需要额外提供证据，来证明无法做到更快落实相关行动。
  - 对于所有的纠正行动，其落实期限均不得超过九个月。

一旦您的纠正行动计划制定完毕，您便可请求执行“纠正行动计划评估”。

重要提示：

我们建议尽早启动落实相关计划，而无需等待“纠正行动计划评估”的结果。
“纠正行动计划评估”通常在您将纠正行动计划提交给审计服务提供商之后方开始执行。

5.4.8. 纠正行动计划评估

“纠正行动计划评估”的目的，是证实您的“纠正行动计划”（如上所述）满足 TISAX 的有关要求。

您需要将“纠正行动计划”提交给审计服务提供商，并由其根据相关要求（见下文）进行评估。如果您的计划符合要求，审计服务提供商将签发更新后的“TISAX 报告”。

这项评估过程通常耗时不长，具体形式可以为面对面会议、电话或视频会议。

5.4.8.1. 纠正行动计划评估的先决条件

执行“纠正行动计划评估”的先决条件为：

- 一次最近执行的[30]初始评估（发现不符合项）
- 或者一份已完成评估的“纠正行动计划”，但该计划不符合要求。

5.4.8.2. 与初始评估结合执行

“纠正行动计划评估”并非一定是一项独立进行的活动。在初始评估的结项会议上，您便已经可以选择展示您的“纠正行动计划”。在此情况下，审计服务提供商可直接执行“纠正行动计划评估”。

如果您将“纠正行动计划评估”与初始评估结合执行，并且您的“纠正行动计划”符合要求，那么您可以与审计服务提供商商议，无需再出具“初始评估报告”。反之，审计服务提供商将着手准备“纠正行动计划评估报告”。该报告可让您直接获得 TISAX 临时标签。

5.4.8.3. 纠正行动计划要求

审计服务提供商将参照以下要求来评估您的“纠正行动计划”：

- 措施合适
- 通过采取适当的整改措施，有效缓解了重大风险[31]
- 落实期限合适
  - 落实期限的起始日期为初始评估结项之日
- 所有落实期限均不长于：
  - 三个月（无需给出理由）
  - 六个月（无需给出理由和证明）
  - 九个月

5.4.8.4. TISAX 临时标签

如果您的整体评估结果为“轻微不符合”，则可获得 TISAX 临时标签。

TISAX 临时标签的优点是，它通常被您的合作伙伴接受；但前提是，您之后会顺利获得 TISAX 正式标签。如果您急需向合作伙伴证明，您的信息安全管理体系运作符合要求，则该标签会对您有所帮助。

获得 TISAX 临时标签的前提条件是，已出具纠正行动计划评估报告，且整体评估结果为“轻微不符合”。

关于有效期期限，TISAX 临时标签：

- 在初始评估结项会议九个月之后失效。
- 在所有不符合项得到解决之前一直有效。
  - 这一点在“后续工作评估”中确定，并记录在后续工作评估报告中。
- 的有效期无法延长。

请注意：

“纠正行动计划评估”为可选项。

在下列情形下，您可直接前往“后续工作评估”：

- 您不需要 TISAX 临时标签
- 您有信心，即使行动计划未经过审计服务提供商批准，自己依然有能力落实相关的纠正行动

一旦所有纠正行动落实完毕，您便可请求执行“后续工作评估”。

5.4.9. 后续工作评估

“后续工作评估”的目的是，评估是否已顺利解决此前发现的不符合项。通常，在您确定已消除所有的不符合项之后，便可请求执行后续工作评估。

执行后续工作评估没有次数限制。评估期间，如果审计服务提供商发现，现有的不符合项未得到解决，或者甚至出现了新的不符合项，那么您只需相应更新纠正行动计划，并重新开始这一部分的评估流程即可。

评估具体形式可以为面对面会议、电话或视频会议。

5.4.9.1. 时限要求

您的审计服务提供商可执行后续工作评估的最长时限为：初始评估结项后九个月内。[32]

5.4.9.2. 前提条件

如果您不需要 TISAX 临时标签，便可直接请求执行“后续工作评估”。您不一定非要先进行“纠正行动计划评估”，然后再执行“后续工作评估”。

5.4.9.3. TISAX 临时标签的时效

如果您需要 TISAX 临时标签，那么您应该希望确保在获得 TISAX 正式标签之前，不会出现什么意外。因此，我们建议您在“最迟可用日期”[33]。 这样一来，一旦在后续工作评估期间发现了轻微不符合项，您将有足够的缓冲时间来解决问题。

5.4.10. TISAX 评估流程图解

现在，我们将以上章节的内容用下列图表进行总结：

插图 32. TISAX 评估流程图解（第 1/2 部分）

1. 您的行动
2. 审计服务提供商的行动
3. 开始
4. 评估准备
5. 由您触发
6. 最长持续时间（九个月）的起始点
7. 初始评估
8. 初始评估报告
9. 发现不符合项?
10. 否
11. e)
12. 是
13. 制定纠正行动计划
14. d)
15. 由您触发
16. 开始/继续实施纠正行动
17. 纠正行动计划评估
18. 纠正行动计划评估报告
19. 否（未完成或不合适）
20. 纠正行动计划是否没有问题?

21 c)
22 b)
24 a)
25 可获得 TISAX 临时标签

插图 33. TISAX 评估流程图解（第 2/2 部分）

1 c)
2 b)
3 a)
4 否
5 纠正行动已完成?
6 是，由您触发
7 后续工作评估
8 后续工作评估报告
9 e)
10 评估结果是否“符合”?
11 d)
12 最长持续时间（九个月）的终止点
13 是
14 TISAX 标签
15 审计服务提供商：上传结果至交换平台
16 您：在交换平台上共享结果
17 AP（可选）:将结果上传给管理服务提供商
18 您：设置更新提醒
19 结束

5.4.11. Assessment ID（评估 ID）

评估范围中的每一项 TISAX 评估都是由一个“评估 ID”进行标识。该 ID 将与您的评估结果和 TISAX 报告相关联。

评估 ID 的外观如下所示：

插图 34. “评估 ID”的格式

1 “评估 ID”的前缀是“A”
2 “审计服务提供商前缀”，由 ENX 协会分配
3 为唯一、任意字符串，只包含字母和数字：
CFHKLMNPRTVWXYZ
0123456789
4 评估计数器
- 初始评估为空
- 遇到后续评估（如“纠正行动计划评估”）+ 1

“评估 ID”主要用于审计服务提供商与您之间的交流。

5.4.12. TISAX 报告

“TISAX 报告”(TISAX report):

- 在每一次 TISAX 评估之后相应更新并签发。
- 记录审计服务提供商的评估发现。
- 包含整体评估结果（符合、轻微不符合、重大不符合）。
- 包含与您的 TISAX 评估相关的所有其他信息，例如评估对象、范围、参与人员和评估地点等。

“TISAX 报告”有以下几种类型（视评估类型而定）：

- *初始*评估报告 (*Initial* assessment report)
- *纠正行动计划*评估报告 (*Corrective action plan* assessment report)
- *后续工作*评估报告 (*Follow-up* assessment report)[34]

“TISAX 报告”的框架结构总是一样的。[35] 在完成每一种类型的评估后，审计服务提供商将仅在原来的基础上更新有关内容。也就是说，您只需参考最终版本的 TISAX 报告即可，因为它必然包含此前版本的内容。

“TISAX 报告”的第一部分是您最终要与合作伙伴共享的。

TISAX 报告的一个主要特点是，您希望与合作伙伴或其他参与者共享报告的哪些部分，这完全由您自己来决定。TISAX 报告的框架结构设计让这一“选择性分享”成为可能。报告的每一章节都包含不同程度的详细信息。

“TISAX 报告”的框架结构如下：

- A：评估相关信息
  公司名称、评估范围、范围 Id、评估 ID、评估级别、评估对象、评估日期、审计服务提供商
  该章节中不包含任何评估结果。
- B：整体评估结果
  评估结果总体概述（符合、轻微不符合、重大不符合）、发现数量、相应风险的抽象分类
- C：评估结果总结
  每个章节（例如“9 访问控制”）和每个标准目录（例如“信息安全”）的评估结果汇总
- D：详细评估结果
  所有评估发现的详细描述、相应的风险评估结果、所需措施、实施期限
- E：ISA 成熟度等级（ISA 结果表）
  各项要求的成熟度等级
  在“交换”步骤（详见下文）中，您可以针对 TISAX 报告内容的级别，相应决定您合作伙伴的访问权限。

5.4.13. TISAX 标签

我们已在注册准备章节简要探讨过这一话题。 如此前所述，TISAX 标签是由评估对象演变而来的。

插图 35. 评估对象和 TISAX 标签

1. 请求
2. 合作伙伴

3. 接收
4. 输入
5. 对象
6. TISAX 流程
7. 输出
8. 标签

TISAX 标签：

- 是 TISAX 评估流程的输出。
- 是对您评估结果的总结。
- 是一种声明，即您的信息安全管理体系符合特定要求。

由于 TISAX 标签代表了 TISAX 评估流程的特定输出，因此，在与您的合作伙伴以及 TISAX 审计服务提供商交流时，使用 TISAX 标签会更加方便。

5.4.13.1. TISAX 标签的等级关系

评估对象与相应 TISAX 标签之间的对应关系十分直接。此外，某些 TISAX 标签之间存在上下级关系，这一点亦十分重要。换句话说，如果您获得了某个 TISAX 标签，您将自动获得该标签所对应等级“之下”的所有 TISAX 标签。

示例（使用缩略标签名称）：如果您的评估对象为“信息——极高保护需求（Info very high）”，那么您将相应获得 TISAX 标签“Info very high”。但由于评估对象“信息——极高保护需求（Info very high）”是“信息——高保护需求（Info high）”的扩展，因而您也将自动获得 TISAX 标签“Info high”。

插图 36. TISAX 评估对象和 TISAX 标签（依存关系和等级关系）

1. 评估对象
2. 成为
3. 标签
4. 依存关系
5. 等级关系
6. 前者要求满足后者
7. 后者包含前者

可能并非每一位参与者都会注意到这一点。但想象一下，您的一位合作伙伴要求您出示 TISAX 标签“Info very high”，而另一位合作伙伴则要求提供标签“Info high”。这种情况下，同时拥有两个 TISAX 标签就轻松得多，因为没有人需要明白，“Info high”是“Info very high”的子集。对于那些要求提供 TISAX 标签来相应满足严格的采购流程要求的合作伙伴来说，这一点尤为重要。这样一来，关于“Info very high”是否要“好于”“Info high”，您亦无需另作解释，只需出示您所有的 TISAX 标签即可。评估执行人员可以很容易发现是否有“Info high”这个“强制性”标签，从而在相应要求前打勾。

5.4.13.2. TISAX 标签的有效期

通常，TISAX 标签的有效期为三年。该有效期限自评估流程结束之时（亦有可能在 TISAX 报告签发之前）算起。

如果涉及 TISAX 评估范围变更等重大事宜，则上述期限有可能会缩短。

例如：公司迁址、添加地点。（关于如何应对此类情形，请参见 章节 7.8.4, “地址变更” 以及章节 7.8.5, “添加地点（范围扩展评估）”。）

请注意：

您仅能在 ENX 门户中查看自己的 TISAX 标签，TISAX 报告中未作记录。

5.4.13.3. TISAX 标签的换发

为了保证 TISAX 标签长期有效，应当每三年换发一次。[36]

为此，您需要再次完成 TISAX 评估流程（注册评估范围、接受 TISAX 评估、共享评估结果）。只不过，注册过程会更加容易，因为您无需重新将公司注册为“TISAX 参与者”。另外，您依然可以使用此前录入 TISAX 数据库的所有联系人和评估地点。

重要提示：

在联系审计服务提供商之前，请注册一个新范围。只有您提供了新的“范围 ID”，审计服务提供商方能启动评估流程。

大多数情况下，注册新范围十分简单，您只需分配一个新的范围名称、添加联系人、选择评估对象并添加评估地点即可。您依然可以使用系统中此前注册范围的联系人和评估地点。

重要提示：

如果您与合作伙伴之间的关系需要以拥有有效的 TISAX 标签作为前提要求，则我们强烈建议您设置日历提醒，以确保能够及时启动标签换发流程。

我们建议，至少在您的 TISAX 标签过期前一年开始着手准备换发。

现在，您已经获得了 TISAX 标签，可以前往下一步骤，即与合作伙伴进行共享。

6. 交换（第 三步）

阅读“交换”章节预计需要 7 分钟。

到目前为止，您已经完成了 TISAX 评估流程，但是您的合作伙伴依然未见到任何“证据”能够证明您的信息安全管理体系有能力保护自己的保密数据。本章节将阐述如何与合作伙伴共享您的评估结果，从而展示所要求的证据。

6.1. 前提条件

TISAX 流程的一个主要特点是，您的评估结果由您自己全权掌控。未经过您明确同意，所有涉及您评估的相关信息均不会与他人共享。

6.2. 交换平台

ENX 门户提供信息交换平台。

您的审计服务提供商负责上传您的 TISAX 报告（前两部分 A 和 B）。 在此阶段，相关信息仅对您可见。

您可以通过注册期间创建的账号来访问门户，并使用交换平台。

您可通过以下地址登录门户：
enx.com/en-US/SignIn

6.3. 一般性前提

只有满足以下两个前提条件，您才可与合作伙伴共享评估结果：

1. 审计服务提供商已将评估结果提交至交换平台。
   评估结果通常会在 TISAX 报告签发后 5-10 个工作日内上传至交换平台。
2. 我们已收到您的付款（如适用）。

在满足这两个前提条件后，您的评估范围状态将为“已通过评估（Active）”。

请注意：

每一项评估范围都会经历一个工作周期。在目前阶段，您的评估范围状态应当为“已通过评估（Active）”。

关于评估范围状态的更多信息，请参见章节 7.5.5, “Assessment scope status “Awaiting your payment”（ 评估范围状态“等待您的付款”）”。

为了验证您的评估结果是否已可以共享（评估范围状态 = Active），可遵循下列步骤：

1. 登录 ENX 门户 (https://enx.com/)。
2. 前往主导航栏，并选择 “MY TISAX”（ “我的 TISAX”）。
3. 从下拉菜单中选择“SCOPES AND ASSESSMENTS”（ “范围与评估”）。
4. 前往表格，并找到您的评估范围所在的那一行。
5. 确定您的评估范围状态为“Active”（ “已通过评估”）（“Scope Status”（ “范围状态”）列）。

6.4. 交换结果操作的不可逆性

重要提示：

发布或共享权限一旦设定，将无法撤销。

原因是，我们希望所有的“被动参与者”均能够稳定地访问其收到的每一项评估结果。否则，他们得自己想办法去管理并存档相关的评估结果。

上述权限在您的 TISAX 评估整个有效期期间均保持有效。

若因不小心错误创建了发布或共享权限，请立即联系我们。

6.5. 共享级别

共享级别与 TISAX 报告的主要部分（A-E）是 1:1 对应的关系。

^	**TISAX 报告主要部分^**	**与交换平台上的共享级别**
1	A：评估相关信息(Assessment-related information)	
2	B：整体评估结果(Overall assessment result)	
3	C：评估结果总结(Assessment result summary)	
4	D：详细评估结果(Detailed assessment results)	
5	E：ISA 成熟度等级（ISA 结果表） (Maturity levels of ISA (result tab of ISA))	

表格 12. TISAX 报告主要部分与交换平台上的共享级别

共享级别越高，相关参与者能够看到的有关您 TISAX 评估的信息就越多。

有关 TISAX 报告各部分内容的更多信息，请参见 章节 5.4.6.4, “TISAX 报告”。

6.6. 在交换平台上发布评估结果

您可通过在交换平台上发布评估结果，来与其他 TISAX 参与者进行共享。通过该操作并相应指定共享级别，所有其他的 TISAX 参与者均能够访问您的评估结果。

只有您的整体评估结果“符合”，您才能够发布结果。

在交换平台上，针对结果发布的共享级别有以下几种执行选项：

- Do not publish (Default) （不发布（默认））
- A: Assessment-Related Information （A：评估相关信息）
- A + Labels （A + 标签）
- A + Labels + B: Overall Assessment Result （A + 标签 + B：整体评估结果）

通常情况下，我们建议选择 “A + Labels”（“A + 标签”）这种发布类型。

重要提示：

只有 章节 6.3, “一般性前提” 中提到的前提条件得到满足，您才能发布评估结果。

为在交换平台上发布评估结果，请遵循以下步骤：

1. 登录 ENX 门户 (https://enx.com/)。
2. 前往主导航栏，并选择 “MY TISAX”（“我的 TISAX”）。
3. 从下拉菜单中选择“SCOPES AND ASSESSMENTS”（“范围与评估”）。
4. 前往表格，并找到您的评估范围所在的那一行。
5. 确定您的评估范围状态为“Active”（“已通过评估”）（“Scope Status”（“范围状态”）列）。
6. 前往您评估范围所在表格行的末尾，并点击向下箭头按钮 。
7. 选择“Scope Information”（“范围信息”）。
8. 在新窗口（“Scope Information”（“范围信息”））中，选择“EXCHANGE”（“交换”）选项卡。
9. 前往“PUBLISHING”（“发布”），打开下拉菜单，并选择需要的共享级别（见上述建议）。

请注意：

评估结果仅发布在交换平台上，并仅能由其他 TISAX 参与者访问。在 TISAX 公共网站上，不会对 所有 TISAX 参与者的信息进行公示，只会提及参与者的大概数量。

6.7. 与特定参与者共享评估结果

除了以上所述在交换平台上发布 TISAX 评估结果以外，您还可以选择性地与特定的 TISAX 参与者（更高共享级别）共享结果。

与上述提到的发布方式不同，即使您的整体评估结果为（重大/轻微）不符合，您依然可以共享评估结果。

共享评估结果是 TISAX 流程的一个重要环节。虽然您的信息安全管理体系只接受了一次评估，但现在您却可以与尽可能多的合作伙伴共享评估结果。

针对在交换平台上共享结果，有以下几种执行选项：

- A: Assessment Related Information （A：评估相关信息）
- A + Labels （A + 标签）
- A + Labels + B: Assessment Summary （A + 标签 + B：整体评估结果）
- A + Labels + B + C: Summarized Results （A + 标签 + B + C：评估结果总结）
- A + Labels + B + C + D: Detailed Assessment Results （A + 标签 + B + C + D：详细评估结果）
- A + Labels + B + C + D + E: Maturity Levels according to ISA （A + 标签 + B + C + D + E：ISA 成熟度等级）

我们建议选择共享级别“A + Labels”（“A + 标签”），这足以满足大多数合作伙伴的要求。您可随时更改共享级别。

请注意：

某些 TISAX 参与者会自动处理其合作伙伴的评估结果，方法是将其系统与 ENX 门户关联同步。因此，只有与该参与者专门共享评估结果，才能使结果得到同步。而仅依照 章节 6.6, “在交换平台上发布评估结果” 所述，来相应发布的评估结果是不被承认的。

在使用 TISAX 的原型设备制造商（OEM），BMW 便是一个典型的例子。如果您是 BMW 的合作伙伴，请确保与其共享（不只是发布）您的评估结果。

6.7.1. 前提条件

关于同您的合作伙伴（或其他任一 TISAX 参与者）共享评估结果，前提条件如下：

- 您只能与其他 TISAX 参与者共享您的 TISAX 评估结果。
- 您的合作伙伴需要是 TISAX 参与者。
- 您需要合作伙伴的“参与者 ID”。[37]
- 您需要付款（如适用）。

重要提示：

只有 章节 6.3, “一般性前提” 中提到的前提条件得到满足，您才能共享评估结果。

6.7.2. 如何创建共享权限

为了与其他 TISAX 参与者共享评估结果，请遵循以下步骤：

1. 登录 ENX 门户 (https://enx.com/)。
2. 前往主导航栏，并选择 “MY TISAX”（“我的 TISAX”）。
3. 从下拉菜单中选择“SCOPES AND ASSESSMENTS”（“范围与评估”）。
4. 前往表格，并找到您的评估范围所在的那一行。
5. 确定您的评估范围状态为“Active”（“已通过评估”）（“Scope Status”（“范围状态”）列）。
6. 前往您评估范围所在表格行的末尾，并点击向下箭头按钮  。
7. 选择“Scope Information”（“范围信息”）。

8. 在新窗口（“Scope Information”（“范围信息”））中，选择“EXCHANGE”（“交换”）选项卡。

9. 前往“SHARING”（“共享”）版块，并点击按钮“Share”（“共享”）。
10. 在新窗口（“SHARE THIS SCOPE”（“共享该范围”）中，输入您合作伙伴的“参与者 ID”（或从邻近搜索框的参与者列表中选择）。
11. 选择所需要的共享级别。
12. 点击按钮“Next”（“下一步”）。
13. 阅读并理解关于共享权限操作不可逆性的说明。
14. 在两个“confirm”（“确认”）复选框前打勾。
15. 点击按钮“Submit”（“提交”）。

其余事项将由交换平台完成。对于共享级别 A 和 B，相关信息会发布在交换平台上，您的合作伙伴可以登录 ENX 门户，并查看您共享的评估结果。[38]

对于更高共享级别（C-E），交换平台会通知您的审计服务提供商，由其将相关信息（匹配所选择的共享级别）发送给您合作伙伴的“主要参与者联系人”。

6.8. 在 TISAX 框架之外共享评估结果

适用规则[39]是，您只能利用 TISAX 交换平台，来让其他 TISAX 参与者知晓您的评估结果。

6.8.1. 实行严格交换机制的原因

TISAX 提供一套标准化的评估结果交换机制。与其他认证体系（如 ISO）那种途径驳杂、所需信息时而不全的结果交换方式相比，TISAX 交换机制较好弥补了这一不足。

原型设备制造商（OEM）尤其青睐这种清晰明确、定义有序的标准化流程机制，而其他公司亦从中受益。

6.8.2. TISAX 公共宣传指南

虽然您无法在公共场合悉数罗列评估结果，但您却可以其他方式提及您所做的 TISAX 评估工作。在 ENX 门户上，我们针对如何进行公共宣传为您提供有关建议。另外，我们还提供 TISAX 徽标，以供您使用。

在登录 ENX 门户后，您可在此处查看相关信息：
enx.com/en-US/myenxportal/marketing/
ZIP 压缩文件下载（文档和徽标）：
enx.com/myenxportal/marketing/tisax-trademark-and-logos-guidelines

或许您在想，我们是否也出具证书，可供您挂在墙上：
回答是，由于以上提到的标准化交换流程，我们不提供此类证书。

6.8.3. 与合作伙伴（非 TISAX 参与者）共享

如果您希望与之共享评估结果的合作伙伴 a) 还不是 TISAX 参与者且 b) 还未获得 TISAX 标签（通过完成评估流程），那么您可遵循下列步骤：

1. 让您的合作伙伴注册成为 TISAX 参与者。
   注意：合作伙伴只需注册为 TISAX 参与者即可，无需继续注册评估范围。
2. 让您的合作伙伴联系我们。
   通常，我们仅在公司注册了评估范围之后，才会处理新注册申请。但您的合作伙伴在提及上述要求后，我们会相应处理其注册。如此一来，该合作伙伴便可成为 TISAX 参与者，可以通过正常的交换流程接收您的 TISAX 评估结果。

该方法的目的是确保，您的合作伙伴同意遵守“TISAX 参与一般条款和条件”，而该规定是管理 TISAX 评估结果交换的基础。

只有注册评估范围才会产生费用，而注册成为 TISAX 参与者则是免费的。因此，您的合作伙伴可以免费接收您的评估结果。只不过，如果没有自己的评估结果，那么合作伙伴最多只能接收五个评估结果，且无法查看任何发布内容。

6.8.4. 与合作伙伴的雇员（无法直接访问 ENX 门户）共享

对于您合作伙伴的雇员而言，只有拥有 ENX 门户的账号，才能够直接查看您的结果。如果您需要向合作伙伴的雇员（无门户访问权限）证明您已获得 TISAX 标签，那么您可使用专门的 PDF 文件。为获得该文件，请遵循以下步骤：

1. 与您的合作伙伴共享评估结果，相关信息请见章节 6.7, “与特定参与者共享评估结果”。
2. 登录 ENX 门户 (https://enx.com/)。
3. 前往主导航栏，并选择 “MY TISAX”（“我的 TISAX”）。
4. 从下拉菜单中选择“SCOPES AND ASSESSMENTS”（“范围与评估”）。
5. 前往表格，并找到您的评估范围所在的那一行。
6. 确定您的评估范围状态为“Active”（“已通过评估”）（“Scope Status”（“范围状态”）列）。
7. 前往您评估范围所在表格行的末尾，并点击向下箭头按钮  。
8. 选择“Scope Information”（“范围信息”）。
9. 在新窗口（“Scope Information”（“范围信息”））中，选择“EXCHANGE”（“交换”）选项卡。
10. 前往“SHARING”（“共享”）版块，并找到共享权限（第一步中所创建）所在的表格行。
11. 前往共享权限所在表格行的末尾，并点击向下箭头按钮  。
12. 选择“Edit”（“编辑”）
13. 在新窗口（“SHARE THIS SCOPE”（“共享该范围”））中，滑动至底部并选择“Request Shared Information as PDF”（“请求共享信息（PDF 格式）”）。
14. 稍等片刻，直到文件生成完毕。
15. 下载文件（“Copy of information shared with ACME.pdf (66.84 KB)”（“与 ACME 共享信息副本.pdf（66.84 KB）”））

7. 附录

7.1. 附录：账单示例

以下是我们发送的账单示例。

更多相关信息，请参见章节 4.3.4, “费用”。

7.2. 附录：确认邮件示例

在线注册流程期间，一旦您完成了所有强制性步骤，我们将向您发送确认邮件。

有关发送确认邮件的更多信息，请参见章节 4.5.8, “确认邮件”。

主题： [TISAX] 范围 S3ZY5V 已核准

尊敬的 John Doe：

感谢您完成 TISAX 评估范围注册。我们已处理您的范围注册事宜，并核准了您的评估范围。附件是“TISAX 范围摘要”，其中包括所有范围信息，以及最新版 TISAX 审计服务提供商目录。

下一步？

利用随附的“TISAX 范围摘要”，您现在可以联系各家 TISAX 审计服务提供商，并就您的评估范围请求报价。

需要帮助？

关于 TISAX，如有其他问题，请阅读“TISAX 常见问题解答”或“TISAX 参与者手册”（https://enx.com/en-US/TISAX/faqs/）。如果需要 TISAX 相关帮助，您可随时通过邮件（tisax@enx.com）或电话（+49 69 986692-777），来联系 TISAX 服务专线。

谨致问候

您的 TISAX 团队

7.3. 附录：TISAX 范围摘要示例

“TISAX 范围摘要（TISAX Scope Excerpt）”随确认邮件一起发送。

更多相关信息，请参见 章节 4.5.8, “确认邮件”。

7.4. 附录：Participant status（🇨🇳 参与者状态）

7.4.1. 概述： 参与者状态

“参与者状态”定义了您（作为一家公司）在 TISAX 流程中所处的阶段。

“参与者状态”有以下几种：

1. Incomplete （🇨🇳 未完成）
2. Awaiting approval （🇨🇳 等待批准）
3. Preliminary （🇨🇳 初步完成）
4. Registered （🇨🇳 已完成注册）
5. Expired （🇨🇳 已失效）

以下各个状态的说明表将解释：

- 所处状况
  （该状态所代表的具体含义）
- 您的下一步行动
  （您如何到达下一状态；如适用）
- 我们的下一步行动
  （我们如何帮助您到达下一状态；如适用）
- 下一状态
  （如适用）

以下示例图展示了，需要哪些行动才可前往下一状态：

插图 37. 参与者状态概览

1. 您
2. 我们
3. 参与者状态
4. 1.未完成
5. 如果注册信息不完整
6. 注册
7. 2.等待批准
8. 审核 + 确认
9. 3.初步完成
10. 已发布并共享评估结果
11. 4.已完成注册
12. 5.已失效
13. 未付账单、合同取消

7.4.2. Participant status “Incomplete”（参与者状态“未完成”）

状态	所处状况	您的下一步行动	我们的下一步行动	下一状态
未完成	您未完成 TISAX 注册。 原因可能是：您未接受“一般条款和条件”； 您未给出主要参与者评估地点； 您未指定主要参与者联系人； 或者我们需要的其他信息缺失。	若要继续，请点击 enx.com/en-US/SignIn	我们会向您发送邮件提醒（通常在几天内）。	等待批准

7.4.3. Participant status “Awaiting approval”（参与者状态“等待批准”）

状态	所处状况	您的下一步行动	我们的下一步行动	下一状态

状态	所处状况	您的下一步行动	我们的下一步行动	下一状态
等待批准	您已完成 TISAX 注册， 但可能（还未）注册评估范围。	等待我们的下一步行动。	通常，我们会审核并批准您的申请。 只不过，一般来说只有您同时注册了评估范围，才会触发我们的审核行动。 我们会为您分配“参与者 ID”和“范围 ID”，并向您发送确认邮件。随邮件一同发送的“TISAX 范围摘要（PDF）”汇总了我们数据库中的相关信息。	初步完成

7.4.4. Participant status “Preliminary” (参与者状态“初步完成”)

状态	所处状况	您的下一步行动	我们的下一步行动	下一状态
初步完成	您已成功完成整个 TISAX 注册流程。	付款（如适用）。 完成 TISAX 评估流程， 发布并共享评估结果。	无	已完成注册

7.4.5. Participant status “Registered” (参与者状态“已完成注册”)

状态	所处状况	您的下一步行动	我们的下一步行动	下一状态
已完成注册	您已成功完成整个 TISAX 评估流程，并获得 TISAX 标签。 您已发布并共享评估结果。 您只有成功通过了 TISAX 评估流程，才能获得 TISAX 标签。 这一情形在 ENX 门户中反映为，评估范围的状态成为“Active”。	无	无	（已失效）

请注意：

如果您希望对您合作伙伴的评估结果进行评估：

理论上，接收其他参与者的评估结果需要符合以下前提条件：

- 您共享自己的评估结果（这一步可以“证明”，您是名副其实的 TISAX 参与者，是汽车行业的一员）。
- 我们基于您在汽车行业的声誉（如作为 OEM、一级供应商），来相应认可您的身份。
- 您自行证明，从其他参与者那里接收评估结果符合自己的合法利益。对此，我们需要通过严谨的流程加以证实，该过程可能产生高昂的费用。要了解更多信息，请联系我们。

7.4.6. Participant status “Expired”（参与者状态“已失效”）

状态	所处状况	您的下一步行动	我们的下一步行动	下一状态
已失效	您未付款， 或者您（我们）取消了双方之间的合同（GTC）。	无	无	不适用

7.5. 附录：Assessment scope status（评估范围状态）

7.5.1. 概述： 评估范围状态

“评估范围状态”定义了您的评估范围所处的工作周期阶段。

请注意，“评估范围状态”不同于“评估状态”。若要进一步了解“评估状态”，请参见章节 7.6, “附录：Assessment status（评估状态）”。

“评估范围状态”有以下几种：

1. Incomplete （未完成）
2. Awaiting your order （等待您的指示）
3. Awaiting ENX approval （等待 ENX 批准）
4. Awaiting your payment （等待您的付款）
5. Registered （已完成注册）
6. Active （已通过评估）
7. Expired （已失效）

以下各个状态的说明表将解释：

- 所处状况
  （该状态所代表的具体含义）
- 您的下一步行动
  （您如何到达下一状态；如适用）
- 我们的下一步行动
  （我们如何帮助您到达下一状态；如适用）

- 下一状态
  （如适用）

以下示例图展示了，需要哪些行动才可前往下一状态：

插图 38. 评估范围状态概述

1. 您
2. 我们
3. 评估范围状态
4. 1.未完成
5. 如果注册信息不完整
6. 信息录入
7. 2.等待您的指示
8. 如果注册未提交
9. 注册
10. 3.等待 ENX 批准
11. 审核 + 确认
12. 4.等待您的付款
13. 付款
14. 5.已完成注册
15. 评估
16. 6.已通过评估
17. A
18. 7.已失效
19. 通常当评估结果过期时

上图中的页面外标识“A”将 评估范围状态“Active”与“评估状态”相关联。若要进一步了解“评估状态”，请参见 章节 7.6, “附录：Assessment status（🇨🇳 评估状态）”。

7.5.2. Assessment scope status “Incomplete”（🇨🇳 评估范围状态“未完成”）

状态	所处状况	您的下一步行动	我们的下一步行动	下一状态
未完成	您未完成评估范围注册； 或者，您未提供所有的所需信息。	若要继续，请点击 🇬🇧 enx.com/en-US/SignIn	我们会向您发送邮件提醒（通常在几天内）。	等待您的指示

要进一步了解该状态的作用，请参见 章节 4.5.7, “评估范围注册”。

7.5.3. Assessment scope status “Awaiting your order”（🇨🇳 评估范围状态“等待您的指示”）

状态	所处状况	您的下一步行动	我们的下一步行动	下一状态

状态	所处状况	您的下一步行动	我们的下一步行动	下一状态
等待您的指示	您还未彻底完成范围注册。	若要继续，请点击 enx.com/en-US/SignIn	我们会向您发送邮件提醒（通常在几天内）。	等待 ENX 批准

要进一步了解该状态的作用，请参见 章节 4.5.7, “评估范围注册”。

7.5.4. Assessment scope status “Awaiting ENX approval” (评估范围状态“等待 ENX 批准”)

状态	所处状况	您的下一步行动	我们的下一步行动	下一状态
等待 ENX 批准	您已完成评估范围注册。	等待我们的下一步行动。	通常，我们会审核并批准您的申请。 我们会为您分配“参与者 ID”， 并向您发送确认邮件。 随邮件一同发送的“TISAX 范围摘要（PDF）”汇总了我们数据库中的相关信息。	等待您的付款

要进一步了解该状态的作用，请参见 章节 4.5.7, “评估范围注册”。

7.5.5. Assessment scope status “Awaiting your payment” (评估范围状态“等待您的付款”)

状态	所处状况	您的下一步行动	我们的下一步行动	下一状态

状态	所处状况	您的下一步行动	我们的下一步行动	下一状态
等待您的付款	您已完成评估范围注册，且已通过审核。 您已收到我们的确认邮件和“TISAX 范围摘要”。	付款（如适用）。 联系 TISAX 审计服务提供商并请求报价。 自“等待您的付款”状态起，您： ▪ 可以开始与合作伙伴共享评估相关信息。[40] ▪ 可以对评估结果的发布进行预设置（仅在您的评估范围状态变为“Active”时，该操作才会生效）。	等待您的付款。	已完成注册

40. 在评估范围状态为“等待您的付款”或“已完成注册”时，“评估相关信息”包括：评估范围地点、评估范围状态和评估对象，但不包括评估结果或 TISAX 标签。

要进一步了解该状态的作用，请参见 章节 4.5.8, “确认邮件”。

7.5.6. Assessment scope status “Registered” (评估范围状态“已完成注册”)

状态	所处状况	您的下一步行动	我们的下一步行动	下一状态
已完成注册	您已注册评估范围。 我们已收到您的全部付款，或者由于其他情况，您的商业状态为“绿灯”。	完成TISAX 评估流程	无	已通过评估

7.5.7. Assessment scope status “Active” (评估范围状态“已通过评估”)

状态	所处状况	您的下一步行动	我们的下一步行动	下一状态
已通过评估	您已成功完成整个 TISAX 评估流程，并获得TISAX 标签。	发布并共享评估结果。 此前阶段中预设置的发布与共享权限现阶段生效。	无	已失效

更多有关发布和共享评估结果的信息，请参阅 章节 6, “交换（第 三步）”。

7.5.8. Assessment scope status “Expired”（评估范围状态“已失效”）

状态	所处状况	您的下一步行动	我们的下一步行动	下一状态
已失效	原因： ▪ 您未在 90 天内完成评估范围注册； ▪ 您未在规定时间内付款； ▪ 您退出了 TISAX 评估流程； ▪ 您的评估结果已过期（三年）； ▪ 您的评估范围出现重大变更（例如：评估范围中的所有地点都不再属于您公司）。	重新启动评估范围注册	无	未完成 或 等待您的指示 或 等待 ENX 批准

7.6. 附录：Assessment status（评估状态）

7.6.1. 概述：Assessment status（评估状态）

“评估状态”定义了您在评估流程中所处的阶段。随着您从一项评估前往下一项评估（如从“初始评估”前往“纠正行动计划评估”），这一状态也会相应发生改变。

请注意，“评估状态”不同于“评估范围状态”。若要进一步了解“评估范围状态”，请参见章节 7.5, “附录：Assessment scope status（评估范围状态）”。

“评估状态”有以下几种：

1. Initial assessment ordered （初始评估已指定）
2. Initial assessment ongoing （初始评估进行中）
3. Waiting for corrective action plan assessment （等待纠正行动计划评估）
4. Waiting for follow-up （等待后续工作）
5. Finished （已完成）

以下各个状态的说明表将解释：

- 所处状况
  （该状态所代表的具体含义）
- 您的下一步行动
  （您如何到达下一状态；如适用）
- 我们的下一步行动
  （我们如何帮助您到达下一状态；如适用）
- 下一状态
  （如适用）

以下示例图展示了，需要哪些行动才可前往下一状态：

插图 39. 评估状态概述

1. 您
2. 评估范围状态
3. 评估状态
4. 指定评估
5. 初始评估已指定
6. 开始评估
7. 初始评估进行中
8. A
9. 完成评估
10. 6.已通过评估
11. 等待纠正行动计划评估
12. 制定纠正行动计划
    请求执行纠正行动计划评估
13. 等待后续工作
14. 请求执行后续工作评估
15. 已完成

上图中的页面外标识“A”将 评估范围状态“Active”与 评估状态“等待纠正行动计划评估”相关联。若要进一步了解“评估范围状态”，请参见 章节 7.5, “附录：Assessment scope status（评估范围状态）”。

7.6.2. Assessment status “Initial assessment ordered”（评估状态“初始评估已指定”）

状态	所处状况	您的下一步行动	我们的下一步行动	下一状态
初始评估已指定	您已选择其中一家 TISAX 审计服务提供商，并请求执行初始评估。	继续 TISAX 评估流程。	无	初始评估进行中

7.6.3. Assessment status “Initial assessment ongoing”（评估状态“初始评估进行中”）

状态	所处状况	您的下一步行动	我们的下一步行动	下一状态
初始评估进行中	您的初始评估： ▪ 已启动 ▪ 已完成，但审计服务提供商还未提交 TISAX 报告	无	无	等待纠正行动计划评估（如适用）

7.6.4. Assessment status “Waiting for corrective action plan assessment”（评估状态“等待纠正行动计划评估”）

状态	所处状况	您的下一步行动	我们的下一步行动	下一状态
等待纠正行动计划评估	审计服务提供商已执行初始评估， 并向我们提交了 TISAX 报告。 评估结果为（重大/轻微）不符合。	制定纠正行动计划， 并开始实施纠正行动。 请求执行纠正行动计划评估。	无	等待后续工作（如适用）

评估状态“等待纠正行动计划评估”限时九个月内完成。更多相关信息，请参见 章节 5.4.8.3, “纠正行动计划要求”。

7.6.5. Assessment status “Waiting for follow-up” (🇨🇳 评估状态“等待后续工作”)

状态	所处状况	您的下一步行动	我们的下一步行动	下一状态
等待后续工作	审计服务提供商已批准您的纠正行动计划， 且您已落实纠正行动。	请求执行后续工作评估	无	已完成

评估状态“等待后续工作”限时九个月内完成。更多相关信息，请参见 章节 5.4.8.3, “纠正行动计划要求”。

7.6.6. Assessment status “Finished” (🇨🇳 评估状态“已完成”)

状态	所处状况	您的下一步行动	我们的下一步行动	下一状态
已完成	审计服务提供商已执行后续工作评估， 评估结果无不符合项。 审计服务提供商向我们提交了 TISAX 报告。	发布并共享评估结果。	无	不适用

7.7. Annex: Custom scopes

Almost all TISAX participants choose the standard scope. However, in certain and *rare* circumstances you may need to choose a custom scope.

There are two types of custom scopes:

7.7.1. Custom extended scope

You can extend the scope. A custom extended scope contains MORE than the standard scope. The audit provider will perform more checks.

Purpose: A custom extended scope may be relevant if you want to use your TISAX assessment for internal purposes or outside of the automotive industry.

TISAX labels and sharing results: A custom extended scope always includes the standard scope. Therefore, a custom extended scope will receive TISAX labels[41]. Other TISAX participants will still accept the assessment result.

Description: While the standard scope has a predefined description, you need to write your own scope description if you need a custom extended scope.

7.7.2. Full custom scope

You can fully define your own scope.

Purpose: If you have locations that belong to different assessment scopes and that use services at a particular site (such as a data centre), you may use a full custom scope for those services. Thus, a TISAX audit provider can easily reuse the assessment result of the service's full custom scope.

Example: You have many locations (possibly part of different scopes) and you have a central IT department at one of those locations. Defining a full custom scope just for the IT department may make it easier to reuse the respective assessment result in the other scopes.

TISAX labels and sharing results: Full custom scopes don't receive TISAX labels. Your assessment result is recorded in the ENX portal with the date, validity period and whether the overall assessment result is conform or non-conform. You could share such an assessment result. But sharing an assessment result without TISAX labels will look like a "failed" assessment to most recipients. Other TISAX participants generally don't accept assessment results of full custom scopes.

Description: As for the custom extended scope, you need to write your own scope description if you need a full custom scope.

Important note:

To emphasize how rare the use of full custom scopes is: There is a 98% chance that your audit provider will revert your full custom scope to a standard scope. No participant *ever* successfully chose a full custom scope without advise from his audit provider.

An assessment with a full custom scope won't receive TISAX labels. We therefore generally advise against choosing a full custom scope — mainly because other participants generally don't accept assessment results with full custom scopes.
Do not choose a full custom scope if you don't have the explicit confirmation that your partner will accept the result and agreed with your particular scope description.

7.8. 附录：参与者信息工作周期管理

以下章节讲述了，如果您的参与者信息及相关事宜发生变更，您应当如何应对。

7.8.1. 公司名称变更

您若要变更公司名称，请联系我们。

7.8.2. 联系人变更

对于您公司的主要参与者联系人，以及其他所有"行政事务联系人"（拥有门户账号），可随时登录 ENX 门户并：

- 添加新联系人
- 删除现有联系人
- 更改现有联系人的联系信息

7.8.2.1. How to add a new contact

To add a new contact, follow these steps:

1. Log in to the ENX portal (https://enx.com/en-US/TISAX/).
2. Go to the main navigation bar and select “MY TISAX”.
3. From the dropdown menu, select “ADMINISTRATORS”.
4. Click the button “Create new TISAX Administrator”.
5. Enter the contact’s data.
6. Click the button “Save Contact”.
7. Go to the table and find the table row with the contact.
8. Go to the end of the table row of the contact and click the button with the down arrow  .
9. Select “Edit TISAX Administrator”.
10. In the new window (“Edit TISAX Contact”), scroll down to the section “ENX PORTAL ACCESS”.
11. Select “Yes”.
12. In the appearing section “WEB ROLES”, click the button “Add Role”.
13. Select the role you want to assign (e.g. “TISAX Administrator”).
14. Click the button “Add Role”.
15. Click the button “Save Contact”.

7.8.2.2. How to delete an existing contact

To delete an existing contact, follow these steps:

1. Log in to the ENX portal (https://enx.com/en-US/TISAX/).
2. Go to the main navigation bar and select “MY TISAX”.
3. From the dropdown menu, select “ADMINISTRATORS”.
4. Go to the table and find the table row with the contact.
5. Go to the end of the table row of the contact and click the button with the down arrow  .
6. Select “Delete TISAX Administrator”.
7. In the appearing confirmation request, click the button “Delete”.

7.8.2.3. How to update details of an existing contact

To update the details of an existing contact, follow these steps:

1. Log in to the ENX portal (https://enx.com/en-US/TISAX/).
2. Go to the main navigation bar and select “MY TISAX”.
3. From the dropdown menu, select “ADMINISTRATORS”.
4. Go to the table and find the table row with the contact.
5. Go to the end of the table row of the contact and click the button with the down arrow  .
6. Select “Edit TISAX Administrator”.
7. Update the details.
8. Click the button “Save Contact”.

7.8.3. 无法访问参与者信息（ENX 门户）

如果您公司里无人能够访问 ENX 门户，从而导致无法查看您的参与者信息，请联系我们。 我们将帮助您重新获得您公司参与者信息的访问权限。

7.8.4. 地址变更

如果仅是街道名称正式变更，您公司的主要参与者联系人只需联系我们即可。 我们将相应更新地址信息。

但是，如果您的其中一处地点迁往新址，则您需要：

1. 扩展评估范围。
   相关步骤请见章节 7.8.5, “添加地点（范围扩展评估）”。
2. 向我们发送邮件，并告知我们，旧地点已不再属于您的公司。
   我们将相应更新评估范围信息，并向您发送确认。

7.8.5. 添加地点（范围扩展评估）

在您现有 TISAX 标签的有效期内，如果您开放了一处新地点，则需要请求审计服务提供商执行“范围扩展评估”(scope extension assessment)。您不能选择另一家审计服务提供商来执行“范围扩展评估”。这项评估与其他评估类型相似，然而，审计服务提供商极有可能考虑重新使用来自以往评估的适用结果。

一旦完成范围扩展评估，且无不符合项，审计服务提供商将：

- 在 ENX 门户中更新您的评估范围。
- 签发“范围扩展评估”报告。

一次“范围扩展评估”并不会延长您现有 TISAX 标签的原始有效期限。

7.9. 附录：ISA 工作周期管理

信息安全评估标准（ISA）的维护工作由 ENX 工作小组负责，而德国汽车工业协会（VDA）负责正式发布新版本。我们制定了一套工作机制，用于确定哪一套 ISA 版本是（特定时间点执行的） TISAX 评估的基础。

如果 VDA 发布的新版本中包含格式及内容变更，我们将相应启动上述工作机制，并将新版本下发给各家 TISAX 审计服务提供商。一般在八周后，审计服务提供商便可依据新版本中的内容来执行评估工作。十六周后，审计服务提供商必须依据新版本来执行评估。这些期限适用于在上述工作机制启动之后收到的评估请求。如果您在上述工作机制启动之前请求执行评估，则审计服务提供商可以依据较早版本的 ISA 来执行评估工作。但是，审计服务提供商通常都会建议使用较新版本。

您可在选项卡“Change history（变更历史）”中，以及 VDA ISA 网页（https://portal.enx.com/isa5-en.xlsx）上查看 ISA 的发布日期。

7.10. 附录：帮助文档

本章节列出了我们认为对您有帮助的文件。

- 指导手册“Harmonization of security levels”（安全等级的协调化）

  “为打造以需求为导向的信息安全等级，一个关键因素便是，对信息实施分类和标注。本指导手册从分类等级的协调化与标准化出发，结合信息保密性原则，为相关工作指明了方向。”

  出版语言：德语、英语

  出版方：德国汽车工业协会（VDA）

  www.vda.de/en/services/Publications/whitepaper-%22harmonization-of-security-levels%22.html
- “信息安全风险管理”指导手册

“该指导手册的目标是，让汽车行业的公司了解面向风险的信息安全管理，并使其能够建立一套有效的信息安全风险管理体系。它旨在协助公司准备或执行 TISAX 评估，从而满足 VDA ISA 控制问题 1.4.1 的要求。该手册内容应被视为实施建议，而非强制性要求。”

出版语言：德语、英语

出版方：德国汽车工业协会（VDA）

www.vda.de/en/services/Publications/white-paper-%22information-security-risk-management%22.html

7.11. Annex: Complaint management

7.11.1. Causes for complaint

Our complaint management differentiates between these two areas:

1. ENX Association — the organisation that governs TISAX
2. Audit providers — the organisations that conduct the TISAX assessments

7.11.1.1. Complaints about ENX Association

If you have a complaint about ENX Association, please contact our “TISAX manager on duty” (see contact details below).

7.11.1.2. Complaints about audit providers

First, you should try to solve the issue directly with the auditor.

The next step should be the person responsible for TISAX at the audit provider.

Thereafter, your next contact would be the person responsible for the audit provider’s quality management.

If the issue is still unsolved, you should contact our “TISAX manager on duty” (see contact details below).

There are even options above the “TISAX manager on duty”. In such cases, you would talk to ENX Association’s managing director.

The VDA has no role in the complaint management.

7.11.1.3. Requirements for complaints

If you want to involve us, we need the following information:

- Who is complaining?
  - Company name
  - TISAX Participant ID
  - Contact (name, email address, phone number)
- Which assessment is it?
  - Assessment ID
  - If the assessment is not yet recorded in the ENX portal: Scope ID
- Who is the audit provider?
  - Audit provider company name
  - Name of the auditor(s)

- What are you complaining about?
  1. General complaint about the performance of the audit provider
  2. Complaint about the approach of the auditor
  3. Complaint about the assessment with regards to content
- For complaints about the assessment with regards to content: Which finding do you object?
  - Control (e.g. 1.6.1 "To what extent are information security events processed?")
  - Finding (full text)
  - Objection against:
    - Interpretation of the control
    - Ascertainment with regards to content (available evidence is not assessed correctly)
    - Risk assessment (appropriateness not considered)
  - Reasoning why you assess things differently

7.11.2. Contact for complaints

Please contact the “TISAX manager on duty”:

Send him an email at: tisax-complaints@enx.com

Or call him at: +49 69 9866927-79

You can reach him during regular business hours in Germany (UTC+01:00 (https://www.worldtimeserver.com/current_time_in_DE.aspx)).

He speaks English and German.

8. 文档历史

版本	注释

版本	注释
2.3	▪ 副标题名称改变 ▪ 将手册的主要格式由 Word/PDF 改为 HTML ▪ 增加其他语种译文（中文和法语，见下一项目符号） ▪ 添加章节“《TISAX 参与者手册》其他语言版本和格式” ▪ ENX 主页的所有链接由 "https://portal.enx.com" 改为 "https://enx.com"（原来的链接依然有效） ▪ “VDA ISA”改为“ISA” ▪ 更新章节 章节 5.2, “基于 ISA 的自我评估”，以反映 ISA（版本 5）所引入的变化 ▪ 针对列出评估对象的所有表格，对表格行进行重新排序，以匹配 ISA 5 中更改后的标准目录顺序 ▪ 对列出评估对象的图表进行更新，以匹配 ISA 5 中更改后的标准目录顺序 ▪ 章节“范围调整” 更新（图 6，更正了打字错误，并更新了评估对象） ▪ 章节“费用”更新，增加了信用卡付款信息 ▪ 章节“TISAX 评估流程图解”更新（图 34，删除引述管理服务提供商的部分） ▪ 章节“附录：帮助文档”更新（增加“信息安全风险管理”指导手册部分）
2.2.1	▪ 纠正打字错误

版本	注释
2.2	▪ 解决封面印刷问题 ▪ 调整所有主页和下载链接 ▪ 增加意大利语服务 ▪ 扩展章节“自定义范围” ▪ 更新章节“评估范围地点” ▪ 删除评估对象“Connection to 3rd parties”（与第三方的关联）；更新图 7、9 和 38；更新表 4、5、6 和 8 ▪ 用词“*with* assessment level”改为“*in* assessment level” ▪ 删除章节“保护需求与评估级别”中引用“TISAX activation list”的内容（不再适用） ▪ 新增章节“评估对象与您供应商之间的关系” ▪ 更新“参与者联系人”章节，增加关于公共邮箱地址，以及邀请联系人使其能够在 ENX 门户中管理参与者信息的内容 ▪ 更新“评估范围注册”章节，增加关于评估范围变更的内容 ▪ 更新“状态信息”章节（图 12） ▪ 更新“处理自我评估结果”章节，增加有关外部帮助（由第三方）的内容 ▪ 更新“地域限制”章节，增加审计服务提供商地域限制检索链接 ▪ 更新“请求报价”章节 ▪ 更新“评估执行人选择依据”章节，增加关于“预评估”的内容 ▪ 更新“TISAX 标签的换发”章节，增加有关需要注册新范围的内容 ▪ 更新“交换（第三步）”章节的若干子章节，以反映 ENX 门户中界面的变化 ▪ 更新“与特定参与者共享评估结果”章节，增加关于共享级别建议，以及自动处理共享评估结果等内容 ▪ 新增章节“在 TISAX 框架之外共享评估结果” ▪ 新增章节“ISA 工作周期管理” ▪ 更新“附录：评估范围状态”章节（新增状态“等待您的指示”，状态“等待批准”更名为“等待 ENX 批准”，状态“已批准”更名为“等待您的付款”，图 40） ▪ 更新“附录：确认邮件示例”章节 ▪ 更新“附录：TISAX 范围摘要示例”章节 ▪ 更新“附录：评估状态”章节（新增状态“初始评估进行中”，状态“等待后续工作评估”更名为“等待后续工作”，图 41） ▪ 删除章节“Annexe: Volkswagen legacy assessments”及相关引述（不再相关）
2.1.2	▪ “您的评估结果得分”与“评估结果最高分”之间的“差距”限制由 25% 校正为 30%
2.1.1	▪ 纠正打字错误

版本	注释
2.1	▪ 删除章节“Managed Service Providers” ▪ 新增 TISAX 评估对象 / 标签（数据保护标签基于 GDPR；原型标签由两个改为四个；重命名：“保护级别”改为“保护需求”；更新选择建议内容） ▪ 由于ISA 版本变更（4.0 到 4.1），而更新相关内容 ▪ 引述新文档“TISAX 快捷群体评估（TISAX Simplified Group Assessment）”——本手册的补充篇 ▪ 新增地点名称与范围名称的分配建议 ▪ “注册费”重命名为“费用” ▪ 新增联系代理人相关建议 ▪ 删除 Selection of charging model

返回顶部

1. Verband der Automobilindustrie e. V.（VDA），https://www.vda.de
2. 您可能会从“占据先手”这个角度出发，考虑参与 TISAX 流程。一些公司这样做，是为了更好地进行准备，因为相对于尚未经过 TISAX 评估的竞争对手，参与 TISAX 评估流程意味着，您熟悉该工作所需要的时间更短，因而可为您带来优势。
3. “TISAX 标签”这一概念是对您评估结果的总结，也是 TISAX 流程的输出形式。更多信息，请参见 章节 5.4.13, “TISAX 标签”
4. 当您作为 TISAX 参与者首次参与评估时，您只需完成大多数注册步骤一次；而在更新评估结果时，您只需更新并确认自己的注册信息即可。
5. 我们将在 ENX 门户网站上发布针对 GTC 的更改，并通知已注册的联系人。
6. 这同样适用于各种补充协议，如行为准则。
7. 该标准范围描述是 1.0 版，鉴于今后可能会更新描述，我们因而加入了版本控制。
8. 解决方法是：a) 从范围中移除该地点；b) 解决问题；c) 之后利用“范围扩展评估”来添加该地点
9. 请注意，当前您的合作伙伴不会自动获得关于新权限的通知。在拿到评估结果后，您可能希望通知自己的合作伙伴。
10. 如果您想加入这个名单，请联系我们
11. 证据是指支持您的论断（如您符合某项要求）的材料，其大多数情况下以文件的形式存在。您将用到的证据必然是公司内部文件。
12. 针对评估级别 2 的评估谈话通常以电话会议的形式进行，您亦可要求在评估现场进行面对面谈话。
13. 我们的日常邮件交流仅限与参与者联系人之间进行，交流信息不会发送给不具备“参与者”资格的账号。为保证我们的邮件能顺利发送给账号的所有者，请确保指定至少一名备选参与者联系人。
14. 理论上，接受“快捷群体评估”的企业至少要有三处地点。
15. 如果您已经知道，自己的信息安全管理体系需要进行改进，那建议您至少要有十二处地点。
16. 为了防止数字和字母之间出现混淆的情况（如数字 8 和字母 B），某些字母不允许出现在参与者 ID 中。但是，某些较早的参与者 ID 中可能出现字母“G”。
17. ISA 也将标准目录称为“单元”
18. 您可在功能区“Data（数据）”的“Outline（大纲）”部分找到这一隐藏的 Excel 功能。
19. 您公司使用的执行类似评估（如 ISO 27001）的审计服务提供商是否亦有兴趣获得 TISAX 评估执行资格？那么，您可与其分享本手册，并告知其与我们联系，来了解如何成为一名 TISAX 审计服务提供商
20. 未列入我们名单的审计服务提供商将不允许执行 TISAX 评估。
21. 如果终止评估流程，您将不会获得 TISAX 标签。
22. 其实，还有第四种类型“范围扩展评估”。由于这属于特殊情况，因而将相关讨论放在附录章节章节 7.8.5, “添加地点（范围扩展评估）”。
23. 正式*立项*会议仅针对初始评估。对于其他 TISAX 评估，您的审计服务提供商将相应安排并组织会议。
24. 一些审计服务提供商可能会使用同义词“启动会议（kickoff meeting）”来代指“正式立项会议（Formal opening meeting）”。
25. 正式*结项*会议仅针对初始评估。对于其他 TISAX 评估，您的审计服务提供商将相应安排并组织会议。
26. 如果无法解决争议，则您可以将问题上报。更多信息，请联系我们。
27. 在这一阶段，您仍然可以更改范围。
28. 关于审计方法和审计力度的更多信息，请参见章节 4.3.3.6, “保护需求与评估级别”。
29. 如果无法解决争议，则您可以将问题上报。更多信息，请联系我们。
30. 初始评估与纠正行动计划评估的时间间隔不得长于九个月。

31. 请注意，即使您已经确定了适当的纠正行动，您的整体评估结果依然有可能是“重大不符合”。出现这一情况的原因是，您的措施并未产生/立即产生效果。

32. 当然，这一点仅适用于初始评估发现不符合项的情况。如果初始评估的评估结果为“符合”，那么便无需再执行后续工作评估。

33. 理论上，该日期可以是初始评估结项之后九个月内。之前较长一段时间内便请求执行后续工作评估。

34. 其实，还有第四种类型“范围扩展评估报告（scope extension assessment report）”。由于这属于特殊情况，因而相关讨论请见章节 7.8.5, “添加地点（范围扩展评估）”。

35. “TISAX 报告”是基于特定模板生成的，所有 TISAX 审计服务提供商均须使用该模板。

36. “换发”这个说法可能有歧义。为了在三年后依然能保住 TISAX 标签，您需要再次完成 TISAX 评估流程，而第一步，便是要重新注册评估范围。

37. 我们不会以列表形式对“参与者 ID”进行公示，原因是，我们不希望因公司名称相似或其他“人为失误”，而导致出现意外共享给他人的情况。因此，您需要直接联系合作伙伴，来索要其“参与者 ID”。

38. 合作伙伴需自行登录门户并查找您共享的评估结果，而不会自动收到关于新共享评估结果的通知。

39. 该规则的解释见“TISAX 参与一般条款和条件”（https://enx.com/tisaxgtcen.pdf (https://enx.com/tisaxgtcen.pdf)）。

41. “TISAX labels” are a concept to summarise your assessment result and are the output of the TISAX process. Please refer to 章节 5.4.13, “TISAX 标签” for more details.