贯标集团-北京TISAX 德系汽车行业信息安全评估认证

产品名称	贯标集团-北京TISAX 德系汽车行业信息安全评估认证
公司名称	贯标集团-华北公司
价格	.00/件
规格参数	
公司地址	华北公司地址：天津市河西区南京路35号亚太大厦13层；总部地址：江苏省南京市玄武区新庄村57号二楼
联系电话	022-23125802 15502200816

产品详情

目前的汽车配置来看，车载电脑已经是车上的标准配备。例如车载导航、影片播放、上网、电话、故障诊断等功能都是车载电脑的应用，但也因网络安全漏洞及资料外泄事件层出不穷，车载信息安全问题成为社会关注的焦点。以下我们汇总在辅导经验中常被询问到的几个常见问题予以说明。

1. 什么是 TISAX？

TISAX（Trusted Information Security Assessment Exchange）信息安全的评估和交换机制是2017年由德国汽车工业联合会 (VDA) 联合欧洲网络交换所 (ENX) 所推出的信息交换平台，把受多数组织成员认可的信息安全评估流程 VDA ISA (Information Security Assessment) 之审核结果放上平台，供参与者在得到被审核者授权后做查询，是一个参考 ISO 27001、ISO 27002等标准规范所制定的信息安全评估结果的交换平台。

ISA: 用于组织的内部控制要求， 接触组织敏感信息的供应商（服务商）的审核要求。

VDA联合ENX推出成员组织认可的信息安全评估流程，将审核结果放在的授权平台上以供信息查询和交换。

ENX:为欧洲汽车工业提供开发、采购和生产控制安全交换关键数据解决方案的协会

ENX协会：TISAX的监管和组织的角色。

由ENX认可审核机构并且监督审核机构的审核结果以及审核的合规性。

通过监管“ ENX治理三角 ”得到保证，包括ENX协会与ENX认可的审核机构之间以及ENX协会与每个参与者之间的合作。

2. 谁会需要使用到 TISAX?

汽车零件制造厂、汽车应用产品厂商及汽车供应链成员。从传统零部件供应商到更广泛的合作伙伴，TISAX审计的对象，一般是面向传统的汽车零部件供应商，从国内覆盖范围来看，无论是跨国企业还是本土企业，审计地点会包括公司总部的办公环境、研发环境，也包括其在各地的工厂、实验室、测试场地等。随着汽车发展变得更加节能和数字化，新能源汽车、移动互联网和自动驾驶领域的公司及其相应的技术研发和相关服务也成为汽车供应链中不可或缺的一部分。许多知名的科技巨头和高创新的初创企业已开始踏上他们的TISAX之路。

此外，从事汽车市场研究、以客户为中心的服务的公司（如研究机构）以及提供支持性ICT服务（包括系统运营服务、邮箱服务、云服务等）的公司也需要向其OEMs客户和/或汽车客户提供有效的TISAX标签。

3. 导入 TISAX的好处?

TISAX平台上的评估结果具公信力，有助取得客户信任。

(TISAX)-VDA ISA的问项内容统一，参与者之评估结果具可比较性。

降低重复性的审核作业，每三年评估一次即可。

许多欧系车厂如 Volkswagen / BMW / Porsche 已开始要求供应链必须取得 TISAX 认证。

4. TISAX目前在国内的现状

目前大众，奥迪和保时捷要求供应商必须通过TISAX认证。后续其他德国车企也会跟进要求供应商通过TISAX认证。

5. 导入TISAX及ISO27001之目的及应用层面有何差异?

两者皆可提升组织的信息安全能力，降低信息安全事件、事故的发生，只是应用层面有所不同。

1. ISO 27001是一应用层面广泛的信息安全管理系统的认证，适于各产业采用。

2. TISAX则提供了汽车产业以信息安全评估结果的平台，在评估方获得被审核者授权后 (在 ENX Portal 上授予权限)，让被审核者可自行决定那些伙伴可在平台得知其信息安全评估结果，藉此让汽车供应链合作伙伴了解其在网络安全及资料保护上的成果。

6. ISO 27001及(TISAX)-VDA ISA之章节内容有何不同.

ISO 27001共包含两部分，除了条文第四章至第十章，另外还有附录 A的 114个资安控制措施，通过 ISO27001认证代表企业已建立、实施及维持及持续改善ISMS要求之事项

TISAX VDA-ISA (Information Security Assessment) 参考 ISO 27001、ISO 27002等规范外，并参酌法规(例如:欧盟个资法 GDPR)及汽车产业之要求做为管制项目，四大管制面向及内容简述如下:

1. 信息安全 (information security)
: 因属核心的强制(mandatory)评估项目，故必须评估，无法排除。及下列选择性事项，共三类

2. 第三方的连接 (Connection to 3rd parties) : 如项目办公室和项目区域。

3. 资料保护 (Data protection) : GDPR第28条资料处理者。

4. 原型保护 (Prototype protection) : 针对尚未对外公布的车、元件、零件之保护。

7. TISAX与ISO27001主要差异为何?

1. 范围: ISO 27001适用产业的范围较 TISAX广。

2. 级别制: ISO 27001无级别制，TISAX则采用级别制，

共有三种审核等级 (Assessment level (AL)，AL1一般是自评，AL2和 AL3需要第三方稽核员对公司进行现场稽核，一般获得 AL2和 AL3才能够获得TISAX的认可。

而 AL2或 AL3则由客户依照与供应商的资料串接情况做选定，各级别评估方式如下:

评估方式	AL1(自评)	AL2	AL3
自评		是	

(self-assessment)	是		
证据 (evidence)	否	真实性检查(Plausibility check)	彻底查证 (Thorough verificat
访问 (interviews)	电话会谈 (Audio conference)	人员现场访谈 (In person,on site)	
现场稽查 (on-site inspection)	不一定		

(source:TISAX Participant Handbook)

另外，TISAX在四大管制面向六个成熟度级别做评分，让组织了解现况级别，并可供往更高ji别进步之参考，六个成熟度级别定义如下：级别0：不完整级别1：已执行级别2：已管理级别3：已建立级别4：可预测级别5：持续优化。

8. 通过TISAX审核的步骤是怎样的?

初始诊断阶段：明确TISAX审核范围，审核等级。

1.风险评估阶段

2.体系文件编写阶段

3.体系试运行阶段

4. 体系完善阶段

5.TISAX审核认证

6.售后服务阶段