贯标集团-北京构建汽车行业的可信商业社会 – TISAX审核标准解析

产品名称	贯标集团-北京构建汽车行业的可信商业社会 – TISAX审核标准解析
公司名称	贯标集团--天津公司
价格	.00/件
规格参数	
公司地址	天津市滨海高新区华苑产业区梅苑路5号金座广场-3318
联系电话	15502200816 15502200816

产品详情

在往期文章中，我们已经对TISAX标签进行了初步的介绍，包含TISAX的背景介绍、注册与自评估及审核流程等。在本篇中，我们将继续围绕TISAX的基础知识，包括TISAX审核标准，TISAX和ISO27001在审核上的异同进行探讨。

1

TISAX与ISO27001审核标准的比较

TISAX 审核基于VDA ISA标准，从内容上看，蕞新的5.0版本依旧基于 ISO 27001与ISO27002的主要内容，但在结构和内容方面进行了优化，区别于TISAX 4.1，TISAX 5.0不再使用ISO27001的框架，而是将其内容分为了7个控制域，然后在此基础之上添加了，样件保护与数据保护控制域，并且，TISAX4.1中的第三方联系控制域也合并入信息安全控制域中。新版本的目的是使用更轻松，更高效，从而减少了公司和审核员的工作量。TISAX审核之所以以ISO27001为基础是因为该信息安全管理要

求已得到了很多国家的认可，是国际上具有代表性的信息安全管理体系标准。VDA建立其“信息安全”工作组已十多年，始终致力于开发成熟的适用于汽车行业的信息安全要求。作为VDA下的一员，之前的ISA标准通常被用于组织的内部控制要求，或者是作为那些能接触组织敏感信息的供应商的审核要求。从供应商的角度来说，频繁地接受来自于不同主机厂的审核，且其审核要求大同小异，已经越来越成为供应商自身运营的负担。为此，VDA联合ENX协会推出了得到大部分成员组织认可的信息安全评估流程，并将据此得到的审核结果放在一个可供信息交换的可信平台（ENX）上，以替代之前各主机厂的频繁审核，供各需求方进行授权查询。

2

TISAX与ISO27001审核方式的比较

从二者审核方式总体上来看，TISAX的成熟度评估是针对每个控制要求的，每个要求必须达到蕞低成熟度。在具体审核时，审计师会对各个单项控制点的成熟度情况进行评分，蕞终得出整体分数。ISO 27001并没有按成熟度评分的机制，而是根据风险评估的结果对风险实施保护控制，并且ISO27001更强调PDCA的概念。PDCA循环的含义是将质量管理分为四个阶段，即Plan计划（包括方针和目标的确定，以及活动规划的制定）、Do执行（根据已知的信息，设计具体的方法、方案和计划布局；再根据设计和布局，进行具体运作，实现计划中的内容）、Check检查（总结执行计划的结果，分清哪些对了，哪些错了，明确效果，找出问题）、Act处理（对总结检查的结果进行处理，对成功的经验加以肯定，并予以标准化；对于失败的教训也要总结，引起重视），而TISAX则没有突出PDCA。另外，在具体操作时，TISAX审核相比 ISO27001也存在诸多差异。如：评估模块与评估级别需要主机厂协助判定，以主机厂的要求为准；样件保护标签可多选，由主机厂确认需要通过哪类标签；TISAX评分需要遵循cutback机制等。

3

VDA ISA 标准

TISAX的审核标准整体基于VDA ISA目录，蕞新的版本5.0包含9个控制域。在实际实施测评时，这9个控制域被包含于3个模块中，其中前7个控制域归于“信息安全”模块，即通用信息安全要求。“样件保护”和“数据保护”基于行业特性，保密性要求较高，各自单独为一个模块，所包含的具体控制点的要求与ISO27001有所区分。

TISAX 审核内容

信息安全制度与组织：内容涉及信息安全策略的创建、发布或分发及定期审查，资产管理，信息安全风险管理。

人力资源安全：内容涉及内外部员工遵循信息安全规定的程度，内外部员工遵守信息安全策略的程度。

物理环境安全：内容涉及对敏感信息处理设施的安全区域的定义、保护和监测，对自然灾害、故意袭击或事故产生影响的应对，信息安全要求和危机事件下的ISMS的连续性的界定、实施、核实和评估。

访问控制：内容涉及访问IT系统政策和程序的适用性，特权用户和技术账户的分配和使用的监督审查，用户遵守创建和处理机密信息约束性政策的情况，授权人员的信息和应用程序的获取，与其他组织共享的环境中的数据分离。

信息安全与网络安全：内容涉及密码学，操作安全，系统采购、需求管理和开发。

供应商关系：内容涉及供应商获得公司信息资产时的风险控制，供应商服务的定期检测、审查和审计。

合规：内容涉及相关法律（特定国家）法规和合同要求的符合情况，个人身份信息的保护，独立第三方定期或发生重大变化时对ISMS的审核。

样件保护：除物理及环境要求、组织架构要求外，内容还涉及整车及零配件处理（车辆或部件在运输过程中根据客户要求的保护情况，停放/存放需要保护车辆或部件的实施情况），测试车要求（预先定义的伪装法规的实施情况，测试场地的保护措施，公开批准试驾的保护措施），活动拍摄及拍照要求（涉及车辆、部件或配件的演示和活动的安全要求，涉及车辆、部件或配件的胶片和照片拍摄的保护措施）。

数据保护：内容涉及数据保护的实施程度，个人身份数据处理的合法性保障措施，内部或工作流程在数据保护法规下进行，有关处理流程在何种程度上记录了其可受理性。

TISAX 审核要求

在5.0的官方目录中，各类要求以表格的形式体现：

“ 必须满足 ” 类别的要求是强制性要求，没有任何例外。

“ 相应满足 ” 类别的要求通常由组织总体实施。但是，在某些情况下，对于不遵守 “ 相应满足 ” 类别的要求，可能有正当理由，如有任何偏差，组织应了解其影响，并有合理理由或补偿措施与控制。

如果评估级别是 “ 高保护要求 ”，则必须另外满足 “ 高保护要求 ” 类别的要求。

如果评估级别是 “ 极高保护要求 ”，则必须额外满足 “ 高保护要求 ” 与 “ 极高保护要求 ” 类别中的要求。

在5.0版本中，原则上不允许有 “ 不适用 ” 项

5

评分方式

TISAX采用“ 成熟度等级 ”的概念用于评估控制项的完成质量，在实际审核过程中，分为六个成熟度等级：

不完整的成熟度为0，表示没有流程或流程未运行（没做），属于重大不符合；

已执行的成熟度为1，表示有运行的流程，但是流程没有被记录（做了没记录），属于重大不符合/轻微不符合；

已管理的成熟度为2，表示运行且有记录的流程，但是同一目标有多个不同的流程（流程不统一），属于轻微不符合/观察项；

已建立的成熟度为3，表示有运行的流程，也有实时更新的运行记录，且流程是在一个统一的信息安全框架下管理的（有流程有记录，但是没测量），属于观察项/无偏差；

可预测的成熟度为4，表示在成熟度3的基础上有运行的流程并可以测量，属于无偏差；

在优化的成熟度为5，表示在成熟度4的基础上有专人负责持续提升优化，属于无偏差。

在评分0-5分的基础上，TISAX还使用了cutback机制，每个大控制点的目标成熟度都是3分，为了确保低分项不会被高分项拉高最终评分，实际得分超过目标成熟度的分数均会被折算为目标成熟度。具体操作如下图所示，当实际成熟度评分为4分或5分时，将调整为3分；实际成熟度评分为1-3分的将维持原分数不变。

TISAX Cut Back 机制

6

结语

TISAX的审核内容介绍到此就告一段落，本篇中我们详细介绍了TISAX审核内容、TISAX和ISO27001的关

系等。我们将在后续文章中，为您深度解析企业在了解了TISAX审核标准与流程之后，如何依据企业实际情况，开展TISAX合规建设，敬请期待！