汽车供应链风险与第三方认证价值

1. INTRODUCTION
1. 简介

汽车行业的特点是复杂的全球供应链，包括众多供应商、制造商和服务提供商。这些利益相关方协同工作，设计、开发、生产和分销汽车零部件和车辆。由于政治压力、经济力量、社会趋势、技术进步、法律要求和环境压力，汽车行业正在经历快速转型，汽车供应商面临着越来越多的挑战和风险。在这种情况下，第三方认证已成为确保汽车供应链弹性和可持续性的关键工具。

本白皮书旨在对汽车供应链风险进行全面分析，并展示第三方认证如何帮助减轻这些风险。通过深入研究汽车供应链的复杂性及其面临的挑战，我们旨在为IAOB及其汽车供应商提供有价值的见解，帮助他们利用认证服务实现更可持续、更有弹性的供应链。

在接下来的章节中，我们将探讨与汽车供应链相关的各种风险，包括质量和合规、环境和可持续性、信息安全、业务连续性和灾难恢复、地缘政治和经济以及法律和监管风险。随后，我们将讨论第三方认证在解决这些风险和提高供应链绩效方面的作用。

最后，我们将概述汽车供应商的相关认证，如ISO 27001、ISO 27701、20000-1、ISO 22301、TISAX、即将推出的42001及其优势。

2. 汽车供应链风险

汽车供应链面临各种风险，这些风险可能会影响行业的整体业绩、盈利能力和可持续性。在本节中，我们将分析汽车供应商面临的最突出的风险：

- **质量和合规风险**

  由于产品的安全关键性，汽车行业受到严格的质量和合规要求的约束。供应商必须遵守众多标准、法规和客户特定要求。不满足这些要求可能导致昂贵的召回、法律处罚和品牌声誉受损。

- **环境和可持续风险**

  环境和可持续性风险对汽车供应链来说越来越重要。这些风险包括资源消耗、废物产生、能源消耗和温室气体排放。供应商必须解决这些风险，以确保遵守法规，保持积极的品牌形象，并满足客户对环保产品的需求。

- **信息安全风险**

  随着互联汽车的兴起和汽车系统的数字化，信息安全风险已成为业界关注的一大问题。供应商必须保护敏感数据，如知识产权、客户信息和专有软件，使其免受未经授权的访问、盗窃和网络攻击。

- **业务连续性和灾害恢复风险**

  汽车供应链高度相互依存，容易受到自然灾害、地缘政治紧张局势和其他不可预见事件造成的干扰。供应商必须制定强有力的业务连续性和灾难恢复计划，以最大限度地减少这些中断的影响，并保持运营弹性。

- **地缘政治和经济风险**

  由于汽车行业的全球性，汽车供应商面临地缘政治和经济风险。这些风险包括货币波动、贸易限制和政治不稳定，这些都会对原材料、劳动力和运输的成本和可用性产生重大影响。

- **法律和监管风险**

  汽车行业受到许多有关安全、环境保护、数据隐私和劳动实践的法律法规的约束。供应商必须持续监控并适应这些监管变化，以保持合规性，避免法律处罚、罚款和声誉损害。

了解和解决这些风险对于汽车供应商确保可持续和有弹性的供应链至关重要。在下一节中，我们将讨论第三方认证在降低这些风险和提高供应链绩效方面的作用。

3. 第三方认证在降低风险中的作用

第三方认证在降低汽车供应链相关风险方面发挥着关键作用。通过对公司的流程和系统进行公正的评估，认证可确保符合行业标准、最佳实践和监管要求。在本节中，我们将讨论第三方认证在解决上一节中概述的风险方面的好处：

- **确保质量和合规**

  第三方认证有助于汽车供应商展示其对质量和合规性的承诺。通过获得相关标准的认证，供应商可以展示他们对行业最佳实践的遵守，这可以增强客户的信任，降低不合规风险，并提高运营效率。

- **提升环境和可持续发展绩效**

  专注于环境和可持续性方面的认证促使汽车供应商能够评估和提升其环境绩效。通过认证的管理体系，供应商可以确定需要改进的领域，减少浪费，并将其对环境的影响降至最低，这有助于建立更可持续的供应链。

- **加强信息安全**

  信息安全认证，如ISO 27001和ISO27701，确保汽车供应商拥有健全的系统和流程来保护敏感数据。通过获得认证，供应商可以证明他们对数据保护的承诺，并向客户和利益相关者保证他们的信息是安全的。

- **增强业务连续性和灾难恢复能力**

  与业务连续性和灾难恢复相关的认证有助于供应商建立和维护有弹性的运营。通过实施经认证的管理系统，供应商可以更好地为破坏性事件做好准备、做出反应并从中恢复，从而确保供应链的连续性。

- **管理地缘政治和经济风险**

  虽然第三方认证不能直接解决地缘政治和经济风险，但它有助于供应商的风险管理工作。通过展示对最佳实践和行业标准的承诺，认证供应商可以将自己确立为可靠的合作伙伴，使其在面临不确定性时对客户和投资者更有吸引力。

- **支持法律法规遵从性**

  第三方认证可以作为证明法律和法规合规性的宝贵工具。通过获得相关标准的认证，供应商可以展示他们对满足法律要求的承诺，这有助于降低处罚、罚款和声誉损害的风险。

总之，第三方认证通过对公司的流程和系统进行公正的审核，在降低汽车供应链风险方面发挥着至关重要的作用。通过利用认证服务，汽车供应商可以增强其弹性，证明其符合行业标准和监管要求，并为更可持续和可靠的供应链做出贡献。

4. 汽车供应商相关服务概述

在本节中，我们将概述汽车供应商的相关认证或服务，这些认证或服务有助于降低与汽车供应链相关的风险。这些认证侧重于信息安全、隐私和业务连续性，所有这些都是可持续和有弹性的供应链的关键方面。

4.1 ISO 27001：信息安全管理体系

ISO 27001是国际公认的信息安全管理系统（ISMS）标准。它提供了一种系统化的方法来管理敏感的公司信息，确保信息的安全。该标准适用于各种规模和行业的组织，包括汽车行业。

ISO 27001认证对汽车供应商的好处包括：

- 通过基于风险的方法增强信息安全
- 改进了对与信息安全相关的法规和合同要求的符合性
- 增强了客户、利益相关者和合作伙伴的信任
- 经证实的信息安全最佳实践承诺

ISO 27001还可以通过以下附加内容得到进一步加强：

- ISO 27017，云服务信息安全控制实施规范
- ISO 27018，作为个人识别信息处理器的公共云中个人识别信息（PII）保护实施规范

4.2 ISO 27701: 隐私信息管理体系

ISO 27701是ISO 27001的隐私扩展，为实施隐私信息管理系统（PIMS）提供了指导。它帮助组织管理和保护个人信息，确保遵守GDPR等数据隐私法规。该标准适用于处理个人数据的组织。ISO 27701认证对汽车供应商的好处包括：

- 改进数据隐私做法和个人信息保护
- 遵守数据保护法规并降低处罚风险
- 增强客户和利益相关者对隐私事项的信任
- 与现有ISO 27001信息安全管理系统集成

- 4.3 **ISO 22301: 商业可持续性管理体系**

ISO 22301是业务连续性管理系统（BCMS）的国际标准。它为组织识别潜在威胁、评估其影响以及制定计划提供了一个框架，以确保在发生中断时的业务连续性。该标准适用于各种规模和行业的组织，包括汽车供应商。ISO 22301认证对汽车供应商的好处包括：

- 提高应对破坏性事件的应变能力和准备能力
- 在出现中断时减少停机时间和财务影响
- 作为可靠且有弹性的供应商，声誉得到提升
- 遵守与业务连续性相关的客户和法规要求

- 4.4 **ISO 20000-1: IT服务管理体系**

ISO 20000-1是国际公认的IT服务管理系统标准。它为组织规划、建立、实施、运营、监控、审查、维护和改进其It服务管理流程提供了一个框架。此标准有助于确保IT服务与业务需求保持一致，并有效、高效、安全地提供。ISO 20000-1有利于汽车供应商预防供应链攻击。

ISO 20000-1认证对汽车供应商的好处包括：

- 提高IT服务质量：通过实施ISO 20000-1标准，汽车供应商可以提高其IT服务质量，从而实现更高效、更可靠的运营。
- 加强网络安全态势：该标准为管理信息安全风险提供了指导方针，使供应商能够识别潜在威胁并实施适当的控制措施，以防止供应链攻击。
- 改进供应商管理：ISO 20000-1要求组织有效管理第三方供应商，确保他们遵守必要的安全协议，并将供应商漏洞导致的违规风险降至最低。
- 简化的IT流程：ITSMS框架促进最佳实践的使用和持续改进，帮助汽车供应商优化其IT流程，降低网络攻击导致服务中断的可能性。

- 4.5 **TISAX汽车行业信息安全**

TISAX（可信信息安全审核）是专门为汽车行业量身定制的信息安全审核和交换机制。它基于VDA ISA（Verband der Automobileindustrie Information Security Assessment），允许汽车供应商和制造商证明其符合汽车合作伙伴的信息安全要求。TIAX评估由认可的审计提供商进行，并得到行业内参与原始设备制造商和供应商的认可。在本节中，我们将讨论TIAX评估对汽车供应商的好处。

TISAX审核涵盖了信息安全的关键领域，包括数据保护、安全开发和访问控制。该审核基于VDA ISA目录，该目录源自ISO/IEC 27001，适用于满足汽车行业的特定需求。TISAX审核结果通过一个安全的在线平台共享，使供应商能够通过一次审核向多个汽车合作伙伴证明其信息安全合规性。

TISAX审核对汽车供应商的益处：

- **简化的信息安全审核：**通过参与TISAX，汽车供应商可以避免接受来自不同合作伙伴的多次信息安全审核，从而减少与多次审核相关的管理负担和成本。
- **增强了信任和可信度：**TISAX审核表明供应商对信息安全的承诺，增加了汽车合作伙伴之间的信任和可信度。
- **竞争优势：**由于TISAX正成为许多汽车原始设备制造商和一级供应商的标准要求，通过TISAX审核可以为供应商赢得新业务提供竞争优势。
- **统一的安全要求：**TISAX确保整个汽车供应链的信息安全水平一致，使供应商能够符合行业最佳实践和要求。

4.6 ISO 42001：AI管理体系

ISO 42001是即将出台的人工智能（AI）管理体系国际标准。尽管该标准仍在开发中，但预计它将为组织管理和管理人工智能体系的部署、运营和维护提供一个全面的框架。该标准旨在解决人工智能的各个方面，包括道德考虑、透明度、问责制和数据隐私。虽然该标准的确切细节尚未最终确定，但ISO 42001可能对在运营中利用人工智能技术的汽车供应商有利。

ISO 42001认证对汽车供应商的潜在好处可能包括：

- **合乎道德和负责任的人工智能实施：**通过遵守ISO 42001，汽车供应商可以确保他们的人工智能系统以合乎道德和负责的方式开发和部署，同时考虑到人权、公平和非歧视。
- **增强透明度和问责制：**该标准有望为确保人工智能决策过程的透明度、建立问责制机制、促进利益相关者、客户和监管机构之间的信任提供指导。
- **改善数据隐私和安全：**ISO 42001可能会解决与人工智能系统相关的数据隐私和安全问题，帮助汽车供应商保护敏感数据并遵守数据保护法规。
- **简化人工智能治理：**通过实施基于ISO 42001的人工智能管理系统，汽车供应商可以简化其人工智能治理流程，促进人工智能技术在其整个生命周期中的有效管理和控制。

一旦发布，获得ISO 42001认证可以帮助汽车供应商展示他们对负责任的人工智能实践的承诺，并为更可持续和更有弹性的供应链做出贡献。通过解决道德问题、提高透明度以及确保数据隐私和安全，汽车供应商可以在其人工智能解决方案中建立信任和可信度，从而促进更安全、更可靠的汽车生态系统。

5. 汽车供应链中的数据泄露

近年来，针对汽车供应链发生了几起数据泄露和网络攻击事件。这些事件凸显了信息安全日益重要，以及行业内采取强有力的网络安全措施的必要性。一些值得注意的例子包括：

- 1. **日产北美数据泄露（2023年）：**

  2023年1月16日，星期一，日产披露，17998名客户受到此次泄露的影响。第三方收到了日产的客户数据，用于为该汽车制造商开发和测试软件解决方案，但由于数据库配置不当，这些数据被无意中暴露了出来。

  2021年，他们经历了类似的数据泄露，暴露了与公司移动应用程序和诊断工具相关的敏感源代码和知识产权。该漏洞归因于配置错误的Git服务器设置，使得数据可以在没有任何身份验证的情况下访问。

- 2. **本田勒索软件攻击（2020年）：**

  本田汽车公司成为勒索软件攻击的受害者，该攻击影响了其全球运营，包括生产设施和客户服务中心。此次攻击被归咎于“Snake”（也称为“Ekans”）勒索软件组织，该组织针对本田的内部系统并加密关键数据。

- 3. **Norsk Hydro勒索软件攻击（2019年）：**

  全球铝生产商和汽车行业供应商Norsk Hydro遭遇勒索软件攻击，扰乱了其在多大洲的运营。这次攻击被归咎于“LockerGoga”勒索软件组织，该组织对文件进行加密，并要求支付赎金。该漏洞最终将影响40个国家的35000名Norsk Hydro员工，并将文件锁定在数千台服务器和电脑上。财务影响最终将接近7100万美元。

- 4. **梅赛德斯-奔驰数据泄露（2021年）：**

  梅赛德斯-奔驰美国公司遭遇数据泄露，暴露了约160万客户和潜在买家的个人信息。暴露的数据包括姓名、地址、电子邮件地址、电话号码和车辆信息。只有不到1000人拥有非常敏感的个人信息，如驾照号码、社会保障号码、信用卡信息和出生日期。该漏洞是由第三方供应商软件中配置错误的安全设置引起的。

- 5. **大众和奥迪数据泄露（2021）：**

  包括大众和奥迪品牌在内的美国大众集团遭遇数据泄露，暴露了约330万客户和潜在买家的个人信息。该漏洞是由一家第三方供应商造成的，该供应商将一个包含客户数据的不安全服务器留在了互联网上。暴露的数据包括姓名、地址、电子邮件地址、电话号码，在某些情况下，还

包括车辆识别号（VIN）和驾驶执照号码等敏感个人信息。该事件突显了采取强有力的网络安全措施的必要性，并强调了确保第三方供应商遵守严格的安全协议以保护敏感客户数据的重要性。

这些事件突显了强有力的信息安全措施的重要性，以及汽车供应商和制造商投资网络安全的必要性。通过获得ISO 27001等认证并接受TIAX等评估，公司可以证明其对信息安全最佳实践的承诺，并降低成为网络攻击和数据泄露受害者的可能性。

6. 结论

汽车供应链面临许多风险，包括质量和合规、环境和可持续性、信息安全、业务连续性和灾难恢复、地缘政治和经济以及法律和监管风险。解决这些风险对于确保可持续和有弹性的供应链能够适应行业不断变化的需求至关重要。

第三方认证通过对公司的流程和体系进行的公正审核，在降低这些风险方面发挥着至关重要的作用。通过获得相关标准的认证，并接受TISAX等评估，汽车供应商可以证明他们对最佳实践和行业特定要求的承诺。在软件是一项服务的情况下，强有力的IT服务管理将改善供应商的整体网络安全状况，增强信息安全、隐私保护和业务连续性。

总之，第三方认证是汽车供应商管理风险、确保合规性和培养与合作伙伴信任的宝贵工具，最终有助于建立更可持续、更有弹性的汽车供应链。

全国免费热线

+86 21 5339 7720

sc.china@intertek.com

intertek.com.cn/ba

Intertek管理体系服务公众号

intertek
Total Quality. Assured.