...making excellence a habit.™

面向航空航天业的 ISO/IEC 27001 信息安全管理体系 (ISMS)

航空航天业正经历着强势增长和快速数字化转型。飞行安全保障始终是重中之重，整个行业以往有着良好的安全记录和信誉。不过，数字化以及新兴技术的采用增加了信息和网络安全威胁的风险。

大量的数据（飞行员和乘客的个人信息，或者与维修、航班信息以及天气系统相关的数据）在不断增长。与这种趋势相伴而生的是用户以远程方式或者通过多个系统访问数据的需求，对数据和连接性的依赖进一步增强，这导致攻击风险不断加剧。而这正是 ISO/IEC 27001 能够发挥作用的“用武之地”。

ISO/IEC 27001 简介

国际公认的 ISO/IEC 27001 是一个帮助组织管理和保护其信息资产从而使其始终保持安全的框架。它能够帮助您持续审查和细化您的信息安全保护方式 — 不仅为了现在而且还要面向未来。

安全可靠地管理信息的能力从未如此重要。ISO/IEC 27001 不仅有助于保护您的业务，而且还向客户、供应商以及市场传递了您的组织有能力以安全的方式处理信息的明确信号。

ISO/IEC 27001 是一个强大的框架，可帮助您确保信息（例如，财务数据、知识产权或者敏感的客户信息）的机密性、完整性和可用性。它能帮助您识别风险并采取适当的安全措施来有效加以应对。因此，ISO/IEC 27001 不仅能够保护您的业务，而且能够保护您的信誉。

隐私聚焦

如果您的组织要处理大量数据，ISO/IEC 27701 隐私信息管理体系 (PIMS) 提供隐私保护指引，能够帮助您满足日益增多的法规（例如，GDPR和CCPA）的要求。

连续性聚焦

如果应对网络攻击、数据泄露或者技术故障是您或您的供应商关注的重点，ISO 22301 提供一个通用框架，可帮助您进行规划和准备，从而对最坏的情况做到防患于未然。

网络安全聚焦

如果网络安全风险是您的组织的关注焦点，您可以借助 BSI 的补充服务（包括渗透测试和 NIST）来基于 ISO/IEC 27001 框架增强网络安全。

ISO/IEC 27001 如何与 AS EN 9100 系列形成优势互补

得益于 ISO 高阶结构，ISO/IEC 27001 能够与新的 AS EN 9100 系列保持一致，这意味着如果您已有 AS EN 9100 系列认证，即可开始将信息安全整合到您的航空航天质量管理体系。拥有互补性的管理体系使组织能够对类似航空航天这样高度竞争且极富创新的行业所带来的风险和机遇进行预测、适应和响应。这为各种规模的组织提供了所需要的韧性和敏捷性以便在全球市场保持繁荣发展。

IAQG（国际航空航天质量协调组织）参考了 AS EN 9100 系列标准中的许多信息安全和网络安全要求。条款 7.5.3.1 规定如下：

“应当对质量管理体系和国际标准所要求的文档化信息进行控制以确保：

- 其在需要时随时可用并且适用
- 其得到充分保护（例如，防止发生泄密、不当使用或者完整性缺失）” [1]

在整个标准中还有更进一步的参考，包括关于“运营规划与控制”的条款 8.1，参考了个人安全（可能包括勒索和身份窃取）、产品安全（可适用于软件和固件的采购与开发）、异物预防和检测（例如，恶意软件）以及建立控制（可适用于软件和固件）。不符合项可能是一个内部漏洞。

关于信息和网络安全的行业建议关于信息和网络安全的行业建议

除了 IAQG AS EN 9100 系列标准，欧洲航空网络安全中心 (ECCSA) 就航空网络安全提出了一些相关建议，包括：

> “航空业中的组织应当获得其企业中最高管理层的支持，并建立一个治理完整性框架以解决产品网络安全问题。” [3.2.a 节]

> “航空业中的组织应当定义产品网络安全策略并任命一位专门的产品网络安全负责人，负责在组织中实施和维护有效的产品网络安全计划。” [3.2.2 节][2]

此外，AIA（航空航天工业协会）民航网络安全行业评估与建议报告指出：

> “所有利益相关方需要通力协作，努力建立一个通用网络安全信任框架，其中包含治理结构以及量化网络安全最低预期的技术标准、互信的方法以及对互操作风险接受度的共识。利益相关方须前瞻性地识别、理解航空体系面临的风险并确定其优先级以减轻风险。” [3]

除了 AS EN 9100 系列，其他需要证明遵循了信息安全和网络安全要求的航空航天业标准还包括 AS EN 9115。此标准旨在处理信息保障、信息安全、网络安全与飞机数据网络 (Aircraft Data Network)、航空业数字信息安全标准 (Aviation Industry Standards for Digital Information Security)、商用飞机信息安全运营概念 (Commercial Aircraft Information Security Concepts of Operation) 以及流程框架和数据链安全之间的关系。

ISO/IEC 27001 如何使组织获益

ISO/IEC 27001 将帮助行业中各种规模的组织管理一系列信息和网络安全风险。具体而言：

- 旅行社处理大量旅客数据，因此，面临着网络攻击威胁。
- 机场面临的风险包括旅客个人数据和活动信息泄露以及安全监控系统、海关和护照管制、边境服务、国土安全以及空中交通管制受到影响。ISO/IEC 27001 提供最佳实践结构以帮助组织了解此类数据流并确保对其进行适当管理。
- 航空公司运营者还面临着大数据在线播放、通信和 WiFi 所导致的旅客数据攻击威胁。ISO/IEC 27001 要求对这些风险进行评估、确定优先级并有效加以应对。
- 制造商和 MRO（维护、修理和大修）需要考虑其内部系统、研发设施以及外购硬件、固件和软件的安全，与预测性维护和智能服务相关的 5G 革命以及测试设备。借助 ISO/IEC 27001 中的 114 种不同安全控制，您的组织将拥有一整套有助于将风险降至可接受的水平的工具。

无论您提供何种产品和服务，确保满足保持客户数据安全的合同、监管或政府义务同样至关重要。这种重要性在军事和国防领域尤为突出，在这些领域有特定的法规，包括由美国国防部 (DoD) 管理的网络安全成熟度模型认证 (CMMC)、英国国防部 (MoD) 规定的要求以及其他国家/地区的同等要求。

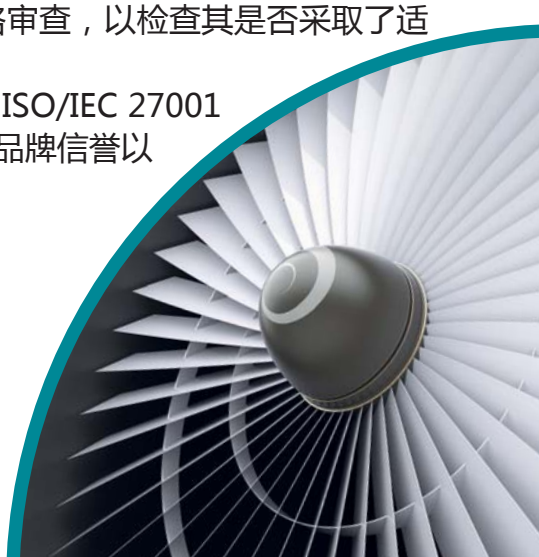
航空航天业存在的漏洞

近年来，有许多引人注目的航空航天业中的组织违规泄露数据的案例，这反过来对信誉和客户认知产生了负面影响。

2016 年，美国国土安全部 (US Department of Homeland Security) 披露曾成功侵入一架在跑道停留的波音 757 飞机。[4] 在过去十个月里，美国国家漏洞数据库 (US National Vulnerability Database) 公布了近 8,000 个经验证的不同软件漏洞。[5]

航空航天业因采用新技术应用而引发潜在数据漏洞的其他示例包括电子飞行包 (EFB)、机上娱乐 (IFE) 以及乘务人员无线服务。

在评论 2018 年行业中一起引发高度关注的旅客数据泄露事件时，英国信息专员办公室 (Information Commissioner’ s Offce) 的发言人指出：“... 法律很明确 — 当你受托处理个人数据时，你必须保护好它。没有做到这一点的组织将面临我们办公室的严格审查，以检查其是否采取了适当措施来保护基本隐私权。”[6]
因此，显而易见的是违规的代价很高，风险将只会继续加剧。借助 ISO/IEC 27001 前瞻性地管理您的信息安全将帮助您更好地保护您的客户、员工、品牌信誉以及业务绩效。



1. AS EN 9100 系列标准
2. 欧洲航空网络安全中心 (ECCSA) 建议
3. AIA（航空航天工业协会）民航网络安全行业评估与建议报告（2019 年 8 月）
4. Tripwire（2017 年 11 月）。一架停在跑道中的波音 757 被远程入侵
5. Info Security Magazine（2018 年 2 月）。2017 年有 7900 个漏洞未被列入 CVE 数据库
6. BBC News（2019 年 7 月）。英国航空公司 (British Airways) 因数据泄露面临创纪录的 1.83 亿英镑罚款

ISO/IEC 27001 为组织带来的其他益处包括：

- 提高信誉和利益相关方的信心
- 让相关各方更好地了解风险
- 在市场中增强信任和信誉，从而帮助您赢得更多业务
- 降低遭受罚款或诉讼的可能性
- 协助遵守相关法规
- 增强所有相关方的信息安全意识
- 降低发生员工相关信息安全事件的可能性
- 证明所有业务层级致力于信息安全
- 提高组织生存力
- 通过最大限度减少事件，降低成本

简化跨境贸易：

由于航空航天供应链中的许多组织在全球范围内进行经营或者贸易，依据 ISO/IEC 27001 开展工作将简化跨境贸易 — 无论是地理、政治、经济、商业或者社会因素如何。简化和标准化能够为您提供市场竞争优势。

需采取的举措？

要开启您的 ISO/IEC 27001 认证之旅，请遵循下列步骤：

- 从 BSI 购买标准副本并认真阅读
- 确保您已获得领导团队的认可
- 向 BSI 预订培训课程以了解标准的要求（BSI 提供一切 — 从 ISO/IEC 27001:2013 的要求到信息安全管理体系审核员/主任审核员培训）
- 识别需弥补的组织差距以满足新要求
- 制定实施计划
- 与您所在地的 BSI 分支机构联络以获得进一步的帮助和支持

航空航天业中的 BSI

By Royal Charter

航空航天工业对每个阶段的质量都有要求 — 并且以严格的安全性和可靠性要求为基础。从评估、认证和培训到软件解决方案、咨询服务和供应链智能，BSI 提供全面的解决方案以促进业务改进，帮助航空航天客户提高绩效、管理风险、实现可持续增长。

如今，BSI 在为智慧城市、物联网、无人机以及数字制造等领域探索最佳实践方面居领先地位 — 使航空航天业中的组织在面对未来挑战时能够更好地有备而战。

要了解有关 ISO/IEC 27001 的更多信息，请访问 https://www.bsigroup.com/zh-CN/

BSI/UK/1683/SC/1219/EN/GRP