



# ISO/IEC 27001再认证 和新版ISO/IEC 27701认证

门兴格拉德巴赫足球俱乐部最大化提高信息安全和数据保护水平

门兴格拉德巴赫足球俱乐部（以下简称“门兴格拉德巴赫”）已经顺利完成ISO/IEC 27001的再认证以及新版ISO/IEC 27701的认证。两项均由TÜV莱茵进行审核。ISO/IEC 27001为信息安全管理（ISMS）建立起严格标准，而ISO/IEC 27701在此基础上纳入了隐私信息管理体系（PIMS），该体系定义了与个人数据相关的角色、过程和指导方针。

## 基本事实

客户	门兴格拉德巴赫普鲁士1900体育俱乐部有限公司
项目地点	德国-门兴格拉德巴赫
服务	根据适用于信息安全管理（ISMS）的ISO/IEC 27001进行再认证，根据适用于隐私信息管理体系（PIMS）ISO/IEC 27701进行认证
基本法规和标准	ISO/IEC 27001、ISO/IEC 27701、ISO 9001

## 出发点：增加信任、扩大过程

门兴格拉德巴赫决定进行认证，并非迫于监管压力，而是期望为合作伙伴、球迷和员工提供最大限度的安全保障，并让这一承诺清晰可见。

严格来说，转变始于约20年前，当时任命了一位数据保护专员。从2012年起，这家俱乐部就根据ISO/IEC 27001运行ISMS，而在2022年，又增加了符合ISO 9001标准的质量管理体系（QMS）。

之所以选择TÜV莱茵，原因有三：

- TÜV莱茵具备充足的专业能力
- TÜV莱茵保持着强大的国际品牌影响力
- 在此之前，双方在其他领域已有合作

目标是创建以明智的方式结合产品和服务质量、安全和数据保护的整合管理体系，同时使治理可衡量、可审核。



“门兴格拉德巴赫决定进行认证，并非受到外部压力或监管要求驱动，而是致力于为客户和合作伙伴确保最高水平的信任和安全。通过该认证，我们希望证明个人数据始终得到可靠保护。”

Frank Fleissgarten

首席信息官/首席安全官，门兴格拉德巴赫普鲁士1900体育俱乐部有限责任公司

### 认证过程：清晰的路线图和实践的现实

ISO/IEC 27001的再认证进展顺利，这多亏了初始认证过程中准备充分，以及根据该标准对体系进行持续维护。

基于ISO/IEC 27701的隐私管理体系实施起来大概花费了12个月时间，是基于现有ISO/IEC 27001体系（ISMS）的有意扩展。

经过精心准备，包括记录当前状态和分析潜在优化措施，在此之后便是两阶段认证审核（阶段1/阶段2）。首先评估体系和文件，然后检验其在实际运行中的有效性。

审核员审查以下方面：风险管理、过程文档、培训内容和反馈管理。为获得ISO/IEC 27001认证，必须提供证据，证明已建立基于风险的信息安全管理（ISMS），并依据ISO/IEC 27002:2022部署了相应的安全控制措施。

对于ISO/IEC 27701而言，增加了隐私管理体系（PIMS）的特定要求，例如数据控制者和处理者角色，以及数据保护流程。

门兴格拉德巴赫的成功因素：

- 把现有过程整合到整合管理体系（IMS）中
- 全面的文档记录
- 集中培训
- 透明的变更管理
- 可以及早发现潜在问题的既定风险管理

ISO/IEC 27001、ISO/IEC 27701和ISO 9001这三个标准的最终审核在短短一周内顺利完成，这强烈表明所有结构和过程都完美契合。

每年将进行监督审核，三年后进行再认证。门兴格拉德巴赫不仅旨在确保当前体系稳定，还使持续改进成为常规操作。

### 结果：最大限度增强信心、降低风险

认证之路和认证本身使门兴格拉德巴赫获益良多：

- **提高效率：**作为修改过程的一部分，结构和过程均已得到优化。
- **增强意识：**关注所有领域的质量、信息安全和数据保护，这意味着可以识别风险并尽早应对。
- **信誉卓著：**官方证书在手，其他公司的审核时间显著缩短。
- **声誉良好：**证明符合国际公认的标准，可以提升公司在合作伙伴、供应商、球迷和公众中的声誉。
- **降低保险费用：**经认证的安全和数据保护措施使得网络保险费用降低。

因此，结合认证在内部和外部都有影响。

顺便说一句，此时下一步已经计划好了：适用于能源管理的ISO 50001认证已于2025年6月顺利完成，依然由TÜV莱茵进行。



## 结论

门兴格拉德巴赫拥有ISO 9001认证、ISO/IEC 27001再认证以及新版ISO/IEC 27701认证，它展示了如今领先企业的管理体系应该是什么样子：优化设计的体系整合了质量、安全和数据保护，从而降低风险、加快流程——包括合作伙伴和审核员的审查流程。

完成最近优化后，该俱乐部不但获得最新证书，而且持续监控各个过程。内部评估和定期培训课程可确保各项措施长期有效，而关键绩效指标（KPI）以可衡量的方式使质量、安全和数据保护保持高水平。

保险费用降低，且临时确认完全符合安全标准，这都说明强有力的治理不仅本身就是目的，还带来成本和效率效益。

对于合作伙伴、供应商、球迷和公众而言，这意味着俱乐部的信誉不是模糊的承诺，而是经独立第三方验证和确认。

其他组织要想走类似的道路，应该从门兴格拉德巴赫获得灵感。它们应该识别并发挥现有优势、系统性地缩小差距、明确责任、建立可审核性，从而增加信任、提高效率。TÜV莱茵随时准备提供支持！

“我把这些认证视为对我们不断努力的肯定，我们一直维护质量、信息安全和数据保护方面的国际标准。这些认证表明：我们可靠地保护敏感数据、不断改进我们的体系，从而为未来做好充分准备。”

Frank Fleissgarten

首席信息官/首席安全官，门兴格拉德巴赫普鲁士1900体育俱乐部有限责任公司

德国莱茵 TÜV 大中华区  
TÜV Rheinland Greater China  
服务热线 Hotline  
4008831300  
+852 21921022 (中国香港 Hong Kong)  
service-gc@tuv.com  
<https://certification.tuv.com>

关注我们的微信：  
TUV 莱茵



 **TÜVRheinland®**  
Precisely Right.