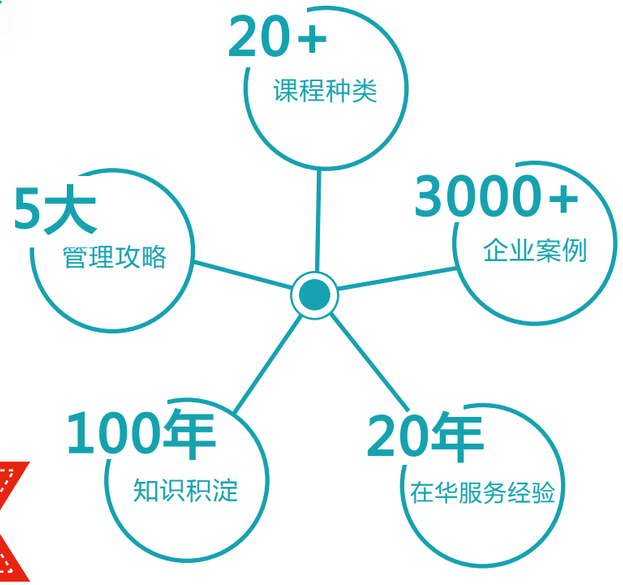
BSI商学院

VUCA环境下组织迈向卓越的最佳合作伙伴。

为您提供组织变革、风险管理、卓越运营及管理（个人）能力发展的精准解决方案。

BSI Business School



2017新课亮相

- 质量领导力
- 沙盘版质量管理
- 打造高绩效团队工作坊
- 从培训到绩效提升六步法
- 基于组织情境的敏控项目管理

更多敬请期待

联系我们，为您的组织和个人定制专属培训与发展方案

BSI全国热线 400 005 0046 | infochina@bsigroup.com | www.bsigroup.com

STANDARDS

BSI中文版期刊:总第20期

标准+

www.bsigroup.com

创新求变
永续发展

创新求变 永续发展

环顾当今世界，变化的体现在各行各业不断涌现，势不可挡，传统业态的市场不断被新生业态所蚕食和替代，网上虚拟商店对实体店的影响大家这几年已经有目共睹，Uber、滴滴、Airbnb、OFO 这些企业的兴起让“共享经济”一词在这两年异常火热，它们的快速崛起不但改变了原本行业的旧格局，给其带来了革命性的突破，也让人们看到了“共享经济”在未来的巨大潜力。**互联网影响传统行业的特点是打破了信息不对称的旧有格局，使上下游透明化，降低了沟通成本，提高了市场运作效率，使资源利用最大化，在其影响下，诸如零售业、批发业、制造业、通信业、物流业、酒店业与旅游行业、餐饮业、金融业、保险业、医疗业等传统行业会在未来持续升温变革。**

然而，互联网企业本身也正在面临来自自身的压力，关联企业和内部信息如何保证安全？对客户个人私隐如何保障？另外，AI 的不断发展使得大数据的运用更趋成熟，解决方案落地更快，**互联网企业所面临的迭代压力可以说比传统行业有过之而无不及。**

除了业务的发展和服务及产品的创新，热播剧《人民的名义》火爆收视也折射了社会对廉政制度的渴望和诉求，**企业和政府想必会加大廉政举措，进一步改善透明度以适应这一形势。**

面对如此种种，企业和部门如何应对？本期我们《标准 +》杂志的作者们对影响企业生存的三个维度，即运营韧性，信息韧性和供应链韧性方面持续分享我们了解到的有关行业和标准变化的信息，为读者提供参考。

林劲
英国标准协会中国区董事总经理

BSI全国热线:400 005 046
BSI官方网站:www.bsigroup.com

Contents 目录

bsi 中文版期刊
总第 20 期 2017

19 | Sector Focused
行业聚焦

云计算安全发展态势及选择云服务的几点建议

信息安全依然是企业和消费者在选择云服务时的首要考量要素。笔者在分析2017年云安全领域发展趋势的基础上，为企业选择云服务提出几点建议。

行业聚焦

17-22

2017年6月　总第20期
总 策 划：林劲
执行策划：韩莹
总 编 辑：李宁宁

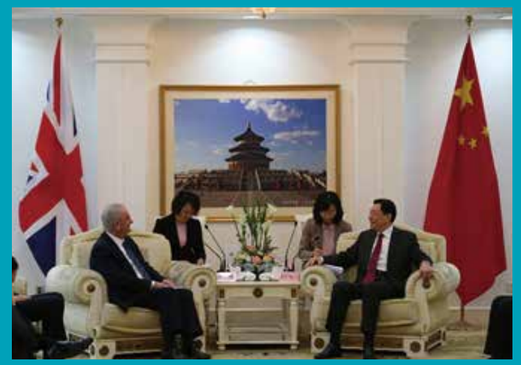
您对本刊有任何意见或建议
欢迎通过以下方式联络我们：
Email:infochina@bsigroup.com
BSI全国热线：400 005 0046
官　　网：www.bsigroup.com

新闻动态
NEWS

01 / BSI集团董事再次访华

2017年4月5日至8日，BSI集团总裁Mr.Howard Kerr率领英国总部核心管理层成员一行人到访中国。这是继2016年10月之后，BSI集团总部再一次盛大访华。此行，Howard先生一行人先后拜访了国家质量监督检验检疫总局（AQSIQ）与中国合格评定国家认可委员会（CNAS），双方望继续进一步在互联网与信息技术、高科技制造、医疗器械、智慧城市建设等方面开展标准化深度合作。

同时，BSI集团领导共同探讨分析了当下中国经济现状、未来中国经济的发展趋势及经济结构化调整等战略性话题，为总部在亚太区的整体战略布局及在中国区下一步的投资计划做深入调研，也再次确认了中国市场在亚太区的中心位置，表示将继续保持对中国区的各方资源支持。



02 / BSI携手UNNC签订合作备忘录

2017年3月3日，BSI与宁波诺丁汉大学(UNNC)签订合作备忘录，双方将在BIM高级管理人才的培养，BIM标准的推进与应用等方面发展深度合作。

凭借在BIM国际先进标准及全球项目实战方面的背景，结合中国本地市场，双方将为中国建筑行业带来全生命周期的BIM管理经验与最佳实践，为中国建筑行业数字化转型提供助力，也为一带一路背景下中国企业走出去提供与国际接轨的平台。除针对BIM管理层所推出的“BIM管理培训”外，双方联合开发的培训内容在明年还将持续升级，“BIM经理人进阶课程”计划于2018年面向国内市场。

03 / BSI即将设立第二家欧盟公告机构

BSI是全球医疗器械法规监管领域的领先服务提供商，根据发展计划，BSI已向荷兰主管当局申请欧盟有源植入医疗器械指令（AIMD 90/385/EEC）和医疗器械指令（MDD 93/42/EEC）的授权。该计划旨在未来两年内扩大并发展欧洲大陆的欧盟公告机构的业务，以及为中国本地企业开拓欧盟市场提供更好的服务。

一旦未来欧盟医疗器械法规（MDR）和体外诊断医疗器械法规（IVDR）付诸实施，BSI 的目标是在荷兰和英国都获得相关授权。

转版进行时，
BSI IATF 16949 系列活动 势如破竹 全国热开

2016年10月，国际汽车工作组（IATF）正式发布 IATF 16949:2016，取代ISO/TS 16949:2009作为规范汽车行业质量管理的标准。值此转版之际，BSI凭借在标准领域的深厚专业实力和卓越的定制化服务，陆续与各地龙头整车厂企业联合举办了多场培训研讨会，BSI全国巡回IATF 16949转版研讨会、IATF 16949新标系列课程，介绍新版标准重要变化点及转换审核注意要点、解析第三代国际管理标准趋势、共同研讨企业最关心的实际问题并分享行业最佳实践，其快速、高效、准确落地，收获了客户一致好评。下面让我们一起回顾精彩瞬间：

BSI携手各地整车厂企业，开展IATF 16949巡回研讨会

- 上汽集团、工业4.0协会@上海
- 广州汽车集团乘用车有限公司@广州
- 潍柴集团@潍柴大学
- 江淮汽车集团@安徽合肥
- 一汽大众@佛山
- 东风汽车有限公司@各地

BSI全国巡回IATF 16949转版研讨会，权威专业的讲解与答疑，第一时间助力企业获取转版热点信息。

BSI IATF 16949:2016系列培训盛宴
全国各大城市火爆开课中

作为业内标准引领者，BSI以其专业与实力，用速度与激情打响了新标转版课程第一枪，重磅推出了IATF 16949新标系列培训，助力不同客户层级的需求。其差异化实践者课程，更是成为业内经典，成为口碑与品牌的象征。

ISO 45001 的最后一里路

BSI 中国区首席专家 | 高毅民

ISO 45001 最新发展动态

前言

自英国标准协会（BSI）在 1999 年订定与发布全球第一个职业健康安全管理体系认证标准 OHSAS 18001 以来，至今借此标准认证的企业数估计已超过 30 万家，而 ISO 组织 (International Organization for Standardization) 对于将此标准提升为 ISO 管理体系标准的讨论与呼声也越来越高。BSI 自 2002 年起，一直努力推动将此标准提升为 ISO 国际标准，终于在 2012 年第三次将此标准提案到 ISO 会员国讨论时获得通过，而 ISO 迅速在来年成立 PC 283 项目委员会，由 BSI 担任委员会主席，开始进行 ISO 45001 职业健康安全管理体系的制订。

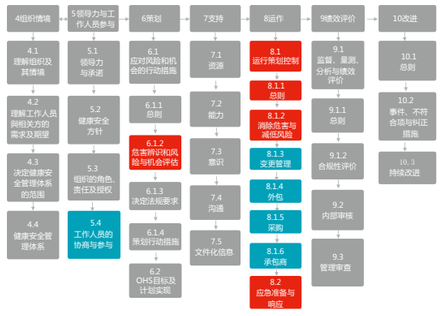
继 ISO 45001 DIS1 (Draft International Standard) 第一版的国际标准草案版在 2016 年 5 月以些微差距未通过会员国的投票，由 BSI 领导的 PC 283 委员会在过去将近一年的时间，针对来自会员国与全球各地超过 3,000 个意见，整理、归纳与讨论，终于在最近完成第二版的国际标准草案版 DIS2，并发给各会员国进行。从今年 5 月 19 日开始投票，预计在 7 月 13 日完成投票。BSI 针对此次 DIS2 相较于 DIS1 的主要改变，整理与分析如下，供关心此次 ISO 标准制订的各界参考。

DIS2 的主要改变

此次 ISO 45001 的主要改变可以分为两个方面，一个是技术内容的方面，另一个就是在条款结构上的变化，说明如下：

1. 技术内容的方面，可分为两个部分：

a）名词与定义：主要将之前 DIS1 中有争议的的三个名词包含「worker(工作人员)」、「participation(参与)」、「hazard(危害)」做进一步的修正。例如在 DIS1 中对工作人员的定义包含「组织具有某些程度控制的人员」，已在 DIS2 中删除，以避免可能的模糊空间。



图一 ISO 45001 DIS2 条款结构

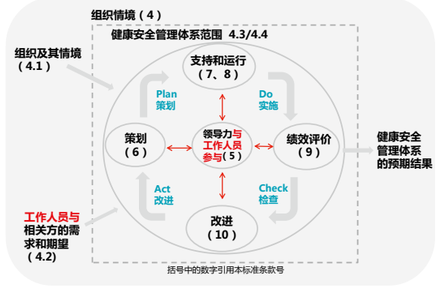
> 新版职业健康安全管理体系认证标准 ISO 45001 完成第二版的国际标准草案 DIS2，从 2017 年 5 月 19 日开始进行投票，预计于 7 月 13 日完成投票。

b）标准内容：这部分的改变并不大，主要对条款中的技术用词进行微调，并增加了一些 note(注解)。例如在备受关注的条款 5.4「工作人员的协商与参与」中新增了工作人员代表、非管理职工作人员的协商与参与，以及无偿培训三个注解，以增加各方引用标准的一致性。

2. 条款结构的层面，也可分为两个部分：

a）与其他管理体系标准的一致性：部分会员国对于 DIS1 与其他管理体系在条款结构上的一致性认为有改进的必要，以便更为符合 ISO/IEC Directive, Part 1 中的 Appendix 2 内容。例如将 DIS1 中条款 5.3 中的「accountability」，以及 7.4 中的「information」删除，请参见图一。

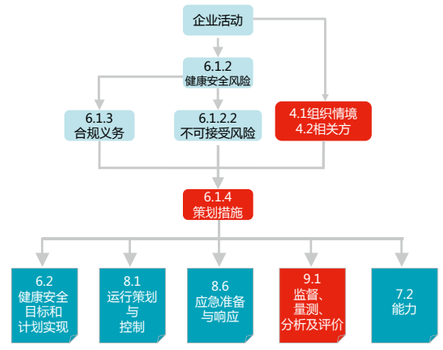
b）与 ISO 14001:2015 新版的一致性：这方面可以说是这次 DIS2 最大的改变。ISO 14001 新版从 2015 年 9 月公布以来已广被接受，且已有大量的企业完成或正在进行改版，因此，要求 ISO 45001 与 ISO 14001 条款结构的高度一致性已是共识。在附图一中可以得知，与 DIS1 相较，DIS2 最大的变化在于条款 8「运行的策划与控制」，原本在 DIS1 中的条款 8.2「变更管理」到 8.5「承揽商」，在 DIS2 中改为条款 8.1.3 到 8.1.6，而原本的 8.6「应急准备与响应」则改回与 ISO 14001:2015 相同的条款编号 8.2。又例如在条款 10 中，在 DIS2 中新增条款 10.1「总则」，并将原本条款中 10.2「持续改进」中的两个次条款 10.2.1 与 10.2 合并并改为条款 10.3。这些的改变主要的目的便是在于使未来的 ISO 45001 更易于与 ISO 14001 整合，毕竟企业往往将 EHS 整合为一个权责部门。



图二 ISO 45001 DIS2 体系模型

体系模型、结构与 ISO 14001:2015 的一致性

DIS2 尽管有了上述的改变，但其体系的模型并未有任何改变，请参见图二。这个管理体系的模型与 ISO 14001:2015 是完全相同的，所以企业在整合 EHS 管理体系时就方便许多。另外更重要的一点是，未来 ISO 45001 与 ISO 14001 体系技术性结构的一致性，请参见图三。从图三中可以了解，ISO 45001 和 ISO 14001:2015 的体系结构是完全相同的，其目的就在于便于企业将此两个体系完全整合，图三中的红色部分表示与 OHSAS 18001 相异的部分结构。



图三 ISO 45001 DIS2 体系的技術结构

结语

综观此次 DIS2 的改版过程与结果，一般认为通过此次 ISO 投票的机会很大，预期投票结果将在今年的 7 月底前公布。众所瞩目的议题是，ISO 45001 正式版本将于何时公布？依据目前 PC 283 所公布的时程，如果将来 ISO 45001 需要进入 FDIS 的阶段，则预计在 2018 年 2 月公布，如果不需进入 FDIS 阶段，则可能于今年 11 月正式公布。OHSAS 18001 自 1999 年公布以来，期望的重要目标之一便是催生 ISO 职业健康安全管理体系的制订，时经 18 年，如今即将诞生，ISO 45001 已在最后一里的路上！■

企业的“社会名片”

BSI 高级讲师 | 张成银

ISO 39001:2012
道路交通安全管理体系

道路交通安全是一个全球关注的问题。据估计，世界各地每天有 3500 人在道路上死亡，10 万人受伤，人身健康和社会经济受到了极大的损害。减少道路伤亡人数和死亡率将能减少痛苦，促进增长，并有助于腾出资源从事更有益的活动。

ISO 39001:2012

Road Traffic Safety Management Systems

道路交通安全管理体系

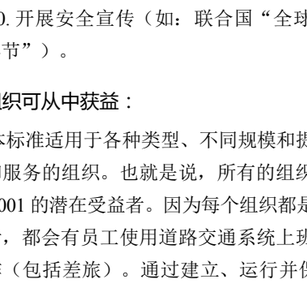
ISO 39001:2012 是第一个专门针对道路交通安全的管理体系标准，该标准以减少和消除道路交通事故造成的死亡和重伤为目标，确定了良好的道路交通安全管理实践，将助力组织实现其预期的道路交通安全结果。

本标准提供了一个工具，旨在帮助组织降低并最终消除与道路交通事故有关的死亡和重伤。

联合国大会在 2010 年 3 月宣布 2011-2020 年为**道路安全行动十年**，其总体目标是通过在国家、区域和全球各级开展更多活动，稳定并随后降低预计的全球道路交通死亡率，最终挽救约 5 百万生命。在这项十年行动计划中，鼓励各国在道路安全战略、能力和数据收集系统框架内考虑五个领域的活动。在可采取的有效活动中，明确提出实行国际标准化组织制定的 ISO 39001 标准。

我们可以做什么：

道路交通伤害是可以预防的。来自世界各地的经验表明，通过整体采用安全系统的道路交通安全管理方法能够大量减少死亡和重伤。ISO 39001 集合了众多道路交通安全专家的宝贵经验和科学系统方法，识别相关的绩效因素：



随着社会和经济的发展，新的道路交通安全绩效因素也将对最终的绩效结果产生重大影响，如机动车保有量持续增加、全球贸易导致交通量的增长、自动驾驶技术推广及共享经济的发展等。

有效的干预措施包括：

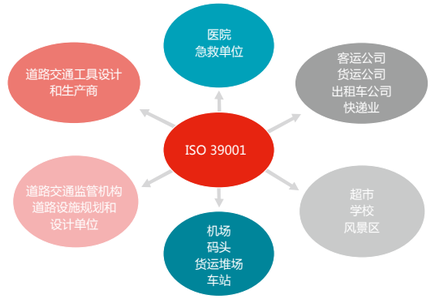
1. 在土地使用、城市规划和交通规划中考虑道路安全因素；
2. 设计更安全的道路，并要求对新建项目进行独立的道路安全审计；
3. 进行安全出行策划，包括考虑出行的必要性，出行量和方式，路线、车辆和驾驶员的选择；
4. 改进车辆的安全性能；提倡公共交通；
5. 通过采用交通缓解措施有效管理车速；
6. 制定和执行在国际上一致的关于使用安全带、头盔和儿童约束装置的法律规定；
7. 制定和执行驾驶员血液酒精浓度限值规定；
8. 将不适宜的车辆和驾骑人员从道路网中清除；
9. 改善对道路交通碰撞事故受害者的救治；
10. 开展安全宣传（如：联合国“全球道路安全电影节”）。

哪些组织可从中获益：

本标准适用于各种类型、不同规模和提供不同产品和服务的组织。也就是说，所有的组织都将是 ISO 39001 的潜在受益者。因为每个组织都是道路的使用者，都会有员工使用道路交通系统上班、下班或工作（包括差旅）。通过建立、运行并保持 ISO 39001 管理体系，尤其让产生往来于受组织控制或影响地点的交通活动，比如超市、学校和有许多访问者的地方，或道路交通系统的服务提供商获益。不仅如此，标准还从更根本的层面关注道路交通安全影响因素，对相关组织提高安全绩效结果提供帮助，适用的组织如：道路设计和规划部门等。

> “ISO 39001:2012 是第一个专门针对道路交通安全的管理体系标准，该标准以减少和消除道路交通事故造成的死亡和重伤为目标，确定了良好的道路交通安全管理实践，将助力组织实现其预期的道路交通安全结果。”

2011-2020年
道路安全行动十年全球计划



道路交通安全事关每一个组织，每一个人，因为我们都是道路的使用者。

世界卫生组织发布的报告显示，全球道路交通死亡者有一半是行人（22%）、骑车者（5%） 和摩托车驾乘者（23%），即“弱势道路使用者”。同时，道路交通伤害是 10 至 19 岁青少年的首要死因，每年使大约 11.5 万名青少年死亡。通过学习和运行 ISO 39001 体系，组织的员工可以将道路交通安全意识和理念传递给身边人，进而影响整个社会。

潜在收益：

- 减少伤害
- 新的合作机会
- 获得持续发展的保障
- 费用减少
- 优化组织形象

企事业单位在其业务活动，以及雇员工作出行等业务辅助活动中，一旦发生交通事故，除了要付出沉重的生命和经济代价，也为业务可持续发展带来重大影响。

如今，道路交通安全问题越来越受到关注，人们已经普遍认识到：**没有人应该在道路交通事故中死亡！**有的组织不仅自身建立了 ISO 39001 管理体系，而且已经开始要求自己的供应商建立体系，或提交实施计划。积极推进并实施 ISO 39001 体系，不仅有利于组织提升道路交通安全管理能力和水平，规避技术性贸易壁垒，更让组织以同步的思维和理念与国际接轨，提高企业的综合竞争力。同时，推进并获得 ISO 39001 体系认证，证明其关注并致力于道路交通安全管理的良好愿望和形象，体现了一个组织对生命的尊重，展示了“以人为本”的人文关怀理念，是一个正向、积极的社会名片，为可持续发展获得新的机遇。■

健身 VS 战略

BSI 高级项目经理 | 葛军

看了这篇健身知识，你就知道什么是战略

一个人需要健身吗？都说健身是屌丝逆袭男神的唯一途径！一个企业需要战略吗？那么企业要逆袭靠的就是战略！如果不为未来打算，恐怕就要从糊里糊涂的现实中走向关门！如果你不好好保持你傲人的搓衣板跟肱二头肌，女神凭什么是你的！

健身和战略，两者有甚关系？习大大说，治大国如烹小鲜；企业也如人生，都是由生命体组成的大生命体，真是这样吗？我们来列个表：

人生	诞生	成长	上学	青春	成熟	生病	衰 老	死亡
企业	成立	发展	学习	巅峰	稳定	困难	下坡路	倒闭

还真是蛮一致的。

如果你决定要健身的话，首先需要考虑的就是，通过健身，你想成为一个什么样的人？或是改变一个怎么样的现状。是像施瓦辛格那样的肌肉男，还是像彭于晏那般身材匀称？是想拥有奥运冠军的运动表现，还是成为精力充沛的“年轻人”？让生活更精彩，是你健身的使命，“穿衣显瘦、脱衣有肉”屌丝逆袭成功然后肆意撩妹，那是你的愿景，是一幅你看了后，心满意足的“自拍照”。你的企业存在的意义是什么（企业的使命）？你的企业成功时，会给大家展现出什么样的景象（愿景）？这就是战略规划的第一步。

既然下定决心成为一个健康的人，下面你需要制定目标，短期的和长期的。有人说，我要每天走 1 万步，在朋友圈里名列前茅。走路是手段，1 万步是指标，并不是目标。不要想着 1 万步走完能有完美身材，那健身房就都倒闭了。所以要先定义，什么目标与健康人相关。体重达到合理的标准，A4 纸腰，马甲线，身体的各项体检参数处于正常的范围，这些都是有具体标准的，可以作为目标。当你决定进入健身房时，将有专业人士给你做体测，各项数据显示了你的现状，然后你要决定的是，如何达成你心目中的目标。目标既要有挑战性，又要合理。每个人都希望通过锻炼迅速获得好的身材，但盲目追求瘦，显然已经不是一个健康、科学的选择。骨感美目前已经不是潮流了。你看看近年来的维密天使们，哪个是弱不禁风的纸片人？要减脂增肌的朋友，就不要死盯着体重数据，而是要看“体脂含量”，男性达到 14-18%、女性达到 21%-24%，是比较健康、合理的水平。

> 管理是一种实践，其本质不在于知，而在于行；其验证不在于逻辑，而在于成果。

>> 战略知识小总结

- **看** 了解企业的使命 / 企业的愿景
- **信** 确定并制定目标
- **思考** 综合内外部条件
- **行动** 制定战略计划 / 实施计划 / 监控计划
- **分享** 绩效评估 / 反馈工作

有人说，我就是要减肚子！教练会告诉你，“臣妾做不到啊”。人是一个整体，牵一发而动全身啊！一个有着马甲线或者人鱼线的人，却有个松松垮垮的蝴蝶袖（松弛的大臂），好看吗？企业也一样，如果你的目标只是赚钱，赚更多是钱，跟只追求 GDP 有啥区别呢？所以目标要考虑从财务、客户、流程和员工成长等多方面考虑。

确定了健身目标，你就要看看外部条件和内部条件是怎样的。如果附近有公园和健身房，有个爱锻炼的伙伴，恭喜你，外部环境提供了你锻炼的机会；如果你住在水泥丛林里，周围除了公路，就是立交桥，这个环境不利于你锻炼，这就是威胁到你实现锻炼计划的因素。你自身的身体素质很好，没啥别的毛病，这是你的优势，如果你膝关节不太好，体重又特别大，有些运动不能做，这就是你的劣势。上述的优势和机会组合在一起，你可以与小伙伴选择在大自然中运动，或者到健身房肆意挥洒汗水。威胁和劣势组合在一起，若没有受虐倾向，你可千万别选择在高层建筑里爬楼梯这样的运动，空气差不说，膝关节也会不堪重负，也许会让你今后再也不能运动，再别折腾自己，好好活着。企业也是一样，要牢牢抓住机会和优势，更要处理好威胁和劣势（致命的短处）。通过对机会、威胁、优势、劣势进行分析（SWOT 分析），就可以找出我们成功的关键因素。这样更容易实现理想，飞上天与太阳肩并肩，不要灰心，女神就要是你的了！

找到了适合的健身方式后，你需要制定锻炼计划，确保达成你健身的目标。是一周两次还是五次？每周都锻炼什么？这也许需要专业的教练给您一些建议。更重要的是，这些计划的可实施性怎么样？您能确保锻炼计划能够被实施吗？会不会经常出差？如果遇到雨季，户外的锻炼计划怎么调整？制定战略时，同样要考虑潜在的问题和风险。如果贵公司处于高科技行业，高端人才举足轻重，那么您需要的人才招聘不到或者流失，该怎么办？把预计到的风险按照严重性和发生概率排序，看看采取什么措施予以规避、解决，或者干脆放手不管，都需要慎重考虑。

健身计划既然制定好了，就一定要付诸实施。若每天都去量体重，也许太频繁了些，但总需要有个持续的监控，看看锻炼的效果。开始也许是一个周，慢慢就变成了一个月，看看各种目标是否达成，达成和未达成的原因都要分析一下，然后再对后面的计划进行调整。如果突然生病了，甚至要重新调整目标。企业也是一样，要定期监控战略计划实施的情况，当内、外部有重大变化时，要及时调整目标和行动计划，这就是要做好绩效评价和反馈工作。

无论是健身，还是战略，都是在实践中不断得到进步的。“葛优躺”永远不会收获强健的体魄。马云曾说，新来的员工不要空谈战略，而是要“看、信、思考、行动、分享”。管理是一种实践，其本质不在于知，而在于行；其验证不在于逻辑，而在于成果。空谈误国，实干兴邦，历来如此！■

浅析个人信息安全与隐私保护

BSI 高级讲师 | 万鑫

随着《网络安全法》的正式实施，个人信息保护再次成为全社会热议的话题，那么在国家法律法规、行业规范的多重要求下，如何能更加系统、更加规范的保护公民个人信息呢？相关国际标准和实施指南给我们指明了方向。

个人信息安全和隐私保护刻不容缓

从 2009 年 2 月至 2015 年 10 月，全国法院共审结出售、非法提供公民个人信息、非法获取公民个人信息刑事案件 969 起，生效判决人数 1415 人。2015 年 11 月至 2016 年 12 月，全国法院新收侵犯公民个人信息刑事案件 495 件，审结 464 件，生效判决人数 697 人。以上数据均表明个人信息泄露问题严重，个人信息安全成为一个全社会高度关注的问题。

个人信息的定义与内容

保护公民个人和隐私信息的第一步是确定保护的对象。关于个人信息的界定，不同的法律法规略有差别，但普遍认可的个人信息是可以直接或间接识别自然人身份的信息。

可参见图 1 相关标准或法律对个人信息的定义。

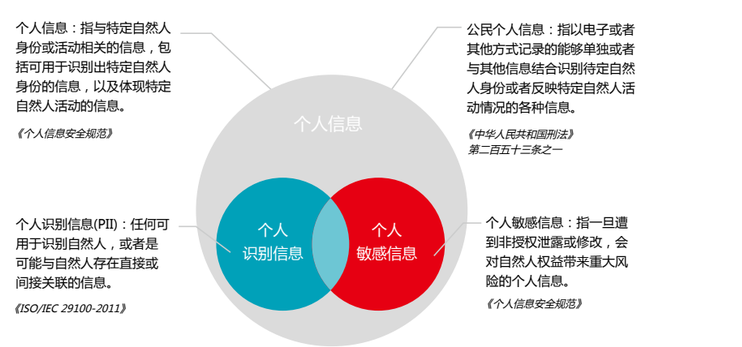


图 1. 个人信息的定义

《个人信息安全规范（征求意见稿）》对个人信息进行具体的列举，将个人信息主要分为三类（如图 2）。个人敏感信息包括个人身份和鉴权信息，以及个人服务和数据内容信息。

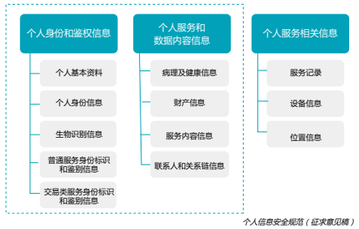


图 2. 个人信息的分类

法律法规对侵犯个人信息行为的处置

根据我国刑法规定，违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。窃取或者以其他方法非法获取公民个人信息的，依照前款的规定处罚。（参见图 3）

最高人民法院、最高人民检察院于 2017 年 5 月 9 日发布《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》。

此次司法解释明确了刑法相关规定中“情节严重”、“情节特别严重”的认定标准，并从个人信息条数、非法所得的金额等角度量化解释了量刑的标准。其中对于非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息五十条以上的；非法获取、出售或者提供住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息五百条以上的；非法获取、出售或者提供以上规定以外的公民个人信息五千条以上的均可以判定为“情节严重”。（参见图 4）

个人信息安全与隐私保护的方法和步骤

根据隐私保护的国际标准 ISO/IEC 29100:2011、个人信息保护的英国标准 BS 10012:2017、云环境下个人信息保护的国际标准 ISO/IEC 27018:2014 的要求，以及国家标准《个人信息安全规范》的建议，结合 BSI 多年来企业信息安全服务经验，我们推荐组织可按如下“**个人信息安全及隐私保护的五步法**”开展相关的风险评估和安全防护工作。

“个人信息安全及隐私保护的五步法”是依据管理学经典理论“PDCA”的思想，从策划 - 实施 - 检查 - 改进的 4 个步骤对个人信息进行循环往复的识别、分析、评价和改进的闭环过程。其风险管控方法论从确定边界与对象、分析影响与要求、识别现状与防护、评估风险与弱点、实施管控与改进等过程入手，(参见图 5)其步骤如下：

> “个人信息安全及隐私保护的五步法”是依据管理学经典理论“PDCA”的思想，从策划 - 实施 - 检查 - 改进的 4 个步骤对个人信息进行循环往复的识别、分析、评价和改进的闭环过程。

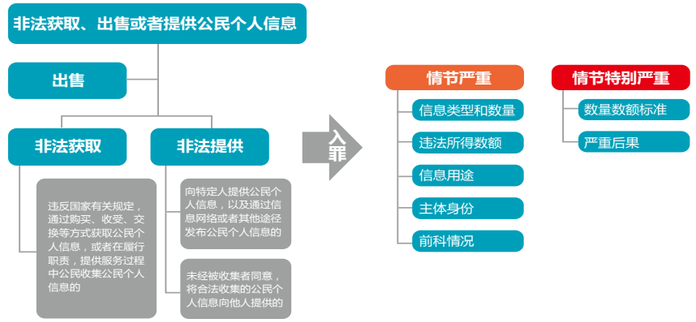


图 3 刑法对侵犯公民个人信息犯罪的定罪解释

（一）边界分析

本阶段主要针对个人信息控制者或处理者的业务处理过程进行全面的调研，识别需要保护的个人信息的种类、形式、依赖的资源（系统）、使用目的和处理方式，形成清晰的数据清单.数据流程图及数据映射图表。调研内容关注个人信息全生命周期的管理，包括信息收集、存储、传输、使用、归档和销毁，同时关注信息的披露和商业应用环节。调研过程中应考虑已下线系统、系统数据合并、企业收购、并购及全球化扩张等情况。

（二）影响分析

本阶段主要根据已完成的边界分析结果，梳理个人信息保护的相关要求。分析个人信息控制者及处理者的业务需求，并识别相关司法管辖权的政策标准、法律法规和行业合规要求，对于某些高监管行业，如金融、医疗、电信，需要特别关注区域的行业标准和规范，比如第三方支付的 PCI DSS、美国关于医疗保险的 HIPPA、国内的银监会监管要求等。影响分析内容还应包括违规及侵害个人信息主体权益造成的风险和损害，这种风险除了会遭受财务惩罚，对企业的品牌和声誉都会产生极大的影响。

（三）保护措施分析

本阶段全面梳理企业作为个人信息控制者或处理者已实施的安全防护措施，该防护措施分析应基于全面标准防护分析框架，从物理和环境安全、网络与传输系统、平台与应用系统、数据与信息资源、流程与操作规范等维度，针对个人信息的全生命周期评价防护措施的充分性、适宜性和有效性。

（四）风险评估

风险评估是个人信息保护最重要的阶段，本阶段主要根据影响分析和保护措施分析的结果，综合分析潜在的安全事件可能对个人信息主体及其他相关方造成的危害，这些安全事件可能是数据泄露、数据篡改、数据滥用、数据错误或丢失，并评估事件发生的可能性，确定风险级别，并给出相应的改进建议。

（五）持续改进

根据前四个阶段的分析和评估，进行有针对性地风险处置和措施改进，可以从软硬件技术、制度规范、物理防护等维度展开。风险处置不是一次性工作，应该在既定时间间隔或企业发生重大变革时进行，持续跟踪控制措施落实情况，并不断评估剩余风险。

结束语

纵观国际改革法案和国际国内标准，关于公民个人信息的使用，从来都是管理和使用并重而不是禁止和限制。在信息化和大数据时代，国家倡导的是“宽准入、严管控”的思路，组织应该在明确个人信息使用目的的前提下，构建“合理利用”的场景，基于动态的隐私风险模型，加强隐私影响评估并按行业标准进行安全管控，最终达到既能符合法律法规，又能充分合理利用信息创造价值。■

图 4. 刑法对侵犯公民个人信息犯罪的量刑解释

图 5. 个人信息保护的风险管理流程

DevOps 与 ITSM 到底是什么关系？

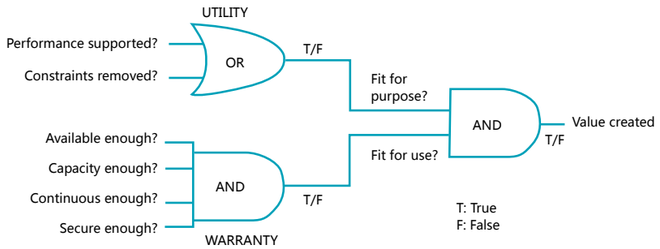
BSI ICT 高级讲师 | 汪明

DevOps 最近火起来了，各种经验总结、实施指南类的文章铺天盖地，但在各种观点中，我们既能看到共识，也能看到分歧，我们似乎可以理解当前的 DevOps 还是一套尚未总结归纳到广为接受和认可的程度的知识体系。

事实上，DevOps 的知识体系迄今为止并未包括任何独立的方法论创新，而是建立于一系列已运用多年的方法论和实践经验。并且，DevOps 也并未像某些人所说的那样站在了 ITIL 或是 ITSM 的对立面上，而更像是以 ITIL 为管理理论基础，为业务快速迭代的企业提供了具体的、有价值的 ITSM 实施思路，并且站在沟通与文化的视角，比 ITIL 更加清晰、具体地解释了 IT 开发与 IT 运维这两个角色之间应该如何打通壁垒，建立具有建设性的合作关系，从而达成真正的敏捷。

有关二者的关系，笔者抛砖引玉，认为至少可以在以下三个问题上进行探讨。

首先，DevOps 强调让每一个团队成员共同树立业务导向的思维模式，即如何使客户的利益最大化，以最有效率的方式提供客户需要的业务服务。其实这并未脱离 ITIL 的基本思想。ITIL 对服务管理的定义是“一套特定的组织能力，以服务的形式为客户提供价值”，而服务的定义是“为客户提供价值的一种手段，使客户不用承担特定的成本和风险就可以获得所期望的结果”。ITIL 认为价值体现为“功用（utility）”和“功效（warranty）”，所谓功用就是让客户得到符合自身目的的功能，所谓功效则是客户在服务的可用性、容量、连续性、安全方面的非功能性需求得到了满足，如下图所示。DevOps 提出建立聚焦于业务持续性的轻量级 ITSM，这一“聚焦”其实就是 ITIL 所说的“功效”类价值；而 ITIL 的“功用”价值与 DevOps 的业务导向也是如出一辙。



图片引自 ITIL® Service Strategy 2011 edition

> DevOps 没有从理论上颠覆或是优化升级 ITIL/ITSM，但还是从落地实践的角度对 ITIL 的敏捷化实施提供了更具体的解决方案。

其次，按照 DevOps 的理念，制造业的“单件流（one piece flow）”思想被引用并提倡，目的在于以最少的延误和等待实现产品流的不间断，但实际上这一提倡最大的价值并不在于减少软件开发团队的人力资源浪费，而是促进了将传统的大规模应用程序简化为模块化的小组件或小服务，在技术上，需要通过可以简化测试、快速部署的“微服务”以及灰度发布、蓝绿发布等这些发布方法来加以支撑。在 ITIL 的世界里，这些说白了就是一种“标准变更”。ITIL 并没有把所谓“规范化流程”认作死理，为了提升效率，减少不必要的资源浪费，企业在实施 ITIL 变更管理流程时，可以把一切低风险、可简化的变更场景定义为标准变更，而标准变更的效率体现在管理层的“预授权”。在我咨询过的传统企业里，最多曾经帮助其中的一家企业把大约 90% 的变更定义为标准变更，这样的做法可以按照 80/20 法则来理解，正是要让他们把更多的精力投放在更关键、风险更大的变更活动里，加强变更管控，保障业务的连续性。所以说，将传统企业体量巨大、关联关系复杂的应用系统朝着解耦的方向进行改造，使其微服务化，并使之适用于灰度发布、蓝绿发布这些减少变更失败风险的发布方法，正是帮助企业更有效地运用 ITIL 中的标准变更的一种方法，并且这些标准变更是十分易于实现自动化部署的。

再次，DevOps 提出了由运维团队向开发团队的“提前持续改善（KAIZEN in Advance）”，即运维与开发保持实时的、充分的沟通，运维团队将问题和需求及时反馈给开发团队。ISO/IEC 20000-1:2011 作为 IT 服务管理体系国际标准，对这个问题也有着相似的解决方案，即“设计和转换新服务或变更的服务”流程。该流程要求“作为策划的输入，服务提供方应考虑交付新服务或变更的服务对财务、组织和技术的潜在影响，以及对服务管理体系（SMS）的潜在影响”，这其中对于技术的潜在影响，正是需要运维团队提前介入需求分析与设计阶段，站在运维 / 运营的视角，充分提出必要的非功能需求，帮助分析新服务上线相关的风险；而该流程还要求提前规划好服务上线后的服务级别要求、运维交接与培训要求，以确保开发到运维的平稳过渡而不是让团队间陷入无休止的纠纷，这些都与 DevOps 的理念相一致。只不过在持续集成的环境之下，DevOps 需要更加敏捷的跨团队沟通机制，因而 DevOps 还提出要在整个 IT 团队中建立更为人性化、高效无纠纷的“免责文化”。

综上所述，DevOps 没有从理论上颠覆或是优化升级 ITIL/ITSM，但还是从落地实践的角度对 ITIL 的敏捷化实施提供了更具体的解决方案，包括：微服务化、灰度实施、自动化技术等。■

DevOps	• 客户导向、需求导向 • 客户利益最大化	• 强调效率、降低发布风险：单件流、微服务、灰度发布 / 蓝绿发布等，自动化发布 • 强调业务连续性	• KAIZEN in Advance • 开发与运维之间敏捷的、实时的沟通形式 • 免责文化
ITSM/ITIL	• 为客户提供价值（功能 / 功效） • 量化的 SLA	• 通过标准变更将低风险的变更发布流程简化，提升效率 • 通过 IT 服务连续性支撑企业业务连续性	• 运维团队参与识别非功能需求、运维需求，识别新需求对运维的影响和风险 • 设计和转换新服务或变更的服务流程，强调从开发到运维平稳过渡

供应链风险管控的系统方法论

麻晓曲
二方审、供应链管理经理

> 基于CTPAT、AEO、TAPA 等要求建立的安全风险管理体系与风险地图和行业标杆数据结合是众多品牌客户乐见的、具备可持续发展能力的系统。

2002 年，也就是 2001 年 9 月 11 日纽约世贸双塔轰然倒下的第二年，一个供应链风险管理领域的新要求 CTPAT 急匆匆问世了。笔者在 2003 年第一次接触到此项目，当时认为与其说这个要求是为了识别供应商的安全管理风险，不如说是因为有人感觉自己不安全，进而把管理的触角延伸到了更遥远的供应链前端。有人甚至戏言，本 . 拉登才是众多供应链安全从业者特别是审核员的衣食父母。15 年过去了，全球供应链风险的管理还出现了 AEO, PIP, TAPA 等等新项目，也出现了很多欧美品牌客户和走在前沿的第三方审核机构的各具特色的审核工具。但有一个现实的问题一直在拷问着笔者，那就是过去的 15 年间我们花费的巨大精力和投入在供应链安全风险管控上，有没有用系统的方法去审视供应链的风险管理过程？

我们知道基于 CTPAT, TAPA, AEO, PIP 等要求的审核检查表是最为广泛应用的风险识别工具，通过审核员的视觉观察一个组织的安全风险管理机制，从实体到程序对这个组织的方方面面做一个全面的评估进行差距分析，进行通过后续的持续改进达到所谓的要求。这看似是一个没有任何毛病的完美套路，但笔者认为这里缺少了两个最为重要的方法论：

第一，**审核检查表的形式并没有形成可持续的改进系统**。审核检查表是快捷、易操作的缺失识别工具，久而久之会演变成照本宣科式的流水线操作工作。审核员也好，被审核的组织也罢，可以依据每一个检查点查漏补缺建立自己的管理办法，只要拿到足够的分数或者等级即可通过品牌、客户、第三方的审核从而获取商业机会。没有人会关心因检查表而建立的某一个或者一组管理制度方法是否适合组织的需求并与潜在的风险相匹配。这正如 ISO 9000 以及其他的类似的管理体系标准形成之前，质量管理的恰当名字应该是质量检查一样，检查表只能做到将良品与不良品区分开来，却并不能从 PDCA 循环上去寻找可持续的改进系统。因此，笔者认为供应链安全风险管理急需引入类似 ISO 9000 的管理体系标准，例如 ISO 28000, 从而将组织的安全风险与自身的管理要求和资源配置以及客户、公众的需求结合起来。否则，CTPAT 审核只会在猫捉老鼠的游戏中急需玩耍下去。笔者听到很多来自客户和组织的抱怨，他们觉得自己已经按照审核检查表的要求把能够配置的资源和程序都建立起来了，但在日常管理中依然有很多例如货物损失、偷盗、通关文件差错、贸易信息紊乱等问题困扰着相关过程。没有系统的管理大致如此，这一点也不奇怪。ISO 28000 的标准结构和理论思路与 ISO 9000 类似，关切组织内外部的需求，注重风险识别，强调持续改进，这里不多赘述，各位看官脑补一下。如果能把客户的需求如 CTPAT, AEO, TAPA 点式的要求用 ISO 28000 的体系管理模式解析出来，必然会形成一个强有力的管理体系。

第二，**风险的差异化管理理念**。供应链的安全风险是相对的，通常的理解是高墙大院、狼狗保安、监控警报和各种巡逻盘查才是安全的信心保障。检查表式的审核对照组织的实体和操作程序进行打分评估，获取最终结果与要求值进行比对，得到风险等级然后确定需要的整改措施。 但我们试想一下，使用同样的检查表在不同的大环境下，比如不同国家、不同地区、不同行业内做无差异化的分析得出的结果靠谱吗？举个例子，一个位于巴基斯坦或者埃及的工厂门口站着荷枪实弹的军人，高墙上的铁丝网带着尖锐的刺角，各种盘查如同进了军事管制区，高清摄像系统遍布整个区域 360 度无死角监控……这样的实体安全够强大吧？检查表上的分数一定不低吧？把视线转回中国，一个普通的工厂或者物流中心，必然不会有那么强大的武力保护措施吧，那检查表上的分数自然也不会有巴基斯坦和埃及的同行们高了。那么问题来了，一个 70 分的中国工厂和一个 90 分的巴基斯坦工厂究竟哪个安全风险更高呢？我想应该还是巴基斯坦，原因不说自明。差异化的风险管理需求在这里必须使用了。BSI 的风险地图基于全球各地每年发生的各类安全事件进行数据分析，对不同地区国家进行风险等级区分。同时，不同行业的风险特性通过长期的数据积累形成标杆，每一个组织都会被移入自己所属的行业中做横向比较。 风险地图和标杆数据使得组织能够从宏观上识别自身风险之于所在国家或地区水平和行业风险控制水平处在何种位置。

基于 CTPAT、AEO、TAPA 等要求建立的安全风险管理体系与风险地图和行业标杆数据结合是众多品牌客户乐见的、具备可持续发展能力的系统。BSI 的智能荧屏 SCREEN 系统能够提供全面的解决方案，而且已经获得了包括 Apple, IBM, Dell, Facebook, Wal-Mart, The Home Depot, Target, JC-Penny 等众多知名品牌的认可。供应链安全管理也由此进入了体系管理的新时代。■

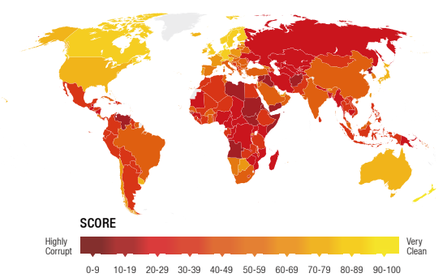
反贿赂管理与 ISO 37001:2016 标准

胡汉
BSI 产品技术经理

基于 BSI 编制的 BS 10500: 2011《反贿赂管理体系规范》，国际标准化组织 (ISO) 于 2016 年 10 月 15 日颁布了国际上首个反贿赂管理体系标准——ISO 37001:2016，该国际标准借鉴了国际上反贿赂的最佳实践，为组织提供了一套反贿赂的系统方法。

贿赂，是指违反适用法律法规直接或间接地提供、承诺、给予、接受或索取任何价值的不当好处（可以是金钱的或非金钱的），以引诱或奖励个人利用职务之便的作为或不作为。作为一种广泛存在的现象，贿赂引发了严重的社会、道德、经济和政治问题，破坏了正常的管理秩序，阻碍了正常发展，扭曲了商业竞争；贿赂侵蚀了正义，损害了人权，阻挠了贫困的消除；贿赂加大了企业营运开支，带来商业交易的不确定性，提高产品和服务的成本的同时却降低了相应的质量，导致生命和财产的损失；贿赂摧毁了相互间信任，干扰市场公平和高效运作。

权威组织“透明国际”公布的清廉指数 (Corruption Perceptions Index, CPI) 年度报告真实反映了全球贿赂影响的分布情况：



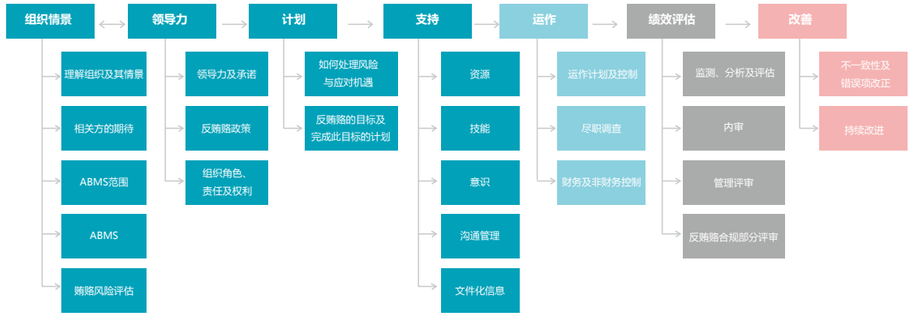
2016年度清廉指数热力图

2016 年度清廉指数热力图表明，欧洲、北美和大洋洲三个地区的清廉指数较高，而亚州、非洲、东欧、拉美和南美洲的指数相对处于低位，全球的贿赂影响仍然严重，需要进行更加有效的控制。

面对日趋严峻的贿赂行为的挑战，2003 年 10 月 31 日召开的第 58 届联合国大会通过了《联合国反腐败公约》，吹响了全球反腐败、反贿赂斗争的号角，并将每年的 12 月 9 日确立为国际反腐败日，以纪念公约的签署和唤起国际社会对腐败问题的重视与关注。各国政府也都积极响应，成立专门的机构，加大打击日趋严重的贿赂行为，出台了相关的反贿赂法律法规，如英国的《反贿赂法案》、美国的《反海外贿赂行为法》、德国的《反贿赂法》和《反不正当竞争法》等，其中英国 2010 颁布的《反贿赂法案》的管理范围相比更为宽泛。无论是公司或个人，若涉嫌违反相关反贿赂法律，将会面临刑事和民事责任的双重风险和巨额罚金。包括许多全球著名企业都曾因贿赂案件受到严厉查处，遭到数亿美元以上的罚款，不仅给业务经营带来了重创，而且严重损害了企业的声誉。

中国在反腐败和反贿赂方面取得了显著的成绩。自 1997 年国家提出“依法治国，建设社会主义法治国家”的治国方略以来，逐步建立一起一套完善的反腐倡廉的法律法规和制度体系，除了《刑法》对贪污罪、受贿罪等一些与反腐败、反贿赂有关的犯罪有明确规定外，各省（部）级以上机关也出台了多项法律法规及其他规范性文件要求，如《反不正当竞争法》、《反洗钱法》、《商业银行法》、《建筑法》、《政府采购法实施条例》和《关于禁止商业贿赂行为的暂行规定》等。2007 年 4 月 22 日颁布的国务院第 495 号令《行政机关公务员处分条例》成为首部全面和系统规范行政处分工作的专门行政

ISO 37001:2016高层次结构



法规，为中国政府持续推行廉政建设奠定了法律基础。新一届政府高度重视反腐工作，各级司法监察部门通过案件侦查，依法查处了各类典型的贪污腐败贿赂案件，为企业、事业单位创造了健康清廉的工作和商务环境，提高了全民的反腐败、反贿赂意识。

随着全球反腐败、反贿赂浪潮的不断高涨，许多组织开始认识到仅有法律法规和监督管理是不足够的，必须建立一个有效控制腐败和贿赂风险的机制。基于 BSI 编制的 BS 10500: 2011《反贿赂管理体系规范》，国际标准化组织（ISO）于 2016 年 10 月 15 日颁布了国际上首个反贿赂管理体系标准（Anti-Bribery Management System，简称 ABMS ）——ISO 37001:2016，该国际标准借鉴了国际上反贿赂的最佳实践，为组织提供了一套反贿赂的系统方法。作为要求和应用指南，ISO 37001:2016 只针对贿赂的管理，旨在帮助组织预防、发现和应对贿赂风险，遵守反贿赂法律和满足合规义务的要求。

ISO 37001:2016 采用与 ISO 9001:2015 和 ISO 14001:2015 相同的 HLS 高层级结构， 其规定的要求是通用的，旨在适用于各种类型、不同规模和性质的组织（或组织的一部分）。这些要求的适用范围取决于所确定的因素，包括组织或组织的环境、相关方的需求和期望以及风险评估的结果。组织可以单独实施反贿赂管理体系，亦可与其他管理体系（如质量、环境等）整合后实施。

ISO 37001:2016 管理体系标准的核心要求包括确定组织的最高承诺、规定适当的程序、进行风险评估、开展尽职调查、实施沟通管理（包括培训）以及监测和评价管理体系的运行。组织通过有效控制关键触点 （Critical Touch Points，CTPS）来管理贿赂风险，持续改进，保持管理体系的适宜性、充分性和有效性。

ISO 37001:2016 标准自推出以来就受到了广泛的欢迎，并迅速在世界各国得到应用。导入和实施反贿赂管理体系将使组织获得如下益处：

（一）协助组织落实反贿赂管理制度，加强现有反贿赂的控制，将贿赂风险损失降到最低的限度，使组织在激烈竞争和不断变化的市场经营环境中求得生存和发展；

（二）帮助企业全面加强内部贿赂风险防控，提高企业内控与合规管理水平，规避贿赂舞弊等风险；

（三）有助于向组织的管理层、所有者及其利益相关方提供保证，该组织已按照国际公认的良好实践进行了反贿赂控制；

（四）满足反贿赂贸易要求，积极应对国际市场反贿赂贸易趋势，同时也带动了供应链的反贿赂意识和行动，形成公正公平的良性竞争循环，提升组织清廉和合规的品牌形象，增强企业竞争力。

BSI 作为标准之源，对 ISO 37001:2016 有着最深刻的理解，将为有需要的组织提供 ISO 37001:2016 标准的培训和认证服务，提高组织的反贿赂意识和管理水平，提升可持续发展的能力，为中国建立更加公平、清廉的商业和管理环境做出贡献。■

BSI 产品认证事业部

BS 1363 标准转版说明

随着用户对于插头插座类产品的使用要求不断的提高，相信势必会令这些具备多种功能的英制插头插座类产品引起越来越多消费者的关注和青睐。

BS 1363 系列标准版本信息概述：

BS 1363 标准从 1967 年第一版发布到 2016 年 8 月 31 日之前，分别于 1984 年、1995 年进行过两次全面转版。尤其在 1995 年转版时，BS 1363 标准被分解成了 5 个分标准，即：

* BS 1363-1: 可接线或不可接线的带保险丝的 13 安培英制插头

* BS 1363-2: 带开关或不带开关的 13 安培英制插座

* BS 1363-3: 英制转接器

* BS 1363-4: 带开关或不带开关的带保险丝的 13 安培接线装置

* BS 1363-5: 带保险丝的转接插头

而 BS 1363-1/-2/-3/-4 的 1995 版标准，总共又经历了 4 次修订。目前 BS 1363-1/-2/-3/-4: 1995+A4: 2012 版标准依然是现行有效的。

值得关注的是 BS 1363 系列标准（第 1 部分至第 5 部分）已于 2016 年 8 月 31 日发布了最新的 2016 版。新版 BS 1363 标准（第 1 部分至第 4 部分）将分别同时取代 2012 年发布的 BS 1363:1995+A4 版的系列标准，而 BS 1363-5 的 2016 版将取代之前的 2008 版 BS 1363-5 标准。这些老版标准在 2019 年 8 月 31 日之前依然保持有效。

针对新、老版本标准的主要差异部分的介绍：

新、老版本标准适用范围的变化：

从新版标准的适用范围来看， 2016 版的 BS 1363 系列标准的内容变得更加丰富，适用的产品范围更广。以英制插头为例，相比老版标准只允许插头配置普通的内置开关和指示灯元件而言，新版标准允许英制插头可以配置防浪涌装置和一些电子开关。另外，该标准还新增了一种可应用于电动汽车充电的插头类型。再以英制插座为例，相比老版标准，新版标准允许英制插座配置防浪涌装置、电子开关以及用于给便携式设备充电的 USB 接口。而所有上述的这些电子元件同样也可配置于各式的英制转接器上。另外，凡是满足相关技术要求的固定式插座还允许被用于电动汽车充电电路之中。除此之外，在英制插座以及接线装置的新版标准中，还被引入 IP 防护等级的要求，这一变化将使此类能够满足一定 IP 防护等级要求的产品不仅可以在户内使用，而且在特定条件下还可以在户外使用。

新、老版本标准技术方面的主要变化：

2016 版 BS 1363 系列标准主要涉及到以下技术方面的变化：

1. 增加了新的专用于电动汽车充电的插头 / 插座类别、测试方法及其评估要求；

2. 增加了一些新的功能，如浪涌防护，USB 电路以及电子开关功能及其评估要求；

3. 增加了插座、接线装置的 IP 防护等级的要求；

4. 增加了 EMC 的评估及测试要求；

5. 调整了一些产品的相关参数；

6. 修改及增加了部分评估、测试程序的要求。

以下将分别从产品分类、标识、结构、测试等方面进行阐述：

标准更替进程说明

（一）产品分类：

新增了是否适用于电动汽车充电的插头或插座分类，是否带开关的插头分类；新增了具有 IP 防护功能的插座或接线装置的分类、新增了是否带电子元件的插座分类以及螺纹式 / 非螺纹式端子的插座或接线装置的分类。

（二）标识要求：

凡是用于电动汽车充电的插头或插座，新增了“/EV”的标识要求，即：一般需要在产品上标注：“BS 1363/EV”。

凡是使用了非螺纹端子的插座或接线装置产品，必须注明非螺纹端子的接线说明。如果 IP>20，则 IP 防护等级及其安装和使用说明等也应该标注在产品上。另外，对于便携式带保险管的插座产品，“Fitted with X ampere fuse”的标贴要求以被取消。而对于转接插头，为了确保不会将用电设备通过转接插头连接到与其额定电压不匹配的电源上，所以需要提醒用户该转接插头并不具备转换电压的功能。从而防止误插误用，因此需要在转接插头上明确标注诸如：“This conversion plug does not convert voltage”的警告语。以提醒用户谨慎合理地使用该转接插头。

（三）结构要求：

新版标准给出了两款标准的插头外形及其尺寸要求（普通型和紧凑型），以确保其能与封闭式结构的插座更好地配合使用。对于插座产品，插合面上台阶的高度从老标准的不超过 2 毫米修改为了不超过 3 毫米。当嵌入式插座或接线装置按制造商要求接线并装上安装盒后，所有突出的带电部件和安装盒内侧凸出的安装孔之间要保持足够的安全隔离。新版标准还明确规定便携式不可接线插座内部不能使用任何螺纹式连接的结构。另外，对于 IP>20 的插座及接线装置，新版标准对于外壳结构、排水孔、密封性等给出了明确规定。

（四）测试要求：

针对用于电动汽车充电的插头或插座类产品，增加了针对插头的滚筒跌落测试的要求、补充了插座的通断测试的参数要求、而且对于此类插头或插座产品还需要额外进行循环加载测试。在对连接两根单芯电缆的不可接线插头做拉拔、扭转以及吊重弯折测试时，作用力应平均分配与每一根电缆上。保险管过载测试电源电压可以设定在 12V 至 250V 之间，不过 BSI 还是主张首选 250V 的电压进行此项测试。由于新版标准允许插头产品可以配置各种电子元件，因此 EMC 测试将可能会被适用于此类产品。

对于插座类产品，插座插套吊重测试时，在测试量规插入插套后，如果被撑开的插套接触到周边的绝缘材料，新版标准要求将该绝缘材料去除后重复之前的吊重测试。新版标准还给出了针对插座及接线装置的 IP 测试要求。而带 USB 的固定式插座或英制转接器，温升测试时，必须同时给 USB 施加相应的额定电流，以模拟一般正常使用的情形。

（五）其他要求：

针对插头产品，保险管额定电流的要求略作修改，如下：

老版标准允许 0.75 mm^2 和 1 mm^2 配线的插头可以装配最大 13 安培额定电流的保险管，而新版标准将此项要求修改为一般可以装配最大额定电流为 7 安培（针对 0.75 mm^2 配线的插头）和 10 安培（针对 1 mm^2 配线的插头）的保险管，不过如果该插头仅用于连接某种特定负载，比如具有冲击负载特性的用电设备时，新版标准依然允许使用最大额定电流为 13 安培的保险管；

而对于 1 mm^2 配线的插头的额定电流在满足特定条件下，比如仅使用于配线长度不超过 2 米的插头接线组件时，可以达到 13 安培的产品额定电流，不过前提条件是该产品能够通过相关的测试评估。对于那些带英制 BS 1363-1 插头的直插式产品，比如：直插式定时器，直插式适配器等，新版标准给出了针对这类产品的插头部分的测试及评估项目。

针对插座产品，0.5mm^2 和 0.75 mm^2 配线不能被用于 BS 1363-2 英制插座而所有插座的额定电流统一为 13 安培。

新版标准对于各类可被用于插头、插座类产品的电子元器件，比如：电路板、防浪涌装置、USB 充电接口、电子开关以及可能与之相关的 EMC 测试评估等分别给出了具体的评估标准。电路板的评估标准为：BS EN 60664-3&BS EN 60664-5；而 USB 的评估标准为：BS EN 60950-1: 2006+A2:2013; 或 BS EN 62368-1: 2014; 或 BS EN 61558-2-16: 2009+A1: 2013/BS EN 61558-2-6: 2009 以及 BS EN 62680-1-1: 2015; 而防浪涌装置主要涉及到的评估标准为：BS EN 61643-331: 2003; BS EN 61643-321: 2002; BS EN 61643-311: 2013 以及 BS EN 61051-2: 1992+A1: 2009; 而电子开关则需要符合 BS EN 60669-2-1: 2004+A12: 2010 的标准。

BSI 的“Kitemark”证书更新的测试要求：

BS 1363-1 / BS 1363-3: 无额外测试的要求。

BS 1363-2：根据不同类型的插座，条款：13.5；13.6；13.15；13.21 需要重新评估。

BS 1363-4：条款 13.2 需要重新评估。

BS 1363-5：条款 7.1.h 需要重新评估。■

云计算安全发展态势及选择云服务的几点建议

万鑫
BSI 高级讲师

信息安全依然是企业和消费者在选择云服务时的首要考量要素。笔者在分析 2017 年云安全领域发展趋势的基础上，为企业选择云服务提出几点建议。

云计算作为一种新兴的商业模式，因其具备的快速部署、弹性伸缩、降低 IT 成本等优势，促进工业和服务业的飞速发展，市场前景极大。然而，信息安全依然是企业和消费者在选择云服务时的首要考量要素。笔者在分析 2017 年云安全领域发展趋势的基础上，为企业选择云服务提出几点建议。

云计算安全发展趋势

结合 BSI 长年针对云计算行业的持续分析研究，以及近年来为国内外知名云服务厂商（以下简称 CSP）提供安全服务的跟踪交流，我们认为 2017 年云安全领域将会出现如下趋势：

1、合规是选择云服务的先决条件

随着《网络安全法》和越来越多的行业信息安全规范出台，符合法律法规要求已经是 CSP 需要首要考虑的问题。识别是否为 CII（Critical Information Infrastructure，关键技术设施）和云服务中是否包含的 PII（Personally Identifiable Information，个人可识别信息）是公有云 CSP 在 2017 年的重点工作。为电信、金融、医疗、能源、交通等行业提供云服务的厂商，国家和行业的法律法规会重点考虑其处理业务的信息保密性、数据完整性、服务可用性和业务连续性。同时，对于提供国际业务的 CSP，需要重点考虑不同国家或司法管辖地区的法律法规要求，例如欧盟的 GDPR（General Data Protection Regulation，一般数据保护条例），美国的 ECPA（Electronic Communications Privacy Act，电子通信隐私法案），英国的 Data Protection Act（数据保护法案）等。

2、第三方安全服务将大行其道

多数公有云 IaaS 服务提供商在提供服务时，会配套提供包含主机、网络、存储在内的安全产品，以及用户认证和接入安全功能。然而由于不同企业 IT 基础设施或私有云的异构特点，公有云标配的安全方案往往不能完全满足企业用户的特定安全需求。

为了满足企业用户个性化的需求，第三方安全厂商能够针对一些特定行业，提供完整的、适配性较强的安全解决方案，包括符合企业业务习惯的统一用户认证和接入，以及对 IaaS、PaaS、SaaS 服务的统一安全策略，或者易于集成到企业整体安全方案的针对一些特定业务安全防护。

3、机器学习 / 人工智能的感知安全将广泛应用

与传统的 IT 架构不同，分散的边界、主机防护理念在云当中不完全适用，弹性网络中大量的东西向、南北向流量，以及数据和应用的大规模集中，使得云成为深度复杂的系统。如果不能对整个云的安全态势进行感知，良好的防护无从谈起。

在 2017 年，机器学习和人工智能持续发展，基于最新技术的大数据安全平台将会在更多的云中部署，与遍布在云中的传感器协同，一刻不停地收集、分析数据并感知其中的威胁，并最终进行针对性的防护处理。

4、IoT 的高速发展会产生更多更新安全攻击事件

随着物联网（IoT）的快速发展，越来越多的智能摄像头、可穿戴设备、工业传感器、家庭终端通过云服务走进了我们的工作和生活。然而众多的 IoT 终端在设计之初，并未充分考虑到安全问题。这些设备作为攻击的跳板，已经在造成数件有影响力的安全事件。例如，2016 年打破 DDoS 攻击 665G 带宽记录的黑客就是利用了数以十万计的智能汽车、监控摄像头和路由器的安全漏洞。

2017 年，数量庞大的有安全风险的 IoT 终端依然存留在在网络中，新的低安全性 IoT 终端将会持续被部署。可以预见的是，与之相关联的云端应用会面临越发巨大的威胁，更大规模的 DDoS 攻击会出现，更多的病毒、木马、APT 会通过 IoT 终端进入到云端。

5、勒索软件将会蔓延到云基础设施层面

勒索软件攻击在 2016 年疯狂增长，我们预计今后会更加猖獗，重要的云基础设施及其承载的数据会成为受害者。病毒勒索早已成为一种成熟的地下黑色产业，随时都可能危害到企业和个人。例如，前段时间波及中国大部分地区的“永恒之蓝”系统漏洞和 WannaCry 勒索软件让我们认识到了勒索软件的巨大危害。

然而，由于很多受害企业很清楚只需支付相对低廉的费用即可摆脱麻烦，这让勒索的成功率居高不下。同时，为了企业声望的考虑也不会公开或者分享攻击特征，从而导致勒索软件被安全公司及时定位清除的难度加大。

选择云服务的考量因素

近年来，企业持续将 IT 基础设施云化并将业务向云迁移，2017 年这一趋势将加快。针对云计算安全的发展趋势，我们认为，当企业和个人在选择云服务时，应重点考虑 CSP 的以下方面：

1、合规标准

首先，CSP 必须通过并获得知名且可信的认证，例如信息安全管理体系 ISO 27001、云安全管理体系 ISO 27017、公有云个人信息保护管理体系 ISO 27018、IT 服务管理体系 ISO 20000、业务连续性管理体系 ISO 22301 等。这些独立认证标志将让消费者能够相信 CSP 的合规要求和 IT 安全级别。

2、提供透明度

随着网络攻击数量和范围不断增加，对于 CSP 而言，提升服务的透明度和规范性是解决客户顾虑并建立信任的前提。同时，公有云作为一种 IT 外包服务，必须明确区分 CSP 和客户之间的角色、权限和责任。CSP 需要根据其提供的云服务模式，明确其提供的服务范为和应尽的职责，并通过官方网站、白皮书等形式，向客户展示其技术架构、安全控制措施、沟通渠道和满足不同行业合规要求的做法。

3、事件响应机制

公有云和企业自有数据中心的一个显著区别是其完全依托在 Internet 之上和 7*24 小时提供服务的特点，因此公有云可能面临比企业自有数据中心更大的网络攻击的可能性。客户应重点考虑 CSP 的事件响应和通知机制，例如，根据网络安全法和的服务组织控制 (SOC) 的要求，CSP 应该与消费者共享事件响应计划并在规定的时间内通过电子方式告知受影响的客户。

4、服务可移植性

当企业将 IT 基础设施迁移到云端以后，意味着其自身业务的稳定和持续性很大程度上依赖于云服务的功能性和稳定性。如果因某些原因准备将业务迁移回企业内部或转移使用其他厂商的云服务，云客户将会面临业务逻辑、软件架构和数据格式等多方面的兼容性问题。因此，选择根据标准或开放协议构建的云服务，或明确提供业务迁移的 CSP 是企业需要重点考虑的问题。■

马海鹏
BSI 高级项目经理

谈谈航空业管理体系整合

以高服务标准、高安全性要求著称的航空服务业，对管理体系的整合与一体化建设提出了非常高的要求。本文将结合案例探讨航空业整合管理体系。

随着我国社会经济的不断发展与进步，越来越多的人选择飞机作为交通工具，航空业在获得高速发展的同时，也受到越来越多的关注。相对于一般服务业，航空业具有几个非常鲜明的特点：一是专业化技能要求高，二是服务标准要求高，三是安全性要求高，四是国际化程度高。因此航空公司的企业管理，一直都强调人性化、精细化、标准化和国际化。

然而就现状而言，国内航空公司管理体系的成熟度普遍还很低，并没有跟上民航业快速发展的步伐。随着航空市场的进一步开放和高铁运输的兴起，航空业的发展逐步由成长期进入到成熟期。在技术趋同、服务同质、安全高压的大背景下，服务创新以及运营效率和成本的管控日益重要，管理体系的完善与否，已经成为影响航空公司竞争能力的重要因素。

基于笔者与多家航空公司的交流经验，总体来看，航空公司在管理体系的建设和运行方面大多存在如下主要问题：

多体系孤立并行，各自为政

受内外部需求的驱动，航空公司大都建立了诸如 SMS（安全管理体系）、SeMS（安保管理体系）、ISO 9001 质量管理体系、内控体系、合规体系等管理体系，然而由于主管部门不同，各体系之间通常相互孤立，各自为政。

质量职能三分离，自说自话

根据专业化分工的行业传统，航空业三大质量属性（安全、正点、服务）的管控通常由不同的职能部门主导。而各主管部门在进行相关制度的建设和维护时，常常基于部门自身的立场自说自话，没有在公司层面形成统一的质量监督管理机制。

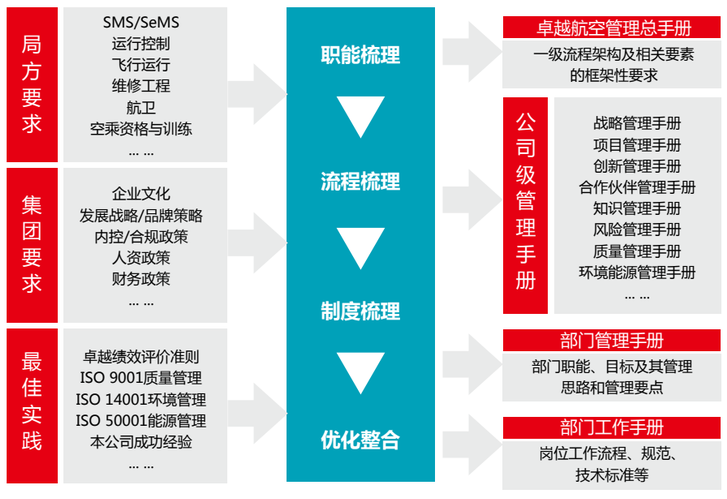


图 1 体系整合框架思路

图 2 卓越航空管理总手册架构图 >>

通用流程不一致，百家争鸣

跨职能、统一的通用流程多有缺失或不完整，如项目管理、创新管理、合作伙伴管理、知识管理、风险管理等流程，各部门都有，但做法都不一样，百家争鸣。虽然设立了一些跨职能的管理委员会，但多数委员会并没有成熟的运作机制，形同虚设，难以发挥应有的统筹与协调作用。

服务标准不统一，无所适从

由于制度建设缺少顶层设计和逐级传导的统筹安排，经常出现总公司与分公司之间、分公司与分公司之间政策不统一的现象。典型的就是服务标准的不一致，让面对同一品牌航空公司的旅客在不同场合遭遇不同政策规定时，无所适从。

航空公司管理体系所存在的这些问题，不可避免地会导致管理权责不清、流程接口不畅、运营效率低下等一系列不良影响，继而可能造成运营成本增加、服务品质下降、顾客投诉与事故多发等不良后果。如何解决管理体系存在的这些问题呢？答案在于整合二字，包括体系整合、流程整合、职能整合，以及标准整合等。如何整合呢？下面的案例取材于国内一家知名的民营航空公司。

体系整合的主要步骤包括职能梳理、流程梳理、制度梳理、优化整合四个阶段，其输入包括法律法规 / 局方要求、体系标准 / 最佳实践、上级单位 / 集团要求三部分，所输出的整合体系架构包括四个层次，分别是卓越航空管理总手册、公司级管理手册、部门管理手册、部门工作手册。体系整合的总体思路详见图 1 所示。

其中，卓越航空管理总手册呈现了体系整合的顶层设计。总手册统筹考虑了各管理体系的管理要素，以及各职能部门的管理职责，重新进行梳理和组合，并通过多个公司级管理手册予以规范化和标准化，以充分实现职能、流程和制度的有机整合。

卓越航空管理总手册的架构如图 2 所示。

需要说明的是，卓越航空整合管理体系的构建，并不应止步于简单的手册整合。整合体系的有效运行还有赖于资源的合理配置，以及目标与绩效等管理机制的协同配合。整合管理体系的构建是管理的系统方法的体现，迈出了正确的第一步。基于自我完善机制的改进循环，会不断优化管理职能、目标、流程与资源配置，直至实现企业管理的效能最大化。■

品牌对话

专访佛山优特：囊获全国首张MDSAP证书

2017年4月，BSI为佛山市优特医疗科技有限公司（以下简称“佛山优特”）颁发了中国首张MDSAP证书。作为全球首批被认可、且在全球颁发MDSAP证书最多的审核机构BSI，近一年，已通过多次对MDSAP医疗器械法规和标准的解读活动，帮助企业正确理解MDSAP所覆盖的五国医疗器械质量体系法规要求，助力企业快速进驻全球市场。

BSI于今年4月，颁发全国首张MDSAP证书。图为BSI中国区副总裁张维德先生代表BSI授证，佛山市优特医疗科技有限公司总经理王晓东博士接受证书。双方更进一步拓展和加强了在医疗器械领域的合作，致力于为消费者提供健康、安全的医疗器械产品。

MDSAP单一审核方案

MDSAP是国际医疗器械监管机构论坛（IMDRF）成员共同发起的项目。

MDSAP审核基于ISO13485，覆盖五国的医疗器械质量体系法规要求：

- 美国FDA
- 巴西ANVISA
- 日本MHLW和PMDA
- 加拿大HC
- 澳大利亚TGA

企业可借助MDSAP单一审核：

- 满足参与国不同的QMS/GMP要求，实现一次进入多元市场
- 降低合规成本
- 缩短市场拓展周期
- 促进企业进行质量体系整合，提高企业管理水平

MDSAP单一审核方案对企业的益处

美国：
替代FDA的常规检查（有因检查和PMA产品除外）

巴西：
对于3、4类医疗器械，可以替代ANVISA的上市前GMP检查，以及上市后的例行检查

日本：
对于2、3、4类医疗器械，可豁免现场工厂审核，并用作提交MAH注册的文件

加拿大：
2019年起强制取代CMDCAS认证，作为分类在2类及以上产品进入加拿大的唯一途径

澳大利亚：
可豁免TGA审核，支持颁发和保持TGA符合性审核证书

世界卫生组织WHO：
可以缩减或者豁免WHO的体外诊断器械的资格审查的现场检查

Q: 请简要介绍一下 UMT 的发展历史和主要业务：贵司何时开始有国际业务？主要出口产品有哪些？主要出口至哪些国家？该产品在国际市场上的地位如何？

A: 佛山市优特医疗科技有限公司（Foshan United Medical Technologies Ltd）是在 2010 年底注册成立的中英合资企业。公司主要产品是纤维类伤口敷料，在 2012 年取得海藻酸盐伤口敷料的 CE 认证，并开始了这个产品在国内外的销售。目前还有改性纤维素伤口敷料，壳聚糖伤口敷料等产品在国外销售。这些产品都受到用户的一致好评。目前公司产品主要是通过 OEM 形式销往欧洲和美国，有些产品也在南美及世界其他地区有销售。

Q: 贵司与 BSI 的合作已有多年，合作中，BSI 主要提供的是第三方认证服务，请问您认为第三方认证机构对贵司的发展尤其是开拓国际市场方面有何作用和价值？

A: 首先这个第三方认证是我们海外销售的必要条件，而 BSI 是这一行业享有盛名的第三方认证机构。行业中大家普遍认为 BSI 对各个标准的理解准确，在不同时间和不同地方的执行标准也一致。此外我们所接触的敷料企业中大部分也是通过 BSI 获得 ISO 或 CE 认证的，因此我们的 ISO 和 CE 证书在客户中获得了广泛认可。往往客户听说我们的第三方认证机构是 BSI 后就不再对我们的质量体系有其他大的顾虑。

Q: 获得中国第一张 MDSAP 认证证书，这将对 UMT 的业务将产生什么影响？您对此有何期待？

A: 佛山优特很荣幸获得了 BSI 在亚洲颁发的第一张 MDSAP 证书，也是国内首张 MDSAP 证书。我们在第一时间就通知了客户，所有客户都对此感到很有兴趣。有些客户他们自己还在准备申请 MDSAP 审核，希望早日也能拿到 MDSAP 证书，为他们业务扩大打好基础。有些客户希望佛山优特给他们传授经验，做好 MDSAP 审核准备。佛山优特希望通过 MDSAP 审核和认证提升其质量管理体系水平，为开发欧美以外市场打好基础，特别是取得在加拿大，巴西和澳大利亚的客户的信心，为在这些地区扩大业务做好前期准备。

Q: 近年来医疗器械行业的整体发展趋势如何？出口形势如何？ UMT 下阶段的国际市场开拓方向和战略是什么？您期待 BSI 如何助您一臂之力？

A: 国际医疗器械行业，特别是敷料行业竞争愈趋激励，一些新兴国家企业都开始研发生产医用伤口敷料，这对国际上所有生产企业都带来很大冲击。好在我们的海外销售都是有很高技术含量的产品，而且我们的质量和服务总是行业中最好的，因此我们的客户群还是比较稳定的。

我们的战略是继续开发和生产有技术特点的和立足于市场前沿伤口敷料，扩大与海外客户的合作。希望 BSI 在这个过程中继续提升服务水平，提高服务效率，为我们的产品认证提供有效帮助。

BSI英国标准协会医疗事业部

BSI医疗事业部拥有顶级行业资源的技术专家，全球排名前25的医疗器械厂商中有92%选择了BSI的服务。BSI在审批高风险产品（如有源植入产品、髋关节、带药支架等）具有领先优势。BSI的审核范围覆盖了所有医疗器械产品，可提供CE认证、质量管理体系审核、MDSAP等全球准入方案，全面支持中国本地企业开拓国际市场，协助企业不断提高核心竞争能力。

BSI携新时代国际管理标准

云安全认证 ISO 27017

云隐私保护认证 ISO 27018

两大标准盾牌为企业保驾护航

BSI ICT产品群及整体解决方案
助力企业直击“互联网+”挑战

ISO/IEC 27001信息安全管理体系标准 / ISO 22301业务连续性管理标准

ISO/IEC 20000 IT服务管理体系标准 / STAR Certification云安全认证

业务详情咨询

BSI全国热线 400 005 0046 | infochina@bsigroup.com | www.bsigroup.com

基于百年经验沉淀
借助全球数万名客户与专家互动交流的最佳实践

BSI重拳打造组织生存力（Organizational Resilience）
从产品、服务至人员、流程
从愿景到价值观
从文化到行为

全面助力企业
将卓越与韧性注入整个组织
实现业务永续发展

还有更多关于BSI组织生存力的精彩内容，请持续关注BSI最新动态
BSI全国热线:400 005 046
BSI官方网站:www.bsigroup.com
BSI官方微信: BSI英国标准协会（BSI_China）