标准+

STANDARDS

BSI 中文期刊: 总第21期

www.bsigroup.com

创新驱动

引领发展

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）

创新驱动 引领发展

林劲
英国标准协会
中国区董事总经理

新的一年又到了，首先祝大家2018年新年快乐！

过去的2017年，国内外政治经济风起云涌，大事不断， 特朗普政府退出 TPP，亚太经济增添变数；英国“脱欧”谈判开启， 法国、德国大选，欧洲经济令人观望；美联储带头加息，多国跟随，全球货币政策回归正常化趋势明显，各国企业积极商讨对策；中国力推“一带一路”，国际合作高峰论坛硕果累累，给国内外企业带来广阔的发展机遇。

纵观国内，十九大召开，雄安新区成立，C919试飞成功，5G标准的建立无不为国内企业带来了不少商机；阿法狗（AlphaGo）完胜柯洁，无人驾驶违章上五环，AI人工智能的使用，自动驾驶汽车成为舆论热点，从互联网+”到“人工智能+”，概念不断，令人耳目一新，眼花缭乱，推动业界不断的揣测下一风口，而共享经济的潮起潮落，更引发人们深入的思考。

同时，我们也看到，WannaCry蠕虫爆发，病毒通过MS17-010漏洞在全球范围大范围传播，引起整个互联网动荡，多国公布禁售燃油车时间表，引发车企对未来布局定位的热议，造假丑闻接连不断“日本制造”走下神坛导致，使制造业反思质量的意义，美国通过30年来最大规模减税法案引发制造业回流，对中国制造业的潜在冲击颇大，也促使企业思考破局之策。

变化本是永恒，不变才是最大的风险，以上种种的变化，让BSI的组织生存力的话题更富有现实意义。

本期的《标准+》杂志，BSI专家们继续和大家深入探讨“组织生存力”三个维度令人关注的话题，从标准的层面助力企业的变革和发展，以适应日益变化的外部环境，进一步对企业的长治久安提供支持。

最后，感谢大家对BSI的长期关注和爱护，在2018年，BSI希望能继续推出新的，基于标准的质量和风险管控方法论，和大家一道互动，和大家一起共同成长，谢谢大家！

ISO 37001:2016是基于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。

BSI助力企业全方位建立反贿赂管理体系，预防、监控以及处理贿赂问题

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）

行业聚焦

19-24

23 | Sector Focused
行业聚焦

卓越绩效模式下的管理思维

卓越绩效模式(Performance Excellence Model）是通过综合的组织绩效管理方法，使组织和个人得到进步和发展，提高组织的整体绩效和能力，为顾客和其他相关方创造价值，并使组织持续获得成功。

2018年4月 总第21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

BSI组织生存力系列活动+

BSI英国标准协会【**年度组织生存力管理论坛**】在中国各地盛大召开，场场爆满，与数百位不同行业的企业精英齐聚一堂、共襄盛宴。BSI全新提出的【组织生存力Organizational Resilience】概念在中国首次正式发布，BSI也是全球业内第一家前瞻性提出此概念的机构。

活动以【**主论坛+3大分会场】的经典模式**，多维度直击“组织生存力-Organization Resilience”话题。同时，BSI资深专家们携手互联网、航空行业、金融、服务以及制造业等全球知名企业的重磅嘉宾带来丰富精彩的主题演讲。

除了一批应用广泛的新版标准外，包括**组织生存力、云安全及云隐私保护、汽车安全管理体系、职业健康安全管理**等在内的一批已应势而出或即将发布的新标准也让大家对标准又有了新的认识。

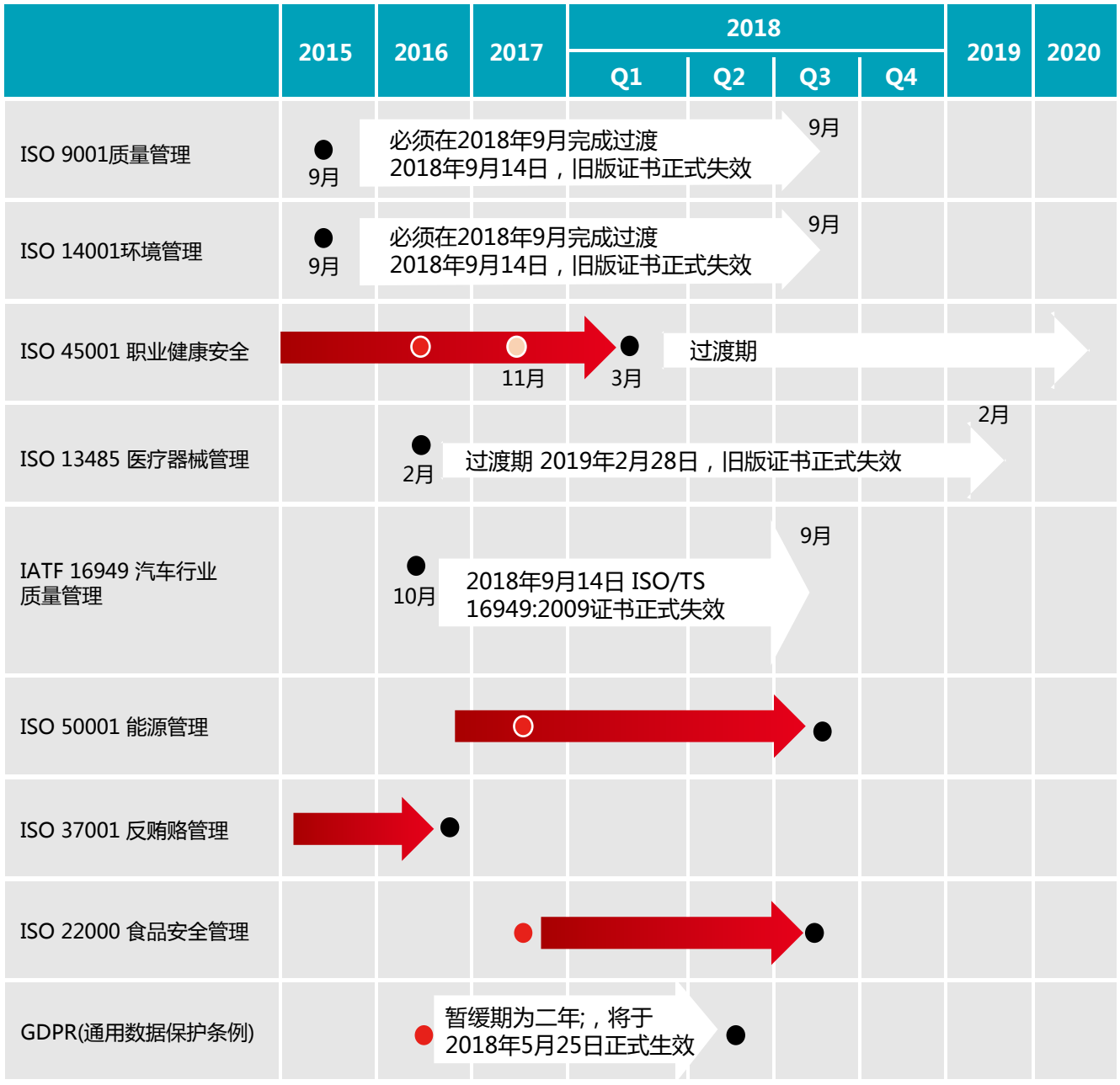
BSI作为标准领域的引领者，百年来一直用权威专业诠释着标准的深度与高度。正如BSI大中华区董事总经理林劲先生所述，BSI作为“**标准的正宗，正宗的标准**”，将继续在不断创新的当西，助力企业永续发展。

【第一站】2016年4月@上海
BSI【组织生存力】发布会

【第二站】2016年10月@北京
BSI 2016年度【组织生存力管理论坛】盛大举行

【第三站】2017年12月@北京
创新求变 永续发展—BSI 2017【组织生存力论坛】

Standards 标准动态 Dynamics



ISO 标准动态时间图

- 国际标准草案（DIS）：已发布或有望发布
- 最终版国际标准草案（FDIS）：有望发布
- 国际标准颁布：已发布或有望发布

整合 + 融合 = 提升组织绩效

乘 ISO 45001:2018 发布之东风，完成整合，提升绩效

BSI 质量分院院长 | 王敏秀

由 BSI 担任委员会主席的 PC283 项目委员会自 2013 年开始起草的 ISO45001《职业健康安全管理体系 - 要求及使用指南》，历经草案版 1（DIS1）、草案版 2（DIS2）、最终草案版（FDIS）后，依据 ISO 官方公布的信息，将在今 (2018) 年上半年正式发布国际标准，但一般估计将在三或四月公布的机会比较大。

ISO 45001 FDIS 采用了和 ISO9001：2015，ISO14001：2015 相同的高层次结构，围绕帮助组织获得职业健康安全管理体系的如下预期结果：

a) 持续提升职业健康安全绩效；

b) 满足法律法规和其他要求；

c) 实现职业健康安全目标。

旨在使组织实现“预防工作相关的人身伤害和健康损害”，以提供“安全和健康的工作场所”。

ISO45001 标准强调，不仅要关心组织自己员工的职业健康和安全，还要考虑组织越来越多的外包场所的服务人员和在现场服务的承包商人员的职业健康和安全。

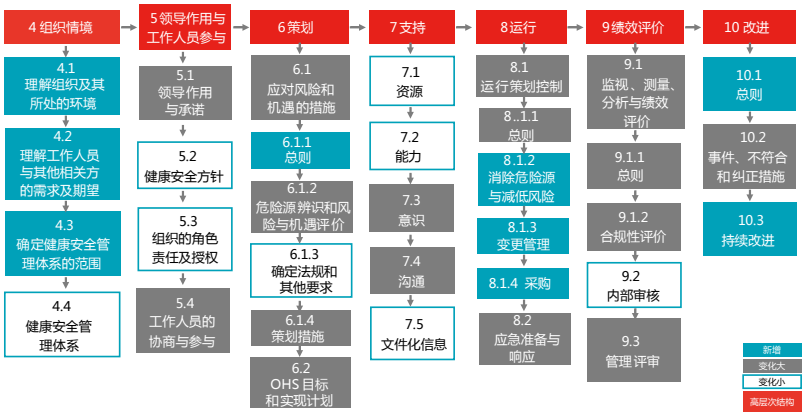
ISO45001 标准还强调，不仅要关注职业健康安全风险，还要关注职业健康安全管理体系的风险和机遇。

ISO45001 标准更强调在建立职业健康安全管理体系时要考虑组织的宗旨和内外部环境及工作人员和相关方的需求，并将管理体系要求融入组织的业务过程。

ISO45001 特别强调领导尤其是最高管理者的作用，确保工作人员的参与和协商。

因此，整合 + 融合就成为组织乘 ISO45001 发布之风需要着手进行的、将多个管理体系如质量、环境、职业健康安全要求整合并融入到组织的业务过程，从而提高组织运行效率和有效性的当务之急。

整合的原理：不同管理体系具备如下



ISO 45001 FDIS 条款总览图

> 整合 + 融合就成为组织乘 ISO45001 发布之风需要着手进行的、将多个管理体系如质量、环境、职业健康安全要求整合并融入到组织的业务过程，从而提高组织运行效率和有效性的当务之急。

- 相同的高层次结构：条款 4-10
- 相同的应用原则：自愿原则、广泛适用、认证依据、相互兼容
- 相同的管理理念：领导作用、全员高度参与、基于证据的决策、改进、关系管理、风险思维、过程方法
- 日常运营必备：组织盈利的前提是产品质量、安全生产、无环境污染

整合的必要性：通过减少重复性工作从而

- 提高管理效率
- 降低资源浪费
- 减少抵制情绪

整合的方式：可通过如下方式实现整合

- 基于业务过程：明确部门职责权限、梳理职责范围负责的过程和相关过程、对应不同管理体系标准条款要求、完成过程乌龟图

- 下表：过程、过程拥有者、相关过程和标准条款对应实例

- 下面 A 和 B：关于 ISO45001 5.4 工作人员参与的文件规定的可读性对照实例

序号	部门	过程名称	过程拥有者	相关过程	ISO9001:2015	ISO14001:2015	ISO45001：2018	IATF16949：2016	ISO13485:2016	……
1	总经办	经营计划管理	总经理	法律法规管理/风险管理	4.1/4.2/5.1/5.2.1/5.3/6.2			5.1.1.1/5.1.1.2/5.1.1.3/5.3.1/5.3.2/6,2,2,	?	?
2		法律法规管理	总经理助理	经营计划理/风险管理管	8个条款	14个条款	17个条款	12个条款	?	?
3		风险管理	总经理	法律法规管理/改进管理	6.1			见具体条款清单	?	?
4		应急计划管理	总经理助理	项目管理/EHS事件管	8.2.1	8.2	8.2	6.1.2.3	?	?
5		改进管理	总经理助理	?	9.3，10			10.2.3，10.3.1	?	?
6	技术部	项目管理	项目经理	?	?	?	?	?	?	?
7	HR	能力管理	HR总监	?	?	?	?	?	?	?
8		绩效管理	HR总监	?	?	?	?	?	?	?
9		培训管理	HR经理	?	?	?	?	?	?	?
10		EHS事件管理	EHS主管	?	?	?	?	?	?	?
11		危险废弃物管理	EHS主管	?	?	?	?	?	?	?
12	工程部	?	?	?	?	?	?	?	?	?
13	采购部	?	?	?	?	?	?	?	?	?
……	……	……	……	?	?	?	?	?	?	?

部门、过程、过程拥有者、相关过程、标准条款矩阵表

A．大量文字描述，不易获取信息

公司需确保以下内容的确定有工作人员和 / 或代表的参加：

1) 确定其协商和参与的机制；本程序规定了协商和参与的机制，本程序的制定和批准需经与工作人员代表的讨论和同意方可生效；

2) 危险源识别和风险和机遇的评估 ; EHS 管理人员组织工作人员及其代表共同进行危险源的识别、风险、机遇的评估，详见《危险源识别、风险和机遇的评估》；

3) 确定消除危险源并减低职业健康安全风险的措施 ; EHS 管理人员组织工作人员及其代表共同确定消除危险源并减低职业健康安全风险的措施；

4) 确定能力要求、培训需求、进行培训和评价培训 ; EHS 管理人员组织工作人员及其代表与人力资源部、安委会共同确定职业健康安全体系的能力要求，确定培训需求，提交给人力资源部，制定培训计划，并组织实施；

5) 确定需要沟通的事项及如何进行沟通 ; EHS 管理人员组织工作人员及其代表共同制定《沟通管理程序》，明确需要沟通的事项以及方式、方法；

6) 确定控制措施及其有效的实施和运用 ;EHS 管理人员组织各单位工作人员及其代表，共同确定各危险源的控制措施，以及如何有效实施和运用。

7) 调查事件和不合格并确定纠正措施；EHS 管理人员组织发生事件、事故、不符合单位的工作人员代表，参与相应事件、事故、不符合的调查、处理工作，共同确定纠正措施，并记录在“事件 / 事故处理报告”中。

B．表格描述，一目了然

结束语：

为帮助组织高效完成整合工作，避免走弯路，提高整合工作的有效性，BSI 在 2018 年即将推出 <ISO45001 实践者 >，< 整合管理体系策划实战 >，< 整合内审 > 等一系列课程，从理论和方法上支持各公司不再将体系作为负担，而是真正融入日常的业务运作，实现管理体系对日常工作的指导价值，同时帮助体系工作人员们走出“质量体系是质量部的事情”“EHS 是 EHS 部门的事情”的困境，最终实现组织的宗旨、战略和预期结果。■

标准条款5.4e)	参与内容	负责部门	参与的人员	参与的时机	参与方式	证据
1）	确定其协商和参与的机制；	EHS 部门	工作人员代表，HR，总经理	体系初建时；工作人员代表认为需要更新时	开会讨论；文件审批	签署的《协商和参与控制程序》；“会议签到表”；“会议纪要”；“知情同意书”等
2）	危险源识别及风险和机遇的评估（见 6.1.1 和 6.1.2）；	各部门领导	各部门工作人员及代表，EHS 部门	见《危险源识别和评价控制程序》		签署的“危险源及其风险和机会清单”
3）	确定消除危险源并减低职业健康安全风险的措施（见 6.1.4）；	各部门领导	各部门工作人员及代表，EHS 部门，总经理	见《危险源识别和评价控制程序》		签署的“危险源及其风险和机会清单”
4）	确定能力需求（见 7.2）	各部门领导	各部门工作人员及代表，EHS 部门，人力资源部，总经理	新增或者有如下变化时： -岗位/职责 -法律法规要求 -顾客要求 -相关方要求	开会讨论；微信群	签署的“岗位职责说明书”；“会议签到表”；“会议纪要”
	确定培训需求（见 7.2）	各部门领导	各部门工作人员及代表，EHS 部门，人力资源部，总经理	-能力不足时 -法律法规要求时 -顾客要求时 -相关方要求时 -个人发展要求时 -公司发展要求时	开会讨论；微信群	签署的《培训管理程序》；签署的“能力矩阵表”；“会议签到表”；”会议纪要“；“培训需求调查表”；“培训申请”；签署的“培训计划”
	进行培训和评价培训（见 7.2）	各部门领导	工作人员代表，EHS 部门，人力资源部	-培训实施前、中、后	详见《培训管理程序》	签署的《培训管理程序》；签署的“培训计划”
5）	确定需要沟通的事项及如何进行沟通（见 7.4）；	EHS 部门	工作人员代表，各部门领导	确定沟通事项前	开会讨论；微信群	签署的《沟通管理程序》；沟通矩阵表；“会议签到表”；”会议纪要“
6）	确定控制措施及其有效的实施和运用（见 8.1, 8.1.3 和 8.2）；	各部门领导	工作人员及其代表，EHS 部门	需要制订措施时	开会讨论；微信群	签署的“危险源及其风险和机会清单”；签署的”行动计划“；“会议签到表”；”会议纪要“
7）	调查事件和不合格并确定纠正措施（见 10.2）。	发生事故的部门领导	工作人员及其代表，EHS 部门	见《EHS 事件管理程序》；《不符合纠正措施管理程序》		事件/事故处理报告，纠正措施报告

体系如何有效整合并融入业务过程

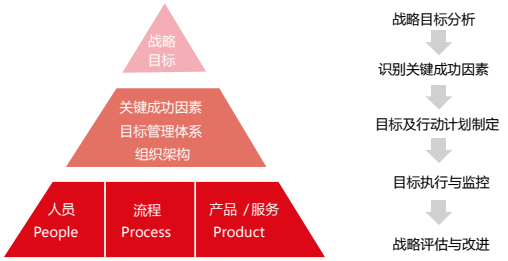
BSI 质量与标准化学院 高级项目经理 | 陈玉群

面对日益复杂多变的内外部组织环境，企业发展面临越来越多的不确定性，如何才能有效增强企业管理能力，越来越成为企业关注重点。近些年来，国际组织根据企业最佳实践制定并陆续发布了各领域的管理体系标准，如 ISO9001、ISO14001、ISO27001、FDIS45001（原 OHSAS18001），以及行业性的管理体系标准如 IATF16949、ISO13485、TL9000 等。这些标准为企业在相关领域的管理规范、能力提升提供了依据。然而，企业在导入各类管理体系的同时也遇到了越来越多的困惑：如此多类不同领域的管理体系，他们之间有什么联系，如何有效整合，如何减少业务部门执行的复杂性，如何确保体系与业务过程融合而不会出现两层皮运作现象等，这显然已成为体系人聚焦的问题。

2015 年 9 月 ISO 发布的质量和环境等管理体系标准采用了相同的高层次结构 HLS，而且未来 ISO 发布的各类管理体系标准将在结构、格式、通用术语和定义方面同样进行统一，这为企业对管理体系标准的有效整合和简约化奠定了基础。但实际应用中如何才能有效整合？根据 BSI 实践观察分析，目前许多企业的体系整合，仅停留在文档整合的层面，即简单地把共性的文件进行合并，如文控、人资、内审等，但这样的合并本质上没有改变管理性质。这实质上也没有真正很好地反映各管理体系标准 5.1 要求的 :“确保将组织的管理体系融入业务过程”。BSI 根据标准要求以及多年的管理实践，提出了“基于业务流程的体系整合”方法，这方法即符合标准精神，也为企业管理能力提升提供了机会。下面笔者简单谈谈企业如何开展基于流程的体系整合。

根据以往管理实践，常见的基于流程的整合项目步骤如图 1，一般包括前期诊断、情境分析风险评估、战略承接、职能梳理优化、业务流程框架搭

“根据以往管理实践，常见的基于流程的整合项目一般包括前期诊断、情境分析风险评估、战略承接、职能梳理优化、业务流程框架搭建流程梳理、制度文件完善、绩效评价机制建立、运行与验证、体系评价与改进等，根据企业需求不同项目过程会有所区别。”



搭建高效战略执行平台

建流程梳理、制度文件完善、绩效评价机制建立、运行与验证、体系评价与改进等，根据企业需求不同项目过程会有所区别。以下重点选择其中几个步骤简要介绍如何有效实施基于业务体系整合。

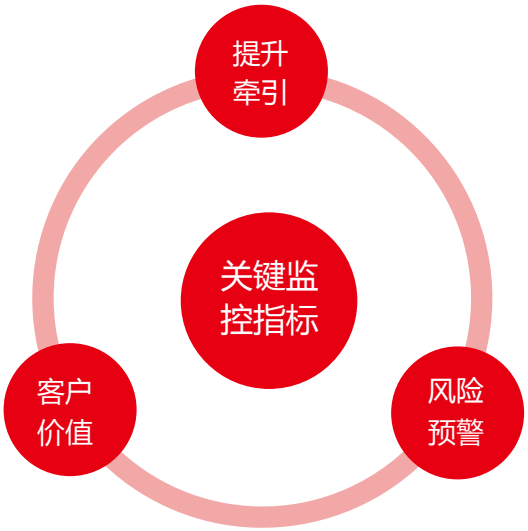
首先，谈谈组织情景分析与风险评估。组织情境分析、风险评估就是对组织面临的内外部环境、相关方需求和期望进行深入分析，了解可能面临的威胁与机会、优势与劣势，辨识风险和机遇。那么让我们先思考下我们为什么需要做这项活动。我们会发现企业在战略规划、经营计划、年度目标或年度重点工作计划制定、流程制度建设等业务过程中都离不开情境分析风险评估。比如年度目标或重点工作计划的制定，首先必须全面分析企业战略发展需求、以往目标执行状况、存在的风险或者说管理痛点，可能的机会等，才能明确后续的目标方向和工作重点；再比如企业流程梳理制度建设，同样必须根据以往信息了解相关业务管理现状、主要存在的风险和机遇，才能明确哪些流程制度是必要的、哪些环节该简化、哪些环节该管理细化或加严。

其次，谈谈战略承接。新版质量管理体系标准在“4.1 理解组织及环境、5.2 方针制定、9.3 管理评审”等多处提到了战略，明确指明了管理体系是为最终

实现企业战略目标服务的，体系方针目标必须与战略一致。即体系要求的方针目标管理，必须与企业的战略目标管理过程融合：对企业的战略进行分析 (4.1/4.2)，识别实现战略的关键成功因素，明确体系管理的重点 (6.1)，然后制定相应的目标及行动计划 (6.2)，并对目标进行监控 (9.1) 和定期战略回顾 (9.3)，这样才能确保体系方针目标与战略一致、确保部门行动协同高效。

再次，谈谈管理体系程序文件和制度建设。新标准弱化了对程序文件的强制要求，但对体系文件建立的适用性、有效性反而更加强化了。标准“7.5.1 成文信息”明确要求组织应确定确保体系有效性所需的成文信息，而且“5.1 条款”要求体系融入业务过程。但是如何有效建立文件并确保体系融入过程呢，实际上标准“4.4 管理体系”已非常详细地描述了业务流程建立、实施、保持和持续改进优化的方法，其方法类似大家所熟悉的 BPM（业务流程管理）方法，其包括识别组织关键业务流程框架地图，并理清各业务过程的职责分工、接口和相互关系及输入输出，形成简约、高效的流程或体系文件。导入的管理体系类型不管有几种，企业核心业务流程永远只有一个平台，故基于业务流程的体系整合，才能确保体系融入业务流程，避免两层皮现象。

最后，谈谈标准要求的绩效评价与改进。绩效评价是标准的第 9 部分，其要求组织首先确定需要绩效监测的内容、方法和时机。监测一般可分为定量和定性的两个维度。定量的绩效监测主要包括过程或结果 KPI 的监控等，可和企业绩效目标管理机制过程整合；定性的绩效监测方式方法很多，常见包括专业检查、过程审核、分层审核、体系内审、



绩效评价

成熟度评价等等。不管采用哪种方式，目的都是对业务过程能力进行有效监督监控评价。另外体系第 10 章改进要求，企业可以结合目前原有的改进活动，如 8D 改善、QC 小组活动、6Sigma 项目等。但对一个组织来说要有效推动持续创新改进，除了要学习改进工具方法，更重要的是建立一持续自我改进的文化。

ISO 发布的新版管理体系标准明确了管理体系是为实现企业战略目标服务的，业务流程是实现战略的平台，企业核心业务流程只有一个平台，导入体系类型再多都只是增加业务流程输入要求，各类管理体系只有基于业务过程的有效整合，才能确保体系融入业务过程，才能搭建一体化整合管理战略协同执行平台，才能实现简约、高效的系统管理，助力战略实现。■

图 1 体系整合项目推进过程

有效的增值审核，源自精心的策划

BSI 高级项目经理 | 唐爱丽

随着 ISO9001 质量管理体系，ISO14001 环境管理体系，OHSAS18001（即将发布的 ISO45001）的职业健康安全管理体系，ISO 27001 信息安全管理体系等等各种管理体系在企业中如火如荼的展开，基于这些管理体系中内部审核的要求，企业为了满足各项标准的要求，已经陆续进行了少则几年，多则十几二十几年的内审，很多人从内审“小白“成长为内审‘大咖”，但在年复一年的内审中仍然会有很多的困惑：

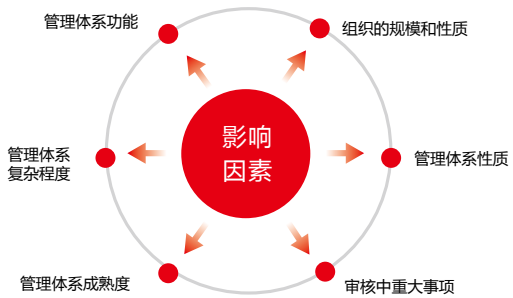
- 是否觉得每次的内审就是简单的重复上一次的内审？
- 是否担心内审对企业的价值越来越小？
- 是否觉得内审总不像外审那么专业？

如何更有效的策划企业内审，提升审核价值，一直困扰着很多管理者。

首先对于内审应有长期和全面的规划，建立审核方案的概念。

审核方案：针对特定时间段所策划并具有特定目标的一组（一次或多次）审核安排。由定义可以看出审核方案是一次或多次审核安排，企业在规划时，既要考虑当年的审核安排，也要考虑近几年的审核安排。此时可以参照第三方认证机构的做法，做出三年的审核方案，做到年年有重点，年年有不同。审核方案策划时至少要考虑“4+1+1”个因素（见图一），其中“4“是指要考虑管理体系自身的性质、功能、复杂程度和成熟度。企业在策划不同管理体系的审核方案时应结合自身管理体系的特点进行，而不是简单的把上一年的审核计划直接复制改个时间就可以了。随着各自管理体系推进，企业管理的成熟度也会不同，那么对管理体系的审核策划也应动态调整。以管理体系性质为例（见表一），可以看出不同管理体系的关注点和重点部门是有区别的。一个”1“，是指企业规模和性质，比如不同的企业规模，在策划审核方案时应有不同（见表二）。和另一个 1 是指重大事件，这些重大事件包括产品质量的关键特性、健康和安全的相关危险源或重要环境因素及其控制措施，这个概念通常称为基于风险的审核。

> 一次有价值的审核，不是简单的策划能够实现，也不是随便一个审核员就能实现的。



图一 审核方案影响因素 4+1+1

管理体系性质	审核策划时需要关注	
	线索（示例）	重点部门（示例）
质量管理体系	顾客需求 产品实现 质量风险	销售　工程 设计　售后 采购　人事 生产　质量 物流　.....
环境管理体系	重要环境因素 合规要求 环境风险	生产　行政 动力　工程 设备　售后 物流　.....
职业健康安全管理体系	危险源 合规要求 职业健康风险	生产　设备 行政　物流 动力　.....

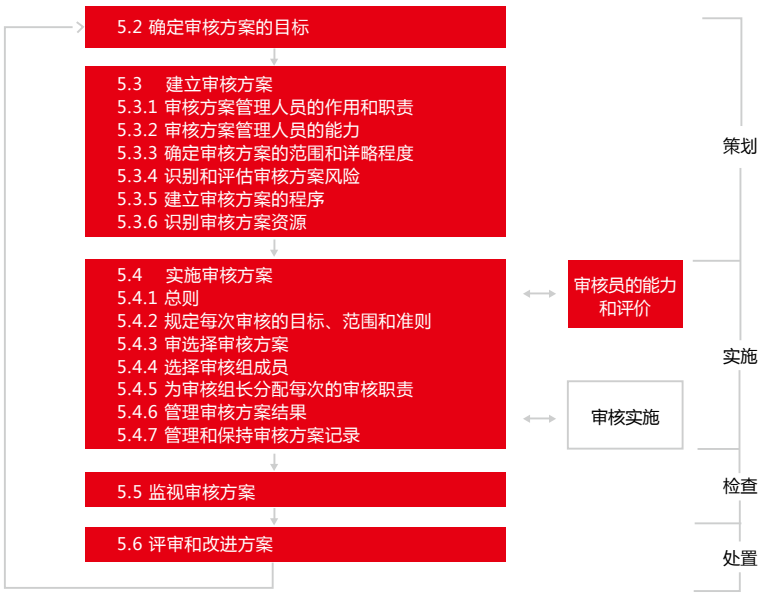
管理体系性质为例（表一）

企业规模	时间（示例）	策划方式（示例）	频次（示例）
中、小企业	3-5 天	审核计划	1 次 / 年
大型、集团公司	2 周以上	审核方案（总） 审核计划（分地点）	滚动

企业规模示例（表二）

其次应对审核进行管理，建立审核方案的管理流程。

现在企业在进行内部审核准备时，通常会比较关注三个方面，审核员审核技巧提升，对标准的理解，以及对企业内部业务流程的熟悉。除了这三个方面之外，还应对审核策划进行管理，参照 ISO 19011：2013 中的要求（参见图二），审核方案的管理要经过 6 步，除了关注审核方案的实施之外，向前看 -- 在建立方案之前，要清晰的知道审核方案的目标是什么，向后看 -- 在实施审核方案时要进行监控，在实施后还要进行评审和改进，即也要遵照 PDCA 的过程进行。在现场审核结束之后，如何完整、准确、简要和清晰的将审核记录梳理成引人入胜的报告，也是一项非常重要的工作。

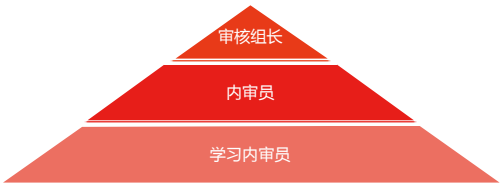


注：图中的条款号与标准中的条款号相对应。

图二 审核方案的管理 6 步曲

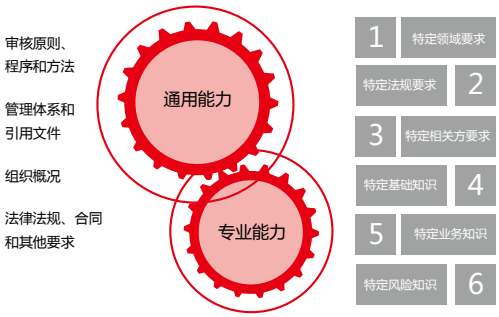
最后应对审核员进行有效的管理，建立审核员团队能力模型。

有价值审核过程的实施，另一个关键因素是内审员。管理体系内审员在企业中多数是兼职的，也有少数内审员是专职的。面对大多数的兼职内审员，有一个不可避免的挑战是内审员团队不稳定，人员水平参差不齐。企业可以考虑对内审员建立等级，明确内审员的晋升路线，并适当通过各层级的数量，实现金字塔式的稳定团队 (见图三)。



图三 内审员金字塔

同时对内审员有明确的能力要求，才能清晰给出对内审员的考核标准。内审员的十全十美能力模型（参见图四）中已经展示出内审员能力要求，既要包括通用能力，包括熟悉审核的基本方法、组织的管理体系文件、组织的基本情况（也就是各新版管理中提到的组织内外部环境）和法规 / 合同等要求，也要具备特定管理体系所要求的专业能力，比如审核环境管理体系，还应掌握生命周期评价、环境设计、环境报告、环境指标和统计等等。



图四 十全十美审核员

由此可以看出一次有价值的审核，不是简单的策划能够实现，也不是随便一个审核员就能实现的，需要体系管理人员首选要有基于“4+1+1”因素的审核策划，其次要对策划过程按照“6 步曲”进行管理，最后还要有“十全十美”的审核员才能保障。 ■

浅析云安全控制框架

BSI 高级讲师 | 万鑫

随着技术的成熟和商业模式的完善，云计算厂商的安全管理水平也在快速提升，许多大型云服务供应商已不再仅仅将安全管控停留在“点”和“线”的层级，而是从更高的控制框架这个“面”的维度思考和规划。笔者借助工作机会，较深入的接触了国际、国内顶尖的云服务供应商，他们或多或少的将安全控制框架的思想运用到具体业务运营中。本文简要介绍业界最主流的几个云安全控制框架，分别是国际标准 ISO/IEC 27001、行业模型 CSA CCM 和 TCI。

一、ISO/IEC 27001:2013—信息安全管理体系

ISO/IEC 27001 是全球范围内最受推崇、接受度最高的信息安全标准，它起源于 1995 年由 BSI 英国标准协会和英国工贸部联合编写的英国标准 BS 7799，现已发展为国际标准，最新版本为 2013 版。ISO/IEC 27001 遵循戴明博士提出的 PDCA（计划 - 实施 - 检查 - 改进）循环提升管理方法论，将组织的安全控制划分为 14 个控制领域，识别了 35 个控制目标，再进一步分解为 114 个控制措施。组织可以根据其所处的环境和利益相关方的需求与期望，基于风险评估的结果，有针对性的选择控制措施，用于自身的安全管理。下图 1 是笔者整理的 ISO/IEC 27001:2013 的控制措施框架：

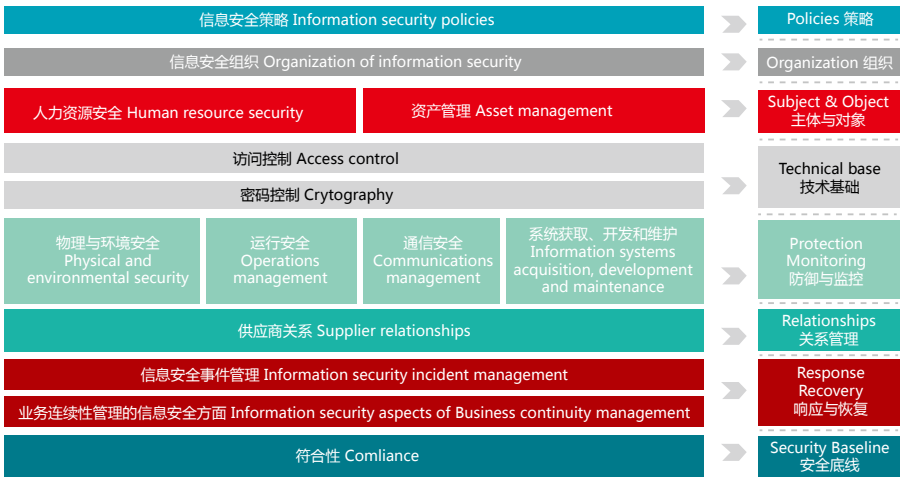


图 1 ISO/IEC 27001：2013 安全控制逻辑框架

二、CSA CCM —云安全控制矩阵

ISO/IEC 27001 作为信息安全管理的国际标准，在世界范围内获得广泛的认可和尊重，但该标准对特定行业安全现状关注还不够细致，特别是云计算环境下的信息安全问题尤为明显。而由云安全联盟（CSA）和 BSI 共同开发的云控制矩阵（CCM，Cloud Controls Matrix）正好对云服务的安全管理进行了补充和细化，CCM 在 ISO 27001 的基础上提出了针对云安全特定的控制措施，分为 16 个控制域、133 个控制措施。

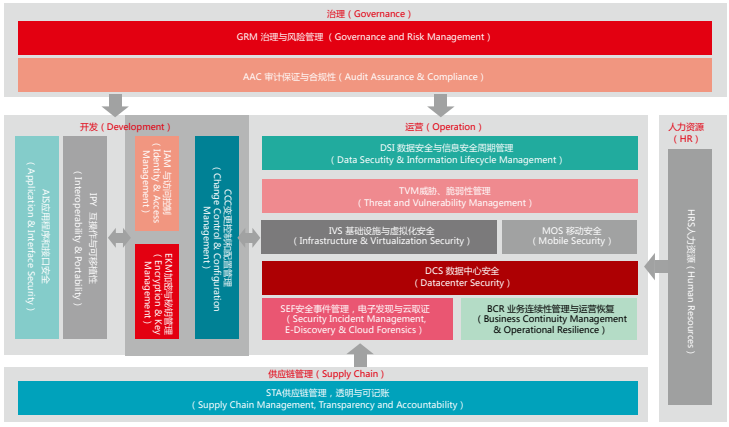


图 2 CSA CCM 安全控制逻辑框架

同样，笔者结合过往交付的云安全实践案例，对 CCM 的逻辑进行了梳理，形成了如下图 2 的控制框架。

CCM 是国际上第一个专门针对云计算安全提出的参考模型和控制框架，被众多知名的云服务供应商采纳。但遗憾的是，CCM 的条文以英文单词首字母的顺序进行排序，逻辑不太清晰，也不太容易理解。

同样，笔者重新梳理了各控制域中控制措施的逻辑，下图 3 是笔者整理的云服务身份与访问管理控制域 IAM（Identity & Access Management）的逻辑。

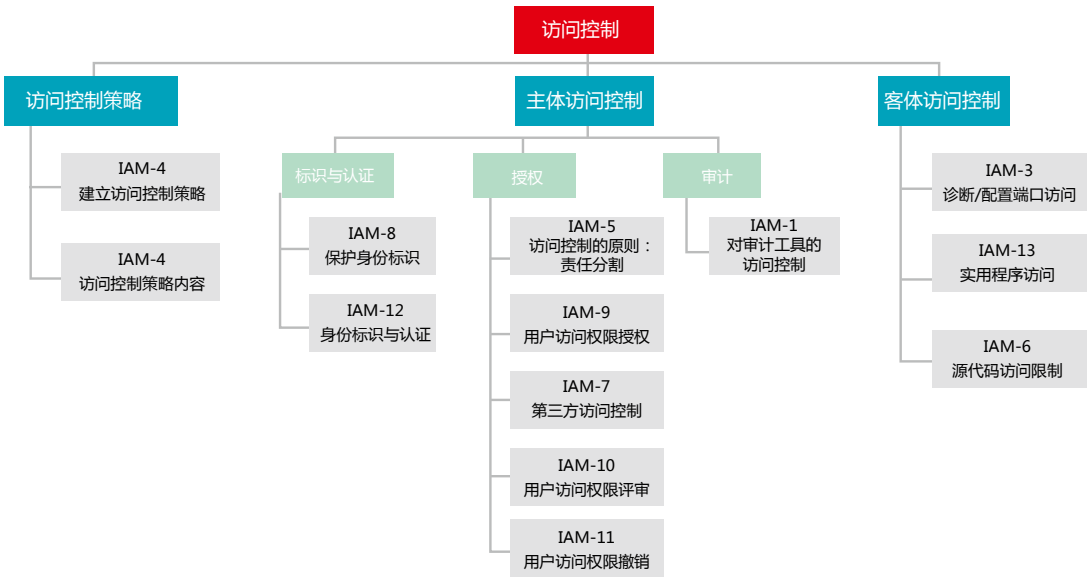


图 3 CSA CCM 的访问控制逻辑框架

三、CSA TCI—可信赖云计算倡议

CSA 在云安全领域进行了大量的调查和研究工作，提出了一系列的安全模型和良好实践报告，除上节所述的 CCM 之外，还推出了综合了 SABSA、ITIL v3、TOGIF、JERICHO 等众多 IT 框架的可信赖云计算倡议 (TCI，Trusted Cloud Initiative)。下图 4 是 TCI 的整体架构。

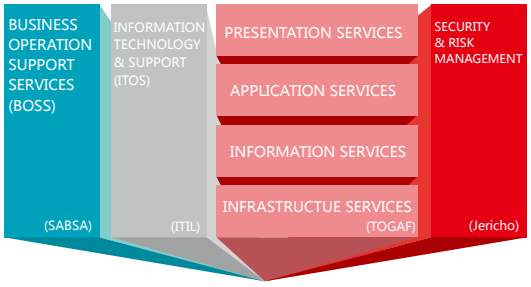


图 4 CSA TCI 整体框架

在该框架中，CSA 梳理了运营（BOSS，Business Operation Support Services）、运维（ITOS，Information Technology Operation & Support）、产品 (Product and IT Architecture)、安全 (Security and Risk Management)4 个云服务的关键职能的主要业务活动以及相关安全控制点。

TCI 框架分为四个层级，第一层是运营、运维、产品和安全这四个主要职能；第二层是每个职能负责的安全管理控制域，如安全职能负责的权限管理控制域；第三层是安全管理控制域里的安全管控对象，如权限管理域包括身份管理、认证服务、授权服务和特权管理四个管控对象；第四层是每个管控对象里的安全控制点，如身份管理包括域唯一账号管理、跨平台账号管理、账号提供、账号安全属性等控制点。

下图 5 是权限管理控制域列举的安全控制点。

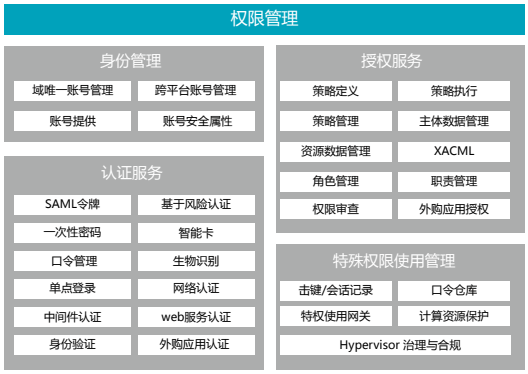


图 5 TCI 权限管理安全控制点

结束语

ISO/IEC 27001、CSA CCM、CSA TCI 均是语言精练但内容极其丰富的标准和框架，笔者深感其博大精深，限于篇幅无法展开描述，本文是笔者在长期的研究和实践中对标准框架的梳理和总结，旨在抛砖引玉，供大家参考和选择。更多内容，读者可在 BSI 的经典课程“ISO 27001:2013 信息安全管理体系主任审核员”和“注册 STAR 主任评估师”中进行了解。■

> 国内顶尖的云服务供应商，他们或多或少的将安全控制框架的思想运用到具体业务运营中。

从信息安全的视角看 DevOps

BSI ICT 高级讲师 | 汪明

出于种种原因，DevOps 与信息安全的关系若隐若现，本文尝试浅析这其中的“分分合合”，并澄清某些可能存在的误区。

1. 什么是信息安全？信息安全的关注点包含哪些方面？

所谓信息安全，不能简单、片面地解释为很多技术人员常常提起的“数据安全”、“网络安全”、“安全漏洞”、“安全攻防”或是“软件产品安全”。

广义的信息安全，应该是覆盖各类组织、各类业务和经营活动的一整套安全体系，可从三个维度加以构建：首先是构建人的安全能力、意识与责任；其次是构建由各方达成一致的、职责明确的安全规范与流程；再辅以与规范流程相匹配的安全控制技术手段。

广义的信息安全，也可以理解为针对敏感信息（如：企业商业秘密、用户隐私、关键信息系统配置和源代码等）保护，或是为保障业务持续稳定运行（即：业务连续性），而对包括数据、软件、设备设施、内外部雇员、内外包服务等在内的信息载体加以全方位的保护，以确保这些信息、信息资产、业务活动的机密性（Confidentiality）、完整性（Integrity）、可用性（Availability）。

国际标准 ISO/IEC 27001 可以帮助我们完整地理解真正意义上的信息安全，可用于指导各类型组织建立起遍布其所有业务和职能活动的信息安全体系。所以，下文中提到的所有安全控制点都能在 ISO/IEC 27001 标准中找到相应的要求。

2. DevOps 如何关注信息安全？

DevOps 最大的关注在于改善开发与运维团队之间的沟通与协作，并通过各种形式的自动化实施，以及简化软件开发与基础设施管理流程，来帮助加快企业的创新速度。同时 DevOps 也关注于质量保证 / 测试（QA）和安全保障，在高频率部署的同时，也强调保障生产环境的可靠、稳定与弹性，也就是保障企业的创新成果能够稳定的运行、运营，让企业更快、更多地创造价值。

DevOps 的一部分典型特征包括：

- 将大型复杂的系统拆分为简单独立的小模块（即：微服务架构）；
- 频繁地进行小规模、渐进式的功能更新与迭代；
- 逐步扩大使用范围的灰度发布部署模式。

在松耦合的系统架构下，每个具有单一特定目的或功能的服务既可以与其他服务相互独立运行，也可以相互接口形成一体化运行的结构，其降低了更新应用程序的协调开销，提升了应用系统的灵活性。而渐进式的迭代和灰度发布模式又能够降低每次部署的风险，还可以帮助运维和开发人员更快速地处理包括应用安全漏洞在内的各种错误异常，缩短系统不可用或功能异常的持续时间。

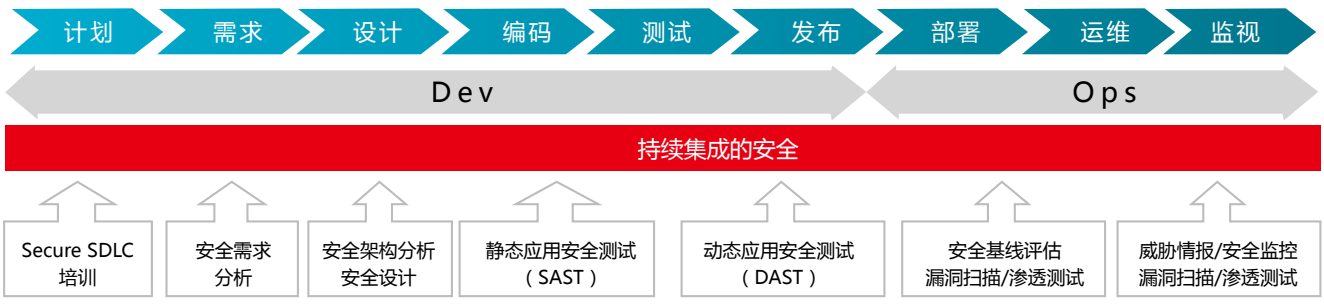
此外，依托于 CMDB 的基础设施管理自动化技术，也有助于维持计算资源的弹性和对频繁变更的适应性，再加上监控和自动化响应技术，又可帮助运维工程师快速响应和解决应用程序和基础设施的性能问题。

以上这些 DevOps 的典型特征，都是从可用性的视角来提升软件产品（即上文所提到的软件类信息资产）的安全，但却不能覆盖软件产品安全的所有方面。

3. 从 DevOps 到 DevSecOps

DevOps 的核心目的不是软件产品的安全，因此尽管在其相关理念或方法论中提及了安全，却并没有特别显性。但在互联网时代，不关注安全的互联网应用产品必将面临被安全攻击行为“秒杀”或是“薅羊毛”的威胁。

与传统的在开发阶段结束时才将安全注入到产品中的做法不同，DevSecOps 提出将安全融入软件产品开发全生命周期，包括：安全需求识别、安全设计、安全编码，



> DevOps 最大的关注在于改善开发与运维团队之间的沟通与协作，并通过自动化实施和简化软件开发与基础设施管理流程，帮助加快企业的创新速度。同时 DevOps 也关注于质保 / 测试（QA）和安全保障。

以及融入持续测试的安全测试。DevSecOps 同时也将安全职责落在了每个人身上，强调每个人都应具备安全意识和安全能力，而不再是专职的安全人员独自“背锅”。此外，DevOps 依赖于自动化手段，DevSecOps 自然少不了自动化，它也提出要使用自动化技术手段将安全以可编程的方式融入到开发和发布部署过程，而无需手动实现，也就是将安全非功能需求的实现加以敏捷化。

因此，DevSecOps 在软件产品安全方面，为 DevOps 作出了全面、坚实的补充。

4. DevOps 对传统安全管理的挑战

DevOps 提倡的是一种团队“融合”文化，但某些公司在实践 DevOps 时却产生了一些理解上的误区，于是违背了我们通常所说的“责任分割”、“权限分离”这样的安全原则和理念。

其实 DevOps 本质上并不是想违背传统的安全理念，对于“融合”，应理解为一种合作式的工作态度和企业文化，目的是为了高效的工作产出。在一些有着优秀的合作文化的传统企业中，弱化权限分离原则的做法也是存在的，但凡事总有个“度”，这种做法并不意味着责任可以模糊甚至免除，也不意味着权限可以完全的放开。DevOps 也并没有要求同一个人应该同时承担多个角色，比如不同团队在同一地点一起工作以减少沟通上的瓶颈和延迟，也是符合 DevOps 的实践方法。事实上，在一些优秀的互联网公司（如：腾讯）中，同样强调 DO（开发与运维）权限分离，而即使是 Google 这样的顶尖互联网公司，其 BeyondCorp 技术也只用在了办公网络，尚未听说它要将其用于关键的生产网络。

此外，自动化的部署流水线相当于在高效工作的同时，也解决了与“权限分离”原则间的潜在矛盾，而自动化的技术手段甚至可以更有效地规避人工违规操作，反而提升了“权限分离”安全控制的有效性。而在一些公司中，运维大数据分析和操作行为审计工具相结合的运用，可以在“权限分离”不足的前提下，即时识别甚至阻断高风险操作、违规操作，可以更加有效地控制操作风险。

综上所述，眼下流行的 DevOps 与安全之间其实没有什么不可解决的矛盾，就像 DevOps 与 IT 服务管理一样，二者反而是相辅相成、相互改进的。相信通过更多企业在 DevOps 方面的实践积累，能够在这些管理理念基础上形成更完整、更趋一致化的知识体系和方法论。■

公司治理进入数据时代

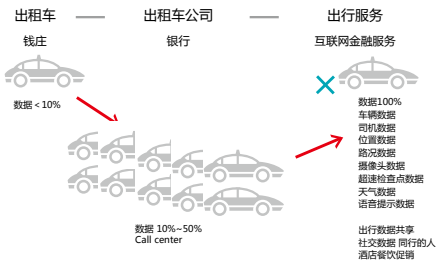
BSI 英国标准协会 | 潘蓉

从 2015 年国务院的《促进大数据发展行动纲要》到 2016 的十三五规划，及最新的十九大报告，都明确了国家层面的大数据项目与实施计划，明确了将大数据作为国家战略，行业转型的驱动力，大数据治理能力也是提高国家治理能力的体现。

十九大报告指出要推动互联网、大数据、人工智能和实体经济深度融合，培育新增长点。

数据正驱动业务转型，组织变革，甚至产业的垂直变革

我们一起来看出租车行业对数据的使用、依赖、创新和发生的变化

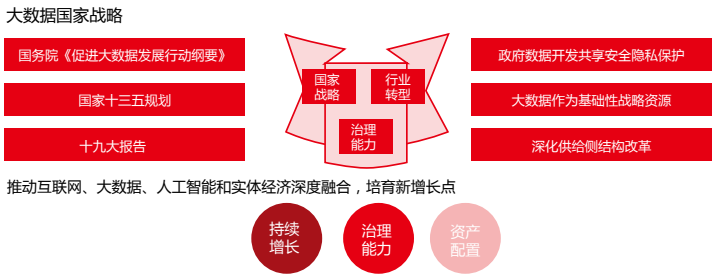


当你拥有一辆车，作为一个司机，你可以开始提供出租车服务了。你对数据的依赖度小于 10%；

当一家传统的出租车公司拥有多辆小汽车和司机，建立了呼叫中心，于是司机们开始上街提供扬招服务，也接受预订的派单服务；为了提高司机和车辆的利用率，降低油料等的损耗，出租车公司进行数据收集和分析，根据其管理的水平对数据的依赖度在 10-50% 之间；

各位都用过滴滴打车，这家公司有汽车吗？有司机吗？没有！它有什么？ 为什么它能提供出行服务？因为它有数据，它是 100% 的数据公司。

它有车辆的数据，车辆型号，位置，司机，乘客的联系信息，它也是一个基于数据的算法公司，它自动匹配最近的乘客与可以接单的司机。



甚至它可以在出行服务的基础上，结合不同的数据衍生出不同的服务和收费模式，比如根据需求与天气调节收费标准；根据到达位置提供附件的吃穿住等服务信息，获得相应的提成；根据起点和终点匹配合适的同行人，变为有社交属性的出行，也降低出行成本。

它还可以记录司机的驾驶习惯，综合驾驶结果，给保险公司提供保险核价参考，多整合一个维度的数据可能多过一项服务收入。

公司治理进入数据时代

数据已经改变了行业格局，也基于数据开拓了全新的业务或服务。对于上市公司董事会可以关注以下的趋势：

据通联数据肖风介绍，耶鲁大学的基金会，过去 20 到 30 年的时间里面，业绩非常好，超越它的大多数同行，很重要的原因或者 90% 的原因是来自于它对资产配置的创新，如果大家都按照最经典的资产配置模型配置自己的资产，那你的回报和其他人的回报一样的，不可能超过同行，远远打败你的基准的资产的业绩回报。它大量的纳入一些另类的资产到这个组合里面，理论界把这个总结叫做“耶鲁模式”。数字资产就是一种新的另类资产，在目前数字资产最主要的表现形式是数字货币，十年之后，我们可以断定，数字资产会成为我们另类资产非常大的门类。

趋势二 用户数据为中心跨界合作

	美的	滴滴
估值、盈利	3821亿/净利润150亿	3900亿/亏损
用户数	1.5亿个家电产品/年 7.5亿用户/五年的家电寿命	3亿下载客户 1500万车主 1400万订单/天
用户需求	豆浆机——黄豆（永和豆浆） 面包机——面粉，蛋糕粉	每次出行就有一次延伸需求跨界合作
积累数据 创造增长 智能家电 物联网		

各位都是上市公司的老总，可以看看资本市场对图中两家的估值。对比发现，亏损的滴滴估值数百亿美元，相比较净盈利的美的，它的商业价值在哪里呢？

滴滴大概有 3 亿下载了客户端的用户，1500 万车主，每天 1400 万订单。众所周知滴滴的主业是亏损的。亏损的原因是前期获客的成本、补贴，营销大战，收购并购，研发及平台运营的基本投入有关，随着时间和客户增长，这些成本会渐渐摊薄。

投资者给滴滴的估值，并不是仅仅因为打车这个主业，主业的营收会慢慢改变，

更重要的是是未来的预期。可以设想一个人经常以餐馆为目的地，以后就可以推荐餐饮美食；经常以写字楼为目的地，那就是个白领，可以推荐爆款优选……

也就是说聚集了大量用户的平台，通过大数据分析，为每个用户提供精准的延伸服务，才是滴滴资本价值的基础。

那么，每年销售 1.5 亿个家电产品的美的，不是也聚集了大量用户吗？原来传统家电企业对客户的接触基本为购买一次性的，最多有个售后服务。按照家电产品平均五年使用寿命计算，美的电器现在聚集了 7.5 亿用户。借鉴滴滴打车的模式，美的客户的的延伸需求也是很确定的，比如豆浆机用户是需要买黄豆的，电烤箱用户是需要买烘焙原料，电饭煲用户是需要买大米的，传统企业如果能收集客户的需求与行为数据，思考以用户需求为中心的延伸服务，美的未来可以比滴滴估值更高。

趋势三 标准指导 统一度量 横向可比

金融	制造	互联网
合规驱动 用户挖掘 征信风控	产品数据 设备数据 用户数据	用户画像 技术第一 成本生命线

不同行业的公司做数据治理的驱动力和主要方向不同，金融行业主要是合规驱动，聚焦征信风控，制造业主要是以产品、设备、用户主数据为主，驱动力是降低重资产的成本，提高产品质量、用户服务满意度；互联网公司是天然的数据公司，善于技术工具落地流程，讲效率和成本，以用户画像为主，提供各类 2C 的服务。

针对不同的驱动，ISO 38505 对组织的董事会和管理层提供了一套工具，从数据治理的价值、安全、合规几个方面，考虑数据全生命周期的策略，以实现数据价值。以标准为指导，并通过标准化的评估，才能对数据治理的能力与水平提供横向可比较可参考的指标。

ISO 38505 作为数据治理的国际标准，给出了 6 个原则和领导的 18 项思考方向和子任务。一年之初，万向更新，制定计划可以参考 ISO 38505 的原则和任务。

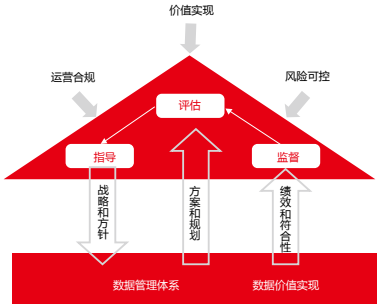
本次活动发布的《上市公司治理指标系统》，也是一个可视化的横向可比的数据化的公司治理度量系统。

公司治理之数据治理

宏观来看，数据成为国家战略，中观来看行业领先企业都在制定数据战略，微观来看，移动互联网新生代成为企业的新生产力，他们天生就是数字化时代的，作为一家企业的领导怎么看数据用数据，运营数据，获取新的增长空间，是亟需思考的。

数据治理需要公司治理层做什么？

ISO38505-1 标准通过模型和原则定义了 3 大任务 6 项原则 18 个子任务



三大任务包括评估、指导与监督，具体的活动下面举例但不限于

一、评估

- 数据的公司战略与商业模式
- 明确组织的数据责任人
- 数据技术工具的使用和流程的改变
- 生态圈数据共享的需求
- 内部数据文化，以正确的形式提供正确的信息，以协助各级决策
- 竞争对手对数据的使用
- 法规要求：个人数据保护，知识产权，跨境流动
- 数据泄露事件的应对

二、决定

- 最优化的数据投资，从组织对数据的投资中获得最大价值
- 基于风险偏好的管理数据风险，
- 各层级的数据保管人委派机制，基于数据的决定及责任制度

三、监管

治理层应通过适当的测量系统监测本组织的数据使用情况。它们应该能够保证自己与数据有关的战略得到了正确的实施，数据的使用和管理符合内部策略和外部要求，如规章和数据管理要求。

- 监管个人数据使用，采用 ISO 29100 的原则和方法
- 监管数据的存储和处理技术风险，采用 ISO 27017 的云安全指南
- 监管数据的利用成本
- 监管数据的质量报告

综上，数据治理能力是数字经济时代公司治理层当今需要具备的能力。■

领导的态度决定了资产配置方向，阿里的未来就是数据

——马云

数据是公司的核心资产，要像经营资本一样来经营数据

——任正非

本文摘自潘蓉在 2018 年 1 月上市公司董事会“金圆桌”论坛演讲的部分资料，面向读者为公司的董事会及高层领导，特别是在数字化时代亟需转型的企业高层。

快速入门，带您了解影响全球数据保护的最大的法规——GDPR（欧盟通用数据保护条例）

背景

随着科技发展，个人数据更容易被储存，运用及传达，大幅增加了隐私权的风险。欧盟委员会于是着手立法，于 2012 年提出通用数据保护条例（General Data Protection Regulation, GDPR）草案。

GDPR 简介

欧盟通用数据保护法规（GDPR）整合隐私保护指令、电子通信隐私保护指令、及欧盟公民权力指令，历经四年讨论方于 2016 年 4 月 27 日经欧洲议会通过，并**将于 2018 年 5 月 25 日正式全面实施**。

GDPR 也在近年来，影响全球数据保护作为最大的法规。不管你是法人或自然人，不论公司规模大小，拥有的欧洲民众个人数据多寡，只要你的核心业务直接或间接和欧洲民众个人数据的搜集、处理和利用有关的话，到 2018 年 5 月之前，都必须要从内部系统到资安政策及时调整，以便能够符合 GDPR 对于个人数据保护的规范和要求。

GDPR——强化数据保护和隐私权

GDPR 的这项改革对企业来说无疑有着深远影响，不仅欧盟境内的公司，所有接触、处理欧盟公民资料的企业组织也将收到影响。

GDPR 改革新制的目标：

- 强化个人隐私权，透过设计符合需求的政策，从法规层面入手
- 强化欧盟内部市场，透过制定清楚、周密的新法规，赋予个人自由转移数据的权利
- 确保新法规实施的一致性
- 设定全球数据保护标准
- 维护各行各业数据保护的黄金标准

企业组织只要有来自欧盟的客户、合作伙伴，就不能置身事外，首先须留意以下 **GDPR 的 7 个重点**：

1. 高额罚款

第一层：最高罚款 1 千万欧元或年度全球营业额的 2%，择金额较高者罚之

第二层：最高罚款 2 千万欧元或年度营业额的 4%，择金额较高者罚之

2. 个人数据删除权

如个人想收回个人数据处理权限，而持有单位无正当理由继续保存该数据，则须予以删除，并且须由数据收集单位负责证明数据有留存必要，而非由个人数据当事人（个人）负责举证。

3. 新法重新修订同意权概念，以确保个人数据使用透明度

收集资料时须充分且明确告知个人数据当事人资料的所有用途，且个人数据当事人现在得基于任何理由随时撤销同意。

4. 资料若外泄，须依法告知

现在若企业发现数据遭到泄露，须于得知 72 小时内汇报主管机构及通知受影响的个人数据当事人。

5. 个人数据可授权

新法规规定，个人数据当事人应有权利将个人数据从原本的数据持有单位（以常用电子格式）转移至另一单位，原持有单位不得阻碍干涉。

6. 隐私权政策设计

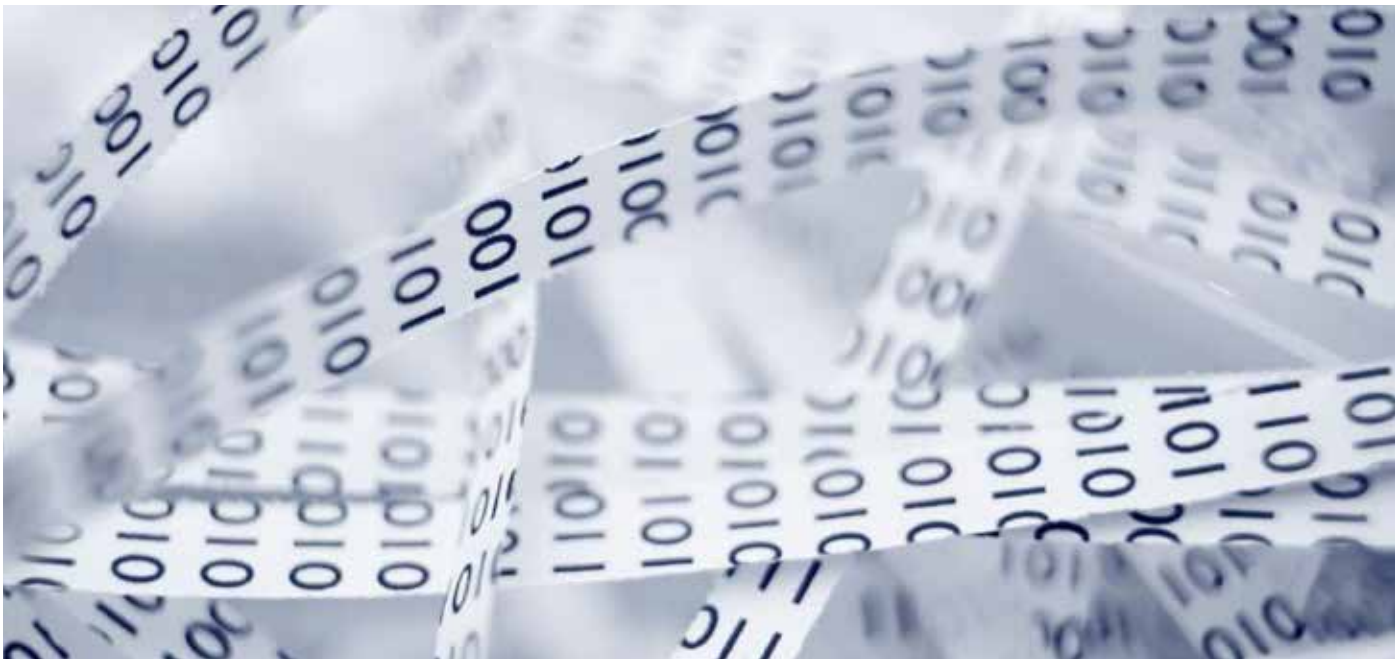
这是新法规的核心京申制衣，旨在改变业界整体思维，以及企业制定数据保护政策的方式。根据第 23 条法规，企业应根据业务程序发展，制定符合需求的个人数据保护政策。

7. 指派个人数据保护官（DPO）

企业现在必须指派个人数据保护官（DPO），而 DPO 须为独立职位，且向主管机构负责，而非董事会。

GDPR 规范的范围：

GDPR 除了适用在欧盟地区注册的企业，或者是不是欧盟注册的企业，但在欧盟营运，或者是，有搜集、处理或利用欧盟民众个人数据的企业或组织等，都在 GDPR 的规范中。



如何达成 GDPR 合规，完成【了解】、【执行】、【改善】三阶段

为符合欧盟 GDPR 法规要求，可依【了解】、【执行】、【改善】三阶段来逐步达成秉持合规状态。

【了解】

1. 董事会和高层主管的意识研讨会
2. 绘制数据资产工作流程
3. 差异分析
4. 法律和法规要求评估
5. 数据保护风险评估
6. 训练及员工教育

【执行】

1. 数据保护负责人（DPO）
2. 隐私权法规遵循架构研发
3. 数据保护和隐私权执行
4. 隐私权设计——隐私权影响评估及变更管理
5. 执行、运作和改善安全措施
   - 渗透测试
   - 加密使用审查
   - 时间管理和数据外泄
   - 安全控制
   - 当事人存取要求、包括电子见证

【改善】

1. 法规遵循专业能力审查
2. 法规遵循和保证评审
   - 隐私权合规审核
   - 内部审核
   - 独立第三方审核
   - 主管机构审核的准备
   - 验证（例如：BS 10012、 PCI DSS）

BSI 现能够为客户提供一些列最佳数据管理实践：

- ISO 27018 云隐私保护
- BS 10012 个人信息保护
- ISO 38505-1 数据治理

想要进一步了解，

可拨打 BSI 全国热线 400 005 0046

> GDPR 近年来，成为了影响全球数据保护作为最大的法规，将于 2018 年 5 月 25 日正式全面实施。如无法符合其要求，组织将可能面临高额罚款。

ISO 37001– 反贿赂管理新里程碑

BSI 英国标准协会中国区首席专家丨高毅民

ISO 37001 反贿赂管理体系介绍

一、前言

「近年来由于贿赂问题的日益严重，已成为国际间阻碍许多国家经济发展的重要问题」，这是世界银行多年来观察与执行反贿赂议题所做的结论。当全球每年以 1.5 兆美金进行商业贿赂，且有高达 30% 的企业通过贿赂来巩固或获取他们的商业利益，全球许多国家已意识到贿赂问题对于国家经济成长的严重冲击。BSI 英国标准协会作为全球标准机构之首，率先在 2011 年制订了「BS 10500 反贿赂管理体系 - 规范」，成为全球第一个针对贿赂管理议题的国家标准，且开启了全球反贿赂管理体系认证的趋势。

取之于英国在 BS 10500 反贿赂管理体系的成功推展经验，并考虑贿赂议题对于全球与许多国家在经济方面的严重影响，国际标准化组织 (International Organization for Standardization, ISO) 在 2013 年 成 立 PC 278 (Project Committee) 以开始相关标准的制订工作，并于 2016 年 10 月顺利公布了「ISO 37001 反贿赂管理体系 - 要求和使用指南」，这个标准的公布引起国际间对于「反贿赂与合规」的重视。

二、ISO 37001 的特色

ISO 37001 标准具有以下的特点：

1. 适用于各种不同类型的组织

各国专家在讨论此标准时有一个很明确的共识，就是 ISO 37001 反贿赂管理体系标准应该适用于各种不同类型的组织，包括公共组织、商业机构，甚至是非营利机构。因为现今的实际状况，各种类型的组织形态虽具有不同程度的贿赂风险，但都面临相同的威胁。

2. 管理体系的功能

ISO 37001 标准对于贿赂风险管理的主要功能有三个，即预防 (prevent)、发现 (detect) 以及处理 (respond)，也就是

> BSI 英国标准协会作为全球标准机构之首，率先在 2011 年制订了「BS 10500 反贿赂管理体系 - 规范」，成为全球第一个针对贿赂管理议题的国家标准，且开启了全球反贿赂管理体系认证的趋势。

建制此管理体系标准的主要目的。此标准强调预防在先的思维，并在可能发生贿赂事件之处早期侦测，最后，如果不幸发生贿赂事件时，必须及时处理后续相关的问题与后果，并采取有效的纠正和预防措施。

3. 基于「风险评估」的管理

任何组织的贿赂事件都有其不同的风险分布，例如一般而言，组织内部的采购与销售部门的贿赂风险会比其他部门明显高出许多，而外部合作伙伴的风险则可能随着行业与地区等的不同而有极大的差异。是故，组织应该对自身的贿赂风险进行评估，以便将风险控制的资源合理分配在风险较高之处。

4. 采用 ISO 管理体系的「高层结构」

依循 ISO 对于管理体系标准制订的原则性要求，ISO 37001 采用 ISO 的高阶结构 (High Level Structure)，请参见图一与图二。从图一可知，ISO 37001 管理体系的模型与其他主要的管理体系，包括 ISO 9001、ISO 14001、ISO 45001，都是一致的，这就便于 ISO 37001 与其他管理体系整合。唯需注意一点，ISO 37001 体系的输入多了「反贿赂风险评估」，这是与其他管理体系不同的地方。

5. 通过认证展示于外部

由于 ISO 37001 也是一个认证规范，所以此标准是可以认证的，ISO 也希望通过认证的机制扩散其影响力，并协助不同类型的组织落实贿赂风险的管理。截至目前为止，全球通过 ISO 37001 认证的组织大约估计在 100 个左右，预计这个数目将在未来几年快速成长。

三、企业实施 ISO 37001 的好处

企业实施 ISO 37001 会有以下的好处：

1. 减少法律诉讼的可能性

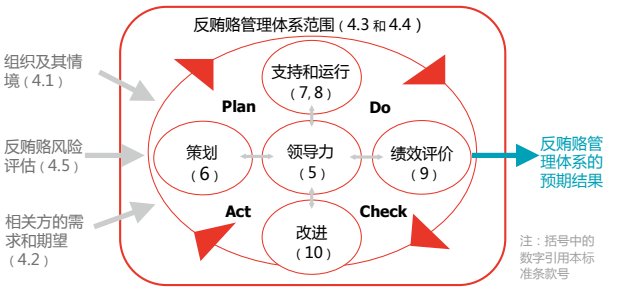
由于 ISO 37001 着重于预防贿赂事件的发生，而其相关的管理要求可减少因贿赂而造成法律诉讼的可能性。

2. 减少因法律诉讼造成的巨额罚款

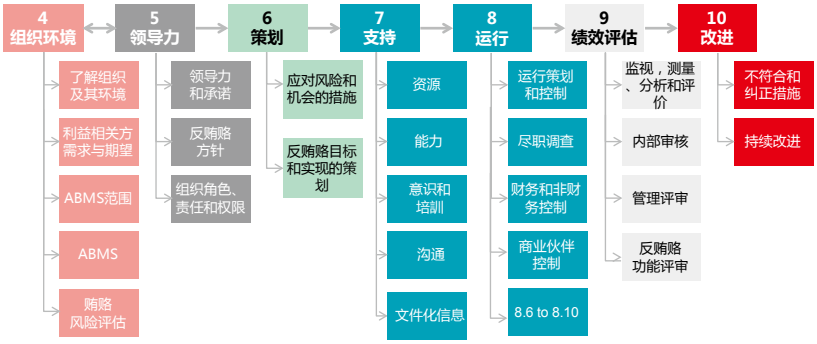
国际间不同国家反贿赂的相关法律虽有所不同，但有一件事却是相同的，就是当组织可以举证已尽其所能预防与避免贿赂事件的发生，法律将减轻甚至免除其法律责任与罚款，而 ISO 37001 反贿赂管理体系的执行记录可提供组织作为法律所需的相关证据。

3. 管控高贿赂风险

通过 ISO 37001 的风险评估，了解自身风险的分布，将管理资源合理的分配在高贿赂风险之处，



图一 ISO 37001 结构与模型



图二 ISO 37001 反贿赂管理体系总览

有效管控高贿赂风险。

4. 向相关方展现健全的合规管理

依据 ISO 37001 建制有效的反贿赂管理体系，可向相关方包括客户、政府机构、合作伙伴等，展现合规的决心与能力。

5. 通过认证展现符合性

由于 ISO 37001 是一个可认证的标准，组织可选择通过认证向相关方展现自身甚至供应链管理对于 ISO 37001 的符合性，以获得相关方对于组织合规性的信心。

四、结语

在 ISO 37001 公布之前，全球有许多国家制订该国家在贿赂 (或贪腐) 方面的国家标准，其中包括最早公布的英国国家标准 BS 10500。随着 ISO 37001 的公布，这些国家逐渐采用此国际标准，使得各国对于反贿赂这个议题有了共同的看法与相互交流的语言。也随着相关系列标准的讨论与陆续发布，许多反贿赂管理的最佳实务也获得了共识，为全球各国在反贿赂议题上的努力提供着极大的帮助，所以，ISO 37001 的公布成为了全球反贿赂管理的一个新里程碑。■

王平
BSI 食品部总监

> SQF 规范认证是特定场所、过程和产品的认证标准，强调系统性的应用食品法典委员会 HACCP 原则与指南，来控制食品安全与食品品质危害。

SQF 规范认证助力食品链的管理

SQF(safety quality food) 是全球食品行业，安全与质量体系的标准。SQF 标准于 1994 年在澳洲首次开发，自 2003 年起由美国食品零售业公会 (FMI) 拥有与管理，2004 年首次获得全球食品安全倡议 (GFSI) 认可为符合其标杆要求的标准。

SQF 规范认证是特定场所、过程和产品的认证标准，强调系统性的应用食品法典委员会 HACCP (CODEX Alimentarius Commission HACCP) 原则与指南，来控制食品安全与食品品质危害。

SQF 认证可支持企业或公司品牌的产品，也为取得认证的场所与其客戶带来益处。SQF 系统的执行能解决购买方对于食品安全和品质要求，且提供企业供应当地与全球食品市场的解决方案。根据 SQF 规范认证所生产的产品，在全球市场保有高度接受度。

食品安全及品质协会 (SQFI) SQF 规范第 8 版已经于 2017 年进行更新並重新設計，供食品行业（从初级产品生产到储藏和配送）所有行业使用，现包含零售商的食品安全规范。第八版于 2018 年 1 月 2 日正式实施，现包括以下标准：

- 生产的 SQF 食品安全规范
- 食品零售的 SQF 食品安全规范
- 包装材料生产的 SQF 食品安全规范
- 初级生产的 SQF 食品安全规范
- SQF 品质规范
- 食品储藏和配送的 SQF 食品安全规范

取得经食品安全及品质协会认可的审核机构所核发的 SQF 认证证书，並非保证该场所所生产的产品安全，也并非保证符合所有食品安全法规的声明。然而，此审核确保该场所的食品安全计划已根据食品法典 (CODEX) 中的 HACCP 方法以及适用的法规要求执行，并且该系统已获得认证与判定为可有效管理食品安全。此外，这也声明该场所对于下列事项的承诺：

1. 生产安全高品质的食品；
2. 遵守 SQF 规范要求，
3. 遵守适用的食品法规。 ■

BSI 可以帮助食品行业进行 SQF 的相关认证。如有需求，请联系：

拨打热线 400 005 0046
邮件至 infochina@bsigroup.com
关注 BSI 官方微信 BSI __ China

为什么选择 SQF ？

ONE WORLD.ONE STANDARD.

SQF 标准

SQF 是唯一适用于**整个**供应链的标准；从初级产品生产到食品加工、分销和食品包装。

SQF 是唯一使用 HACCP 方法识别和控制食品质量危害的标准。

SQF 是唯一有单独的标准来评估“**质量**”属性并允许在产品上或进行营销时展示质量盾牌标志的标准。

SQF 是唯一要求由指定的**现场从业者**负责体系实施和维护的标准。

SQF 支持

SQFI 是唯一提供全职**客户服务**和支持中心的 GFSI 计划。

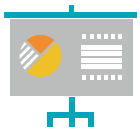
面向希望在食品安全和食品科技领域供职的本科生和研究生的**奖学金**机会。

与支持 SQF 体系实施和维护主题相关的免费**网络讲座**。

唯一在线免费提供所有**文档**和指南信息的计划。

SQF 体验

作为 FMI 的分支，SQFI 与**食品零售商**以及相关监管机构（ 例 如，FDA、FSIS、AMS 和 USDA）有直接联系。



SQFI 以在线方式或者通过我们获得许可的培训中心提供广泛的**培训课程**。

SQFI 对所有获得许可的 SQF **审核员**进行培训，并且拥有由任何 GFSI 计划美国审核员组成的最大的网络。

SQFI 举行年度教育和联谊**会议**，有 700 多利益相关方参会。

欧盟新法规（EU）2016/425 来了，您准备好了么？

——个人防护装备 PPE 新法规浅析

刁立新
BSI 高级讲师

BSI 作为首批获得 PPE 法规证书颁发资质的公告机构，确认具备能够颁发（EU）2016/425 新法规证书的授权。

根据欧盟要求，2018 年 4 月 21 日新 PPE 法规（EU）2016/425 将正式生效，届时，原 PPE 指令 89/686/EEC 将被废止。

欧盟新法规（EU）2016/425 作为强制性要求，凡是在该法规管辖范围内的个人防护装备产品出口到欧盟地区必须符合该法规要求。该法规于 2016 年 4 月 21 日在官方公报中发布，并给予成员国和公告机构 2 年过渡期用于准备引入该新法规。

面对实施已迫在眉睫的新法规，您准备好了么？

首先我们来看一下，相较原指令，新法规较为显著的几点变化：

1. 听力防护 PPE 产品类别由 II 类变为 III 类；
2. 救生衣类 PPE 产品类别由 II 类变为 III 类；
3. 为某些特别用途所专门订制的 PPE 也进入了 PPE 法规的管辖范围；
4. 证书有效期被强制要求不得超过五年；
5. 针对每个 PPE 产品均须出具一份符合性声明或提供一个可以获得该声明的链接；
6. 对进口商和经销商提出明确要求，

其次，对于不同类别 PPE 产品，与原指令相比，新法规下执行的产品合格评定程序也有一定的变化：

PPE 类别	新 PPE 法规 (EU) 2016/425	备注
I 类 Simple PPE	Module A	制造商自我声明
II 类 Intermediate PPE 和 III 类 * Complex PPE	Module B 与 Module C	EU 型式测试
III 类 Complex PPE	Module B 与 C2 或 Module B 与 Module D	含持续监督（测试） 或持续监督（审核）
* 仅指某些特殊情况下的 PPE 产品		

此外，对于 PPE 新法规来说，除了 PPE 法规所覆盖的产品本身必须满足该法规的要求之外，整个产品供应链的各环节也必须遵守此法规要求。这意味着，当新法规生效时，不仅对于商品的制造商，而且对于商品的进口商、经销商或任何其他参与供应和分销的链条中各环节也要求其必须采取适当的措施来确保只有符合法规要求的产品才能在市场上销售。

那么作为进口商，需要格外关注哪些问题呢？其中主要包括：

- 进口商只能将符合法规要求的 PPE 产品投放市场；
- 在将 PPE 产品上市前，进口商应确保制造商已执行了相应的符合性评估程序，

并起草了相关技术文档。而所有产品上已按照要求标注了 CE 标志；

 当进口商认为或有理由相信该 PPE 产品不合格，则不应投放市场，且应通知制造商和相关市场监管当局；

 进口商要在 PPE 产品上标注其名称、注册公司名称或注册商标以及可联络到的邮寄地址。而这些联系信息须使用能够被最终用户以及相关市场监管部门所理解的语言来书写；

 进口商要确保在其管控下，PPE 产品的仓储和运输条件不会危及其符合性；

 在某款 PPE 产品投放市场后的 10 年内，进口商必须保存该产品的欧盟符合性声明，且可随时供市场监管当局查阅，并确保在监管部门要求时，进口商可以即时向该监管部门提供该 PPE 产品的相关技术文档；

 在有关的国家监管部门的合理要求下，进口商须能够向该监管部门以纸质或电子文件的形式提供相关 PPE 产品的信息和技术文档从而证明该 PPE 产品的符合性。而这些资料须使用能够被相关监管部门所能够理解的语言文字进行表达。另外，进口商须积极配合有关监管部门针对已投放市场的 PPE 产品采取必要的措施以消除这些 PPE 产品可能带来的风险。

而经销商同样需要关注以下几点：

 将 PPE 产品投放市场时，经销商须关注 PPE 法规的要求，确认该产品的符合性；

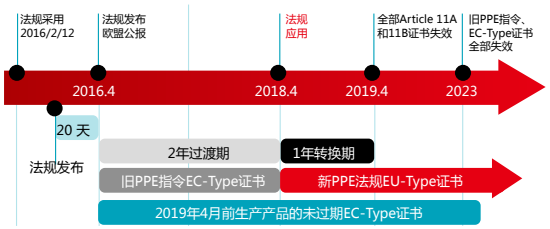
 在 PPE 产品投放市场前，经销商应核实 CE 标志已被标注在产品上，而其所附带的相关文档及说明书使用能够被消费者或其他最终用户所理解的语言表述。除此之外，经销商还须确认制造商和进口商是否已按照法规要求将他们的名称、商标或者注册商标、联系地址信息标注出来。而产品型号、批号或序列号等重要的产品识别信息也须标注在产品或法规允许标注的位置；

 经销商要确保在其管控下，PPE 产品的仓储和运输条件不会危及其符合性；

 如果有理由认为已投放市场的 PPE 产品不符合本法规，经销商应采取必要的纠正措施修正这些问题，或对这些问题产品予以撤回或者直接从市场上召回。此外，如果经销商发现某些 PPE 产品具有某个风险，经销商要立即向相关国家监管部门报告该风险详情，并就这些不符合的问题点给出详细的纠正措施。

 在国家有关监管部门合理要求下，经销商须能向其以纸质或电子文件形式提供相关 PPE 产品的信息和技术文档从而证明该 PPE 产品的符合性。而这些资料须使用能够被相关监管部门理解的语言文字来表达。另外，经销商须积极配合有关监管部门针对已投放市场的 PPE 产品采取必要的措施以消除其可能带来的风险。

在了解以上各相关方须关注的责任义务后，执行的时机便显得尤为重要。与 PPE 新法规执行有关的几个重要时间点，请务必把握：



-PPE 指令 89/686/EEC 将于 2018 年 4 月 21 日起废止

- 自 2018 年 4 月 21 日起必须使用 PPE 法规（EU）2016/425

- 成员国在 2019 年 4 月 21 日前不得阻止旧 PPE 指令 89/686/EEC 覆盖下产品进入市场

- 原 89/686/EEC 指令下的 EC 型式测试证书在 2023 年 4 月 21 日前仍然有效，除非证书在该日期前已到期。

BSI 作为首批获得 PPE 法规证书颁发资质的公告机构，确认具备能够颁发（EU）2016/425 新法规证书的授权。作为历史悠久底蕴百年的 PPE 认证机构，我们将一如既往在头面部，四肢和躯体以及呼吸等 PPE 领域为使您持续满足新法规要求提供助力，继续为您的 PPE 认证项目保驾护航！ ■

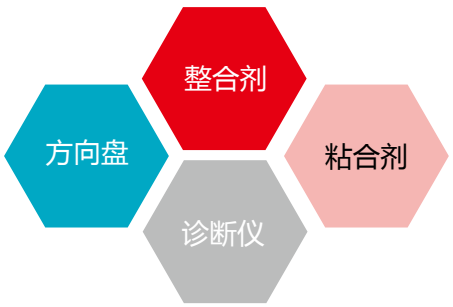
卓越绩效模式下的管理思维

张伟龙
BSI 商学院院长

卓越绩效模式(Performance Excellence Model)是通过综合的组织绩效管理方法，使组织和个人得到进步和发展，提高组织的整体绩效和能力，为顾客和其他相关方创造价值，并使组织持续获得成功。

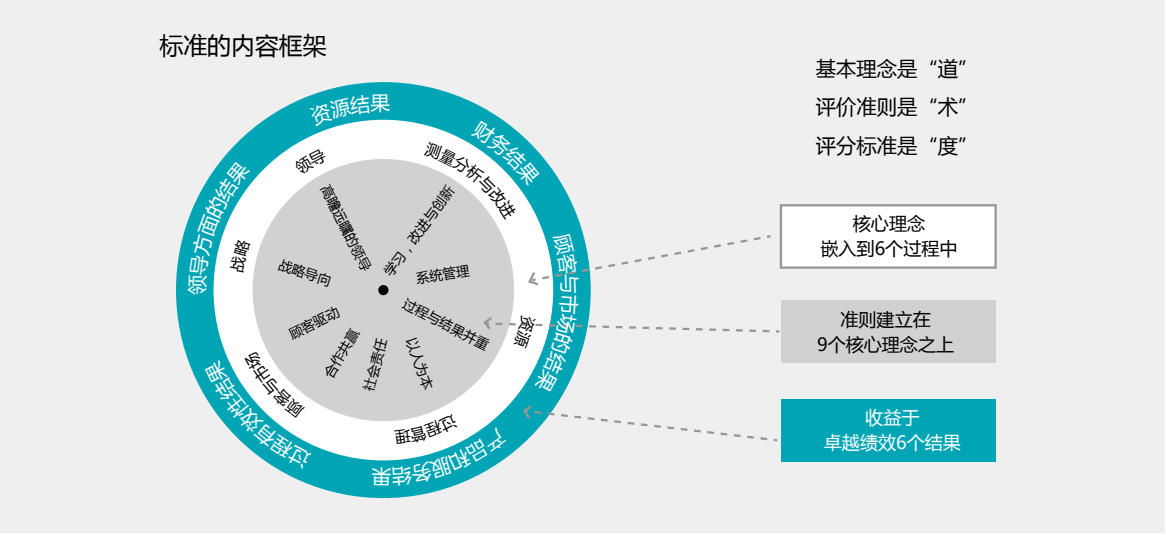
瞬息万变的当今世界，顾客需求不断变化、高质量诉求不断提升、技术创新不断加速，在这种世界经济一体化的浪潮下，如何提高组织绩效与竞争优势、如何保持持续成功与追求卓越，已然成为全球企业必须正视的一个重大课题。进入二十一世纪的中国企业如何进一步提高质量管理水平，如何实现以“战略为统领”、以“顾客以导向”、以“重视过程和关注结果”以及以“学习与创新为基础”的竞争优势，已然摆在广大获得 ISO9001 质量管理体系认证企业面前的现实问题。解决这些问题的有效方法 --- 世界级成功企业公认的提升企业竞争力的“卓越绩效模式”已得到广泛认可，同时也成为我国企业在新形势下经营管理的努力方向。

卓越绩效模式(Performance Excellence Model)是通过综合的组织绩效管理方法，使组织和个人得到进步和发展，提高组织的整体绩效和能力，为顾客和其他相关方创造价值，并使组织持续获得成功。其内容全面、系统，囊括了组织经营管理的方方面面，强调组织治理、战略管理、顾客导向、绩效监控和经营结果等内容，它所关注的质量已扩展到经营质量，同时使全面质量管理 TQM 更加规范化、条理化、标准化。



卓越绩效模式，在九项基本理念的引导下，通过对六大过程和六大结果进行评价，全方位地诊断组织经营管理的成熟度水平，为企业的有效管理发挥着巨大作用。卓越绩效模式的导入，有利于制定企业发展战略规划，确立核心价值理念，引领企业发展方向，使企业的市场开发、资源配置及绩效分析等围绕战略展开，明确发展目标，指明发展方向，起到企业发展的“方向盘”作用；通过成熟度的评价，对照卓越绩效评价准则在各工作领域开展自我评价，有利于查找出企业发展中存在的问题和不足，为企业提升管理水平奠定基础，起到企业管理的“诊断仪”作用；实施卓越绩效管理模式，在确定组织的使命和愿景后，对照标杆、坚定信心，使全体员工团结一致向目标前进，横向密切配合、纵向整体推进，有利于增强企业凝聚力和发挥整体效能，起到企业发展的“粘合剂”作用；企业管理经过长期积累，各领域、各板块都采用了不同的管理工具和多种管理方法，形成各种管理体系，实行卓越绩效管理模式有利于减少管理过程中不必要的重复和资源浪费，有利于提高全局管理的系统性和协调性，起到企业管理的“整合器”作用。

世界各国许多企业和组织纷纷实施了卓越绩效管理模式，并取得了巨大的成就。在国外，通用、微软公司等世界级企业都是运用卓越绩效模式取得出色经营结果的典范。在国内，为了贯彻落实国务院的《质量发展纲要》，深入推进质量兴邦战略，引导企业正确理解和实施卓越绩效管理模式并提升企业质量管理水平，我国于 2012 年



对《卓越绩效评价准则》（GB/T19580：2004）进行改版升级，并且国家质检总局和中国质量协会分别实施了以此标准为重要评奖依据的中国质量奖和全国质量奖的评奖事宜，比如中国航天科工集团、上海大众就是获得全国质量奖的知名企业，与此同时各省市的质检部门也正开展此类活动。再比如，烟草行业的优秀管理典范厦门烟草工业有限责任公司自 2012 年起，就已按照卓越绩效管理思维，利用卓越绩效评价模式梳理和整合各层级的管理要求、促进管理模式的上下一致、左右协同，通过搭建“四大管理系统”、稳步践行“企业级、职能级、部门级、班组级、岗位级”等五层级卓越绩效落地机制，例如在企业层级相继构建并运行了“领导战略目标绩效一体化”、“运营管理集成化”、“综合绩效分析与洞察”、以及“基于三驾马车的综合创新”等机制，促进了企业管理水平的快速提升，在提高了经营质量的同时也为实现公司的愿景提供了有力保障。

最后把**美国前总统克林顿在颁奖时的一段话作为本文章的结束语送给每位读者：**“马尔科姆 . 波多里奇国家质量奖在使美国经济恢复活力以及在提高美国国家竞争力和生活质量等方面起到了主要作用……”■

信息安全管理7问

陈颢明

信息安全圈的老兵，从业**17**年
目前是海航科技集团 信息安全总监
2017-10/2015 中国惠普
信息安全服务部门总经理

Q:《标准+》杂志编辑

A: 陈颢明

Q:《网络安全法》颁布以来，对于企业信息安全管理是否起到了积极的推动作用，影响如何？

A: 去年6月《网络安全法》颁布后，全国范围掀起了学习《网络安全法》的热潮，首先，有法可依是企业信息安全管理体系落地的基础，尤其是对于关键基础设施的明确定义，帮助企业明确了信息安全管理的策略和机制，明确了网络运营者的安全义务，明确了敏感数据保护要求。提升了企业安全管理者在企业的话语权，安全管理得到了业务和行政管理部门的高度重视，信息安全管理的执行和落地更加顺畅和高效了。

Q: 如何做好企业信息安全管理， 您有什么秘诀吗？

A: 凡事都得专业度+勤奋细心+智慧才能把事情做好，信息安全也一样，我并没觉得自己做的有多好，因为信息安全管理的范畴和领域太多。通常我做信息安全管理有两大法宝： 一个是ISO27001体系的PDCA，把信息安全管理形成闭环和循环上升的状态。 第二个是 PDR 信息安全技术防御模型，按照防御，检测，响应的理论来构建安全技术体系，关键是建立企业强大的信息安全检测和响应能力。

Q&A

Q: 信息安全的管理和技术是如何区分和整合的？

A: 理论上讲，信息安全是管理和技术融合的学科，是复杂的综合性学科，做好信息安全需要技术和管理的融合。但真正兼具管理和技术思维的人毕竟是少数，以我的经验，我更倾向于纯粹的人，也就是或者是纯管理思维的人，或者是纯技术思维的人，通过细化的管理流程把大家的工作和经验整合起来。这样避免了思维上的冲突，还能发挥各自的优势。

Q: 能展望一下未来信息安全发展的趋势和方向吗?

A: 个人认为信息安全大趋势不会变，并不会像一些人想得，越来越重要，也不会说关注度减弱，对于企业而言信息安全是常态化工作，是稳定需求。当然，新技术会推动信息安全技术的提升和发展，包括：大数据和人工智能。尤其是数据安全和用户行为安全，个人认为可能是未来安全创新的趋势和方向。

Q: 信息安全的管控和便利是个茅盾，如何平衡两者的关系呢？

A: 这个问题确实是最困扰我们的问题，用户，业务部门，企业高管其实天天都绞尽脑汁在提速，在创新，在转型，大部分的安全管控功能是反向的，是对他们业务活动的限制，很多安全功能还带来用户体验的降低。这里面涉及的问题很多，关键点是需要企业信息安全管理团队要充分了解和熟悉本企业的业务，针对业务情况给出科学合理的评估结论：放弃某个安全控制点导致的业务损失程度和损失概率，充分相信领导的智慧和对全局的视野。

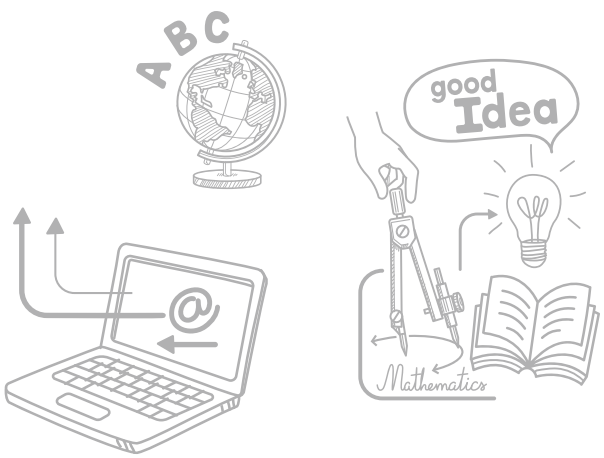
Q: 互联网，新商业模式，新技术的不断涌现，对于信息安全管理的冲击和影响大吗？您如何应对这些影响？

A: 影响非常大，信息安全管理者需要不断地快速学习，现在安全技术人员已经青黄不接了，更关键的是所有这些新的东西对于原有的信息安全技术和产品是巨大的颠覆，原有的防护体系已经不兼容了。最好的办法其实也没啥好办法，就是颠覆自己，主动改变。比方说，企业现在导入devops方法进行软件开发和运维，那安全就得考虑从软件生命周期去嵌入安全控制点，对于云架构和大数据，就得考虑自适应安全，对于物联网就得考虑微小化的安全模块。

Q: 您理想中企业信息安全管理的状态应该是什么样子？

A: 安全功能自适应嵌入式，发现和检测智能化，管理流程工具化，安全响应工单化，控制措施自动化。

作为信息相关标准领域的引领者，BSI一直致力于信息安全管理、网络安全、隐私保护、云安全等标准的发展，帮助诸多行业标杆建立了强劲的信息韧性，我们也很高兴与这些标杆客户携手合作，为广大客户不断提供最佳经验，一起努力践行安全之路。



职业健康安全管理体系（ISO 45001:2018）正式发布

BSI权威新标解读 尽享先发之势

BSI ISO 45001:2018系列课程 全国盛大启动

《BSI ISO 45001:2018实践者课程》

《BSI ISO 45001:2018内审员课程》

《BSI ISO 45001:2018标准精要课程》

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