

一、 什么是 IT 多管理体系融合咨询

随着信息技术的不断发展深化，企业开始逐步通过建设各类管理体系并通过认证来提升自己的管理水平，常见的管理体系包括ISO27001 信息安全管理体系、ISO20000 IT服务管理体系等，为了确保企业内部各类管理体系的有效运转，提升管理体系运作效率，降低类似工作的重复开展，企业有必要开展多管理体系融合咨询活动，常见的IT管理体系融合一般是将信息安全管理体系与IT服务管理体系进行融合，部分企业为了提高整体业务水平，还通过了ISO9000质量管理体系，在这种情况下，也需要考虑与质量管理体系的融合。

二、 多体系融合的重要意义

1. 提升工作效率

通过开展IT多体系融合工作，可以将管理体系共性的内部审核、绩效评价、管理评审、纠正预防等工作的开展实现同步开展，简化工作流程，提高工作效率。

2. 明确工作事项

通过开展IT多体系融合工作，可以将各管理体系之间的部分进行有效梳理，通过对相关体系文件的修订完善，实现各管理体系具体要求之间的有效关联映射，避免各项具体要求的重复或冲突。

3. 便于考核评价

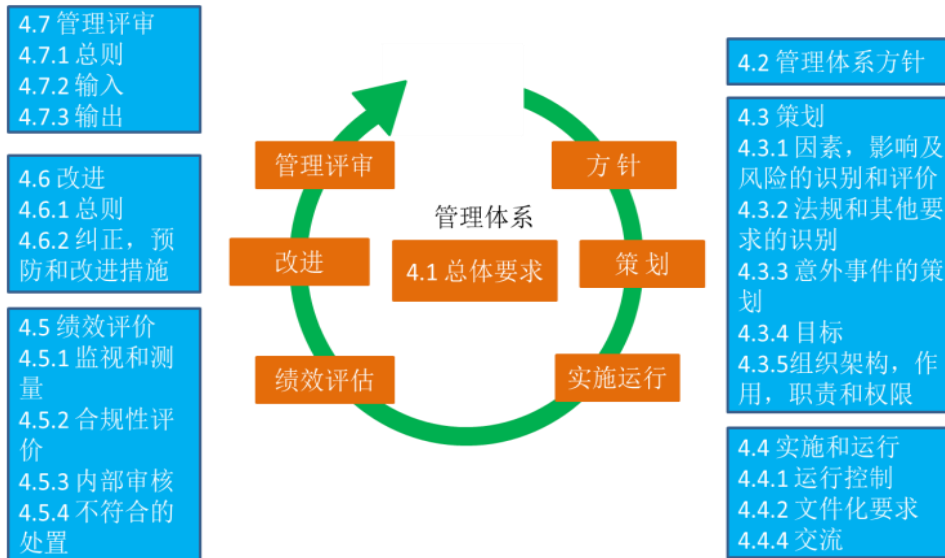
通过开展IT多体系融合工作，可以将针对各管理体系的考核评价进行有机整合，从实现对企业自身信息安全管理与IT服务管理的综合评价，为企业发现内部IT工作的不足，有效推动后续改进提供支持。

三、 多管理体系融合的基本方法

多管理体系融合时需要考虑管理体系自身运作要求以及体系各项具体要求

1. 体系自身运作要求

无论何种管理体系基本都会包含体系方针、策划要求、运行要求、评价要求、改进要求和管理评审要求等



2. 体系各项具体要求

以信息安全管理体系和 IT 服务管理体系的融合为例，在信息安全管理体系中包含了供应商信息安全管理、变更安全管理、容量管理、信息安全管理、业务连续性安全管理等相关内容。IT 服务管理体系中包含了变更管理、信息安全管理、容量管理、事件管理、连续性管理等相关内容。

通过上述分析可以看出，信息安全管理体系和 IT 服务管理体系之间存在诸多交叉关联的内容，在进行管理体系整合时，应分析各体系之间的交叉内容，对相关体系文件进行合理修订完善，实现完善的关联映射关系。

四、多管理体系融合的注意事项

针对多管理体系融合工作，安言咨询认为应该抓住管理体系建设的实质，尽量减少体系建设和运行中的重复环节，避免重复建设，应重点注意：

1. 尽量使用统一的文控管理规范 and 编码规则，梳理不同体系文件之间的相互关联关系，减少交叉内容，明确外部引用，避免文件的重叠和冲突；
2. 采用统一的体系管理组织建设思路，按照“管理层、协调层、执行层”的三层架构进行构建。使得该管理架构可以适用于任何一种体系建设标准，只需要在各层次内指定相应的工作角色，而不需要对组织架构进行大的调整。
3. 建立统一的审核管理和体系度量机制，信息安全管理体系的内审活动、管理评审活动和体系有效性度量的组织和开展与 ISO20000 遵循相同的方法和步骤，差别仅在

于具体内容和侧重点不同。

一套制度文件

- 制度应保持唯一性和一致性，无论ISO27001、ISO20000、ISO20000、BS25999乃至CMMI。

一套组织架构

- 按照三层架构（“管理层--协调层--执行层”）建立统一的体系管理组织。

一套审核机制

- 对于内部审核、管理评审、纠正预防等活动采用统一的审核（包含后续改进）机制。

此外，在具体的实施工作过程中，从体系文件编写、关键活动设计、人员资质和经验能力、人员配备等各个方面均应对体系整合问题应加以重点考虑。具体包括：

1. 体系文件的整合

- 在引入或者建设一个新的管理体系，应首先考虑修订已有的文件制度，通过文件版本的升级，使现有的文件制度能够体现新的管理体系的要求。对于增加新的文件制度应慎之又慎。
- 在引入或者建设一个新的管理体系时，应充分使用索引或文件名称引用的方式，禁止已有的管理制度要求在新的制度里重复出现，以避免随着时间的推移，两个制度文件因版本更新步伐不一致而导致制度之间的冲突。

2. 关键活动的设计

- 无论 ISO20000 体系还是 ISO27001 体系，实施过程中内审、管理评审、检查度量等关键活动的形式和方法是一致的，有关体系文件控制、记录管理的要求也是相同的。因此，本项目的关键活动应与 ISO20000 体系维护中的关键活动进行统筹考虑，明确项目各个阶段的具体关键活动目标、内容和形式，避免重复组织和实施活动，减少体系运行的资源消耗。

