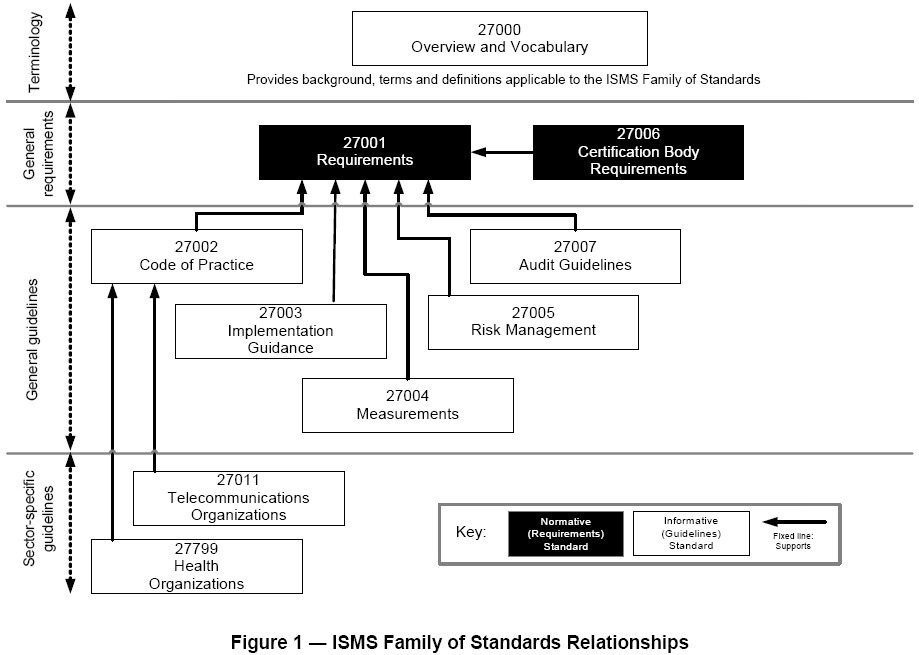
**ISO27001认证业务常见问题**

Q：ISO27001认证是什么？

A：ISO27001是国际标准，全名是IEC/ISO27001信息安全管理体系规范，他是整个ISO27000标准系列当中的一个标准，该系列标准中包含很多其他标准；另外一个大家常说的标准ISO1779:2005-信息安全实施细则也是与信息安全管理相关的，这个标准当前已经改名为ISO27002:2008了。无论是ISO27001还是ISO27002，都是ISMS标准系列（ISMS Family of Standards）之一，ISMS标准系列如下图所示：



大家常说的ISO27001认证，就是企业宣称的认证范围内符合ISO27001标准正文里的所有要求，并且有选择的满足ISO27001标准附录A中的内容。附录A中的内容对应标准ISO27002：2008第5章到第15章，企业是可以根据自身的实际情况来选择适用的控制措施，也就是说该标准里的133个控制项不是强制要求通过认证的用户都必须满足的，通常是通过《适用性声明SOA》文件来表达这种适用，因此，通常在通过ISO27001证书里会包含所选《适用性声明SOA》文件的。

Q：与BS7799认证有和区别？

A：ISO27001认证和BS7799认证的区别得从ISO27001标准发展的历史谈起，ISO27001的发展过程如下图所示：

BS7799认证是指企业信息安全管理体系符合英国国家标准BS7799-2，由于BS7799具有广泛的国际认可度，在BS7799-2成为国际标准ISO27001之前，全球企业在选择信息信息安全管理体系认证时，会选择BS7799。

Q：到目前为止，国内ISO27001认证情况发展如何？

A：目前在国内通过ISO27001认证的企业数已经达到了199家（截至200906），尽管绝对数还不大，但是增长特别快，从下图能观其大概：

在这颁发的199张证书里，其中数DNV和BSI颁发占绝大多数，下图是各认证公司颁发证书的统计表（截止到2009年6月）：

目前国内认证公司有中国信息安全认证中心（简写为ISCCC，09年5月份CNAS认可），华夏认证中心有限公司（UKAS认可，国内试点证书），广州赛宝认证中心服务有限公司（国内试点证书），中国电子技术标准化研究所（国内试点证书）四家，从公开渠道能够查询到的信息来看，截止到2009年7月20日，只有中国信息安全认证中心对外颁发了19张证书，而其他国内认证机构还没有颁出证书。

Q：获得ISO27001认证有什么好处？

* 强化意识，转变观念
* ISO27001认证是一个组织证明其信息安全水平和能力符合国际标准要求的有效手段，它将帮助组织节约信息安全成本；
* 信息安全风险管理的目的是保障企业业务赖以运行IT系统的持续、稳定、安全运行，保障企业业务的连续开展，而不是为企业业务的开展横加了一道枷锁，强调安全保障以业务为中心；
* 信息安全工作应该是以IT部门为主导，全员参与的全公司范围内的活动，强调人人有责；
* 信息安全管理应该遵循风险管理的思想，强调事先防范，事中控制以及事后总结的工作思路，而不是“问题驱动”的救火思路；
* 信息安全问题的解决不应该是“头疼医头，脚疼医脚”的局部问题解决方式，强调整体、系统的分析和解决问题；
* 规范操作，有法可依
* 按照PDCA的方法管理企业信息安全风险，使公司信息安全管理从“无序、零散、被动”的问题补救行为转变为“系统、科学、连贯、主动”的风险驾驭状态；
* 完善各类安全管理制度，规范了企业内部各种与信息系统、信息保密等相关的各种操作行为和方式；
* 良好形象，合规要求
* 企业获得国际认证，能提升客户、业务伙伴、投资人对公司重要、以及敏感信息保护能力的信心，提高组织的公众形象和竞争力；
* 满足监管单位的合规性要求，以及合作伙伴的信息安全审核的要求；

Q：企业初次如何开展ISO27001认证（ISMS建设）项目？

企业开展ISO27001认证时，一般都是由IT部门牵头，业务部门配合参入。但是对于规范较小的公司，IT部门的力量非常有限，往往是由质量管理部门牵头主导项目，因为这些公司一般都有实施过管理体系认证（ISO9001或者CMMI）或者项目的经验，信息安全管理体系同质量管理体系具有较大的相似性。

前期咨询公司的参入帮助引导主导部门甚至企业领导正确认识信息安全，信息安全管理以及ISO27001认证，就本项目对信息安全的理解和目标达成一致。这非常关键，因为这关系到项目实施过程顺利与否，以及项目目标的达成与否。

项目范围的确定在前面已经做了说明，这里不再累赘。ISO27001项目的招标同其他项目没有区别，一般按照企业既定的招标流程走。ISMS体系的建设实施在此也不多说，也有专门的问题。

ISMS体系认证工作一般分为两个阶段的工作，第一阶段是文件审核，这个阶段审核员只关注管理体系文件，查看体系文件是否齐全，ISMS建设的方法是否合理，文件查看的重点一般为风险评估方法，业务连续性和管理体系测量等几个方面。第二阶段是现场审核，审核员将根据ISO27001标准的要求以及企业自身信息安全策略的要求，在认证范围内，现场核实制度的实施情况，检查运行记录是重要的审核手段。现场审核将以末次会议的形式结束整个审核工作，如果审核员没有发现重大不符合项，审核员会在末次会议上宣布企业通过现场审核。

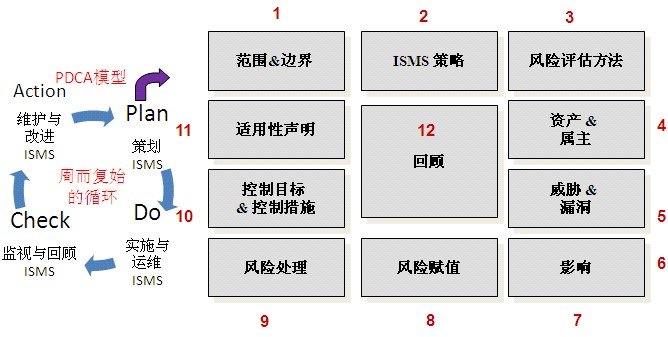
Q：企业ISO27001认证的范围如何来确定？

A：认证范围的选择将影响达到认证要求的难易度以及成本。反过来，难易度和成本是选择认证范围的重要参考。难易度一般由企业自身当前的信息安全管理水平决定，而成本则与企业的预算相关。在考虑难易度和成本的基础上，企业一般会把核心业务部门以及支撑核心业务的IT部门和人力资源部门纳入认证范围。认证范围的描述一般使用业务活动范围、地域场所、信息资产及技术来表达。到目前为止，像比较著名的认证机构比如BSI，DNV等在国内颁发的证书一般只使用业务活动和地域场所来描述认证的管理体系范围。

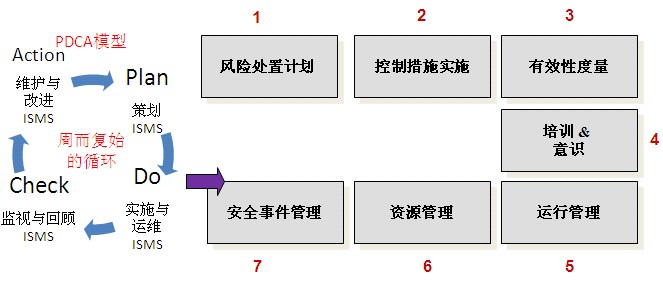
Q：企业建立符合ISO27001标准的ISMS的过程大致是怎样的？

A：ISO27001认证实施不同咨询公司的做法也不一样，但是基本上会按照标准里的内容，从ISMS（信息安全管理体系）规划、ISMS实施与运维、ISMS监视与回顾、ISMS改进与提高四个阶段。 详细如下图解。

阶段一：



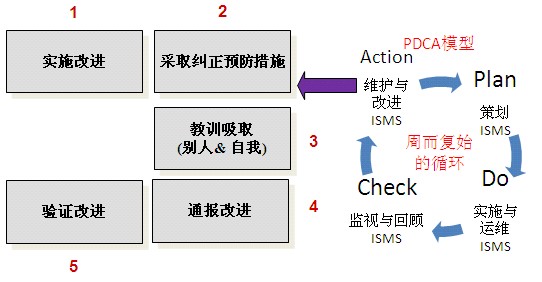
阶段二：



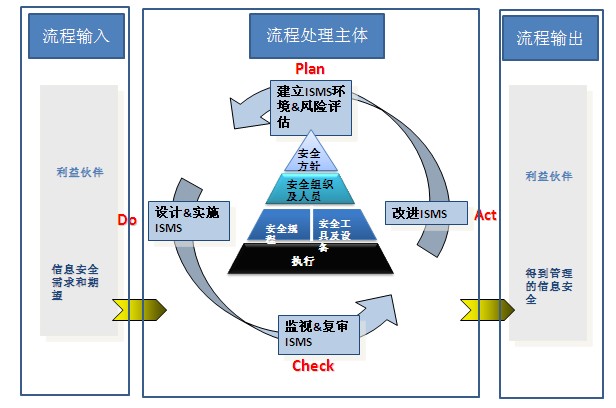
阶段三：



阶段四：



××公司的ISO27001认证咨询实施方法是建立在对ISO27001标准的深刻理解以及过往实践积累总结的基础上的。ISO27001信息安全管理体系的核心是基于PDCA流程的方法。利益伙伴，客户，股东等是信息安全需求做企业信息安全管理体系的出发点，在企业内部业务活动的开展，需要各种各样资源，包括人财物的投入，同时也必须遵守各种各样的安全制度，好的信息安全管理体系最终给利益伙伴，客户和股东带来价值。



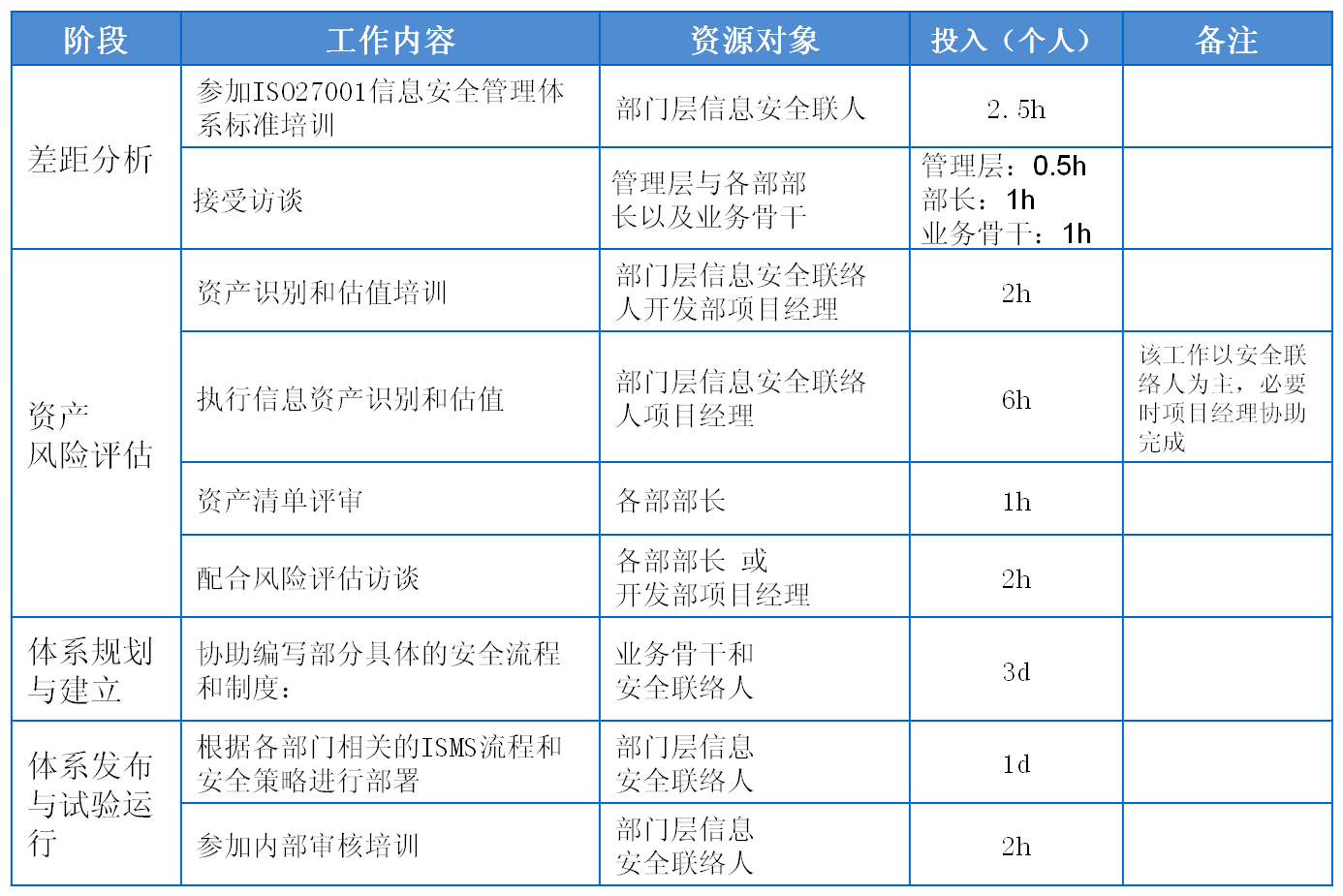
PDCA是个周而复始的循环活动，发现问题，制定问题处理计划，实施计划，检查回顾执行的执行，监视评估实施的效果，发现不足及时改进。企业在PDCA思路的指导下，大循环套小循环，不断推动企业信息安全管理水平提升，始终使企业信息安全风险处在可控的状态。××公司在实践中总结出了一套辅导企业通过ISO27001认证的方法。整个实施方法分为五个阶段，按照实施顺序分别是差距分析、资产风险评估、体系规划和实施、体系发布与试运行和协助外审，每个阶段都有关键输出。详情请参看图-实施方法总概。

五个阶段活动都包含相应的子活动以及阶段主要成果，详细见下表：

|  |  |  |
| --- | --- | --- |
| **实施阶段** | **关键子活动描述** | **阶段主要成果** |
| **现状调研** | * ISO27001基础培训 * 人员访谈 * 现有安全制度收集与分析 * 安全技术现场评估 * ISO27001差距分析 | * ISO27001培训教材 * 人员访谈记录 * 制度分析报告 * 安全技术报告 * 差距分析报告 |
| **全面风险评估** | * 风险评估方法培训 * 资产清点 * 威胁与弱点分析 * 风险赋值 * IT流程风险评估 | * 风险评估培训材料 * 资产清单 * 资产风险表 * 风险评估报告 |
| **ISMS体系建立** | * 管理体系规划 * 技术体系规划 * 风险处理计划 * 安全制度编写 | * 体系规划报告 * 风险处理计划 * 安全管理制度（包括方针，规定，指南，手顺等） |
| **ISMS体系运行** | * 安全制度培训 * 信息安全内部审计 * 管理评审 | * 安全制度培训材料 * 内部审计报告 * 管理评审报告 |
| **ISMS体系认证审核** | * 应对外审培训 | * 应对外审培训材料 |

Q：企业在项目实施过程中，需要多少资源投入？

A：企业在实施ISMS建设时，项目实施方管理层关心的除了付给咨询方的费用以外，还特别关心在ISMS建设过程中企业人员还需要投入多少人天。总的来说，企业的人天投入不同阶段是不一样的，而且参与的人员也会有所不同，从管理层到普通员工在实施工程中都会有参与。下面以一个范围为200人的公司实施ISMS建设为例，从ISMS项目实施的五个阶段，在不同项目阶段不同角色参与项目的单位时间来说明。



其中：h表示小时,d表示天

Q：如何选择认证公司？

在认证公司的选择方面大致可以分为国际公司和国内公司，企业如果有涉及到出口，离岸外包等国际业务时，建议选择国际认证公司；如果企业业务仅仅涉及限于国内客户，且企业自身要满足国内监管方信息安全监管要求，建议选择国内认证公司。国内认证公司由于在开展ISO27001认证的业务起步较国际认证公司晚几年，因而在客户认可性方面比起国际认证公司要稍微差些。

国内企业选择国际认证公司时间，一般选择BSI和DNV较多，国内认证公司目前只有中国信息安全认证中心正式被中国合格评定国家认可委员会(简称认可委)正式认可，而其他三家（赛宝认证中心，华夏认证中心，中国电子技术标准化研究所）目前（截止2009年6月）还是颁发试点证书。

Q：企业获得ISO27001认证之后，在应对认证公司审核还需要做哪些工作？

A：ISO27001证书一般都是3年有效期，3年过后，必须历经一次全面审核，由认证公司重新颁发证书。在认证注册资格后，在三年有效期内，将接受乙方3 次定期监督审核及必要的不定期审查。其中，获证之日起6 个月安排首次监督审核，其后监督审核间隔不得超过12 个月，有异常情况时酌情增加监督审核的频次。因此，企业必须仍然按照标准PDCA的要求，不断发现或回顾信息安全风险状况。

Q：如何成来保证一个ISMS项目的成功，这些成功因素主要包括哪些？

1. 项目范围内相关部门以及各层领导就项目的目标理解一致。
2. 信息安全策略必须要反映企业的业务目标。制定的安全策略是规范员工的行为，更好的服务企业，为企业业务目标的达成提供信息安全的保障，安全策略不能与业务目标相违背，更不能成为业务开展的绊脚石。
3. 实施过程与方法要与企业的文化保持一致。项目实施过程中，需要顾问与企业人员不断的沟通和交流，这些交流方式要与企业当前的企业文化相一致。
4. 来自管理层可见的支持以及承诺。管理层需要在项目的各个关键节点，如项目里程碑参加会议，公开表明态度，并保障必要的人力以及财力支持。
5. 为员工提供适当的培训和教育
6. 易理解且一致的度量系统以评估信息安全的效能。安全控制的效果如何是能够通过一种从公司管理层到普通员工所有成员都理解的方式来衡量。就如人身体的好坏能够通过血压，脉搏等等指标就能知道。
7. 自动化的安全策略管理工具的使用。需要有一个工具来自动的管理当前的安全策略，员工也能够通过这个工具，快速查找到他需要的安全制度。

Q：ISMS的范围确定之后，如何来解决范围之外的一些信息安全问题呢?

A：企业内部面临信息安全问题的时候，目前虽然不是以前上某种安全产品就解决一切问题的那种一劳永逸的想法，但是大多数的企业都希望尽可能多解决一些问题，这种心情是可以理解的。

ISMS建设时，都会确定一个明确的实施范围，比如IT部或研发部或财务部，那么在实施ISMS的过程当中，范围之外的部门或组织一般都不会深入涉及，再次实施的重点明确在已定的范围之内，在咨询顾问的帮助下，建立合理的信息安全组织框架，培养出能够胜任安全管理体系运作的相关人员，比如掌握了风险评估方法的人员，内部审计人员等等，提高人员的安全技能以及安全意识，在范围内，提高信息安全的运作水平，降低相关安全风险。然后依此作为示范，一步一步的扩大ISMS的范围，并且按照PDCA模型使企业的信息安全水平不断提升，最后全公司范围内推广实施。实际上这也是企业在信息安全体系的建设过程当中，在一定的人财物的投入的条件下，按部就班，循序渐进，并秉承关键部门、以及高安全风险的地方优先控制的原则，切忌一步而蹴。

Q：哪些问题属于信息安全风险，而哪一些问题则不属于信息安全风险？

A：信息安全风险是指自然（环境）因素或者人为因素利用信息系统漏洞（技术漏洞）、管理（或流程）缺陷，对企业造成危害的潜在事件。包括信息系统的开发、部署、运行（使用）、监控、维护及退出等过程中由于IT操作流程缺陷、系统的业务流程控制缺陷、信息系统脆弱性、操作人员无意/蓄意失误、外部事件等因素直接影响信息系统的安全、可靠、平稳运行，并可能导致业务运营中断乃至欺诈事件等业务操作风险，并间接导致信用、市场、法律、声誉等企业。

信息系统开发时的业务需求分析风险、信息系统项目管理风险等等则不属于信息安全风险。

Q：信息安全风险管理的定义及其范围？

A：信息安全风险管理是指通过建立有效的机制，实现对信息安全风险的识别、计量、评估、预警和控制，确保信息系统高效、可靠、安全、平稳、持续运行，规避因为信息技术应用而引起的各种风险。一般包括风险评估、风险处理、风险接受、风险通报、风险监控、风险回顾。

应用系统中的业务流程可能存在因流程控制缺陷而引起的操作风险。此类风险与信息技术应用的关系密切，并且极有可能因为自动化、网络化的实现方式而被放大，因此必须将其纳入全面信息安全风险管理的范围：

* 应用系统中业务流程操作风险本质上仍属于业务操作风险，此类操作风险的识别、评估以及提出流程控制要求等职责原则上属于业务流程主管条线；
* 但是通过系统实现的业务流程与传统手工方式有较大的区别，信息技术的应用使业务流程的风险情况发生了较大的变化，因此此类风险的管理课题横跨IT技术与业务运营两个领域；
* 所以从实现全面风险管理的角度出发，应将协助管理此类风险的职责纳入信息安全风险管理的范围，由IT部门采取适当的方式积极参与其管理工作；

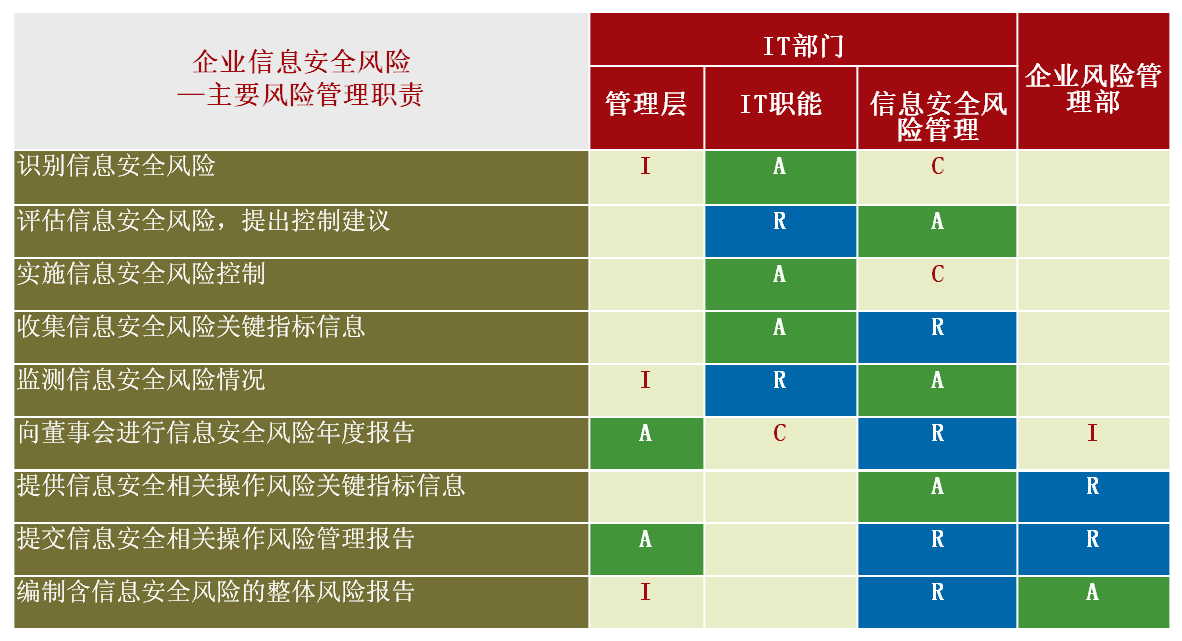
Q：怎样算是实现了有效的信息安全风险管理？

A：明确职责与分工，建立良好的互动机制，由信息安全风险管理团队进行协调、检查、督促并提供专业支持，实现共同协作、分散控制的信息安全风险管理环境，全面掌控直接、间接的隐藏风险，将所有影响信息系统高效、可靠、安全、平稳、持续运行的隐患控制在可接受的范围内。

Q：企业里谁应该承担信息安全风险管理的哪些职责？

* 信息安全风险专业性强、涉及领域广，适宜在IT条线内部进行管理，IT部门承担信息安全风险的管理职责，具体落实在部门内的信息安全风险条线；
* 业务部门承担系统中业务流程自身的操作风险；
* 企业风险管理部门对信息安全风险管理提供指导；
* 信息安全风险管理职能应向企业风险管理部门提供信息安全风险管理报告，以汇总到企业整体风险管理报告中；

其中：



* R = Responsible谁负责,负责执行任务的角色，具体负责操控项目、解决问题。
* A = Accountable谁批准，对任务负全责的角色，只有经其同意或签署之后，项目才能得以进行。
* C = Consulted咨询谁，在任务实施前或中提供指定性意见的人员。
* I = Informed告知谁，及时被通知结果的人员，不必向其咨询、征求意见。

Q：IT部门内谁应该承担信息安全风险管理的哪些职责？

A：IT条线内部的信息安全风险遵循“责任到位、任务明确、各司其职”的原则，定位如下：

* IT条线管理层整体负责，并向董事会进行年度信息安全风险报告；
* 建设开发、运行维护等IT职能为IT风险的第一责任人，承担识别风险、实施信息安全风险等职责；
* 信息安全风险管理职能承担着制定风险计量标准、开发评估工具、建议控制方案、督促控制执行、监测风险情况、应急响应、编制风险管理报告等职责。

Q：需要组建怎样的队伍来管理信息安全风险，队伍中各角色的职责是什么？

A：在IT治理组织结构成果的基础上（没有的话，则从头建立），建立垂直专业管理的信息安全风险管理条线；建立常设的风险评估、监控扫描等专业团队，并以虚拟团队的方式覆盖整个企业；设立安全信息监控中心（运维中心）等实体化的信息安全支撑中心。组织结构如下图所示：

* **信息安全风险主管**
* 协助管理层确定信息安全风险管理目标、风险偏好
* 确定信息安全风险管理策略；
* 协调相关信息安全风险相关主要资源；
* 向管理层汇报整体风险管理状况；
* 协调信息安全风险管理相关方工作；
* 组织制定信息安全风险管理政策。
* **总部信息安全安全风险管理：**
* 组织和管理整个公司信息安全风险管理工作
* 组织制定信息安全风险管理规划
* 组则整体信息安全风险管理组织建设
* 负责信息安全风险管理团队、专业团队与内外部的协调工作；
* 组织信息安全风险管理意识的宣传培训及信息安全风险管理专业培训；
* 对专业团队及分行风险管理团队进行业务指导。
* 汇总整个公司风险管理信息，撰写风险管理报告；
* 执行合规性检查；
* 对所有信息安全项目的信息安全需求进行评审，确保安全需求，控制项目风险。
* 综合管理（后勤/人力）。
* **总部信息安全风险咨询团队：**
* 分析风险管理现状与风险管理技术趋势；
* 起草风险管理政策；
* 制定相关技术标准、操作规程。
* **信息安全风险项目管理与专业建设：**
* 负责信息安全相关项目的项目管理，协调负责安全开发与部署的开发中心/数据中心；
* 负责加密技术等小部分核心信息安全技术的专业建设与开发。
* **信息安全风险管理专业团队**
* 研究信息安全风险管理发展趋势，协助管理层制定信息安全风险管理政策，判断风险管理现状；
* 提供信息安全风险管理专业服务支持，为分行及数据、开发中心提供信息安全风险管理技术支撑与指导。
* 负责应急响应的管理与执行。

Q：采用怎么样的方式来管理信息安全风险，需要开展哪些工作？

A：在业务需求及流程操作风险评估、项目风险自评估、技术风险（信息安全风险）评估的基础上完善系统建设开发方案审批及风险管理机制，并建立正式的IT内控与安全检查评估、漏洞扫描与渗透性测试等流程，将这些工作制度化、日常化，并与需求确定、验收测试、上线审批、绩效管理等相关工作进行结合。

Q：需要哪些信息安全风险管理制度，怎样加强这些制度的执行？

A：包括IT 风险管理制度体系与信息安全制度体系，并明确相关政策管理流程以加强规范化管理、提高执行力度；同时应将信息安全风险控制措施融入各IT工作的相应制度中以提高其执行力度，并更新IT内控手册对这些控制措施进行汇总与映射。

Q：需要哪些技术能力支撑信息安全风险管理？

A：在信息安全管理方面需要建立预防、检测、响应、恢复的技术能力；在IT流程风险管理方面需要建立流程控制固化、绩效与关键风险指标监控等技术能力；同时还需要针对全面的信息安全风险实现政策管理、控制点管理、风险敞口跟踪等综合管理能力。

Q：有哪些技术方案能够提供信息安全风险管理需要的技术能力？

A：技术方案主要集中在较为成熟的信息安全技术领域。信息安全技术架构在信息安全基础设施上定义了信息安全服务、网络安全、应用安全、安全管理与安全工具体系，其中主要的技术方案包括安全信息与事件管理服务、身份与访问管理服务、威胁与脆弱性管理服务、数据安全服务、网络准入控制等。