ISO27001 在日企外包行业的实践探讨

谷安天下 高级顾问 陈岌

《ISO27001:2005 信息安全管理体系规范》国际标准发布之后，ISO27001 成为炙手可热的企业信息安全管理体系建设蓝本，各行各业，特别是外包行业，开始广泛参照该标准并结合企业的实际情况，对信息安全活动进行全面的管理，期望提升安全管理水平。但是现实与理想总是存在差距，尽管可以用 ISO27001 指导各行各业的安全管理活动，但是并不是包治百病的良药，比如制度难以落实，控制失效等等。是洋标准水土不服还是“病人”身子板太差？作为信息安全咨询顾问，本人有幸主导实施了多个软件外包公司的 ISMS 建设项目并跟踪了 ISMS 在企业的推进情况，颇有感受，在此与大家探讨。

1. ISMS 如何结合企业环境

企业按照 ISO27001 建立组织的信息安全管理体系时，要么聘请外部咨询顾问，要么让企业内部有体系建设经验的专业人士实施，当项目完成之后，企业的安全管理框架基本建立，但是在体系运行过程当中还存在种种问题，主要表现如下：

1) 安全制度难以落实执行；
2) 推行过程困难重重，很多活动留与形式；

ISMS 运行成果的好坏，诚然，由两个方面所决定，一方面是 ISMS 搭建者的能力，另一方面是企业的内部环境。从 PDCA 的思路来看的话，归根到底还是取决与企业的内部环境。人们常说要量体裁衣，建设有效的 ISMS 必须考虑企业的实际情况。那么建设 ISMS 时，需要考虑哪些企业环境信息呢？

1) 企业组织架构，包括决策，权利分配，责任分工；

曾经碰到这么一个客户，他们的 ISMS 建设由质量管理部门来主导实施，但是质量管理部门由开发本部直接领导。试想一下，下级部门督促监督上级部门做某项“费力”的工作，在这么一个环境中推行安全改进其困难何其大。

2) 全体员工的安全意识水平

员工的信息安全意识简单说是能够对可能发生的安全事件保持一定的警惕心；发散开来可以理解为以下几个层次：就是能够认知可能存在的安全问题，明白安全事故对组织的危害，恪守正确的行为方式，并且清楚在安全事故发生时所应采取的措施；

3) 企业文化

企业环境的因素中非常重要的是企业文化，企业文化主导了员工行为方式和企业对外形象，或规范、或随意等等。在华日企外包企业应该说传承了日本企业的基本的文化特点，体现在：

1) 看重企业诚信，诚信可以成为企业成败的关键

在日本，企业如果发生信息泄露等信息安全事件，按规定是要主动向有关政府部门报告的，如果隐瞒不报一旦被发现将会严重影响公司信用，后果是十分严重的。不二家这个创立于 1910 年的西点食品连锁企业，就是因为隐瞒使用过期原料进行生产的事实被曝光而发生严重的信用危机，砸了自己的百年老字号，现在超市已经看不到不二家的东西了。

2) 企业非常重视信息安全

从 *ISMS International User Group* 对全球通过 ISO27001 认证的企业数目上可以看出，

日本到当前为止已有 2800 家企业，占全球通过企业数的 50%以上。参看来自下表。由此可见日本企业对信息安全的重视；另外，在 05 年 4 月生效的《个人信息保护法》是日本保护个人信息安全的根本法律，企业从各种方面加强了对个人信息的保护。在华日企外包公司主要为日本提供外包服务，客户如此重视信息安全，外包企业不跟上形吗？

Japan	2863*	Netherlands	11	Bulgaria	2
India	433	Singapore	11	Canada	2
UK	368	Philippines	10	Gibraltar	2
Taiwan	202	Saudi Arabia	10	Isle of Man	2
China	174	Pakistan	10	Morocco	2
Germany	108	Russian Federation	10	Oman	2
USA	82	France	9	Qatar	2
Hungary	74	Colombia	7	Yemen	2
Korea	71	Slovenia	7	Armenia	1
Czech Republic	66	Sweden	7	Bangladesh	1
Italy	54	Slovakia	6	Belgium	1
Hong Kong	38	Croatia	5	Egypt	1
Poland	36	Greece	5	Iran	1
Australia	28	South Africa	5	Kazakhstan	1
Austria	26	Bahrain	4	Kyrgyzstan	1
Ireland	26	Indonesia	4	Lebanon	1
Malaysia	26	Kuwait	4	Lithuania	1
Spain	26	Norway	4	Luxembourg	1
Brazil	20	Sri Lanka	4	Macedonia	1
Mexico	20	Switzerland	4	Moldova	1
Thailand	17	Chile	3	New Zealand	1
Romania	16	Macau	3	Ukraine	1
Turkey	15	Peru	3	Uruguay	1
UAE	14	Portugal	3	Relative Total	4997
Iceland	11	Vietnam	3	**Absolute Total**	4987

Number of certificate per country (来自 *ISMS International User Group*)

那么建设 ISMS 时如何考虑环境因素并最终把安全体系嵌入企业环境中呢？

1) 建立合理的信息安全组织架构

合理的信息安全组织架构应该包含三个层次，决策层、管理层和执行层；从角色上来讲可以分为普通员工、信息安全专业人员、安全审核员；信息安全是“一把手”工程，由企业的总经理直接挂帅领导。

2) 建立全员信息安全教育和培训制度

一方面按照企业人员级别以及业务性质的不同，对不同人员实施不同侧重内容的培训，关注不同级别人员对信息安全的关注点；另一方面，实现员工在企业整个就业期间，实施不间断的持续培训，从员工入职到最后离开企业。当然，在安全教育和培训方面，不必拘泥与形式，除了正常的集中人员面对面的培训之外，还可以采取网络教程，flash 动画、张贴墙报、定期发送电子报、开展信息安全知识竞赛等等。通过多方式，全方位的宣传和教育，把信息安全融入到企业文化当中。

3) 让员工承诺负责

让员工咨询阅读与其业务相关的安全策略，让员工承诺遵守公司的安全制度并签字；

2. ISMS 如何从业务需求出发

企业从事信息安全的人员在业务部门往往不怎么受欢迎，因为在业务部门的眼中，信息安全捆绑了业务发展的手脚，降低了工作的效率。这是误解呢还是事实呢？显然，对于信息安全从业人员来说，无疑伤了他们的积极性，信息安全的目的不但没有达到，反而逆其道而行之。归其原因，主要是信息安全控制与业务需求脱钩；

外包公司的主要业务是承接了客户业务链中的某个环节业务，而外包公司所提供的这些服务的失败可能会影响到发包公司整个业务。比如软件外包，这可能会涉及到某些具有知识产权的技术，也可能会涉及到客户数据的机密，也有可能会涉及到某些商业秘密等；那么 ISMS 如何满足业务需求呢？

1) 分析业务驱动

业务驱动是指在信息安全方面业务开展的需求，软件外包公司的业务驱动主要包括以下方面：

- ✓ 发包方与接包方之间在信息安全方面要建立广泛的信任，必须要引入信任的第三方；
- ✓ 发包企业往往是跨国或者高科技企业，其自身对信息安全要求很高；
- ✓ 提供一个安全的开发环境，开发团队使用的信息系统不至于遭受外包恶意软件的攻击而不能正常工作；
- ✓ 互联网的环境，软件系统面临更多的威胁，需要开发出安全的软件（软件功能健壮，不存在严重的安全漏洞）；
- ✓ 保障客户信息的机密性；
- ✓ 保持邮件系统 7×24 小时正常运行，与客户保持良好信息沟通；
- ✓ 保持网络通畅，保证开发团队（发包方与接包方）能够正常协同开发；
- ✓ 维护客户知识产权；
- ✓ 保障与开发系统相关的一切设计文档、源代码的机密性；
- ✓ 保持开发团队的相对稳定性；
- ✓ 出差人员能够通过安全的方式访问企业内部信息；

2) 明确业务属性

业务属性是指那些企业想要保护或者支持的事务。业务属性可以从用户属性、运维属性、风险管理属性、法律法规属性、业务战略属性等几个方面来看。

用户属性是指用户在系统中的信息安全的体验，这里的“用户”主要是指软件工程师，软件项目管理人员。运维属性是指企业日常运行的安全；风险管理属性指要识别的安全需求的集合以及管理业务风险；法律属性涉及符合性问题；业务战略属性是指高层管理和股东对于公司以后发展的想法；下面，摘取业务属性的一二略加展开。

如用户属性：

用户属性	属性解释
可访问性	对于授权能够访问的项目文档信息以及信息安全过程改进文档，用户能够容易的找到并且有适当的访问权限；
更新性	给用户所提供的信息，包括软件过程改进以及信息安全过程改进文档等必须是保持最新；

职务分离	软件开发与软件测试工作必须由不同工程师担任；项目配置库服务管理人员与审计人员必须不同人员担任；
教育和意识	用户必须接受必要的培训和教育，使他们必须具备必要的安全技能，对安全问题有足够的风险意识，并明确那些行为是符合公司安全策略的；
受保护	用户的信息和访问权限必须受到保护，以防止被他们滥用；
可靠性	为开发部门员工所提供的系统服务，包括邮件通讯服务，远程网络访问服务等，交付时应达到可靠的服务质量水平

运维属性：

运维属性	属性解释
可靠性	企业业务开展所依赖的信息系统和网络应该稳定可靠，满足约定的服务级别水平；
持续性	严重事故甚至灾难所致的信息系统的宕机导致业务中断在企业的所允许的最大业务中断时间之内；
可检测性	重大的安全事故能够发现并及时报告；持续监视系统的性能、容量状况以满足其他的规范。任何系统安全策略的违背都有相应日志记录；
可恢复性	系统在遭受崩溃或者灾难之后，按照既定服务级别水平，能够恢复其全部功能；

从以上的分析当中，可以看出，业务驱动与业务属性存在着多对多的关系；比如业务驱动“保障客户信息的机密性”与业务属性的“教育与意识”以及“可检测性”对应；

3) 设计安全架构并实施

通过对业务的安全需求的充分调查与分析，ISMS 的安全控制措施才能有的放矢，真正做到符合需要，符合企业业务发展的需要。

3. 知识产权问题

近年来，知识产权问题在离岸外包业务中屡屡出现问题。印度在近 20 年来成为世界的 IT 外包中心，除了高性价比的劳动力和规模效应之外，就是知识产权得到政府和企业等多方的保护，这让发包方有充分的安全感。但是，近年发生在印度数桩技术机密遭到恶意泄漏和贩卖的案例，引发行业的广泛思考。

而在国内，众多的企业还在探索外包市场，知识产权的保护还停留在起步阶段。要达成商务部提出的“千百十工程”在全国建立十个国际外包基地城市，推动 100 家世界著名跨国公司将业务外包业务转移到中国，扶持 1000 家具有国际外包能力的大中型企业的目标还任重道远；这一方面要求政府加速推进知识产权方面的立法和执法工作，另外一方面，要求企业在内部建立完善的知识产权保障团队，可由公司具体外包业务部门、质量监控部门、信息技术部门和人事部门负责人组成。所有新员工入职时，就要接受相关培训。信息技术部门则在工具技术上提供一种安全的环境和屏障；同时，质量人员在检验项目的流程中都会介入，按照我们对客户的承诺，一条条检查知识产权方面的保护；业务部门的主管人员就会自始至终控制着整个过程。

当然发包方也应有专业的知识产权保护方法，外包不等于撒手不管，外包安全需要发包方的介入，才能确保外包长期的安全。至于发包方如何确保外包安全，超出了本文的范围；

另外，在软件外包公司，还存在着一个有趣的且对质量管理部门棘手的问题。那就是软件开发公司一般都会参照 CMMI 来建立企业软件开发过程改进体系，而 CMMI 体系中就要求过

程改进部门，往往是质量部门，去收集一个个已经完成的项目，并且整理归档，为下一个类似项目提供参考，但是这无疑违背了与客户之前签订的外包合同中所涉及的知识产权甚至保密性约定。对于质量管理部来说，已经收集的项目数据就成了烫手的山芋。面对这个问题，有以下两个可能的解决方法：

一是在与客户签订外包合同时，明确详细的知识产权保护范围；

二是清除已项目文档中的与客户相关的所有的敏感信息；

4. 管理层如何体现对 ISMS 支持

管理层的明确有力支持对推动企业 ISMS 的有效运作发挥极其重要的作用。所谓兵熊熊一个，将熊熊一窝；如果公司高层在 ISMS 中无所作为的话，那整个企业的 ISMS 就是徒有空壳，无血无肉，谈何有效运行呢？至于如何获得管理层对信息安全的认可，需要向管理层推销安全，这是一个非常有趣的话题，已超出本文的范围，在此就不多说拉。

ISMS 在企业应“自上而下”推行，高层管理在公司以下活动中向全体员工传递积极信号：

1) 投入足够的人员和资金支持 ISMS 过程改进，建立过程改进组织机构，并充分授权；根据实际情况，投入专职人员进行过程改进；向各部门传达过程改进的信息和得到各部门主管对过程改进支持的承诺。
2) 对参与过程改进人员投入 ISMS 改进的工作量和本职工作的平衡的支持。
3) 对绩效考核与 ISMS 过程改进结果挂钩的支持，对项目成功后人员的奖励
4) 在 ISMS 过程改进期间，对过程改进活动的持续关注，可通过公司例会上对过程改进活动的讨论，或者不定期对 ISMS 过程改进的状态进行评审。
5) 当过程改进取得阶段性成功时，表达对过程改进参与人员的感谢和鼓励，并在全员面前宣布成功和并进行鼓励。

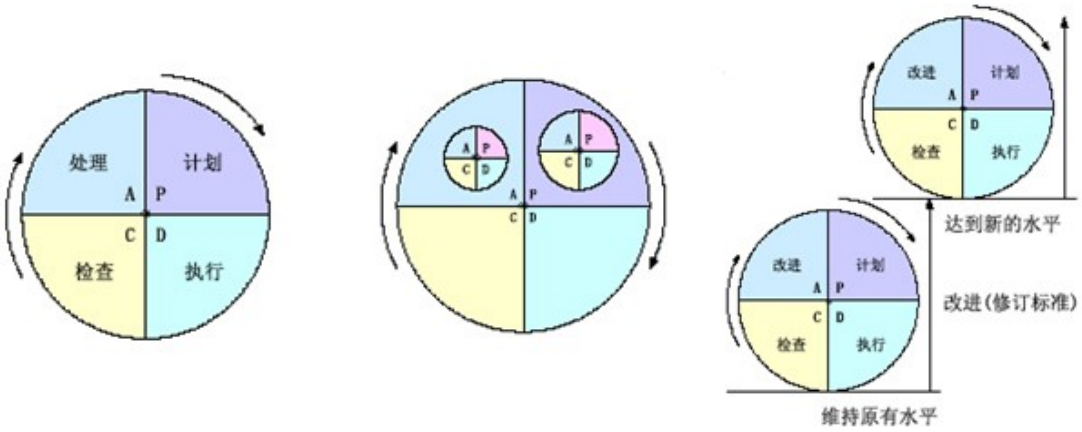
5. ISMS 如何做过程改进

ISMS 的过程改问题进不仅仅在目企外包行业，可以说几乎所有行业所有的过程改进都存在相关问题。ISMS 的过程方法强调需要理解企业的信息安全需求，以此建立企业的信息安全策略和目标，接下来要去实施和运用安全控制把企业安全风险降低到一个可以接受的水平，并且不断监视和审查以及回顾安全控制的有效性以及执行的符合性，对照之前的安全目标，发现问题，明确差距，不断改进提高。每个环节都有输入和输出，下个环节的输入就是上个环节的输出。ISO27001 标准采纳了 PDCA 的过程方法；PDCA 的特点是：

1) 顺序进行，周而复始：解决了一部分问题，可能还有问题没有解决，或者又出现了新的问题，再进行下一个 PDCA 循环。

2) 大循环套小循环：组织中的每个部分，甚至个人，均有一个 PDCA 循环，大环套小环，一层层地解决问题。

3) 阶梯式上升：每经过一次 PDCA 循环，都要进行总结，巩固成绩，改进不足，并提出新的目标，再进行下一次 PDCA 循环。



目前在企业的 ISMS 的过程改进中，无论是企业内专业人士还是咨询顾问，大家普遍认为比较难，之所以难，归纳原因，大致有三：

1) 过程改进首先意味改变。

对于外包软件开发项目，除了软件开发过程本身的改进任务之外，还增加了在安全的环境中开发出安全的软件的新的过程改进要求，这无疑加大了改进的难度，增加了开发人员的抵制情绪。比如以前可以随时访问 Internet，以查阅相关资料获取信息，而现在由于保密性的要求而限制访问 Internet。

2) 过程改进是一项额外的工作，重要但不紧急。

按照 ISMS 的要求，一个新的软件项目立项之后，势必将产生各种各样的数据和文档，需要依赖相关的信息系统，而这些数据文件以及系统就是企业需要保护的信息资产。这些信息资产要纳入风险管理的范围，资产识别、分类分级、弱点和威胁的识别和评价等等随之而来。人们往往会忽略那些重要的但是不紧急的工作，因此这项目工作常常被推迟甚至被取消；

3) 过程改进部门与业务部门沟通存在问题

在业务部门的眼中，信息安全是可有可无的东西，甚至被认为是业务的绊脚石，太多的安全控制降低了他们的工作效率，因此想法设法来阻碍信息安全过程的改进，甚至歪曲现有的安全控制效果；

已知病症，对症下药即可：

1) 改变先从一个项目入手，建立成功的典范，然后再推广。

一来通过试点可以积累经验，面对的阻力较小，二来有了成功的典范之后可以给其他项目以信心，项目组找不到更好的理由来拒绝改变；大家都知道，中国移动在推出新业务时，先在某个省试点，成功之后然后在全国推广。其实这应该是典型的做法。企业的信息安全有很多工作要做，所谓欲速则不达，对于从业人员来，不要尝试把整个海洋煮沸。

2) 把过程改进中的任务加入到项目计划当中，

信息安全工作成为项目中不可或缺的一部分，这样的话，信息安全不再是额外的工作，而是分内的工作。项目组除了完成之前的开发任务之外，还有过程改进的目标。改进目标的设定应该在企业信息安全整体目标的指导下，且是符合企业实际需要的，可以采取平均代码重大安全漏洞数，项目组信息安全事故次数等等来衡量。

3) 过程改进本身也是一项重要的管理工作

信息安全的效果是通过业务部门的参与得以体现，改进的信息安全过程能够增加公司核心业务和产品的附加值(客户更加信任)，让业务部门从安全改进中尝到了甜头，才能更积极的参与到改进中来。

过程改进需要全体员工的参与，上到管理层，下到普通的工程师。上文我们提到，过程

改进就是过程改变，员工的参与也就是要改变之前的做事方法。人们为什么要做出改变呢，只有让人看到好处，让参与的各个级别的人员能够满足其诉求。因此，信息安全经理要仔细分析他们的关注点。在信息安全改进过程中，在企业内部，安全经理需要与三个方面的人员做好沟通：高层管理者，中层业务经理，工程师。高层管理者关注信息安全对于企业长期的重要性，一般在各种场合都会表示对信息安全工作的支持。而中层业务经理则要关注多项指标，项目进度和质量、人员技能提升等等，信息安全只是其中指标之一，而他们需要在多项指标中寻找平衡。工程师在项目压力不是很大的情况下，还是非常乐意学习新的技能和方法。

了解他们的关注点之后，信息安全经理再与他们的沟通时要有针对性。对于高层管理者，只需说明新方法概况，目的和初步计划，人员投入等，无需过多细节。面对业务部门经理，除了上述要点之外，还要说明信息安全工作如何与他们的目标挂钩，这一新方法不仅是为了满足客户安全需求，还能帮助完成更安全的软件，并且就投入多少时间，涉及哪些人员，风险降低何种程度进行讨论。如果与高层管理者和业务部门经理都已经达成共识，再与工程师来讨论新方法的推行就会很顺畅。

ISO27001 国际标准做为全球在信息安全管理方面的最佳实践之一，是他人的经验总结。在当前国内企业管理水平整体相对较低的情况，我们唯有努力学习他人经验，并切实结合自身的实际情况，打造有效的 ISMS。