信息安全风险评估的策划

Preparation for information security risk assessment

科飞管理咨询公司　　王毅刚　吴昌伦

摘要：本文提出了组织在进行信息安全风险评估时，在策划阶段应关注的一些问题，以保证整个风险评估过程的有效性。

关键词： 信息安全 风险评估 策划

Abstract: This paper gives some suggestions to information security risk assessment in preparation stage in order to keep the course effective.

Keyword: information security; risk assessment; preparation

随着各类组织的信息化程度的提高，使得信息系统越来越复杂，在业务运作的过程中生成大量的数据，组织的发展对信息的依赖程度也越来越大，这样信息安全管理成了组织风险管理的重要组成部分。如何保障信息安全是每个现代组织所面临的共同问题，信息安全风险评估逐渐被引入组织的管理体系当中。目前，我国也正在制定相应的风险评估及风险管理指南。国际上的风险评估（管理）指南，基本上比较注重可操作性和通用性，对于风险评估的过程描述得比较清晰，也强调了风险评估的准备阶段的要求和任务，笔者认为风险评估作为一个过程，应该特别注意其策划阶段的活动，本文主要结合实施风险评估的一点经验，简单提出在策划阶段应关注的一些问题。

一、 确定风险评估范围

风险评估作为一个过程，或者说一个项目，在最初应确定其范围。组织进行风险评估可能是由于自身商业要求及战略目标的要求，相关方的要求或其他原因，因此应根据上述原因确定风险评估范围。范围可能是组织全部的信息和信息系统，可能是单独的信息系统，可能是组织的关键业务流程，也可能是客户的知识产权。例如国内某半导体代工企业为了满足其技术合作方在技术转移方面的要求而采取 BS7799-2:2002 **标准建立信息安全管理体系（**ISMS**），在建立体系的过程中，他们设定了** ISMS **的范围，这个范围其实就是包含客户** IP **的信息流所涉及的业务流程和部门。这样在体系建立过程中的风险评估就针对这样的范围进行，以满足相关方的要求。**

组织在确定范围的时候，不应该是随便指定一个范围，而是应该清醒的分析组织业务战略的要求，否则整个风险评估可能耗费大量的资源，却没有达到预期的效果。如果风险评估的范围过大，经常会导致对于收集到的信息进行分析分析时感到困难，设定一个对于组织来说“易于管理”的范围对于风险评估的项目安排及活动的实施都会降低其难度。范围的界定可以从下面的一个思路进行考虑：

1） **为满足组织业务战略要求，组织承担着那些重要的商务活动；**

2） **流程当中有哪些信息和信息系统是必须依赖的；**

3） 重要的商务活动涉及到那些人员和部门；

上面三个问题基本上涉及到了组织的业务流程、信息资产、地理范围，风险评估的范围也可以从这三个方面来进行描述。实际上对于组织而言，划定范围就是把最重要的“区域”放在最优先、最高频率的位置上进行评估，而不是将全部“区域”的信息资产一把抓，解决好了哪些“区域”是“重要区域”的问题，范围就可以清晰地被定义了。

二、 确定风险评估目标

组织应明确风险评估的目标，为风险评估的过程提供导向。支持组织的信息、系统、应用软件和网络是组织重要的资产。资产的保密性，完整性和可用性对于维持竞争优势，现金流动，获利能力，法规要求和一个组织的形象是必要的。组织要面对来自四面八方日益增长的安全威胁。一个组织的系统、应用软件和网络可能是严重威胁的目标。同时，由于组织的信息化程度不断提高，对基于信息系统和服务技术的依赖日益增加，一个组织则可能出现更多的脆弱性。组织的风险评估的目标基本上来源于组织业务持续发展的需要、满足相关方的要求、满足法律法规的要求等方面。

三、 建立适当的组织机构

组织在进行风险评估时，完全将其委托给外部的信息安全专家是不合适的，针对上面所定义的风险评估范围及目标，组织应建立适当的组织结构，以支持整个过程的推进，如成立由管理层、相关业务骨干、IT 技术人员等组成的风险评估小组。组织机构的建立应考虑其结构和复杂程度。完备的组织机构能够确保风险评估过程中的职责能够地得到明确的定义，能够从管理和技术两方面认识组织的安全状态，能够保证风险评估过程中的沟通与决策。

四、 建立系统性风险评估方法

现在对于国际范围内信息安全风险评估的标准、指南采用较多的有BS7799-2:2002《信息安全管理体系——规范及应用指南》、ISO/IEC 13335《信息技术——IT安全管理指导方针》、NIST SP800-26《IT系统安全自评估指南》、卡耐基梅隆大学OCTAVE[1]方法、GAO/AIMD《信息安全风险评估——先进组织实践》、SSE-CMM《系统安全工程能力成熟度模型》等。我国目前也在积极应对各类组织日趋增长的风险评估、风险管理的需求，起草适应我国国情的风险评估、风险管理指南，立足于我国信息化建设现状，对我

1 OCTAVE: 是Operationally Critical Threat, Asset, and Vulnerability Evaluation首字母的缩写

国当前信息安全风险评估实践工作的总结、归纳、简化与提升。笔者在这里不想谈论各种标准指南的具体方法和过程。只希望对于组织在面对如此众多的标准及指南的时候如何选择的问题，提几点建议。

风险评估的基本理论涉及到的要素及相互关系（图1）在各个标准及指南中的体现

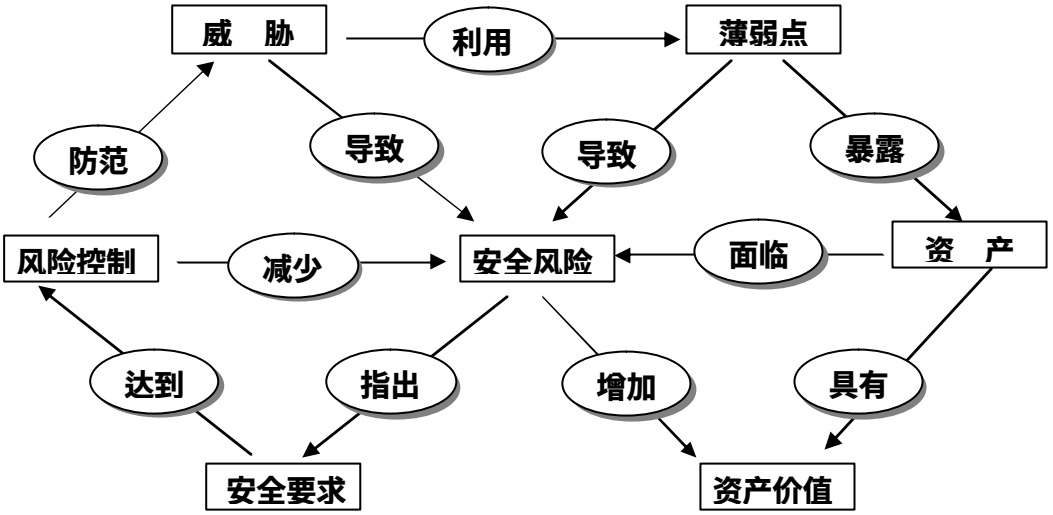

图1　　风险评估要素及相互关系

基本相同，但在各个标准及指南中都存在着一定的特殊性要求及过程。组织在风险评估策划阶段能够考虑范围、目的、时间、效果、组织文化、人员素质以及具体开展的程度等因素来确定评估的方法，使之能够与组织的环境和安全要求相适应，对整个评估过程的成败具有决定性作用。比如组织进行风险评估的目的之一是为了满足BS7799标准的要求建立信息安全管理体系，那么就必须满足BS7799对于风险评估的要求及过程，其他标准及指南基本上仅可以作为参考。如果组织是为了了解自身信息系统风险状况，开展风险管理的目的，那么NIST SP800-26可能是一个好的选择。在选择了参考的标准或指南之后，基本上确定了评估的方法论及评估流程，但是一些具体的准则的制定还是因组织的不同而不同的。例如信息资产的划分，虽然各种标准指南都给出了一些分类的方法，但也仅仅是一种参考，组织此时就必须根据对自己的“诊断结果”，制定适当的分类原则。再如对于威胁、薄弱点的识别与评价，小型的组织或简单的评估范围，选择头脑风暴的方式或许就能够达到目的，但是如果把评价等级制定的过于细化，可能对于小型组织就会带来资源的浪费和评估过程的复杂。因此选择适当的标准或指南制定明确的评估流程，策划适应组织的评估方法及科学的评估参考准则，是组织应该多花一点时间的，必要时笔者建议可以在小范围内试点，以检验策划的评估流程。组织在选择自评估的指南时，在某些关键阶段引入外部专家的培训可能也是在策划时应该考虑的问题，

毕竟风险评估还是一个专业性较强的过程。

评估过程中还可能选择一些辅助的工具，这里所说的工具是指风险评估过程软件，不包括类似于漏洞扫描之类的工具。虽然目前的各种工具并不是太成熟，但工具的成本投入一般较高，在选择的时候应该与策划的评估方法相适应，可以通过试用版检验一下其适用性。笔者的观点是 Excel 表格可能是最好的工具了，基本上不用培训，具有很强的统计计算功能。无论如何适合的就是最好的，风险评估的过程、方法、工具的选择都应遵循此原则。

五、 获得最高管理者对风险评估策划的批准

风险评估成败的关键性因素之一就是领导作用的体现。领导者的关注、资金的支持、资源的提供是风险评估项目过程中，组织的领导层应该充当的角色。风险评估的策划应充分考虑组织的商业需求及战略目标、企业文化、业务流程、安全要求、规模和结构、员工素质等因素，因此作为组织的最高管理者应该从全局的角度，对风险评估的策划结果进行评审。评估的范围和目的是否明确，是否合理；风险评估的流程及方法是否能够与企业文化及员工素质相适应；所提出的安全要求及所覆盖的业务流程是否符合组织的战略目标的要求，这些都应该得到最高管理者及管理层的认同。并且应该将批准的结果向评估范围所覆盖的部门及人员进行沟通，充分体现全员参与的原则也是保证风险评估过程及评估结果不出现较大偏差的保证。

六、 结束语

风险评估作为一个系统的过程，完善的策划过程十分重要，本文仅仅对一些重要的因素做了粗浅的讨论，希望能够对组织进行风险评估时的具体实施提供一点参考。相信在国家的指导下，通过国内各大安全厂商、先进组织、业内专家的共同努力下，我们必将建立适应我国国情、科学、系统的风险评估指南，使风险评估能够利用更科学的方法，不断提高水平，从而促进我国信息安全保障体系的建立，并进而推动我国信息化的建设历程。