atsec information security
Tel: +86-10-82893001
Fax: +86-10-82890017
www.atsec.com

如何高效地执行信息安全风险评估

信息安全风险评估工作对于组织进行信息安全风险的有效管理、识别并修复安全风险点具有非常重要的意义。而在风险评估工作的执行过程中，难免会走入一个极端：会因为合规或监管的要求而在极短时间内执行完成，因时间和人力等方面的分配，往往难以有效地发现和准确评价各种威胁的影响，使得风险评估流于形式。

在实际执行过程中，有些组织会将风险评估工作委托给专业的安全风险评估机构来执行。诚然专业评估机构具有很强的方法论和知识积累，然而如果对每一个客户都用完全相同的方法和知识库，难免会出现对某些风险评价的偏差甚至缺失。笔者认为，信息安全风险评估是一个安全性很强的工作，组织除了依赖于专业评估机构的能力以外，组织本身仍然需要明智地进行管理和影响，使得组织通过该过程可以真正有效地管理所面临的风险。以下是对于信息安全风险评估过程的一些理解和思路，也非常欢迎业界朋友批评指正。

一、组织所面临风险的定制化

在风险评估的准备阶段， 需要针对组织当前的情况进行大量的信息收集，再加上对信息的分析与整理，这将占用大量的时间资源。而如果不进行梳理，则无法达到风险评估的预期效果。而制定适合组织当前状况的评估项，相关的实践经验如下：

1、扩展安全威胁信息库以覆盖组织面临的主要风险

如基于常见的信息安全风险来开展，难免存在对于威胁的忽略和偏差。组织可以从以下角度来考虑威胁数据库的构建：

- 威胁的种类

比如可以从对组织产生影响的角度，扩展组织所适用的威胁库分类。atsec 在执行风险评估的积累过程中，将充分考虑物理、人员、流程、技术、法律以及合规等多个角度来进行威胁库的确定。

- 威胁的来源

组织在确定威胁的过程中，除了考虑自身面临的风险外，推荐从风险合规的角度来扩展威胁的信息来源。比如可以从 ISO-27001 的角度，侧重于在线业务的组织可以从 PCI-DSS 数据安全合规的角度来展开。当然，更多地也可以充分考虑所处行业的监管要求和行业安全标准等。

2、高效地进行资产的识别与评价

对于组织的信息资产，尤其是数据资产，难以进行有效地衡量和梳理。然而，风险评估过程中则需要对所影响的信息资产的价值纳入到评价体系。由此看来如何明智地组织资产的评价体系，并对资产进行合理评价是一个具有挑战性的工作。在该过程中，atsec 的执行经验如下：

- 建立有效的资产层次

通常的资产层次可以从物理位置（如 XX 组织的生产机房），到物理概念上的资产（如 XX 机房的 XX 服务器），再到操作系统，进而到应用软件，最终到其中的数据。经过多层次的资产划分后，其好处是使得威胁与资产具有了明确的关联关系，便于后续的风险评价。

- 有效地使用“资产组”的概念

在建立资产层次后，也会带来资产类别和梳理过程的工作量的成倍增加。在 atsec 执行风险评估的过程中，会充分考虑低层级资产的梳理难度，更多地从业务流程划分的角度进行归类，在最大程度上使用“资产组”的概念，尽最大可能使用组合的方法降低难度。

3、快速收集与评价组织的管理体系

风险评估的执行更多地侧重于发现安全管理过程中的差距，管理体系梳理与具体评价应更多地由内部或外部审计来完成。然而，在此过程中也需要有一定的介入并给出初步评价，以便于安全流程等方面的实际评估。

二、科学地提升执行效率和准确性

在风险的评估与评价阶段，项目团队的成员应把绝大部分精力投入到风险项的识别和级别定义，除了依赖于执行者的信息安全评估的经验外，使用有效的方法论和工具方法对于提升执行效率和准确性也具有非常重要的意义。

1、建立有效的风险分析模型

在风险评估过程中，atsec 所使用的风险分析模型会包括多个层面，以更有效地进行风险评价。模型方法如下：

- 风险发生的可能性
- 初步的控制措施
- 风险发生对客户业务的影响
- 风险发生对客户品牌的影响
- 风险发生对客户收益的影响

对于具体的分析过程，由评估人员基于访谈情况、渗透情况以及相关的信息输入，从品牌、收益和客户三方面的影响进行展开。每一选项的赋值基于方法论中的准则进行确定，下图为整个风险评估过程中，对数据库和应用系统存在威胁的评定示例：

Scenario Index	Scenario	Description	Threat	Vulnerability	Existing count	Things to remember for "Measures"	Incident likelihood (EW)	Main Asset	Brand impact (BI)	Financial impact (FI)	Customer impact (CI)	Potential damage (SA) = (BI + FI + CI)/3	Risk (EW * SA)
数据库													
DB	数据库安全	数据安全											
DB_r1	DB2数据库存在安全漏洞		数据库遭到攻击	机密信息泄	无	安装缺失的数据库补丁	B - low	DB2	4 - large damage	5 - very large damage	2 - small	4 - large damage	medium
DB_r2	MSSQL数据库存在安全漏		数据库遭到攻击	机密信息泄	无	安装缺失的数据库补丁	B - low	MSSQL	4 - large damage	5 - very large damage	2 - small	4 - large damage	medium
DB_r3	相同的密码应用在不同		数据库遭到攻击	相同密码的系	无	引入集中管理的认证机制	C - medium	数据库系统	1 - very small damage	3 - medium damage	1 - very small	2 - small damage	medium
DB_r4	没有密码规则或者弱的		数据库密码猜测	数据库账户密	无	引入密码策略	C - medium	数据库系统	1 - very small damage	1 - very small damage	1 - very small	1 - very small damage	small
应用													
App_vul	应用系统安	应用系统漏											
App_vul_r1	跨站(XSS)安全漏洞		互联网攻击	威胁客户的安全，业	无	研发人员对应用程序进行修改并定期对应用程序进行安全检测	D - high	业务系统	5 - very large damage	1 - very small damage	5 - very large	5 - very large damage	very large
App_vul_r2	CGI通用的Cookie注入漏洞	CGI Generic Cookie	互联网攻击	威胁客户的安全，业	无	研发人员对应用程序进行修改并定期对应用程序进行安全检测	B - low	业务系统	1 - very small damage	2 - small damage	3 - medium	3 - medium damage	medium
App_vul_r3	服务端远程执行	CGI Generic SSI	互联网攻击	业务系统被注入恶意	无	研发人员对应用程序进行修改并定期对应用程序进行安全检测	C - medium	业务系统	3 - medium damage	3 - medium damage	2 - small	3 - medium damage	medium

2、使用半定量化的风险计算方法

因威胁本身具有不断变化和难以测量的性质，推荐明智地使用半定量化的测试方法。在具体的执行过程中，atsec 的做法是通过对每个威胁的评估结果给出半定量的评级，并进一步通过风险计算方法使最终的评估结果更精确。因篇幅原因，在此不展开具体的风险计算方法。

3、使用自动化的风险计算工具

基于风险评估在执行过程中，atsec 使用自有开发的计算工具，以最大程度上节省风险计算所占用的工作量。

4、最大限度地使用辅助工具

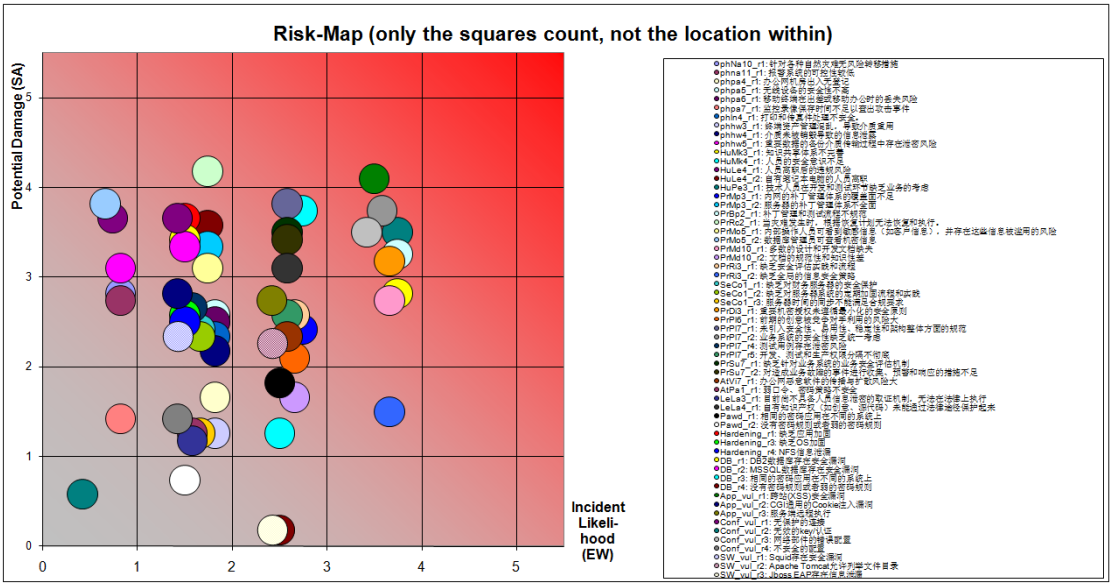
在对技术类威胁的评估过程中，如关键帐号和口令安全性，通过管理访谈方法通常难以做出准确的判断。atsec 则会在类似的过程中尽最大限度地使用各种辅助工具和手段，比如密码安全性验证、服务器的技术漏洞等。

三、评估结果的高效使用

在对所有的威胁完成风险评估后，如何有效地将风险结果转化为组织进行高效改进的发动机呢？

1、自动、清晰地呈现风险发现与结果

在发现并对信息安全风险进行评价后，自动地呈现风险结果与发现不仅可以极大地节省风险评估过程中的资源，也将使得管理层清晰地知晓关键的信息安全风险。这对于信息安全风险评估项目的收益具有非常重要的意义。在风险评估过程中，atsec 会通过自动化工具全面展现风险评估的发现与结果，如下图所示：



2、全生命周期的风险管理

一旦一个风险被识别出来之后，将对其整个过程进行管理和控制。通常的处理方法包括：风险降低（如通过技术手段降低其影响或可能性）、风险转移（如购买保险或通过第三方合同转移）和风险接受（管理层正式接受风险及其影响）等。建议组织在执行过程中使用自动化的工具跟踪每一个风险的最终处理方法，以避免风险项被忽略和措施不到位的情况。

3、自上而下的管理决策

对于识别到的风险，需要管理层投入资源进行处理，在此看来自上而下的管理决策非常重要。atsec 在风险评估管理过程中，会通过自动化的工具列举出来，然后需要组织的管理层首先进行低级别风险的接受，最后将工作着眼于中、高级别风险整改措施的确定。

4、通过投入产出比指导安全措施的制定

在排除可接受的风险后，所剩余风险项的管理也是风险评估后期的难点之一。在此过程中，atsec 推荐从投入产出比的角度考虑措施的制定。笔者认为，在整个信息安全风险评估过程中所做出的努力不仅仅是一项时间、金钱和人员的投入，而是一项为组织避免由安全风险带来更大安全损失的核心。能做到这个的关键一点是在风险整改措施的投入方面，应至少

要小于所避免的安全损失，这就要求借助于半定量化的指标来指导安全措施的选择，以达到最大的投入产出比。

在整个风险评估过程中，atsec 采用的半定量化的方法和结果仍然可用于达到此目的。举例来看，对于识别出的“应用层 XXX 漏洞”的整改措施，则可以基于应用的价值以及该漏洞的风险值确定该风险的损失值，而安装 WAF 设备、使用商业应用层漏洞扫描工具、使用开源工具进行应用扫描、由开发人员进行安全代码检查等措施每个的投入也可以从工作量和设备投入角度进行确认，这将使得最终的措施或措施组合为组织产生更大价值。