风险评估在 IT 运营管理中的应用

摘要

本文概括性阐述了风险评估工作在保险类行业中的运营管理模式，简要说明了风险评估工作中所包含的几个基本工作阶段和各阶段所需要注意的项目要点，在如何把风险评估工作的各项流程融合到企业 IT 治理的大环境、大框架中，如何使用风险控制的管理思路，改善企业 IT 基础架构的运营方面，做出了一定的探索和思考。

1、项目背景

太平人寿保险有限公司是经国务院同意，中国保险监督管理委员会批准的第六家全国性寿险公司，自从 2002 年全面恢复国内经营人身保险业务以来，被誉为"中国保险界的一颗新星"。

随着国家近年来对保险市场的大力推动和发展，保险行业开始进入迅猛发展的阶段。作为企业正常业务支撑基础设施的 IT 基础架构，也面临着新的挑战。一方面 IT 基础设施在企业业务开展的过程中作用越来越重大，大量的核心和支持业务系统都运行在 IT 设施上；另一方面，IT 设施的建设也必须能够迅速平稳的发展，才能够稳健的支持企业传统业务的升级和新业务的拓展。在这样的前提下，IT 设施的运营保障开始成为企业巩固和发展的核心议题之一，诸如 IT 安全保障和业务持续性计划之类的问题成为 IT 系统运营管理方面的主要任务。

为了对太平人寿的信息安全建设进行整体的规划，太平人寿经过长时间的调研、考察和交流，最终选择了天融信网络安全技术有限公司作为未来在信息安全方面的合作伙伴，并且和太平人寿共同做好风险评估、风险控制和安全战略规划等方面的工作。在本次项目中，天融信公司作为太平人寿的安全顾问对现有的信息系统进行了一次全面的安全风险评估，通过这次安全评估，充分分析了太平人寿目前安全现状和现有信息系统中存在的各种安全风险，并以此为依据和太平人寿共同制定了未来几年信息安全规划。

2、组织现状

太平人寿保险有限公司是一家全国性的寿险经营企业，在国内复业几年以来，迅速根据国内的市场情况推出了多种保险受理业务，遍布全国的分支机构也发展到数十个。在公司业务发展和开拓的过程中，IT 基础设施良好的支撑公诉主要业务的运作，同时随着业务发展，IT 基础设施的建设也在迅速扩展，并且越来越深的结合到企业的核心业务运营过程中。到今天，太平人寿已经建立了横跨全国十几个城市的广域网络，实现了各地营业部的业务数据集中化管理，建立了一个数据中心，包含数十个业务系统和上百台台服务器，并且目前正在

紧锣密鼓的进行业务持续性计划的建设中。

作为一家寿险公司，太平人寿的主要业务是为客户提供人寿保险服务，为保障业务的快速发展，适应市场的激烈竞争，必须大力推进信息化建设。通过普遍采用 IT 技术让自动化运营流程替代手工流程，逐步实现运营大集中和业务管理及决策信息化。总而言之，太平人寿对信息技术的依赖性将越来越高。

在企业发展的过程中，太平人寿管理层早已已充分认识到信息安全的重要性，并意识到信息安全不仅仅是负责 IT 工作的部门的责任，也是公司所有部门、员工的责任，因此之前太平人寿在 IT 管理和信息安全方面也做了很多工作。

在管理制度方面，太平人寿制定了《太平人寿信息系统安全管理办法》、《太平人寿计算机网络管理暂行规定》、《太平人寿机房管理暂行规定》、《太平人寿计算机病毒防范管理办法》和《太平人寿邮件系统管理办法》等信息安全管理制度。

在信息系统架构上，太平人寿的业务信息系统采用了数据大集中的模式，这种模式的好处在于，业务数据集中，通过有效的安全措施可以确保的数据的一致性和完整性，对公司业务的快速拓展提供了有力的支持。

在业务系统生命周期管理上，子业务系统在平台的选取上多数采用 UNIX / Linux + Oracle 的架构，此架构保证了一定的信息安全性。在子业务系统的开发过程中，对测试数据和源代码进行了严格的保护和控制。

当前所有关键的的 IT 设备和数据服务器都集中存放于数据中心机房，机房安装有门禁系统和监控设备，能有效地阻止未授权访问。

在网络架构上，进行了比较良好的网络拓扑规划，同时在主要边界和隔离节点上合理部署了防火墙、IDS 等安全设备。

通过以上一些方面的规划设计和安全措施，在一定程度上保障了整个信息系统的安全和稳定运行。这从太平人寿的信息安全历史数据也可以看出，在太平人寿的历史上从未出现过影响比较重大的安全事件，证明这些安全措施还是起到了很好的实际作用的。但是同是也需要认识到，由于缺乏完整的信息系统架构规划和安全保障计划，在信息安全的建设过程中没有总体指导方针，往往是在业务系统的建设过程中随应而上的，因此在某些方面存在一些缺陷和漏洞。并且随着业务系统规模的进一步扩大，各信息子系统之间的安全策略一致性、相容性、可实施性将受到比较大的影响。缺乏统一的安全规划，在未来的安全建设中难免会出现头痛医头、脚痛医脚的状况，这对整个信息系统的正常运营乃至信息系统对常规业务的支撑都是非常不利的。随着业务的快速发展，IT 基础设施的核心地位提升，太平人寿管理层迫切地感到，在 IT 基础设施运营方面需要一套全面的、稳固的、具有发展性眼光的完整安全体系作为信息安全管理工作的指导和支撑，才能应付瞬息万变的网络安全态势，在安全保障的战役中立于不败之地。

在逐步完善企业安全架构和 IT 治理框架的过程中，太平人寿希望能够找到一种合适的方法，明确清晰地分析出信息系统的安全现状、潜在风险和可能的影响，并以此为改进需求

的蓝本，规划出未来几年内信息系统的安全架构和方针策略。作为规划过程的重要起始步骤，信息系统风险评估能够分析出信息系统的安全现状和潜在风险，从而为后来的安全规划提供依据和指导，信息系统风险评估是一项重要而且不可缺少的工作。

3、项目目标和原则

太平人寿作为一家金融服务企业，对信息系统的安全性有着很高的要求。从理论上来讲，要消除太平人寿的目前所有安全风险是不切实际的，甚至也是不可能的。因为所要求的安全级别越高，在安全上花费的成本也会越高，同时高级别的安全设置也会导致系统运行的性能受到一定的影响，所以我们建议运用最小成本方法来实现最合适的安全控制，将风险降低到一个可接受的级别。

本次规划的目标是围绕信息系统安全的远景趋势和架构设计而制定，主要目标就是在保证信息安全的三要素（保密性、完整性和可用性）的前提下，建立健全企业信息安全组织和信息安全管理制度，完善各种信息安全技术防护体系，通过管理、技术、运维等多个方面，贯穿信息系统的规划、建设、交付、运行、废弃的完整生命周期，确保太平人寿信息系统安全、稳定、可靠的运行，为实现太平人寿的企业目标和使命服务。

在这样的使命要求下，作为一项严谨的系统性工程，太平人寿也对评估的过程控制和方法方式提出了一些原则性要求。

- 宏观性原则

  本次风险评估是分析信息安全的远景趋势，并建立未来的信息安全架构，这要求评估工作必须具有长远的眼光，立足在更高的层次上，进行信息安全的宏观性分析。

- 整体性原则

  风险评估工作作为建立安全体系框架的决策性依据，企业的信息安全目标必须符合本组织的总体战略，要求能够全面、完整的评估信息系统安全现状，绝不能以偏概全、管中窥豹的看问题。

- 扩展性原则

  风险评估工作不仅是建立安全体系框架的一个关键步骤，也是贯穿在整个信息系统安全建设周期中的一项重要周期性工作。作为一项循环的持续性工作，这要求风险评估的过程不仅要实现统一化、规范化，还要具有良好的模块化特性和通用型，这样随着信息系统的完善壮大，风险评估工作才能够良好的应用和推广到新建设的分支机构和业务系统中，实现整个组织安全策略建设的一致性、完整性。

- 延续性原则

  风险评估工作是一项系统工程，它并不是一成不变的固定模式。在安全建设的过程中，风险评估的流程也必须能够不断的完善和改进，才能更加贴近企业的管理文化和业务特色。并且随着信息系统的建设和进化，风险评估工作也必须能够不断接受新思想、新思路，跟随技术现状的进步而发展。

- 适用性原则

  信息安全风险的控制，应当是全方位的，它涉及到企业内部的每一个人、每一条方针、每一个业务模块。因此风险评估的过程必须能够切合务实的贴近企业实际情况，能够结合企业常规业务的具体特点，能够做到游刃有余的细致分析。

4、评估对象和范围

本次评估的范围是太平人寿信息安全所需覆盖的全部内容，包括总公司和各地分公司的所有信息系统软硬件的安全及所涉及到的相关人员、制度和流程等等。在整个项目过程中，太平人寿和天融信紧密结合，精诚合作，通过资产识别和资产价值评估、资产威胁评估、资产脆弱性评估、和综合风险分析等阶段，从管理、运行、技术三个方面，全方位的分析了企业信息系统的风险现状。

在本次项目对照的评估范围中，天融信按照国际安全标准 ISO17799 十大管理要项分析了太平人寿的安全管理现状，同时对包括所有数十台核心层、汇聚层、接入层和广域网连接的网络设备、近百台业务系统服务器、办公工作站 PC 共数百台的技术弱点评估。

在管理安全方面评估了信息安全策略、组织安全、资产的分类和控制、个人安全、物理和环境安全、通信和操作管理、访问控制、系统的开发和维护、业务连续性管理、策略一致性等十个重要方面。

- ✓ 安全策略（Security policy）的目标是管理层制定一套清晰的策略指导，为信息安全提供管理性的指导和支持。
- ✓ 组织安全（Organization security）的目标是管理组织内的信息安全；维护组织内被第三方访问的信息处理设备和信息资产的安全；维护信息处理外包给另外一个组织时信息的安全。
- ✓ 资产的分类和控制（Asset classification and control）的目标是为组织的资产提供适当的保护；确保信息资产得到了适当级别的保护。
- ✓ 个人安全（Personnel security）的目标是减少人为错误、盗窃、欺诈或设备误用造成的风险；确保用户意识到信息安全的威胁和利害关系，并做好准备在日常工作过程中支持组织的安全策略；把安全事件和故障造成的破坏降低到最低，监控并从事件中汲取教训。
- ✓ 物理和环境安全（Physical and environmental security）的目标是防止对商业基础设施和信息的非授权访问、破坏和干扰；防止资产损失、被破坏和商业活动的中断；防止对信息和信息处理设备的盗窃和损坏。
- ✓ 通信和操作管理（Communications and operations management）的目标是确保信息处理设备正确、安全的运行；将系统故障的风险降到最低；保护软件和信息的完整性；维护信息处理和通信服务的完整性和可用性；确保网络中信息的安全和基础支撑设施的安全；控制并从物理上保护介质来防止资产损坏、商业活动的中断；

防止组织间进行信息交换时信息的丢失、被修改和误用。

- ✓ 访问控制（Access control）的目标是控制对信息的访问；防止对信息系统的未授权访问；防止未授权用户的访问；保护网络服务；防止未授权的计算机访问；防止对信息系统内信息的未授权访问；探测未经授权的活动；确保移动办公和远程工作的安全。
- ✓ 系统的开发和维护（System development and maintenance）的目标是确保将安全融入信息系统的组成部分；防止应用软件系统中用户数据的丢失、改动或误用；保护信息的机密性、源认证和完整性；确保 IT 支持活动在安全的方式下进行并控制对系统文件的访问；维护应用程序系统软件和信息的安全。
- ✓ 业务连续性管理（Business continuity management）的目标是抵抗商业活动的中断并防止关键商业流程受到重大故障或灾难的影响。
- ✓ 策略一致性（Compliance）的目标是避免违反任何刑法和民法、法定的或者合同约定的义务、安全要求；确保系统符合组织的安全策略和标准；最大化审计的效果，并最小化影响审计和审计造成的干扰。

在技术性评估方面，天融信结合渗透测试、远程漏洞扫描、本地安全策略分析和漏洞检查等多种白盒和黑盒测试手段相结合，分别对十多个业务系统所属的网络设备基础设施、操作系统、数据库、数据中间件、应用服务器平台、应用软件进行了多层次、全方位的完整技术评估，并针对发现的漏洞提出解决方案或改进建议。

- ✓ 操作系统脆弱性评估整个信息系统中的七十多台各平台服务器操作系统（Windows Server 2000、Redhat Linux 9.0、Redhat Linux AS 2.1/3.0、Aix 5.0）进行了远程和本地漏洞扫描，并检查了本地安全的完整性、可靠性和一致性。
- ✓ 数据库平台评估对信息系统中重要的数据库和数据运作流程进行了深入分析，对数据库进行了以漏洞扫描为主的远程安全漏洞评估，和以本地安全配置检查为主的本地安全策略评估，完整地分析了数据库平台网络配置、系统漏洞、角色和账号管理、审计措施等各方面的安全问题。
- ✓ 应用服务器平台和应用软件评估，通过源代码黑盒测试、应用渗透测试、远程漏洞扫描、开发文档和安全策略分析等多种措施，针对各类应用服务进行了准确的脆弱性调查，比较完整的分析和提取了应用系统中可能存在的安全弱点。
- ✓ 网络设备评估，通过对网络设备的远程漏洞扫描、网络管理措施分析、系统网络架构分析、本地安全策略分析等多层次的手段，全方位的分析了整个信息系统中的网络基础设施和网络架构安全性，对于网络方面的主动和被动安全弱点有了比较深入的了解。

在整个信息系统的运行评估方面，天融信和太平人寿方面对应业务系统相关人员共同一起通过对资产管理、终端管理、物理和环境安全管理、通信和操作管理、角色和访问控制管理、系统的开发和维护流程管理、业务连续性管理等多个方面，结合信息系统管理安全评估

工作，对整个信息系统在运行维护和应用系统流程方面可能存在的弱点进行了全面分析。本部分评估工作作为一个中间型机体，良好的融合到了信息安全管理性评估和技术性评估工作中，有机地实现了对各业务系统安全状况的立体分析。

5、评估思路和方法

风险评估是一项系统工程，在风险评估概念发展的过程中，也出现了许多种用于生成评估结果的评估方法，是否能选择出一种合理、客观、准确、并且能够适用于相关业务，能够融和于企业发展文化的风险评估方法，是风险评估能否准确反映客观现实，取得良好结果的重要因素。在本次风险评估工作中，经过太平人寿和天融信双方的研究和协商，最终摸索出了一套适合太平人寿自身的风险评估方法，能够良好的结合到太平人寿的 IT 治理框架中，能够取得客观准确的评估结果，能够为后续的信息安全管理和 IT 治理工作提供良好依据。

5.1、评估指导思想

在风险评估工作的开展过程中，考虑到本次项目的最终目标、项目的投入和成本需求、工作方法的适用性和可用性、太平人寿的企业文化等诸多方面的因素，我们拟定了进行风险评估的基本工作思想：定性结合定量，自动结合主动，客观结合主观。

- 定性结合定量

  因为太平人寿进行风险评估工作的主要目的是作为信息安全架构设计的前驱步骤，为后续的安全管理和安全建设作决策支持，主要目的是给出风险分布的蓝图，只要分析出风险可能涉及的信息系统方面和程度即可，并不要求给出具体精确的经济损失等量化数据，因此太平人寿的风险评估工作方法上主要采取分级、定性的思路，同时在一部分需要并且也可能明确具体数据的方面采取定量的方法。例如在威胁评估、资产价值、和风险综合分析的过程中，都普遍采用了分级定性的方法；同时在资产统计、脆弱性详细评估等重要而且具体的细节工作阶段，采取了精确的定量分析方法。

- 自动结合手动

  考虑到太平人寿的风险评估工作，不仅是一项一次性的工作，而且还要结合到未来的 IT 治理框架和信息安全保障体系中，作为一项周期性的工作开展，因此在工作方法上也要求快速、有效。因此在风险评估工作的过程中，在大量重复性工作中，我们采取了很多自动化的工作步骤，力求快速、准确的取得所需的评估数据，在尽可能少的影响到业务系统正常开展的前提下，尽可能逼近实际情况的取得所需数据。例如在资产统计和评估阶段中，我们采取了 nmap、solarwinds 等设备发现工具，结合一些自动化脚本，很快的取得了大致的资产分布状况；同时在未来的 IT 治理过程中，正在尝试部署一套合适的资产管理软件，为未来的 IT 管理和风险评估工作减轻工作负担；在脆弱性评估方面，我们使用了 Nessus、ISS InternetScanner 等自动化漏洞扫描工具，准确快速的取得了信息系统的脆弱性分布数据；在风险综合计算分析阶段，采用了大量的自动化分析

和风险评估过程控制工具，快速准确的计算出了风险评估的数据结果和定性表，同时产生可视化的数据结果，给评估工作生成直观的报告和参考。

同时由于仅靠自动化工具，是难以满足千变万化的业务和信息系统现状的，所以在评估过程中，各种手动分析手段也必不可少。手动性工作主要集中在管理评估部分，关于工作站安全、安全管理制度的制定、安全策略的执行等方面，都需要大量经验丰富的工作人员进行精确、细致的严谨检查和认真分析；同时在信息系统的技术安全评估方面，也需要安全专家进行深入的准确分析，例如应用系统源代码分析、操作系统的本地安全评估、网络安全设备的安全配置策略检查、网络设备的系统漏洞和策略缺陷分析等等。

■ 客观结合主观

风险评估工作的重要原则就是数据的准确性、客观性。但是在实际的工作过程中，因为接触到的很多因素都是抽象的、逻辑的、主观的，同时例如资产威胁等因素的概念相对空泛，在历史上风险评估的方法论中也没有提出过很好的具有客观性、准确性并且为各方所共同认可的评估方法。在风险评估工作中，切不可一味的求准、求全，否则很容易影响到整个工作的宏观思路，容易产生挂一漏万的片面性结果。因此在太平人寿的风险评估工作中，确定了客观为主，结合主观的评定方法。在大多数风险因素的分析工作中，都秉承客观准确的工作原则，例如对资产的清理和统计、资产脆弱性的详细分析、安全策略的分析等，都给出了完整精确的客观报告。但在某些相对难以评估的风险因素上，采取一定的由安全专家和信息系统管理人员的历史经验得来的评定方法，从而把精力更多的方在其他重要因素的分析上，节省时间和精力，加快项目的开展进度。例如在资产的间接风险价值和影响评估工作中、资产受到风险威胁的可能性评估工作中，主要是根据管理人员和维护人员的历史经验和协商认可，给出相关数据的定性分级表数据。

5.2、风险综合分析算法

风险评估的一项核心内容就是风险因素计算方法。历史经验中较常使用的几种评估计算方法主要有预定义风险价值矩阵法、风险大小相对威胁的排序表计算法、风险可能性结合危害评估资产价值计算法、风险接受程度计算法等。

各种计算方法的内容和特点恕不赘述，在本次评估项目中，经评估小组协商和讨论，综合考虑太平人寿信息系统的现状和企业文化等因素，摸索出了一套符合自身实际情况和未来工作框架的评估算法，以模糊集合理论为基本数学依据，对资产重要性进行分级，从资产重要性(或保护等级)及资产脆弱性出发，结合威胁分析，使用粗略的矩阵相乘算法得出风险分布的分析结果。

基本的思想为如下公式：

风险 = 威胁发生可能性 x 系统脆弱性利用的可能性 x 对系统的综合影响(或系统的重要性等级)

在评估过程中充分体现了前段所述的基本工作思路，即以定性为主、定量为辅的思想。在评估过程中的威胁、影响等过程都采用定性分析的方法，在系统脆弱性的现场调查分析阶段，对详细的漏洞分布情况采用定量分析的方法。

在风险评估的实际操作过程中定量分析步骤主要集中在现场调查阶段，针对系统关键资产的安全因素进行定量的调查、分析，为后续评估工作提供参考依据。

在资产价值分析时采用传统的资产评估方法模型，以资产识别为基础，依次对信息系统中各业务所包含的物理资产、软件资产、数据资产以及各资产受到安全威胁时所产生的关联影响进行量化分析，生成每个业务系统和资产的资产价值量化表。

$V=\{ H,S,D \}$

$A=\{ [V,..],M,E \}$

V: 物理资产价值；H: 硬件价值；S: 软件价值； D: 数据价值；

A: 业务(信息系统)总价；M: 业务关联； E: 业务影响。

在分析系统威胁因素时采用威胁树模型。威胁树就是将信息系统所面临的各种威胁因素以树状形式描述出来。根节点分别是系统信息资产的 CIA 属性，然后逐层进行分解。上层节点由下层节点构成，下层节点描述的威胁可以触发上层威胁。

$T=\{G,E,Q\}$

G:节点；E:节点间的通路；Q:影响系统功能的子树通路

根据威胁的不同作用形式，存在两种构成关系：

串连关系：对威胁实施者而言，必须完成每个步骤才可以达到最终的目标，即“与”的关系。

并联关系：对威胁实施者而言，只要完成其中的一个环境，就可以达到攻击目标的目的，即“或”的关系。

在对威胁进行分解时应遵循以下步骤：

- 定义相关安全目标作为系统分析主题。
- 从攻击模式确定分析主题的威胁，进行分解，形成中间节点。
- 将中间节点进一步分解，根据需要将子节点作为分析目标重复进行分解。
- 形成最终相互独立的叶子节点。

对于一个威胁通路可以表示为：

$q_i:G_i(U_j(V_k(X_m(Y_o\cdots\cdots))))$

其中 q 代表通路；G 代表根节点； U、V、X、Y 等分别代表中间节点和叶子节点。

对分析主题的威胁集可以用各子树的通路集表示：

$TC=\{q_1, q_2, q_3\cdots\cdots q_n\}$

威胁树中的叶子节点表示了系统可能受到的最小威胁。

最后，在风险评估的风险综合分析阶段主要采用定性的分析方法。由于该阶段所需数据往往很难精确统计或统计成本过高，通常采取结合人员经验的方法进行实施。

在风险分析模型公式中，发生频度、可能性因素都不能够用非常精确的数据进行表示。

而如果将威胁事件对系统的综合影响用定量的数据进行说明的话，则要从系统设备价值、维护成本、运行成本、经济损失等方面计算影响，其中还不包括对资产所有者信誉损失的衡量。

在实际的操作过程中，将上述因素进行定性量化是切实可行的方法，在量化结果生成后，根据相对坐标再把量化的数据结果换算成定性分析的结果。

在综合分析阶段，首先对威胁树中的各种威胁因素出现的可能性进行定性分析，可以划分为以下几个等级：

低	中	高
威胁因素存在但发生的可能性极小	威胁因素存在且有一定的发生可能性	威胁因素存在且发生的可能性极大

然后，对系统技术和管理脆弱性的利用也可定性划分为三个级别

低	中	高
组织管理中没有相关的薄弱环节，很难被利用	组织管理中没有明显的薄弱环节，可以被利用	组织管理中存在着明显的薄弱环节，并且很容易被利用

低	中	高
技术方面存在着低等级缺陷，从技术角度很难被利用	技术方面存在着一般缺陷，从技术角度可以被利用	技术方面存在着非常严重的缺陷，很容易被利用

风险的计算我们采用风险矩阵计算公式方法，风险的计算公式函数为：R=f(A，T，V)，其中 R 代表风险，A 代表资产，T 代表威胁，V 代表安全弱点，每项因素对应相应级别分别赋权值为(1,2,3)，使用矩阵相乘算法实现风险因素的平均分布。这里我们将风险也分为高中低三个级别，综合资产、威胁和安全弱点的因素，根据矩阵相乘公式最终得到风险的值。

安全风险的严重性与风险值的对应关系如下：

高：　　风险值 R >= 12

中：　　风险值 11 > R >= 5

低：　　风险值 4 > R >= 0

参考上述的标准，结合专家经验和历史数据可以确定出风险评估计算公式中各因子的数值，为威胁树中的各项威胁因素计算出对系统构成的风险，最终形成对整个系统的风险评估。

低	中	高
事件影响很小； 局部业务受到轻微影响；	事件有一定影响； 造成一定的声誉损失；	事件影响极大； 造成声誉的重大损失；

	一定的经济损失； 整体业务受到一些影响；	巨大的经济损失； 整体业务严重受到影响；

5.3、管理评估主要方法

在管理评估阶段，评估小组主要采取以下方法收集信息供分析使用。

■ 调查问卷

为了收集相关信息，评估人员设计并分发调查表给太平人寿相关人员填写，调查表也可以在面对面交流的方式下使用。

■ 人员访谈

通过访谈管理和技术人员，评估人员可以收集到大量有用的信息，也可以了解到被访谈者的安全意识和安全技能等自身素质。由于访谈的互动性，不同于调查表，评估人员可以广泛提问，从多个角度获得多方面的信息。

■ 文档检查

为了分析现有的或计划采取的安全控制措施，需要检查策略性文档（例如政策法规、指导性文档）、系统文档（例如用户手册、管理员手册、系统设计和需求文档）和安全相关文档（例如以前的审计报告、风险评估报告、测试报告、安全策略、应急预案）等。

■ 现场勘查

评估人员也会对办公环境和机房内设备作现场检查，寻找是否有违反安全策略的现象，比如敏感文件随意放置、人员离开电脑不锁屏幕、设备的网络连接情况等。

5.4、技术评估主要方法

在技术评估阶段，评估小组主要采用自动化评估辅助工具、配置检查等技术手段对现有系统的技术措施进行识别是进行资产技术脆弱性分析的重要方法。

对于信息系统中固有的漏洞、弱点可以通过评估工具获得具体数据信息。如针对主机、服务器等设备进行漏洞扫描，生成完整的扫描报告；对于系统、应用的日志审计，从中发现问题。

为系统中关键设备制定检查列表，在现场按照检查列表对相关设备的系统安全配置、应用安全配置、完整性进行调查，如系统帐号安全情况、系统访问控制策略等，参照安全标准对系统安全性配置进行评估。

根据系统网络拓扑结构，明确系统网络边界；检查网路设备的配置情况，如交换机 ACL、VLAN 等；标明网络薄弱点；对网络的可靠性和安全性进行评价。

对现有安全技术措施的评估主要为检查设备配置的合理性，安全策略的设置是否满足需求，是否存在配置缺陷等。可以采用检查列表的方式进行。

通过评估工具获取业务系统的数据流量以及峰值流量出现时间，描述出业务数据的流向，采用流程图方式表述系统业务流程。根据应用安全需求，判断各业务流程中存在的安全性问题。

6、项目过程控制

在整个评估过程中，天融信的资深安全专家和太平人寿信息系统相关人员共同组成评估小组，严格遵循 CMMI 安全工程模型和 ISO9000 PDCA 的质量管理思想，循序渐进、稳扎稳打的完成了评估的各阶段工作。并且在实践过程中，不管改进评估方法，总结出了一套符合 ITIL 管理规范的模块化评估工作方法，使其能够良好的结合和运用到今后的信息安全建设过程中，作为一项常务性、周期性的工作在整个信息系统各子部分的运作周期中良好开展。

整个风险评估项目的主要过程如下：

- 资产统计。

统计了太平人寿的网络设备、机房服务器、PC、其他非 IP 设备、软件清单和文档清单，为划定评估范围作准备。

- 威胁评估。

双方项目组举行座谈会共同分析太平人寿所面临的安全威胁来源，分析其利用弱点造成破坏的可能性。

- 技术弱点评估。

通过网络扫描方式分析网络设备和服务器开放的端口和所运行服务的弱点，结合人工本地评估方式分析服务器的安全配置，主要存在一些弱口令和补丁未打的安全隐患。采取调查表和顾问访谈方式收集太平人寿现有 13 个业务系统的信息，并对其中 5 个系统进行了远程渗透测试，得出太平人寿现有业务系统的安全现状。

- 安全管理评估。

对太平人寿现有安全策略、安全制度、机房和办公环境的物理安全进行了调查和现场勘查，并访谈了公司高层领导和维护管理员，详细分析了目前的安全管理制度和策略体系。

- 信息系统综合风险和现状分析。

通过对信息资产、威胁和安全弱点的评估，综合分析生成安全风险的评估结果。

7、项目成果和经验

经过太平人寿和天融信双方共同的协作和努力，太平人寿保险有限公司信息安全咨询项目工作最终圆满完成，并基本达到了项目设计的预期目标。通过本次项目，进一步完善了太平人寿企业安全组织和安全管理制度，完善了各种安全技术防护体系，初步建立了太平人寿保险有限公司信息系统安全保障体系的思想框架，从而对确保太平人寿信息系统安全、稳定、可靠的运行，为实现太平人寿的企业目标和使命提供安全保障，对保障正常业务的快速发展和企业目标的稳步推进起到了良好作用。

在本次项目中，通过整个项目的开展和进行，提升了整个公司业务人员的安全意识，提高了组织管理人员和系统维护人员的安全管理认识和技术水平，为整个企业信息系统的安全建设和发展打下了扎实基础。

在风险评估工作过程中，通过项目组双方人员的良好互动和认真仔细的检查，完成了太

平人寿本次项目相关范围内的资产普查、威胁分析和漏洞检查等工作；对部分业务人员工作站进行了随机抽查，分析了太平人寿在安全意识培养和安全管理方面存在的弱点；分别从技术、管理两个方面，结合企业的业务系统特点和业务流程，全面细致的分析了整个信息系统中存在的安全缺陷。最后，对安全管理体系、网络架构、主机设备、应用系统等方面多层次、全方位的进行了综合分析，并提出解决方案或改进建议。

通过本次风险评估项目，天融信和太平人寿安全评估小组共同对太平人寿信息系统进行了全面细致的评估，并取得了一系列非常有价值和指导意义的评估分析报告：

《太平人寿资产调查总结报告》

《太平人寿安全管理评估报告》

《太平人寿安全威胁分析报告》

《太平人寿网络架构安全分析报告》

《太平人寿主机设备安全分析报告》

《太平人寿应用安全分析报告》

《太平人寿安全渗透测试结果报告》

《太平人寿安全风险评估和现状报告》

在评估阶段完成后，紧接着项目组又完成了初步风险控制和安全整体规划阶段的工作，依赖于前一阶段中风险评估的成果，针对太平人寿的业务情况和企业特色，分析和撰写了安全整体规划、安全管理制度、培训建议书、安全组织管理体系等一系列企业信息安全架构的规划文档，用于今后进行安全建设的指导方案。对于今后分步实施、逐步完善安全体系的建设，并且跟随业务系统的进化而进行安全保障体系的改革都起到了良好的指引作用。

通过本次安全评估和咨询项目，太平人寿保险有限公司实现了项目规划中的预期结果和设计目标，圆满完成了各技术部分的基础工作，比较完整的完成了安全管理体系方面的建设，在一定程度上提升了整个企业的安全保障水平，并为未来的持续性安全建设和保障过程建立了坚实良好的基础。