策略是组织对信息系统的安全风险进行有效的识别和评估后，所采取的各种措施和手段，以及建立的各种管理制度和规章等。

请以“**论信息系统项目的风险管理与安全管理**”为题，分别从以下三个方面进行论述：

1、概要叙述你参与管理过的信息系统项目（项目的背景、项目规模、发起单位、目的、项目内容、组织结构、项目周期、交付的成果等），并说明你在其中承担的工作。

2、结合项目管理实际情况并围绕以下要点论述你对信息系统项目风险管理和安全管理的认识。

（1）项目风险管理和安全管理的联系区别。

（2）项目风险管理的主要过程和方法。

（3）请解释适度安全、木桶效应这两个常见的安全管理中的概念，并说明安全与应用之间的关系。

3、请结合论文中所提到的信息系统项目，**介绍在该项目中是如何进行风险管理和安全管理的（可叙述具体做法），并总结你的心得体会。**

论信息系统风险与安全管理

摘要：

2018 年 3 月，我作为项目经理参与了某省执纪审查工作管理系统的信息项目建设。该项目总预算为 670 万元，总工期为 12 个月。该项目目标是为省纪委及下属各地市派驻纪检组纪检监察员为其提供各类执纪审查工作综合性服务，提高纪委审查工作效率。在项目建设中，我深刻认识到信息系统风险与安全管理是本次项目成功实施的关键，我做好规划风险管理，风险识别，风险定性和定量分析，风险应对措施。风险控制和安全管理的工作，通过这些措施保障了系统的安全、高效、可靠，有效降低该系统信息泄露、篡改等的安全风险，有效为执纪审查做好保密支撑工作。最终，项目按预期顺利完成，项目组得到了公司与客户方的一致好评。

正文：

2017 年 3 月我公司顺利中标某省纪委的《执经审查工作信息管理系统》，合同额 670 万元，历时 12 个月，于 2018 年 3 月全面通过业主方验收。该系统采用 B/S 模式开发，是为省纪委及下属各地市派驻纪检组纪检监察员提供各类执纪审查工作综合性服务。项目启动后，我被公司任命为乙方的项目经 ，全面负责项目的建设管理工作。**【背景字数偏少】**

由于系统中保存执纪审查案件有关数据信息，**其安全性要求相当高，如果系统在安全性设计上不够完善，那带来的风险是巨大的。省纪委领导相当重视，一再要求确保安全性。在项目建设中，我将风险管理和安全管理列为本次项目成功实施的关键。因此在项目初期，在制定风险管理计划的同时，同时也制定适度安全策略，保障了系统的安全、高效、可靠的运行，最终项目按预期顺利完成，项目组得到了公司与业主方的一致好评。以下我从风险与安全策略为出发点，从规划风险管理，风险识别，风险定性和定量分析，风险应对计划，风险控制，在风险管理的过程中加强安全管理工作等方面对进行论述。**

一、在规划阶段做好规划风险管理、风险识别、风险的定性和定量分析，根据风险登记册做好风险应对计划，根据适度安全的相关标准做好防止“木桶效应”的相关计划和措施。

在风险管理的规划阶段，我召开相关会议，与相关干系人和相关专家，根据项目管理计划、项目章程、干系人登记册、事业环境因素和组织过程资产等等相关资料制定了风险管理计划和安全管理计划。其主要内容是：根据合同及国家相关标准执行风险和安全管理，加强风险和安全的相关知识培训，进行全面质量管理，让干系人时刻保持安全和质量意识。该项目的风险分为已知风险和未知风险，分别做好应急储备和管理储备。安全管理计划的核心策略是做好“七定”（定方案、定岗、定位、定员、定目标、定制度、定工作流程），提高系统的安全性和稳定性。首先定方案按照适度安全的标准，我们设定等保是第二级系统审计保护级，并制定安全管理

未知的风险有国家政策和技术标准的变动，自然灾害等等，分别制定了相关应对措施清单，风险责任人，并制定了相关的应急储备和管理储备。之后整理会议，得到风险登记册，并更新相关文件。

根据风险登记册等等相关资料，我们采用风险分类和风险紧迫性评估技术进行风险定性分析，对相关风险进行排序，已知风险的顺序是：沟通不到位，质量问题，范围蔓延，成本超支，安全管理不到位；未知风险的顺序是：自然灾害，国家政策和技术标准的变动。随后我们采用了定量风险分析和专家判断技术进行了风险的定量分析，我首先将风险发生的概率分为“极低、低、中、高、极高”这五级（对应值是 5、4、3、2 和 1），沟通不到位影响程度是 5。质量问题影响程度是 5。范围蔓延影响程度是 4。成本超支，影响程度是 3，安全管理不到位影响程度是 4。对于未知风险：自然灾害、国家相关政策变动、技术更新影响程度是 5。随后进行项目文件更新。根据风险登记册，我们采用风险应对策略技术制定了相关的风险应对措施，对于沟通不到位我们采用定期、不定期采用会议，发放需求调查表和问题提交表等等方式就行沟通处理。加强全面质量管理和培训，提高质量意识。**在安全管理方面严格按照系统审计保护级实施了粒度更细的自主访问控制，通过登录规程、审计安全性相关事件和隔离资源，使用户对自己的行为负责。因为信息系统就和一个木桶一样，其安全水平是由构成木桶最短的那快木板决定的，因此我加强设备安全、数据安全、内容安全、行为安全管理，减少“木桶效应”。会议中对其它风险做好应对计划，做好应急储备和管理储备。会后把风险应对计划上报高层，经其批准，随后更新相关的项目管理计划和项目文件。**

二、在风险和安全控制阶段，严格按照相关制度和流程进行风险和安全管理，依据风险应急计划处理相关风险，减少“木桶效益”。

在该过程组中，我要求项目管理办公室定期或不定期的到相关科室收集需求调查表和问题提交表，总结归纳，然后交于我们项目团队进行处理。我每天都对当前活动收集齐 AC,EV,PV,CV,SV 等相关进度、成本工作数据，对其进行分析，对好的、坏的都进行分析归纳，找出其中的机会和威胁，进行相关的措施。为减少“木桶效应”严格执行系统审计保护级的规定，进行系统安全再评估、日志分析等控制方法，同时对重点监控日志采取了动态评估及定期评审，我以周和里程碑为单位，定期对系统安全日志实行再评估、审计。每周的项目例会中将系统安全管理作为单独一个议程，对系统威胁应对措施实施的有效性以及当前系统的状态进行检查。如果发现问题，团队成员集体讨论，对应对措施进行纠偏。

在该项目的风险和安全管理中，好的安全管理可以减少或减轻风险带来的危害。严格按照安全管理制度执行相关安全工作，是保证信息系统安全的有利保障。同时如果不注意安全管理的相关工作，就会给项目带来更多的风险，因此加强设备安全、数据安全、内容安全、行为安全管理是十分必要的，减少了“木桶效应”，提高大家的安全意识。

该项目经过全体成员的努力，在 11 个月内完成了该项目，实际花费 650 万元人民币，比合同提前了 1 个月，节约近 20 万元人民币，赢得了一致好评。回顾而言，项目的成功很大程度上归功于我在项目的风险管理中采取了我采取积极的措施，积极的沟通、培训、实施全面质量管理来应对风险。但是在项目培训过程中，由于对一些工作人员的工作时间没有充分考虑，耽误及三天的时间，增加了培训直接成本，之后我采取措施，根据工作安排调整了该培训计划，晚上或周末休息时间对没有参加培训的人员进行加班培训，这次教训告诉我在以后的工作中一定要结合实际情况，及时了解相关干系人的工作和休息时间，来制定计划。我把这次教训总结在我自己的工作失误笔记中，以备后期项目提供组织过程资产。

2018 年 5 月，我有幸参加了国网 XX 省电力公司电子商务平台系统项目的建设，该项目为项目型组织结构，我担任项目经理。项目历时 1 年，投资 450 万元人民币，是国网**省电力公司信息化计划的重点工作。项目于 2019 年 5 月，顺利通过甲方的验收，赢得甲方的一致好评。该系统由采购公告、专家评审、合同管理、供应商管理、财务管理、质量监督等模块组成，每个模块下设若干个子模块。本文结合我的实际经验，以该项目为例，讨论了信息系统项目建设过程中的风险管理和安全管理，按照规划风险管理、识别风险、实施风险定性分析、实施风险定量分析、规划风险应对、控制风险等方面内容，就如何实施安全管理步骤进行阐述，有效提高了风险管理和安全管理水平，满足了项目干系人的需求和期望。

【正文】

国网 XX 省电力公司电子商务平台系统项目是在国网**省电力公司信息化计划的重点工作的背景下于 2018 年 5 月启动，我公司中标该项目，中标金额为 450 万元。本人在该项目中担任项目经理。项目历时 1 年，通过甲方的验收。该平台的成功建立，为国网**省电力公司建立一个公平、公开、公正的采购环境，最大限度控制采购成本，降低企业的运营成本，实现资源集约化管理，防止招标采购环节的暗箱操作，预防腐败，对招标信息“阳光化”具有重要的意义。电子商务平台系统实现了信息管理公开化、透明化，招标环节模块化，流程化管理，规范采购审批流程，提高了决策效率和协同化办公。该系统由采购公告、专家评审、合同管理、供应商管理、财务管理、质量监督等模块组成，每个模块下设若干个子模块，系统按照高内聚，低耦合的原则进行研发。招标电子商务平台使用 C/S 架构，数据库采用 oracleIOG,服务器采用联想小型机器，编程语言为 C++中间件使用 weblogic,采用 SVN 工具作为配置管理工具。为保证项目的进度和质量，我结合以往的项目管理经验及该项目自身的实际情况，在项目内部分为商务及外协小组（3 人），需求分析小组（2 人），系统规划及架构小组（4 人），开发小组（10 人），测试小组（3 人），现场调试小组（2 人），系统集成小组（5 人）。

针对这样一个专业性强、涉及面广、实施复杂、周期性较长以及与客户密合度高的项目，要使项目能够顺利实施，执行严格的风险管理和安全管理至关重要。风险管理就是要在风险成为影响项目成功的威胁之前，识别着手处理并消除风险的源头。而安全管理就是从物理安全、运行安全、数据安全三方面开展工作，确保信息安全，做好安全管理工作有利于降低项目的风险。在本项目中，我根据项目具体情况，遵循风险管理和安全管理的方法，对项目风险管理和安全管理进行了探究，包括规划风险管理、识别风险、实施风险定性分析、实施风险定量分析、规划风险应对、控制风险等进行阐述，带领团队成员经奋战，获得了项目的成功。

一、规划风险管理，执行安全管理制度

俗话说，凡事预则立，不预则废。作为一名有多年项目管理经验的项目经理，我做任何事情之前必须进行规划，因为好的规划是成功实施的基础。根据项目章程和项目管理计划，编制风险管理计划。我参照干系人登记册，邀请相关项目干系人和风险管控专家参加了会议，共同讨论后制定出风险管理计划。风险管理计划包括了方法论、角色与职责，预算，时间安排，概率与影响矩阵，报告格式等。**结合本项目的特点和电力公司的系统安全生产规范，我制定了该系统的安全制度规范。**

二、识别风险

识别风险就是判断哪些风险会影响项目，并以书面的形式记录其特点。风险识别是一个需要全员参与的、反复的过程，因为可能随着项目的进展，会有新的风险出现。我带领团队以风险管理计划、成本管理计划、范围基准、项目文件等为依据，用 SWOT 分析方法，从项目的优势、劣势、机会和威胁四个角度研究，识别项目中存在的风险，并深入讨论对风险，最后形成初步的风险登记册。**在本项目中，识别出网络安全风险，而网络安全是系统安全的重要组成部分。在后面会做进一步的分析。**

三、定性风险分析，重视安全管理

定性风险分析就是要做好对风险概率和影响的评估和汇总，进而对风险进行排序，以便随后的进一步分析和行动。我们召开风险分析会，根据风险管理计划中的定义，对风险进行风险概率和影响评估，将风险影响分为“很高”、“高”、“一般”、“低”四种等级，并通过建立概率与风险矩阵来确定风险的优先级。**确定网络安全作为风险的第一位，因为一旦出现网络安全的缺失，可能会影响项目的进度，进而影响项目的整体绩效。特别系统涉及电力公司的一些机密的信息，比如站线变户信息、用户信息、用电情况等敏感数据，因此确保网络安全是非常重要的。会后，我们对风险登记册等文件进行了更新。**

五、制定风险应对措施，做好应用安全

制定风险应对措施就是针对项目目标制定提高机会、降低威胁的方案和行动。对于积极的风险，可以采取的应对策略有开拓、提高、分享、接受；对于消极的风险，可以采取的应对策略有规避、转移、减轻、接受等。针对风险登记册里面的每一个风险，我们都制定了风险应急策略。**适度安全就是在安全管理工作中，要制定合适此系统的安全策略。木桶效应就是一只木桶能装多少水取决于它最短的那块木板。因此要全面做好安全工作。比如，在应用安全上，我们会做好出厂功能及性能测试，入网安评测试，代码审查，安全设计方案等。在管控项目中可能存在用户越权操作的安全风险的时候，我们制定的措施是对用户的权限的配置是配置满足需求的最小权限。除此之外我们还做好安全渗透测试，挖掘是否存在跨站，越权操作等应用安全的风险，及时补齐短板，再——修复 BUG。**

六、控制风险，落实安全策略

在整个项目生命周期中，跟踪已识别的风险、监测剩余风险、识别新风险，实施风险应对计划，并对其有效性进行评估。在本项目中我们主要采取风险评审、技术绩效测量等方法，通过每两周开展风险例会的形式，及时发现项目建设过程中存在的风险，提高项目团队成员的风险意识。当然在风险监控过程中，也不可避免的产生一些变更，我们都是按照变更控制流程处理的，召开变更会议，并及时请业务部门主管签字确认变更内容。**在这个过程中，我们做好安全风险的监控，重视人员安全、网络安全、应用安全、数据安全，并按照安全策略做好安全风险监控工作。通过我的监控，项目顺利进行。**

国网 XX 省电力公司电子商务平台系统项目于 2019 年 5 月全部上线，并顺利通过甲方的验收，至今已经稳定运行 6 个多月时间，运行状态良好，得到用户的一致好评。在本项目的风险管理中，我总结了要坚持不懈地做好项目的风险和安全管控工作，可能在项目执行的过程中会出现一些意料之外的问题，需要分析偏差，及时更新过程文件，才能更好地完成既定的项目工作。

然而虽然本项目取得了较好的成绩，但也存在一些不足：比如对项目干系人分析不到位，项目的管理过程中注重了向相关业务科室负责人和局领导的汇报，而忘了物资部的业务骨干，造成系统需求获取不全面，项目组及时发现了这一问题，深入调研物资部及下属供电公司物资域同事的实际工作需求，得以及时改正。在以后的项目管理中我要以此为经验，加强项目的风险和安全管理，不断滚动识别风险，做好安全策略，更好的完成项目的管理工作。