会话管理主要是针对验证通过之后，服务端程序对已建立的、且经过验证的会话的处理方式是否安全，一般会从以下几个角度检测会话管理的安全性：

- Session 是否随机

Session 作为验证用户身份信息的一个重要字符串，其随机性是避免外部恶意用户构造 Session 的一个重要安全保护机制，通过抓包分析 Session 中随机字符串的长度及其形成规律，可对 Session 随机性进行验证，以此来确认其安全性。

- 校验前后 Session 是否变更

通过身份校验的用户所持有的 Session 应与其在经过身份验证之前所持有的 Session 不同。

- 会话储存是否安全

会话存储是存储于客户端本地（以 cookie 的形式存储）还是存储于服务端（以 Session 的形式存储），同时检测其存储内容是否经过必要的加密，以防止敏感信息泄露。

(22) 无效验证码

目标系统管理入口（或数据库外部连接）存在缺少验证码，攻击者可利用弱口令漏洞，通过进行暴力猜解，获取网站管理权限，包括修改删除网站页面、窃取数据库敏感信息、植入恶意木马；甚至以网站为跳板，获取整个内网服务器控制权限。

1.8.5.应急事件响应服务体系

应急事件响应，是当安全威胁事件发生后迅速采取的措施和行动，其目的是最快速恢复系统的保密性、完整性和可用性，阻止和降低安全威胁事件带来的严重性影响。

应急事件主要包括：

- 病毒和蠕虫事件
- 黑客入侵事件
- 误操作或设备故障事件

但通常在事件爆发的初始很难界定具体是什么事件。通常根据安全威胁事件的影响程度来分类：

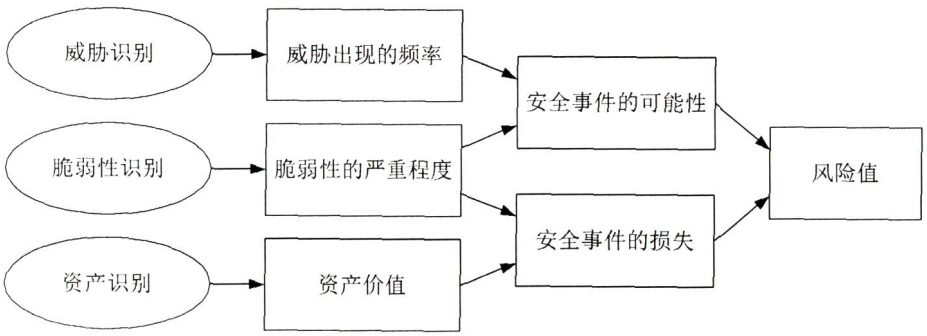
- 单点损害：只造成独立个体的不可用，安全威胁事件影响弱。
- 局部损害：造成某一系统或一个局部网络不可使用，安全威胁事件影响较高。
- 整体损害：造成整个网络系统的不可使用，安全威胁事件影响高。

当入侵或者破坏发生时，对应的处理方法主要的原则是首先保护或恢复计算机、网络服务的正常工作；然后再对入侵者进行追查。因此对于紧急事件响应服务主要包括准备、识别事件（判定安全事件类型）、抑制（缩小事件的影响范围）、解决问题、恢复以及后续跟踪。

1.8.6.风险评估

1.8.6.1.风险评估原理

风险评估中要涉及资产、威胁、脆弱性等基本要素。每个要素有各自的属性，资产的属性是资产价值；威胁的属性可以是威胁主体、影响对象、出现频率、动机等；脆弱性的属性是资产弱点的严重程度。



风险评估的主要内容包括：

- 对资产进行识别，并对资产的价值进行赋值；
- 对威胁进行识别，描述威胁的属性，并对威胁出现的频率赋值；
- 对资产的脆弱性进行识别，并对具体资产的脆弱性的严重程度赋值；
- 根据威胁及威胁利用弱点的难易程度判断安全事件发生的可能性；
- 根据脆弱性的严重程度及安全事件所作用资产的价值计算安全事件的损失；
- 根据安全事件发生的可能性以及安全事件的损失，计算安全事件一旦发生对组织的影响，即风险值。

1.8.6.2.风险评估原则

- 保密原则

评估方将严格遵循保密原则，服务过程中涉及到的任何用户信息均属保密信息，不得泄露给第三方单位或个人，不得利用这些信息损害用户利益。并与业主单位签订保密协议，承诺未经允许不向其他任何第三方泄露有关信息系统的信息。

- 互动原则

在整个信息安全风险评估过程之中，将强调客户的互动参与，不管是从准备阶段，还是识别阶段。每个阶段都能够及时根据客户的要求和实际情况对评估的内容、方式做出相关调整，进而更好的进行风险评估工作。

- 最小影响原则

信息安全风险评估工作应尽可能小的影响系统和网络的正常运行，不能对业务的正常运行产生显著影响（包括系统性能明显下降、网络阻塞、服务中断等），如无法避免，则应对风险进行说明。

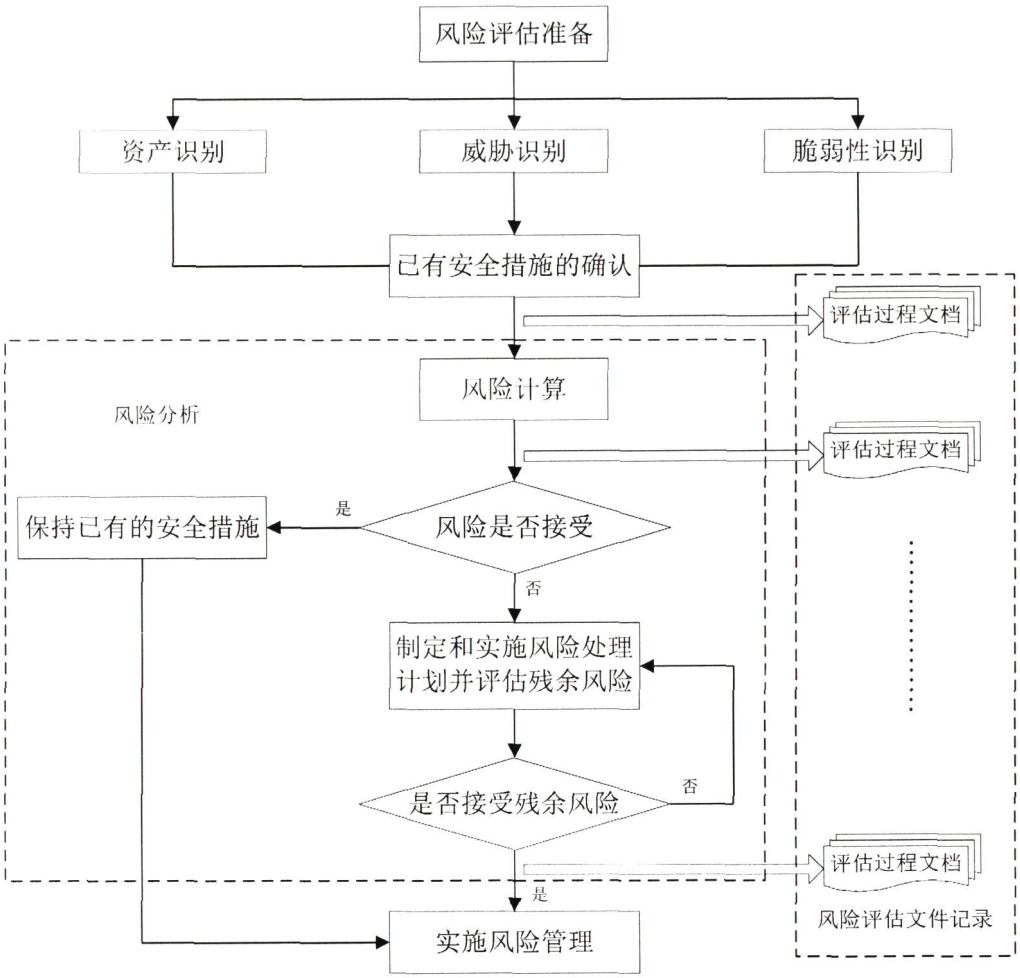
- 规范性原则

信息安全风险评估服务的实施必须由专业的安全评估服务人员依照规范的操作流程进行，对操作过程和结果要有相应的记录，提供完整的服务报告。

- 质量保障原则

在整个信息安全风险评估过程之中，将特别重视项目质量管理。项目的实施将严格按照项目实施方案和流程进行，并由项目实施小组从中监督、控制项目的进度和质量。

1.8.6.3.风险评估实施流程



1.8.6.4.风险评估的准备过程

风险评估的准备过程是信息系统进行风险评估的基础，是整个风险评估过程有效性的保证。信息系统对信息及信息系统进行风险评估是一种战略性的考虑，其结果将受到信息系统业务需求及战略目标、文化、业务流程、安全要求、规模和结构的影响。因此在风险评估实施前，应当：

1. 确定风险评估的范围；
2. 确定风险评估的目标；
3. 建立适当的组织结构；
4. 建立系统化的风险评估方法；

5. 获得最高管理者对风险评估策划的批准。

1.9. 设备与软件配置

本项目充分利用现有软硬件资源，保护原有投资。在现有信息系统的基础上，对系统二次开发，实现与数据对接互联互通平台的连接。新的应用模块的开发，，充分利用数据对接互联互通平台提供的开发与运行环境，使面向不同需求的新的应用可以被快速开发，避免重复建设和资金浪费。确保系统的安全性和可扩展性。要从系统设计、软硬件选型等方面进行全方位、多层次的安全防范，保证系统高效、稳定、不间断地运行。平台提供开放的接口，便于各类应用系统连接，以满足业务和系统不断拓展的需要。

2. 项目组织机构与人员

2.1. 项目组织机构

根据本项目业务需求和特点，拟组成项目建设领导小组。领导小组下设项目办公室，具体承担项目的联络、协调工作。办公室下设若干工作组，分别负责工程的相应工作。同时，成立项目专家顾问组，对项目实施方法和每个阶段产生的成果进行评审、咨询，为工程实施提供技术支持。通过招标确定具有资质的单位对项目进行全过程监理。

2.1.1.项目专家咨询小组

项目专家咨询小组由项目相关领域专家组成，为本项目的设计与实施提供咨询和建议，协助审核各阶段的计划、实施方案，对重大变更向领导小组提供建议。专家组成员应包括：政策理论、技术（网络、数据库、软件、信息安全等）、标准制定和业务等层面的专家。

2.1.2.项目管理机构

2.1.2.1.项目管理小组

项目管理机构负责落实项目建设资金，并对整个项目的实施进度进行督促、检查。它的职责：配合项目资金主管部门做好沟通协调，保障项目建设资金按时到位；督促、检查项目建设资金使用情况，做好内部项目审计；向武进区信息服务平台领导项目小组汇报项目资金执行情况。

2.1.2.2.项目管理过程

开发标准：参照 ISO9001 的相关标准进行。

代码编写管理：项目开发在编写代码时必须遵循一个统一的代码编写标准，其内容主要是常量、变量、对象、函数的命名，注释的风格，缩排等等。

文档编写：为了保证在软件系统开发的各个阶段中工作的规范、健壮、可延续等，各个阶段的工作都必须形成相应的文档。

责任分工：设立项目开发组长，协调小组内的所有任务，小组内的每个成员根据各自特长分工，当遇到相应的问题时，都有相应的人员来解决。

协调与沟通：小组定期检查进度及解决所发生的问题。

修改方案、设计等的管理办法：需要改动时，由具体相关人员向组长提出申请，经讨论通过后执行修改，并将相关资料存档。

出现问题的解决办法：小组内的问题由组长协调解决，小组内不能解决时，由更高层协调解决。

双方的配合及沟通办法：定期进行项目开发进度沟通，通报项目进展情况，双方积极配合、相互支持协商解决遇到的问题。

2.1.2.2.1.　项目进度管理

项目进度计划的编制必须满足用户的需求。

实施项目进度计划。项目经理根据项目进度计划，合理安排好项目各阶段的资源投入，确保实际进度与计划进度相一致。

跟踪项目进度计划。在项目实施过程中，项目经理负责定期跟踪、检查项目进度实施情况。当项目发生脱节、脱期时，应及时分析原因，提出项目报告，调整项目进度计划。

检查、跟踪项目进度的方式可以采用《项目进度报告》、重要节点处的评审、汇报、会议纪要等形式。

编写项目进度报告。工程项目进度报告是项目进度的检查、控制手段。在项目实施过程中，项目经理应根据项目开发计划，定期对项目进展情况进行必要的检查和分析。在项目阶段评审时，填报《项目进度报告》。

2.1.2.2.2. 项目质量管理

- 质量保证规划：在项目规划阶段，质量保证应协助项目经理及项目组成员完成项目的质量策划和质量计划的编制指导。
- 质量保证人员组织编制《质量保证计划》。
- 质量保证工作计划指明了质量保证对于项目的管理承诺和职责，明确了要进行的质量保证活动。质量保证计划要经过质量保证主管审批。审批后质量保证严格按照计划执行质量保证活动。
- 质量保证实施：质量保证根据计划所进行的评审和检查活动，以及活动后进行的质量保证反馈。活动可以根据相关的检查列表提示问题进行，也可以根据项目实际进行检查。重点是：
- 鉴别和帮助减轻项目风险；
- 提供给高级管理者对开发活动的可视性；
- 提供在软件开发过程持续改进的反馈效果。
- 质量保证检查和改进：质量保证活动本身也要定期进行检查和持续改进活动，因而质量保证活动中要注意收集度量数据，根据检查情况进行持续改进。
- 对质量保证的检查工作由质量管理部组织。

2.2. 项目建设机构

2.2.1.规划协调小组

规划协调小组负责整个项目系统规划、总体设计、总体技术方案的落实。它的职责是：根据工程建设的总体目标、建设规模与总体方案规划设计的要求，在业务及其计算机应用现状进行全面调研以及反复研讨的基础上，编制工程开发实施的指导性文件，并在工程开发实施过程中，进行必要的咨询与支持。

2.2.2.技术支撑小组

技术支撑小组负责对整个项目的开发过程，进行全面的组织、协调与管理。它的职责是：拟订项目的总体计划、阶段目标、项目规章制度、项目标准与规范；跟踪项目进度，进行资源调度，按照工程总体计划进行实施监督指导；向武进区农村改革试验工作领导小组汇报项目进展情况，提出项目工作报告；同时加强软件开发、质量保障和支持服务。

2.2.3.项目开发小组

项目开发小组负责整个项目的具体实施、设计工作。主要包括项目经理、专家指导委员会、分析设计小组、开发小组、测试小组、质量与控制小组。各角色人员负责项目开发的不同阶段工作，保证项目正常部署上线。

2.3. 运行维护机构

为了保证本项目建成后的良好运行，将成立一支经验丰富、技术过硬、管理规范的信息化人才队伍，主要负责平台运维工作，包括网络、操作系统、数据库、应用系统、安全系统、备份系统、硬件维护等工作，保证系统平台的稳定运行。

2.4. 技术力量和人员配置

本项目的开发实施技术力量和人员配备，有以下人员参与：项目经理、系统构架师（技术负责人）、需求分析人员、数据库设计人员、程序设计人员、程序编码人员、项目管理人员、质量保证人员、实施人员等。

2.4.1.项目经理

主要职责：

- 整个项目的规划、资源调配、监控和进度报告。进行人员、设备、其它资源的统筹与管理。
- 与用户方相关人员协商制定项目实施总体计划，确认项目阶段目标（里程碑）的设置，并监督完成情况。
- 对项目进行总体监控，审查确认项目状态，监督项目进展。
- 协调解决关键性、全局性问题。
- 重大问题、解决方案的决策，审核确认重点流程或方案。
- 及时向用户方相关项目负责人汇报项目进展情况。

2.4.2.专家指导委员会

1、主要职责：

- 对项目组提供业务指导。
- 理解项目的业务目标，定期对项目情况进行评审，把握项目方向。
- 定期审阅项目工作报告，监督项目进展；
- 评审项目计划和其他一些全局性的项目决策。
- 对项目变更进行评审。

2、人员组成：

由用户业务专家和技术专家，以及其他方业务专家组成。

2.4.3.分析设计小组

主要职责：

- 进行软件系统的需求调研、分析工作
- 进行软件系统的设计工作，对系统需求的技术实现与系统性能负责。
- 参加有关需求和设计方案的讨论，提出技术实现方面的意见。
- 协助实施人员制定测试计划和测试用例。

2.4.4.开发小组

主要职责：

- 完成项目的编码和单元测试，对软件的质量和开发进度负责。
- 配合测试工程师进行测试工作，并负责修改测试过程中所发现的缺陷。

2.4.5.测试小组

主要职责：

- 制定测试计划、编写测试方案和测试用例。
- 负责进行软件的功能测试和性能测试。定期发布测试报告以及缺陷统计报告。
- 配合开发工程师修改测试过程中所发现的缺陷。

2.4.6.质量与控制小组

主要职责：

- 对项目质量进行总体监控，定期进行项目健康检查。
- 对项目进行过程中的问题，及时向项目管理委员会汇报。
- 具体组织项目的各项评审工作。
- 负责项目的配置管理工作。
- 负责项目相关环境的配置。提供开发工具的支持。
- 负责软件版本的发布

2.5. 人员培训

2.5.1.培训目标

➢ 进一步提高用户方对本项目的认识和对信息技术的掌握程度；全面提高业务人员操作和系统应用水平；培养一批既懂现代信息技术又各部门业务的高素质的信息技术骨干队伍。

➢ 方法论转移。在项目定义阶段我们将进行有效的沟通和培训，以标准开发流程为蓝图，按照本项目的实际情况进行剪裁和定制，提交完整的实施文档。

➢ 产品知识转移。在实施过程中从浅到深的多层次的培训，建立客户基本产品知识；再在实施过程中双方共同实施，实现全方面的产品知识转移。

➢ 技术转移。除了完善的技术培训，帮助用户方技术人员拥有足够的技术能力维护和发展系统，免除客户后期维护的后顾之忧。

2.5.2.培训计划

培训对象：所有相关使用人员，包括决策人员、管理人员、操作人员等。

提供资料：培训计划安排表、各部门培训大纲及教材、操作手册、岗位职责。

培训目的和内容：根据三个层次的培训安排，分别对用户方决策层、管理层、操作层制定各自的培训目标和内容。

培训工作重点：

➢ 会同项目实施人员与系统的业务流程，并在培训过程中强化和推行新的业务流程。

➢ 在管理层培训中根据不同部门有所区别。整个培训过程中进行技术操作培训和管理培训。

➢ 根据系统业务流程和应用功能，培训人员编写操作手册，作为产品的帮助文件，并且随着新功能的应用，对操作手册进行添加。

2.5.3.培训质量保证与控制

➢ 有计划地安排各种培训，提高员工技能水平。

- 对项目培训质量进行总体监控，定期进行培训效果检查。
- 对项目培训进行过程中的问题，及时向项目培训小组汇报。
- 对项目培训的各项内容进行考核。维护培训的最终考核在用户方现场进行。考核设备的组成、基本原理、调试、检查、和操作运行，日常设备维护及突发事件应急处理等。

3. 投资匡算

3.1. 投资匡算的有关说明

3.1.1.估算范围

本次项目武进区农村集体经济组织“一户三权”数字化集成管理项目基础层、支撑层、应用系统层、展现层的建设工作。投资内容包括软件购置、开发、测试及安装。

3.1.2.编制依据

本项目可行性研究报告中的主要建设内容及投资估算主要依据为：

- 《电子建设工程概（预）算编制办法及计价依据》（HYD41-2005）
- 《电子建设工程预算定额》
- 《计算机、网络设备及布线安装工程》
- 《电子设备技术场地安装工程》
- 《国家电子政务工程建设项目管理暂行办法(55 号令)》
- 国家及地方其他有关估算规定和取费标准

根据实施单位现有条件和项目具体情况，设备费及软件费主要根据厂商报价及以往采购中标价。

3.1.3.估算说明

（1）本项目投资概算编制依据国家建设项目投资估算的有关规定编制，投

资估算遵循“符合规范、结合实际、经济合理、不重不漏、计算正确”的指导原则。

（2）前期工作费用主要包括可行性研究，参照计投资〔1999〕1283 号文中的计算方法进行估算。

（3）项目专家评审费用参照当地的专家评审劳务报酬标准

（4）项目监理费用为项目施工过程中付给监理公司的费用，参照发改价格〔2007〕670 号文中的计算方法进行估算。

3.2. 总投资匡算

本项目建设预计固定资产投资约为人民币 110 万元，

（一）农村集体资产资源“一张图”开发，经费 50 万元；

（二）“一户三权”融合管理开发，经费 35 万元；

（三）电子权证服务开发，经费 25 万元；

工作量投入明细表

序号	项目阶段	子项	工作成果	计划投入工作量（人/天）
1	需求设计	需求调研	会议记录等材料	3
2		需求分析	角色功能划分	3
3			业务流程图	5
4			数据流程图	8
5			功能分析	18
6		原型设计	原型设计图	5
7		需求文档编写	需求规格说明书	2
8	demo 设计	前端 demo 设计制作	可向客户汇报的交互静态 demo（含地图）	20
9	软件开发	一户三权融合管理	可上线运行的软件安装包	420

10		农村集体资产资源一张图管理	可上线运行的软件安装包	500
11		电子权证服务开发	可上线运行的软件安装包	310
12	软件测试	测试用例（测试点）编写	测试用例（测试点）	10
13		功能测试	测试规格说明书	40
14	项目实施	安装配置	软硬件配置清单	5
15		项目验收	验收材料	20