LanSecS 信息安全等级保护综合管理系统技术白皮书

北京圣博润高新技术股份有限公司

2010-10

目 录

1. 系统开发背景.....1
2. 系统概述.....3
3. 系统架构.....7
4. 系统功能.....9
4.1. 定级备案管理.....10
4.2. 建设整改管理.....11
4.3. 等级测评管理.....12
4.4. 安全检查管理.....13
4.5. 风险评估管理.....14
4.5.1. 风险评估测评.....15
4.5.2. 风险评估管理.....17
4.6. 日常办公管理.....18
4.7. 统计分析.....19
4.8. 基础数据管理.....20
4.9. 分级管理.....21
4.10. 系统接口.....22
5. 系统特色.....23
5.1. 等级保护管理工作流程化.....23
5.2. 信息系统安全性评价标准化.....23
5.3. 丰富的报表和数据展现能力.....24
5.4. 快速生成结构化文档.....24
5.5. 支持多级部署.....24
5.6. 完备的数据接口.....25
6. 系统安全性.....25
7. 系统部署.....26
8. 系统配置要求.....26

1. 系统开发背景

1994 年国务院颁布的《中华人民共和国计算机信息系统安全保护条例》 明确规定，“计算机信息系统实行安全等级保护”。2003 年中央办公厅、国务院办公厅转发的《国家信息化领导小组关于加强信息安全保障工作的意见》明确指出，“要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度，制定信息安全等级保护的管理办法和技术指南”。

2004 年公安部等四部委共同会签印发了指导相关部门实施信息安全等级保护工作的纲领性文件——《关于信息安全等级保护工作的实施意见》，该文件对我国信息系统安全等级保护工作的重要意义做了明确的阐述，提出了信息安全保护制度建设的原则和基本内容，明确了实施信息安全等级保护的职责分工、工作要求和实施计划。这一文件的出台标志着我国信息安全等级保护工作进入正式的启动阶段。

2007 年公安部等四部委联合出台了《信息安全等级保护管理办法》，该文件是在开展信息系统安全等级保护基础调查工作和信息安全等级保护试点工作基础上，由四部委共同会签印发的重要管理规范，主要内容包括信息安全等级保护制度的基本内容、流程及工作要求，信息系统定级、备案、安全建设整改、等级测评的实施与管理，信息安全产品和测评机构选择等，为开展信息安全等级保护工作提供了规范保障。

2007 年 7 月 16 日四部委又联合会签并下发了《关于开展全国重要信息系统安全等级保护定级工作的通知》，并于 7 月 20 日联合组织召开了“全国重要信息系统安全等级保护定级工作电视电话会议”。上述文件的出台和工作会议的召开，拉开了我国重要信息系统安全等级保护定级和备案工作的序幕。随后《信息系统安全等级保护基本要求》、《信息系统安全保护等级定级指南》等一系列信息安全等级保护国家标准相继颁布，在相关标准支持下以及公安部牵头组织的信

息系统安全等级保护定级培训工作的基础上，各行各业迅速展开了重要信息系统的等级保护定级备案工作。在两年多的时间里，基本完成了行业内的重要信息系统安全等级保护定级和备案工作。信息安全等级保护工作取得了阶段性的成果。

2009 年，在全国信息系统安全等级保护定级工作基础上，公安部又印发了《关于开展信息安全等级保护安全建设整改工作的指导意见》，开始部署和开展信息系统等级保护安全建设整改工作。2009 年下半年公安部组织各部委和各行业开展了信息安全等级保护安全建设整改工作的集中培训，明确了我国信息安全等级保护安全建设整改工作的工作目标、工作对象、工作内容和要求，并对具体的工作流程和工作方法提出了指导意见。要求各行业利用三年时间，通过组织开展信息安全等级保护安全管理制度建设、技术措施建设和等级测评等三项重点工作，落实等级保护制度的各项要求。

2010 年上半年，公安部又印发了《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》，该文件提出了等级保护测评体系建设和等级测评工作的目标和工作内容。

由上述可以看到，我国信息安全等级保护工作已经全面展开。从目前已经完成的信息系统等级保护申报的情况看，已经备案的信息系统大约为 5 万个。我国的信息安全等级保护工作将成为我国未来数十年国家信息安全建设的重点工作内容，并将通过持续开展和循环改进，成为国家信息安全建设的一项基本制度和重点工作。

未来一段时期内，我国信息安全等级保护工作的任务非常艰巨，工作量非常庞大。统观我国信息安全等级保护工作的各个环节（如重要信息系统定级备案、安全建设整改、风险评估、等级测评、监督检查等），在信息安全管理制度建设、技术体系建设和管理体系建设等关键活动中，必然离不开技术工具和管理工具的支撑。相关部门和机构也陆续研发了多种工具，如公安部开发了等级保护定级备案管理平台，为重要信息系统的定级备案工作开展提供了工具支持；公安部第一研究所与北京圣博润合作开发了信息安全等级保护测评与评估支撑系统，为信息安全等级测评机构开展等级测评工作提供了工具支持。

这些工具的应用，显著提高了我国信息安全等级保护工作的效率。但是，不可否认，这些技术工具尚未形成体系化的工具库，还无法满足我国信息安全等级

保护工作对管理工具的迫切需求。因此，如何促进相关管理工具的开发，是信息安全等级保护监管部门、行业主管部门、行业用户和信息安全企业共同面临的迫切问题之一。

在此类工具中，目前监管部门、行业主管部门和行业用户需求最为迫切的是一个以等级保护为核心的信息安全基础工作平台。通过这个基础工作平台可以为用户提供信息安全等级保护工作的日常管理和常态化运行管理，从而提高等级保护工作的效率，减少信息安全管理人员的管理压力。

圣博润公司正是在这一背景下，很早就开始与相关职能部门进行密切的交流，了解和跟踪信息安全等级保护综合管理系统的实际应用需求，从 2007 年开始信息安全等级保护综合管理系统的相关技术研究、产品研发和持续改进等工作。并推出了具有自主知识产权的 LanSecS 信息安全等级保护综合管理系统 V3.0 版本。

2. 系统概述

“LanSecS 信息安全等级保护综合管理系统”是一套适用于我国信息安全等级保护工作业务管理的综合信息管理平台。通过该平台，可对信息安全等级保护工作中定级、备案、安全建设整改、等级测评和安全检查等各个工作环节中的信息和数据进行集中管理和统计分析，并对上述各个工作环节的工作流程进行规范化管理。具体来说，产品可解决如下几个方面的问题：

1) **信息安全等级保护信息与数据缺乏集中管理**

当前信息安全等级保护工作中各种信息和数据大多依靠简单的 EXCEL 表格进行管理，手工操作任务繁琐，不利于信息与数据的汇总和统计，本项目产品将解决这一难题，有效提高等级保护工作效率。

2) **信息安全等级保护工作流程缺乏必要的约束**

各行业开展等级保护功过过程中，难以有效避免因人而异、因时而异、因事而异的工作状态，各项工作流程缺乏必要的约束。本项目产品的应用，将有利于提高等级保护工作流程的规范性。

3) **缺乏有效的信息安全等级保护工作考核依据**

各行业等级保护主管部门对等级保护工作的执行和工作成效的考核没有统一的量化的标准，对等保工作和人员的考核缺乏依据。本项目产品将有效解决这一难题。通过提供标准化、流程化的办公平台，为等级保护工作的考核提供数据支持。

4) 信息安全建设整改工作统一指挥和协调难

等级保护安全建设与整改工作是一项任务紧迫、形势复杂、周期较长的工作。这一工作必须要统一指挥和协调，才会取得良好的工作成效。本产品为各行业的安全建设整改工作提供了一个统一指挥和协调的工作平台，将有效解决安全建设整改工作的指挥和调度困难问题。

作为等级保护工作开展所依赖的基础工作平台，信息安全等级保护综合管理系统可在如下方面促进信息安全等级保护工作的开展。

1) 实现信息与数据的集中管理和分析处理

信息安全等级保护综合管理系统可对各种信息安全等级保护基础数据实现集中存储和管理，不但保证了数据的完整性和一致性，也为行业等级保护工作的开展提供了可靠的数据支持。通过数据统计和分析，可为等级保护工作的进一步开展提供决策支持。该系统可管理的数据包括如下多种类型：

- 系统定级、备案数据；
- 建设整改数据；
- 等级测评数据；
- 安全检查数据；
- 风险评估数据；
- 等级保护政策标准；
- 安全管理制度与管理措施；
- 信息资产；
- 安全事件；
- 测评机构与人员；
- 专家库；
- 教育培训数据。

针对上面各类数据，本系统能够进行集中管理和统计查询，并快速生成种类丰富的报告和报表，极大的方便了等级保护工作的信息系统定级、备案、安全建设整改、安全测评、安全检查等工作。

2) 规范等级保护工作流程，提高工作效率

信息安全等级保护综合管理系统为信息安全等级保护的多个工作环节提供了基于工作流引擎的工作流程管理功能，如安全建设整改、安全检查、风险评估等。通过流程定制，使得行业管理人员可按照统一的工作流程开展行业的等级保护工作，避免了不同单位、不同管理人员在执行等级保护工作过程中的随意性。促进了等级保护工作环节的标准化和规范化。另外，通过流程管理，使得数据处理和工作部署实施的自动化程度大大增强，从而有效提高了等级保护工作的效率。

3) 提升行业等级保护工作管理的透明度

信息安全等级保护综合管理系统通过预置部门、人员、角色和工作流程，实现了行业用户等级保护工作开展过程中的部门、角色的分工协作。通过内置的办公管理模块，让等级保护工作执行人员及时受理和完成分配的工作任务，让管理人员及时掌握等级保护工作的开展情况，实现可视化的等级保护工作管理。

行业主管部门通过该系统可以对等级保护工作的进度进行跟踪。可有效改善原有等级保护工作对整体管理过程的不可跟踪性和管理效果的不可预见性。

行业主管部门通过该系统还可对每个等级保护参与人员的工作进度、工作状况、工作结果进行直观的检视。同时，根据预定义的评价指标，对等级保护工作的执行效果进行客观的考核和评价，大大增加了管理的透明度。

4) 提升行业等级保护工作的整体实施能力

通常，各行业的等级保护工作执行人员并不一定是安全领域的技术专家，这往往会导致等级保护工作中出现领导层与执行层工作脱节，具体执行工作难于直观的反映到信息安全保障工作的直属领导层面，出现信息安全等级保护工作执行上的不透明，直接导致管理工作的执行不彻底和不到位。

信息安全等级保护综合管理系统在各行业开展等级保护工作的过程中，通过规范工作流程、完善数据管理、提供教育与培训等，提高等级保护工作人员的等级保护工作意识、理解等级保护工作职责、促进等级保护工作的规范化。利用系

统的内置的各种工作流程，可将等级保护工作要求迅速分解到相关技术部门和人员，大大降低了单位内部的协调复杂性，提升了行业等级保护工作的整体实施能力。

5) 促进等级保护工作管理的常态化

信息安全等级保护综合管理系统提供了安全整改活动、等级测评活动、安全检查活动和风险评估活动的流程管理功能，为各行业开展的新一轮安全建设与整改工作以及等级测评工作提供了可靠的技术支撑。

信息安全等级保护综合管理系统的定位和目标是为我国各行业开展的等级保护工作建设一套运行可靠、管理严密、控制有效、信息全面、监管有力、便于维护、高效安全的工作平台。实现信息系统定级备案、安全建设整改、等级测评和安全检查等工作的信息化管理，提升等级保护工作的效率和管理水平。

信息安全等级保护综合管理系统提供了涵盖等级保护工作所有工作环节的管理功能，是一个以等级保护为核心的集成的、综合的信息安全基础工作平台。该系统可有效促进各行业等级保护工作管理的常态化。

3. 系统架构

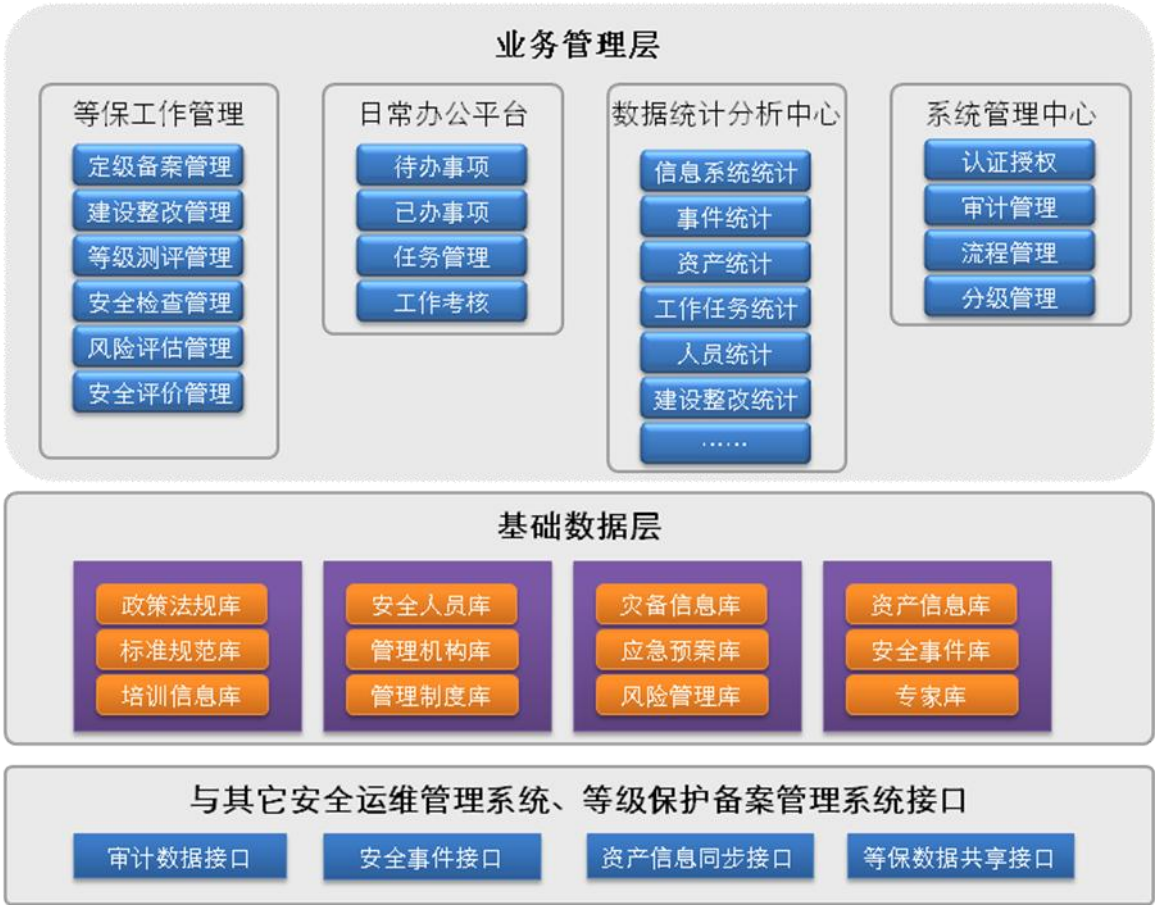

图 1 系统架构示意图

上图是 LanSecS 信息安全等级保护综合管理系统的总体框架结构示意图。系统总体分为业务管理层、基础数据层和接口层三个层次。业务功能层是软件主体功能，包括等级保护工作管理、日常办公管理、数据统计与分析和系统管理几个部分。基础数据层维护等级保护工作所需的各类基础数据，接口层负责与其它安全运维管理系统或等级保护相关系统的数据共享和交互。

1) 等级保护工作管理

等级保护工作管理以信息安全等级保护工作为主线，对等级保护工作中的定级备案、安全建设整改、等级测评、安全检查、风险评估、安全评价等各个工作环节进行规范化管理，包括信息与数据的收集、工作流程管理等。

2) 基础数据层

基础数据管理为信息安全等级保护综合管理所需的各种基础信息与数据提供统一的维护与管理。包括政策法规、标准规范库的管理，安全管理机构、人员

和管理制度库的管理，灾备信息、应急预案、应急演练的管理，教育培训管理，专家库管理，资产信息管理，信息安全事件管理等。

3) 接口层

接口层负责提供本系统与其他系统之间的数据共享和交互接口。例如本系统的定级备案数据向公安部定级备案信息管理系统的数据输出接口，信息安全运维管理系统收集的数据向本系统的数据输入接口等。

LanSecS 信息安全等级保护综合管理系统的业务体系架构以及各业务模块之间的关系如下图所示。系统用户通过浏览器访问 LanSecS 信息安全等级保护综合管理系统，经过系统身份认证和权限控制，进行等级保护业务管理工作。普通用户以日常办公管理作为主要操作界面。系统管理员则可对基础数据、工作流程、具体等级保护工作环节的业务活动进行统一维护管理并可对工作过程进行监控、对信息和数据进行统计分析等。

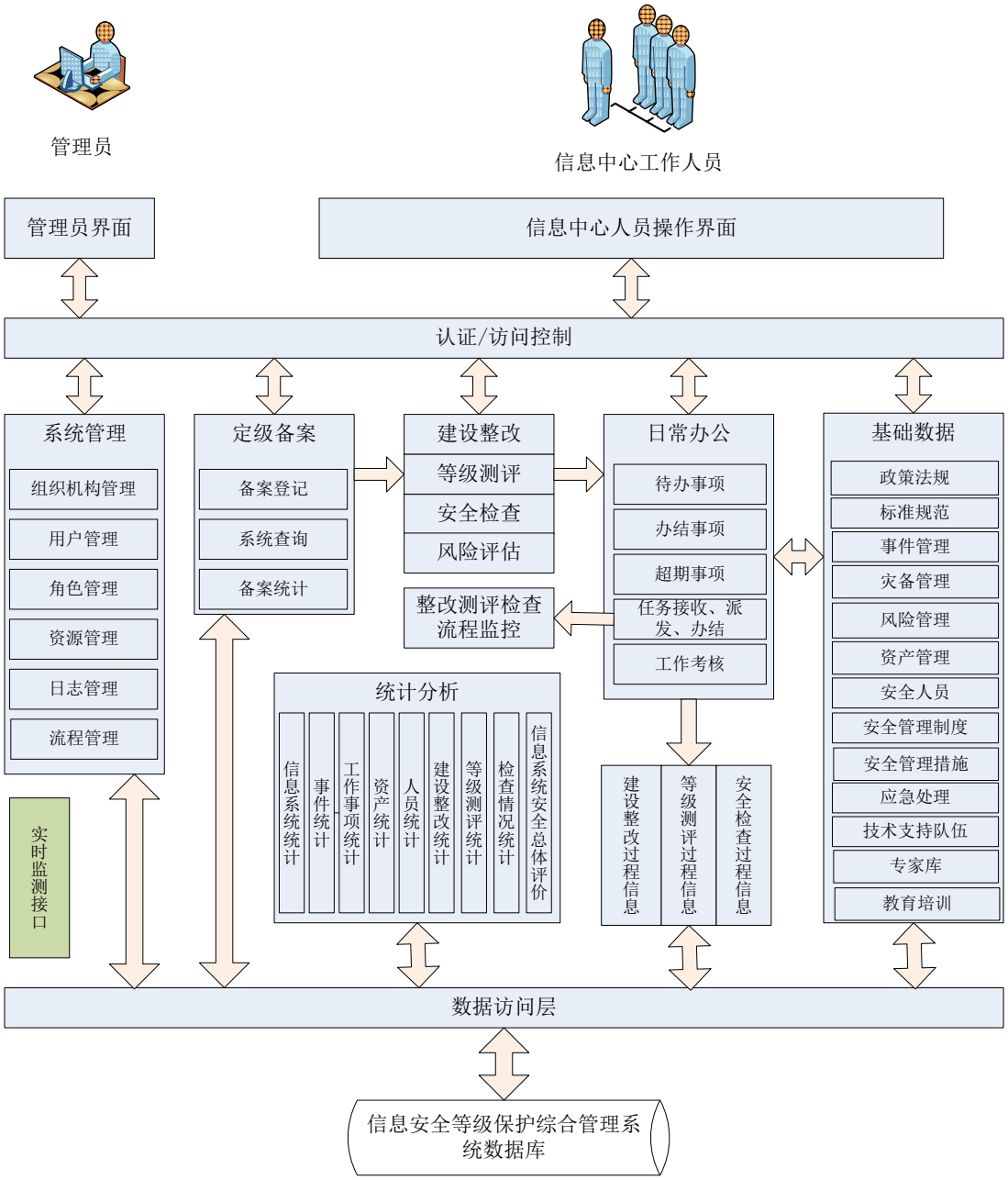

图 2 系统业务架构和业务关系示意图

4. 系统功能

“LanSecS 信息安全等级保护综合管理系统”主要功能包括如下几个方面：

1） 定级备案管理

2） 建设整改管理

3） 等级测评管理

4） 安全检查管理

5） 风险评估管理

6） 日常办公管理

7） 统计分析

8） 基础数据维护

4.1. 定级备案管理

重要信息系统的定级与备案工作是我国信息安全等级保护工作开展的基础。各行业均应对本行业内各单位的重要信息系统进行定级，并将定级情况向公安机关备案。目前大部分行业用户，均通过手动方式填写备案登记表，备案表在本单位的留存也是以离散文档的形式存储。这种备案方式非常不利于备案信息的维护，也不利于备案信息的查询、检索和统计。也就无法为主管部门快速提供本单位的信息系统备案状况。

本系统可为各行业的重要信息系统的定级和备案提供方便的管理功能。定级备案管理模块功能逻辑结构如下：

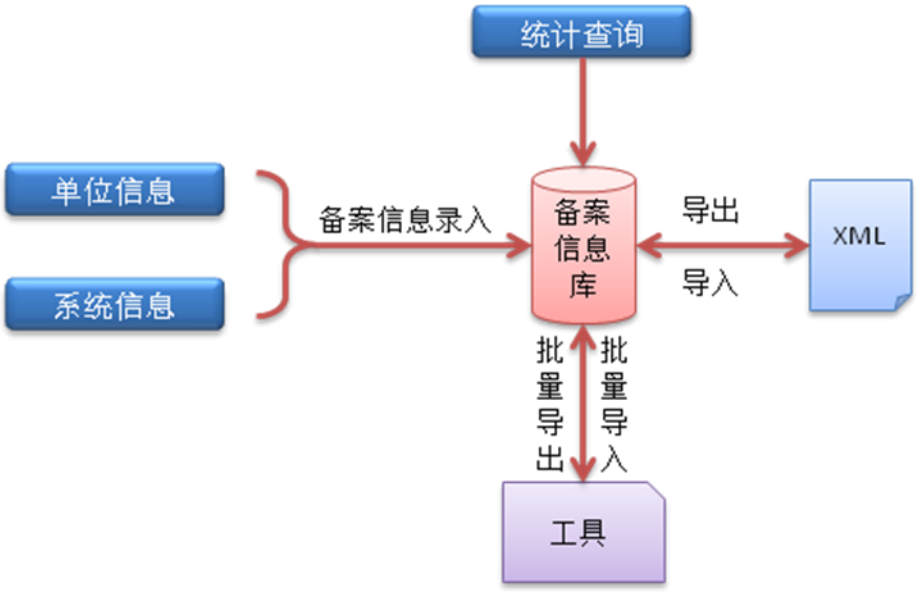

图 3 定级备案管理模块逻辑结构

“定级备案管理”主要完成重要信息系统的定级备案信息维护与管理，包括备案信息的录入、查询、统计，备案信息表的导出和导入、备案数据采集等。具体如下：

1） 备案信息填报：完成重要信息系统备案信息的填报；

2） 备案情况查询（更改）：按照备案单位或备案信息表中任何一个字段进行单项查询或组合查询，查询结果显示为备案信息（分为以单位为主导和以信息系统为主导两类，即允许用户按单位查也可以按信息系统查），为一项或多项。提供关键字段的准确和模糊查询；

3） 备案信息导出：将备案信息导出，供导入备案数据采集工具或监督检查工具使用；

4） 备案情况统计：提供特定备案时间段的信息系统数量、单位数量等，统计显示形式为统计表；

5） 附加信息管理：完成备案附加信息的添加；

6） 备案数据采集工具

- 备案表填报:完成备案表信息的填报；
- 备案表校验和审核:完成备案表信息的校验和核对，以及系统自动给用户提供一个备案表编号供用户酌情选择使用；
- 备案表 WORD 文档生成：完成备案表 xml 格式到 word 文件格式的转换和具体文件的生成；
- 备案表信息打包：完成备案表信息、附件的合并和压缩，生成可上传文件包；
- 批量入库：实现文件包的解析和批量入库。

4.2. 建设整改管理

本系统将整改建设分为五个步骤环节：

1） **工作部署：**制定信息系统安全建设整改工作规划，对信息系统安全建设整改工作进行总体部署；

2） **现状分析：**开展信息系统安全保护现状分析，从管理和技术两个方面确定信息系统安全建设整改需求；

3） **整改方案：**确定安全保护策略，制定信息系统安全建设整改方案；

4） **整改实施：**开展信息系统安全建设整改工作，建立并落实安全管理制度，落实安全责任制，建设安全设施，落实安全措施；

5） **整改结果：**开展安全自查和等级测评，及时发现信息系统中存在安全隐患和威胁，进一步开展安全建设整改工作。

建设整改执行流程如下图所示。

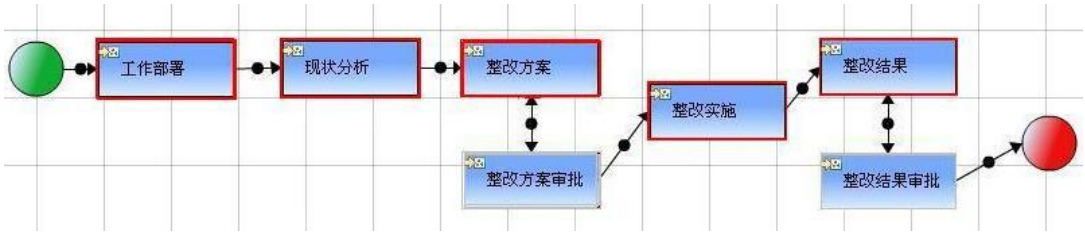

图 4 建设整改工作流程

“建设整改管理”主要完成已备案信息系统的建设整改活动的跟踪记录与管理。包括建设整改信息的录入、查询、统计。

1） 建设整改信息录入：将建设整改活动过程中的所有相关信息记录入库；

2） 建设整改信息查询：对入库的建设整改信息，按照单位、系统或者整改信息表中的任何一个字段进行信息检索和查询，查询结果可生成报表；

3） 建设整改信息导出：将建设整改信息导出，生成可以阅读的 word 文档格式。

4.3. 等级测评管理

等级测评管理模块负责对行业用户发起的由第三方测评机构主导实施的等级测评活动的组织和管理。行业用户在新上线的信息系统建设完毕或者对旧的信息系统安全建设整改完成时，均需要委托第三方测评机构对信息进行等级测评，以验证信息系统的安全建设是否符合定级要求。等级测评模块主要负责对测评机构的管理、测评流程的管理、测评结果的汇总与记录、测评活动的监控等子模块。各子模块之间的关系如下图所示：

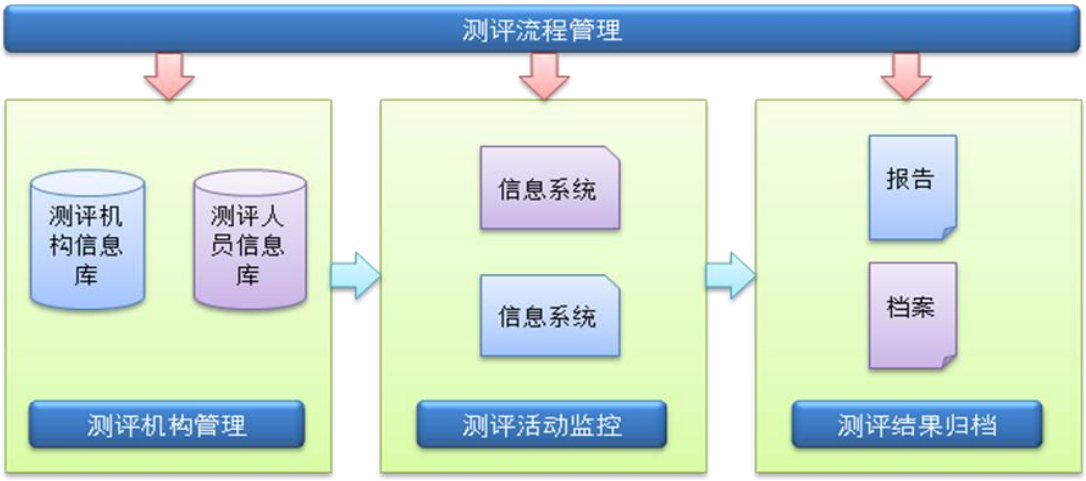

图 5 等级测评管理示意图

1） 等级测评信息录入：将等级测评过程中的所有相关信息记录入库；

2） 等级测评信息查询：对入库的等级测评信息，按照单位、系统或者等级测评信息表中的任何一个字段进行信息检索和查询，查询结果可生成报表；

3） 等级测评信息导出：将等级测评信息导出，生成可以阅读的 word 文档格式；

4） 等级测评机构管理：等级测评机构的相关信息管理；

5） 等级测评报告管理：对已经取得等级测评报告的信息系统所对应的测评报告进行集中归档管理。

4.4. 安全检查管理

“安全检查管理”提供对安全自查、主管部门检查和公安机关检查等安全检查活动状况的跟踪记录管理。包括：

1） 监督检查制度管理：对监督检查规章制度等级入库，并提供查询和打印服务；

2） 安全自查管理：对安全自查活动状况进行信息记录，并提供查询、统计服务；

3） 主管部门检查管理：对主管部门的检查活动状况进行信息记录，并提供查询和统服务；

4） 监督检查数据导出：完成用户从主系统中导出需要监督检查单位及其系统的相关信息，并转换为桌面系统能解析识别的文件系统；

5） 监督检查信息录入：供用户直接在主系统上填写监督检查相关数据（或直接导入监督检查工具生成的检查数据包），填写完成后可生成符合《信息系统安全等级保护监督检查表》格式和内容的 Word 文本；

6） 监督检查情况查询：要求按照检查表中任何一个字段（包括检查时间等）单项或组合进行查询，还可按检查次数、是否超过检查期限等条件查询，查询结果显示为一项或多项，信息为单位或信息系统监督检查信息；

7） 合规性检查：对检查结果进行分析，并与已知标准进行比对，判断所检查的信息系统是否合规。

8） 监督检查工具

- 备案信息导入：可以将主系统导出的数据导入到监督检查工具中，便于在监督检查过程中实时查询信息系统的备案信息；
- 监督检查填报：完成用户独立填写监督检查数据，登记信息、填写完成后可生成符合《信息系统安全等级保护监督检查表》格式和内容的 Word 文本；
- 监督检查数据导入：完成桌面系统特定文件格式（特定的格式包，内可含文本、图象文件等附件信息）的监督检查数据导入进服务器端主系统。

4.5. 风险评估管理

风险评估管理主要负责对信息系统风险评估活动的相关信息的维护管理，规范本单位在委托第三方进行风险评估过程中需要进行配合的相关事项和流程，并对整个风险评估活动过程中的各种数据进行汇总记录。

风险评估管理主要由风险评估测评、风险评估管理两个子模块组成。风险评估测评子模块采用内置工作流引擎进行风险评估工作的流程规范及过程推动；风险评估管理子模块可对已经进行过的风险评估测评项目的相关信息进行查看管理，并可对当前正在进行风险评估测评的项目的执行情况进行监控。

4.5.1. 风险评估测评

风险评估测评通过内置的工作流引擎，以系统预先定制的风险评估流程引导并规范风险评估测评工作的展开，具体的工作流程示意图如下：

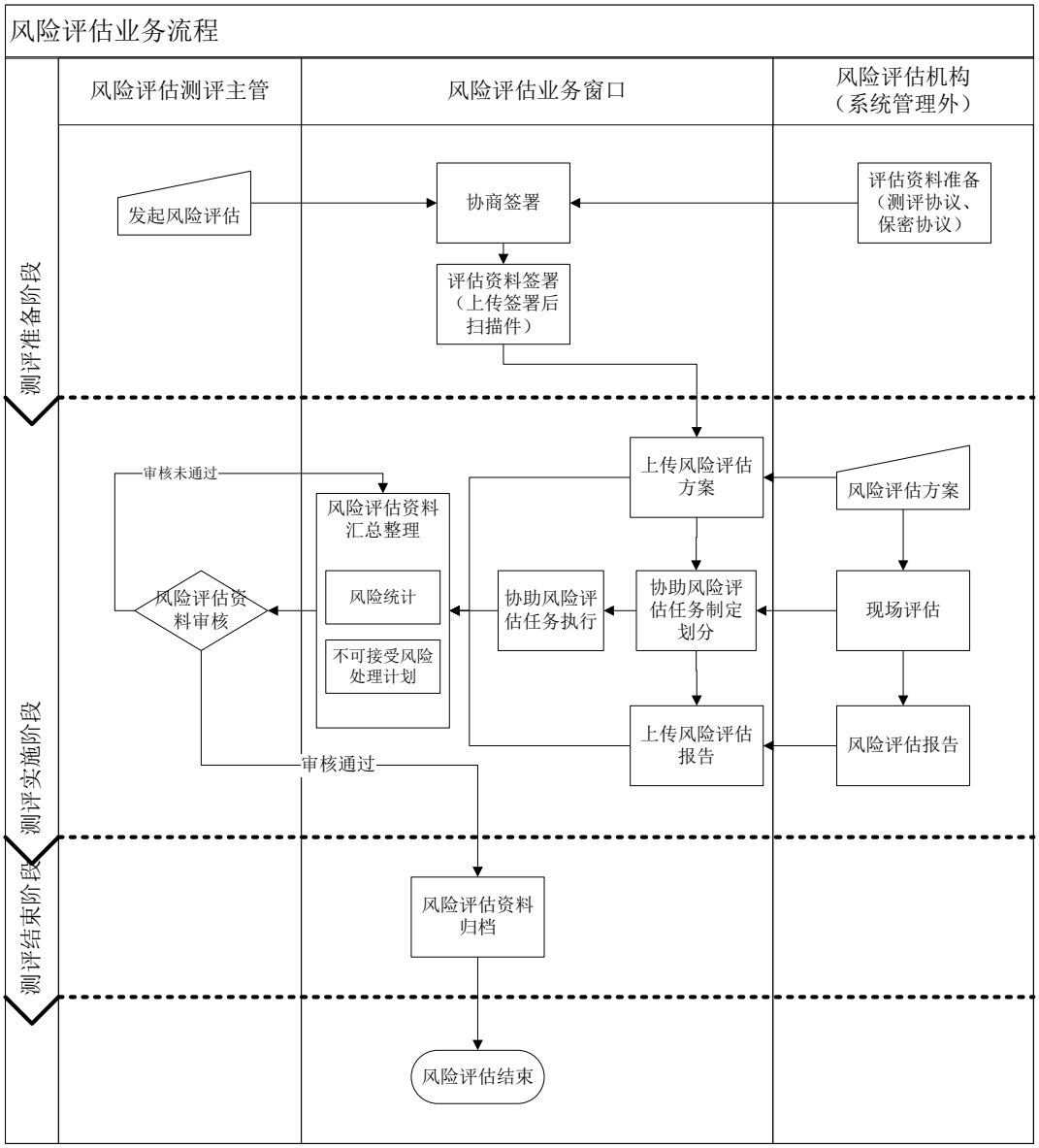

图 6 风险评估流程图

如上图所示，风险评估流程主要由发起风险评估、风险评估准备资料上传、风险评估方案上传、风险评估协助任务制定划分、风险评估报告上传、风险评估资料汇总整理、风险评估资料审核及风险评估资料归档等几个环节组成。

1） 发起风险评估

信息系统风险评估的第一个流程是发起一个风险评估项目，系统可记录当前项目发起的日期、主要目标、主要任务和发起人等相关信息。风险评估发起后，此次风险评估即被纳入流程管理，发起者可以指定相关人员进行下一步的风险评估准备资料上传工作。

2） 风险评估准备资料上传

风险评估准备资料上传负责风险评估所需的各种资料文件的上传和管理，例如与第三方风险评估机构签署风险评估合同和保密协议等。系统可记录的信息包括文件的签署人，签署日期和文件描述等相关信息。

3） 风险评估方案上传

风险评估方案上传负责将本次风险评估方案文件上传并保存到系统中，系统可记录信息包括方案提供方的单位及人员，方案接收方的人员、日期等信息。

4） 风险评估协助任务分配

风险评估协助任务分配负责对风险评估方案中的各项任务进行分配，需要协助的风险评估任务主要包括为风险评估单位提供信息系统相关的信息，协助风险评估人员入场、离场，并签署入场离场相关文件，协助风险评估单位人员执行工具测评，并对测评结果签字确认等相关事项。

5） 风险评估协助任务执行

风险评估协助任务执行负责通知各相关人员按照完成风险评估协助任务，并及时记录任务完成的情况和相关信息等。

6） 风险评估报告上传

风险评估报告上传负责将第三方风险评估单位提供的风险评估报告上传到服务台并保存，系统可记录提供报告文件的单位及人员和接收报告文件的人员等相关信息。

7） 风险评估资料汇总整理

风险评估资料汇总整理负责将本次风险评估活动的其它相关资料逐一入库汇总，由系统进行集中管理。方便系统使用单位将风险评估的结果做为建设整改的依据，帮助系统使用单位构建一个良性循环的信息安全环境。

8） 风险评估资料审核

风险评估资料审核是指由系统使用单位对风险评估测评单位提供的风险评估相关资料的评审与审核。

9） 风险评估资料归档

风险评估资料归档主要提供电子文档归档功能，并可记录文件档案存放位置等相关信息，方便系统使用单位集中管理风险评估相关信息。

4.5.2. 风险评估管理

风险评估管理主要提供对历史风险评估项目信息的查看管理以及对当前正在进行的风险评估项目的监控功能。

风险评估项目信息的查看管理主要包括查看历次风险评估项目基本信息，历次风险评估资料档案信息，历次风险评估中的风险统计和不可接受风险处理计划的功能。

风险评估监控的主要功能包括查看当前正在进行的风险评估活动的最新状况，当前正在进行的业务节点以及当前进行业务节点的处理情况、处理人和处理日期等相关信息，另外可以查看已经完成的业务节点的处理情况、处理人和处理信息等相关信息。

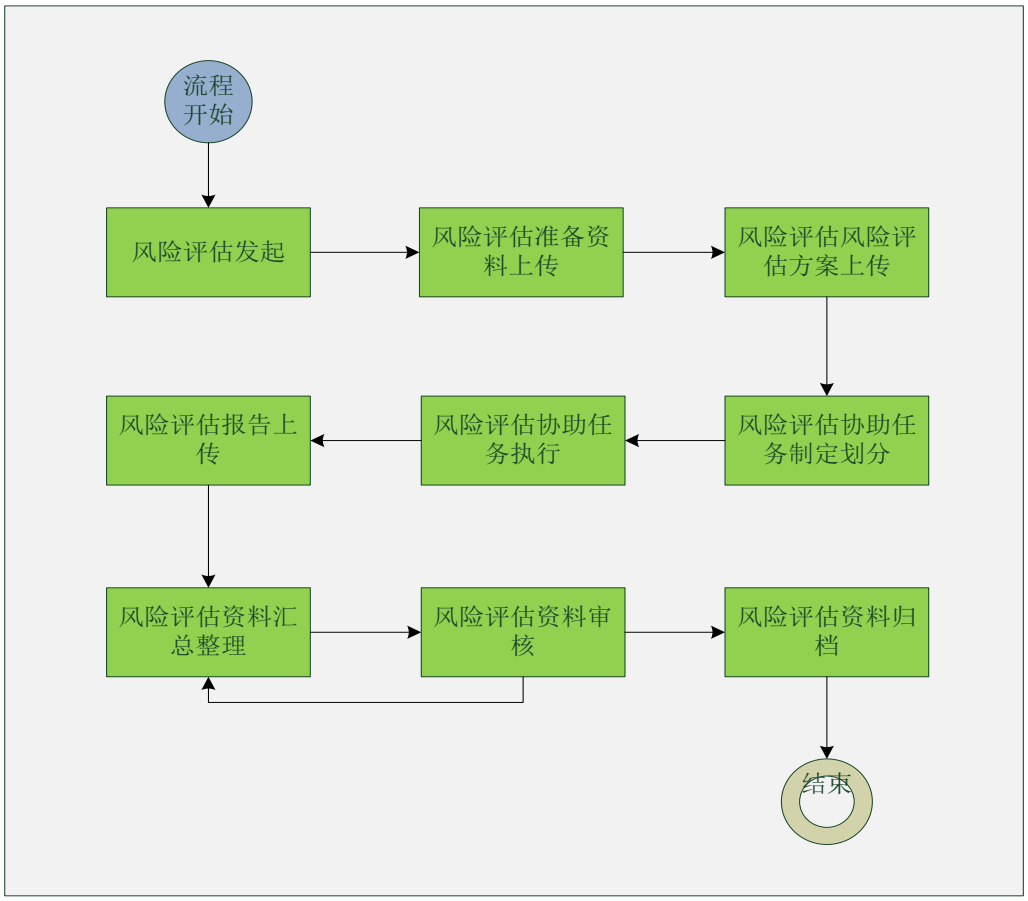

图 7 风险评估监控图

4.6. 日常办公管理

日常办公管理为系统用户提供了一个日常工作的平台，由待办事项，办结事项，任务管理，工作考核四个部分组成。基本囊括了与等级保护相关的事项的管理，其中系统内部事项直接在此处提供统一入口，系统外事项在此处提供统一任务管理入口，纳入到系统管理，方便等级保护工作的开展。具体关系如下图：

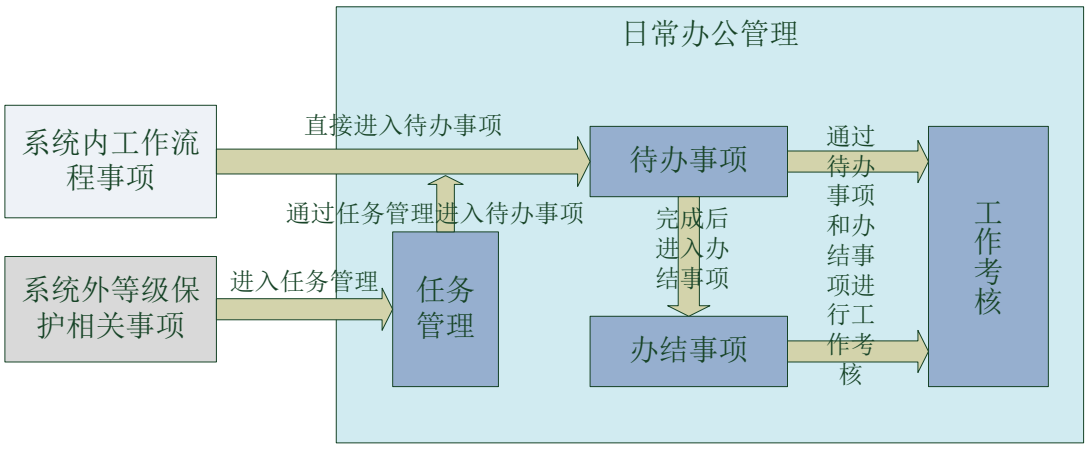

图 8 日常办中的不同事项关系图

1） 待办事项管理：提供需要办理事项的记录功能，并可标记事项当前进展状态；

2） 待办事项查询：对已经录入的事项，可按照待办、办结和超期等条件进行归类查询，并按照其他条件进行复合查询；

3） 任务管理：对上级派发的等级保护工作任务进行登记管理，并提供任务执行状况的跟踪记录能力，可对任务进行复合条件查询和统计；

4） 工作考核：对等级保护各个环节的工作状况进行考核，并给出综合考核结果。

4.7. 统计分析

统计分析管理主要提供等级保护相关的重要数据的统计及分析功能，包括信息系统统计，安全事件统计，工作事项统计，资产统计，安全机构统计，安全人员统计，建设整改统计，等级测评统计，检查情况统计等，并提供相应的分析图表。

1） 统计信息查看：提供统一的统计信息查看功能，统计信息包括：

- 信息系统统计
- 事件统计
- 工作事项统计
- 资产统计
- 组织机构统计
- 人员统计
- 建设整改统计
- 等级测评统计
- 检查情况统计
- 信息系统安全总体评价

2） 统计报告生成：对统计结果生成统计报告，并可导出到常见的文件格式，如 word、excel 等。

4.8. 基础数据管理

基础数据管理提供对等级保护管理工作当中各个环节所需的基础数据进行综合管理。包括：

1) 政策法规库管理：提供国家、部委、行业、部门等各个级别的政策、法规的管理，包括录入、修改、查询、报表、打印、导出等维护操作。
2) 标准规范库：提供国家、部委、行业、部门等各个级别的标准规范的管理，包括录入、修改、查询、报表、打印、导出等维护操作。
3) 事件管理：提供安全事件的录入、查询、统计、报告等维护操作。
4) 资产管理：提供资产的手动录入、自动收集，资产查询、统计和报告等管理。
5) 组织机构：提供组织机构创建和维护管理。
6) 安全人员：提供人员的管理。
7) 安全管理制度：提供人员管理、系统建设管理、系统运维管理等管理制度的录入、查询和报告等功能。
8) 安全管理措施：提供人员管理、系统建设管理、系统运维管理等管理措施的录入、查询和报告等功能。
9) 应急处置：提供应急预案和应急演练等活动的信息管理功能。
10) 技术支持队伍：提供技术支持队伍信息的录入、查询和报告等功能。
11) 专家库：提供专家库信息的录入、查询和报告等功能。
12) 知识库：提供知识库的维护管理。

基础数据管理模块对系统的基础数据的管理操作包括：

1) 数据的收集、录入和汇总

系统可管理的基础数据分类多达十余类，该模块针对不同的数据分类，分别进行信息的收集、录入，存储到数据库中进行汇总保存。

2) 数据查询与报表

针对不同类型的基础数据，该模块提供风格统一的数据查询、展现和报表功能。通过查询和报表，用户可将关心的数据筛选出来，形成数据报表，指导信息安全等级保护工作的开展。

3) 数据统计分析

该模块还负责对不同类别的数据，按照不同的统计方式，生成统计图表，统计图表可为等级保护工作状况的综合分析提供帮助。

4) 数据备份

基础数据作为基本的等级保护管理数据，需要定期备份。该模块可按照用户设定的条件，对不同类别的基础数据进行定期备份。该模块还提供备份数据的人工恢复。

图 9 基础数据管理

4.9. 分级管理

对于大型行业用户，其信息系统分布在不同的行政区域或辖区，这些信息系统的维护管理也由辖区内下级单位负责管理。但是上级单位又需要了解和掌握下级单位的信息安全等级保护工作开展情况。鉴于此，本系统提供了分级管理功能。

分级管理功能，可在多个等级保护综合管理系统之间（一般的，在上级系统和下级系统之间）建立关联关系。确定上下级关系后，下级系统可以将本级的信息和数据定期或实时上传到上级系统中。如此，上级单位可对下级单位的等级保护工作信息和数据进行集中管理，如查询、统计和分析等。从而掌握下级单位的信息安全等级保护工作的开展状况。

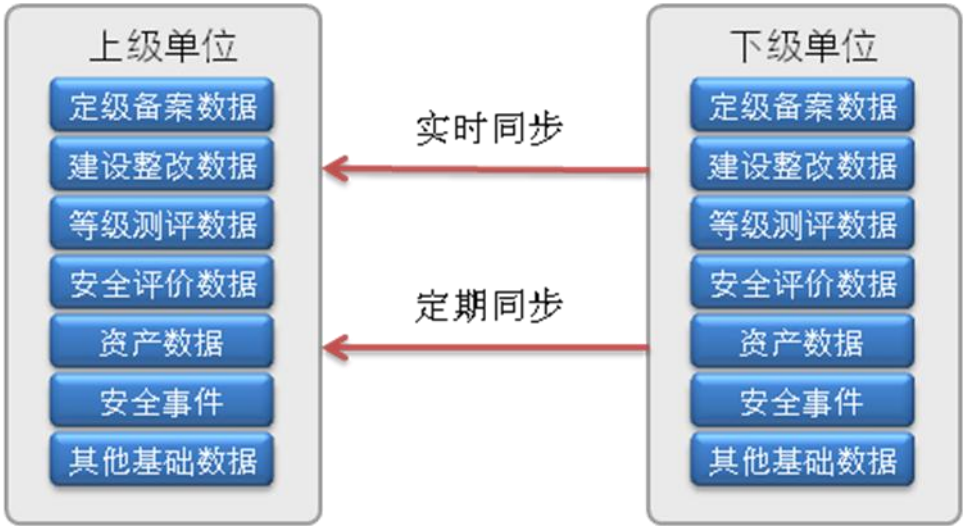

图 10 分级管理数据同步

4.10. 系统接口

LanSecS 信息安全等级保护综合管理系统由数据采集和共享中心负责提供与其他各种安全系统和应用系统的接口管理。数据采集和共享中心对系统接口进行统一封装和集中管理。数据采集和共享中心采用插件化的接口设计与管理，可以根据不同用户的需求，定制适合用户需要的系统数据采集和共享接口。数据采集和共享中心作为基础接口支撑平台，为用户的系统数据采集和共享提供了灵活的手段和方式。数据采集和共享中心的接口分类两大类，数据采集类和数据共享类。

1）数据采集接口

数据采集接口负责从其它信息系统或者安全设备收集信息和数据，将采集的信息和数据存储到系统数据库中。这些数据为等级保护综合管理系统的各项工作管理提供更加丰富的数据支持，为安全建设整改方案和安全检查方案的制定提供依据。例如，通过等级测评数据采集接口，可将信息安全等级保护测评与评估系统的测评数据导入本系统，为系统的等级测评活动提供测评依据；通过资产信息采集接口，可将其他资产管理系统的资产数据直接导入本系统，省却了资产信息的收集和录入；通过安全事件采集接口，可将其他安全运维管理系统的安全事件实时导入本系统，由本系统负责统一的安全事件管理。

2）数据共享接口

数据共享接口负责将等级保护综合管理系统的自身数据共享给其他信息系统使用，为其他信息系统提供丰富的数据来源，以便对数据进行进一步的分析和处理。例如，本系统的安全评价数据，可输出至专家评价系统进行信息系统的综合安全评价；本系统的定级备案数据，可导入公安部定级备案综合工作平台，完成行业用户的定级备案工作。

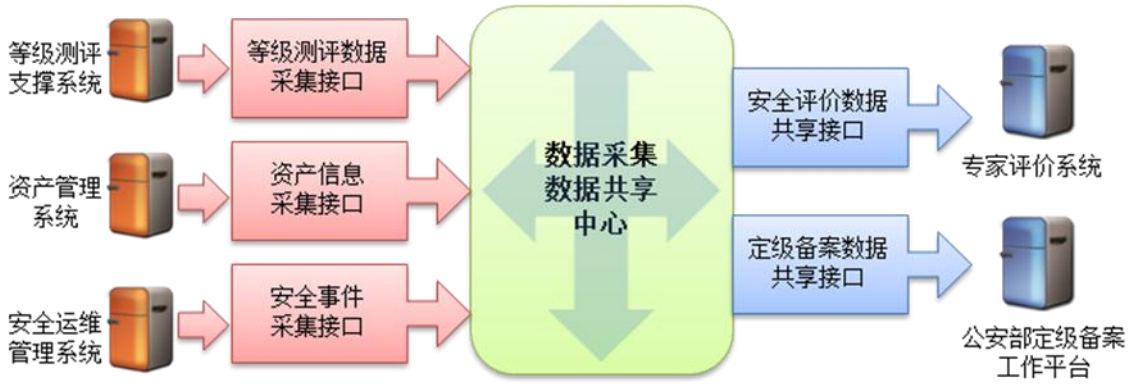

图 11 系统接口

5. 系统特色

5.1. 等级保护管理工作流程化

LanSecS 信息安全等级保护综合管理系统内置工作流引擎，可实现流程定制功能，满足用户业务动态变化和扩展的需要。系统以信息系统等级保护定级、备案、整改、测评和自查为主线，将流程化管理与等级保护管理进行结合，实现用户等级保护主要工作的信息化和流程化。

5.2. 信息系统安全性评价标准化

系统提供了重要信息系统的安全性评价功能，通过建立重要信息系统安全性评价专家体系，对重要信息系统的安全性进行评价，以等级测评、风险评估、专家评审、执法检查、行业检查和自查的结果为评价指标，对信息系统的安全性进行评价。由于评价数据的完备性和科学性，可为行业主管部门、执法单位或者第三方测评单位对行业信息系统的安全性提供标准化、可度量的评价结果。通过评价可详细反映重要信息系统等级保护工作的计划、实施、检查和改进的情况，为管理层的等级保护工作安排提供指导。

5.3. 丰富的报表和数据展现能力

系统具备完善的查询、报表和统计功能，可谓用户提供丰富的数据展现，从而对等级保护管理工作的下发情况、执行情况、进度情况、督办情况提供图形化的统计数据和报告，满足管理层、执行层人员对安全工作全面掌控的需求。

5.4. 快速生成结构化文档

在系统开发中，圣博润公司针对综合管理系统中文档数量众多、处理繁琐的业务特点，提出和实现了结构化文档生成技术。通过结构化文档生成技术，可以快速格式化测评业务过程中输入输出的各种文档，例如、整改方案和整改报告的自动生成，可以在 1 分钟内生成数百页的测评方案和测评报告，且可以保持格式化的文档结构与排版版面，完全兼容微软的 OFFICE 办公软件。这一技术的创新与应用，大大提高了安全等级测评与评估过程中的文档处理能力，简化了文档管理，提高了测评和评估工作的效率。

图 12 结构化文档生成示意图

5.5. 支持多级部署

系统可按照部级→省级→市级的三级部署架构进行部署，实现上级机构对下级机构等级保护工作执行情况的监管，下级机构对上级机构等级报工作情况的上报，通过三级联动的模式，完成定级、备案、整改、测评和检查等主要工作，并按照需求的工作的完成情况进行汇总统计分析，生成统计报告，记录工作进度和汇报工作情况。

5.6. 完备的数据接口

系统具有完备的数据接口规范，通过数据接口，一方面可对重要信息系统的信息进行收集和管理，为信息系统的安全状态评估提供基础数据；另一方面，可与公安部的等级保护监察管理系统进行数据上报，将行业信息系统的备案信息上报到公安部等级保护监察管理系统。

6. 系统安全性

系统设计充分考虑了自身的安全性，主要采取了如下技术措施保障系统自身的安全性。

身份认证方面：本系统有专门的身份认证模块，系统自身设计采用了双因子身份认证。通过统一的用户管理功能保证用户标识的唯一性。用户登录失败会话自动无效，自动限制登录失败次数。

访问控制方面：本系统实现了基于角色的访问控制技术，按数据和功能授予用户权限。专门的拦截过滤器检查用户的每一次访问是否符合授权要求。授权和审计管理分开。

安全审计方面：本系统对用户的访问行为按功能、数据对象记录了详细的日志，并提供了日志查询和统计功能。

剩余信息保护方面：敏感信息不得写入静态字段，内存自动回收技术保护了内存中的剩余信息。定期检查系统使用临时文件夹，清除过期的临时文件。

通信完整性和保密性方面：本系统为 B/S 架构，通过对 SSL 协议的支持实现通信完整性和保密性方面的要求。

软件容错方面：用户提交的信息，系统在处理前进行数据有效性检查。所有的异常必须得到有效正理。对于外部采集的数据导入，则规定必须进行严格的数据检查后才准导入。多线程技术防止了单个用户的错误不会影响系统的其它用户的业务操作。故障报警机制使用管理员及时地处理系统故障。提供灾难时的数据恢复功能。

资源控制方面：禁止用户的并发登录，设置合适的会话失效时间，当用户登录错误超过一定次数时自动锁定。并记录日志。

代码安全方面：通过工具扫描、代码复审保证程序代码符合编码规范，查找可能存在的恶意代码。

7. 系统部署

系统支持两种部署模式，一种是独立部署，一种是分级部署。通过分级部署，可以将下级系统的信息和数据实时或周期性同步到上级系统中，为上级部门的等级保护工作管理提供更加完备的数据支持。

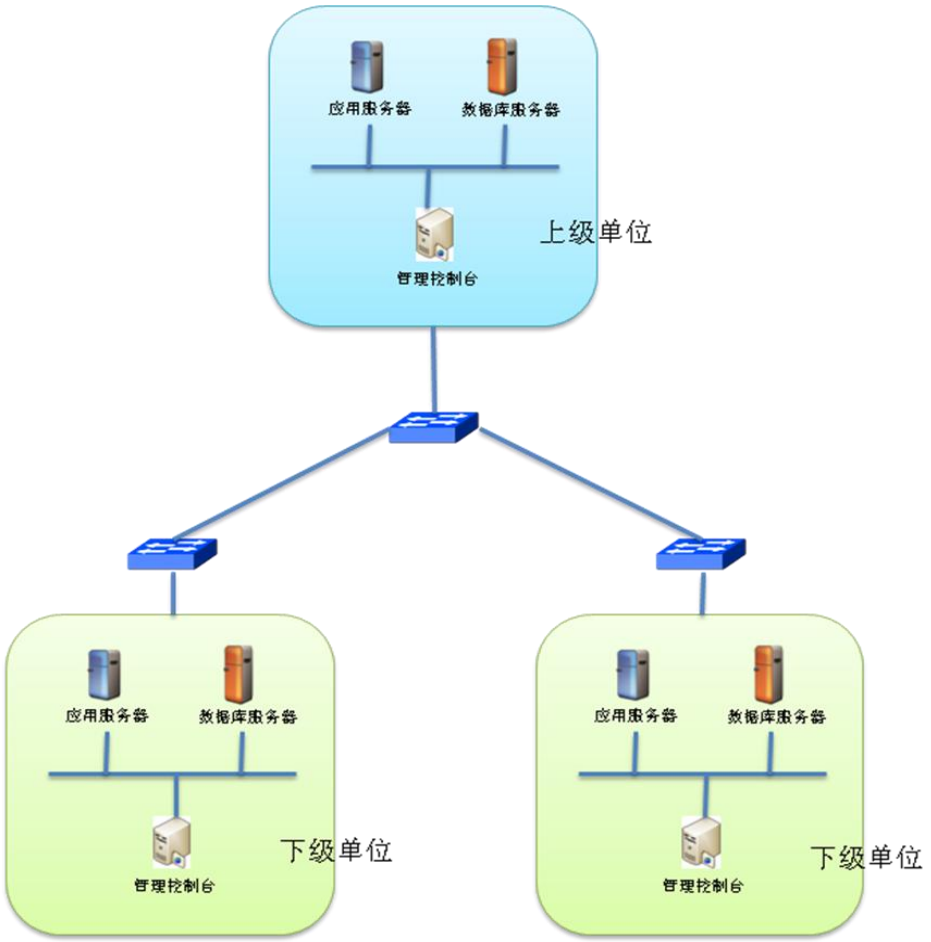

图 13 系统分级部署模式示意图

8. 系统配置要求

本系统的配置要求如下：

1） 数据库服务器：用于提供基础数据和等级保护工作数据存贮服务，配置要求为双 CPU Xeon 3.0G 以上，500G 硬盘以上，内存 4G 以上；

2） 应用服务器:用于部署本系统服务器程序,配置要求为双 CPU Xeon 3.0G 以上，120G 硬盘，内存 4G 以上；

3） 系统管理主机：用于本系统的管理，通过浏览器进行系统的管理。配置要求为 Xeon 3.0G CPU，120G 硬盘，内存 1G 以上。