信息安全管理体系的研究与建立

杨东娴

社科院 计算机网络中心

【摘要】信息时代，迅猛发展的信息技术和日益丰富的信息资源极大地影响着人们的工作和生活。在社科院，信息化建设的成果（如各类电子资源和业务应用系统等）不仅是院内科研人员进行各类科研活动不可或缺的基础资源，同时也是我院重要的信息资产。随着信息化进程的不断推进，成果的拥有量不断增加，科研人员对它们的依赖程度也逐渐增强，使得电子资源和业务应用系统等信息资产的安全保障和安全管理问题逐渐为我院各级信息化管理部门所重视。本文从国内外信息安全管理的现状分析着手，阐述在我院建立完善信息安全管理体系的重要性和必要性。同时依据我院信息安全保障和信息安全管理的基本需求，基于 PDCA 循环模型，参照国际标准 ISO/IEC27001 的相关规程，通过适当的裁减，引入风险管理和安全事件管理等理念，设计并建立一套可持续改进的、符合我院实际的信息安全管理体系。

【关键词】信息安全管理体系、PDCA 循环、风险管理、安全事件管理

1 引言

信息时代，迅猛发展的信息技术和日益丰富的信息资源极大地影响着人们的工作和生活。信息技术的运用不仅引起了人们生活方式和思想观念的巨大转变，而且也给组织机构的发展带来了新机遇。一般来说，组织机构的信息化成果大多以信息系统的形式直接参与到组织机构的运作和管理流程中，而随着对这些信息系统使用频率的增加，组织机构对它们的依赖程度也逐步加大，随之而来的信息

安全问题也逐步为各组织机构所关注。

在社科院，信息化建设的成果（如各类电子资源和业务应用系统等）不仅是院内科研人员进行各类科研活动不可或缺的基础资源，同时也是我院重要的信息资产。随着信息化进程的不断推进，成果的拥有量不断增加，科研人员对它们的依赖度也逐步增强，使得这些信息资产的安全保障和安全管理问题逐渐为我院各级信息化管理部门所重视。而面对日益严峻的信息安全形势，此类信息资产的信息安全问题也正成为我院信息安全保障工作乃至信息化建设中必须面对的经常性问题。

一提及信息系统的安全，人们的第一反应就是：这是个技术性问题，要确保信息系统的安全，就要装备足够多和足够强健的安全产品。但事实上，信息系统的安全保障工作不能仅依靠简单堆砌多种安全技术或安全产品来实现，与之相关的信息安全管理工作也不容忽视，毕竟影响信息系统安全的不仅有技术因素，还包含了靠纯粹技术手段不能完全解决的非技术类因素，如：与人员相关的安全、信息安全成本投入和产出的平衡、业务连续性保障等。正如管理学箴言「三分技术，七分管理」所述，一套完整的信息安全保障体系应该包括技术和管理两个层面，即信息安全技术体系和信息安全管理体系。只有以信息安全管理体系为基础，以信息安全技术体系为支撑，通过加强信息安全管理工作，持续地进行风险识别和控制，不断的监督指导信息安全技术的贯彻落实才能有效的保障信息安全。因此，为了保障院内的信息安全，信息安全管理工作的加强和标准化工作刻不容缓。

2 信息安全管理现状分析

信息安全的内涵很宽泛，若从安全属性方面定义，信息安全就是信息的保密性（Confidentiality）、完整性（Integrity）和可用性（Availability）等安全属性或安全目标的保持；另外也可包括真实性（Authenticity）、可核查性（Accountability）、不可否认性（Non-repudiation）和可靠性（Reliability）等安全属性的保持。相对应的，信息安全管理就是各组织机构为了实现以上的信息安全属性或安全目标，运用一定的手段，对信息安全进行系统管理的各项活动。自信息安全理念产生至

今，它已经经历了三个发展阶段：技术浪潮阶段、管理浪潮阶段和制度浪潮阶段。随着对信息安全认识的加深，人们意识到制度浪潮阶段的信息安全要以体系化的方法来实现[1]，而这也进一步的促进了信息安全管理体系的产生。

2.1 国内外信息安全管理现状

信息安全是一个多层次、多因素、综合性的动态过程，是一个需要系统体系来保证的持续发展过程[2]。为完善信息安全的体系化，我国分别从管理、技术和法规制度等 3 个方面进行部署，加强了对信息安全的综合管理。在管理方面，我国加强了宏观管理力度，强化了各主管部门的信息安全管理工作；在技术方面，我国不仅加大了基础关键技术的科研支持力度，大力推进信息安全技术的产业化进程，而且非常重视信息安全技术的学术交流；在法规和制度建设方面，我国不断规范信息安全工作，建立健全各项信息安全相关的法律法规和规章制度。

国际上，自美国「9·11」事件发生以后，各国逐步改变了以往对安全问题的思考方式，为解决信息安全策略与管理战略脱节、整体安全文化建设未完善等管理和技术脱节问题，纷纷采取措施调整信息安全管理重点，信息安全受到广泛重视。

2.2 我院信息安全管理现状

我院的信息安全管理工作包括了院内信息化项目在项目立结项、建设、运行、维护和废止等过程中，保障信息系统、信息、环境和操作安全的一系列管理活动。近年来，院里已经从思想意识、管理机制、组织机构和技术保障等多个方面建立起了基本的信息安全管理架构，制定了相关的信息安全管理制度和信息系统访问控制策略，从物理环境、网络环境、主机环境、应用环境、用户环境等多个层面，采用多种安全防护技术，通过科学有序的运维工作，加强信息系统的安全监管，实现了对信息基础设施和信息化成果的机密性、完整性和可用性的有效保障。

虽然我院已经基本建立起了保障信息安全的信息安全管理架构，但仔细分析院内的信息安全管理现状，不难得出以下的不足之处：

- 与信息安全管理相关的规章制度仍需完善，现有制度的执行力度不够深入，考核测评机制尚未建立。
- 内部管理比较薄弱，对终端计算机和移动存储介质的管理有待加强。
- 对恶意程序的技术防范和管理仍需加强。
- 信息系统日常运维和管理工作仍需加强。
- 风险的评估和管理工作有待加强。
- 院内信息安全整体意识仍需加强，需要制定统一的标准规范和安全策略，全面部署安全防范措施。
- 信息安全管理全员参与意识有待加强，多数所局的信息安全责任和工作落在信息化部门。

从上面的介绍可以看出，大多数的不足之处与「人」这个因素密切相关，不论是对信息安全理念的认识和接受，还是信息安全策略的贯彻实施，「人」都是其中最活跃、最关键的要素。另外，因为信息安全管理本身就是一个复杂的系统工程，所以为了保证其全面性、有效性和适用性，需要引入体系化理念，建立信息安全管理体系（Information Security Management Systems，简称 ISMS）。

由此可以看出，我院的信息安全管理工作只有真正做到从「人」这个角度出发，通过建立 ISMS，推行信息安全文化，使信息安全理念和操作规程渗透到院内各位工作人员的日常行为中，同时配合相应的管理和技术措施，才能全面提升我院的信息安全保障能力。构建并部署实施 ISMS 后将针对以上的不足之处采取以下的应对措施：

- 强化信息安全意识，规范组织信息安全行为，提高整体安全意识。

ISMS 建立后，不仅可以通过人员管理的部署实施加强对「人」这个关键要素的管理，同时还可以借助教育培训管理，通过分类进行安全培训的形式，增强院内工作人员对既定信息安全目标和策略的理解和认识，逐步规范其信息安全行为，增强个体的安全意识，进而提高整体安全意识，形成院内特有的信息安全文

化。

- 全面掌握安全问题，明确安全风险。

通过 ISMS 的建立，系统地进行信息资产梳理、风险识别、风险评估、差距分析等活动，了解院内的安全现状，找出安全隐患，对院内的关键信息资产进行全面而系统的保护。

- 指导信息资产的安全建设。

ISMS 以风险管理为核心，与风险识别、评估和分析等管理活动相关的产出物可以为信息资产的控制规划和安全整改提供参考依据。

- 规范内部管理。

ISMS 本身就是一整套已经标准化和规范化的通用最佳实践集，通过对其中规程、过程和制度的参照和运用，达到规范内部管理的作用。

- 加强对外包服务的管控。

ISMS 建立后，将各类外包服务纳入其管理范围，为第三方服务的管控提供相关的约束和控制措施。

- 进行流程梳理，促进流程改造。

通过 ISMS 的建立，可以对现有的工作流程进行重新梳理，为流程改造和流程标准化创造条件。

- 进行持续改进。

ISMS 的建立和实施以持续改进为目标，有利于对院内信息安全管理工作进行持续性的改进。

- 贯彻和落实国家相关信息安全管理制度。

我国信息系统等级保护制度的实施是基于风险管理的理念，通过全面实施各项信息安全管理活动来保障信息系统的安全，这与 ISMS 的构建要求相同，因此可以在 ISMS 构建过程中融入等级保护制度的相关要求，切实落实好国家相关的

信息安全管理制度。

基于上面的分析，我们认为参照现有的信息安全管理标准，通过适当的裁剪，构建和部署实施我院适用的信息安全管理体系不仅是可行的，而且必要的。

3 信息安全管理体系的构建

ISMS 是一个组织机构在整体或特定范围内制定信息安全方针和目标，以及实现这些目标的方法论的集合。它将基于业务风险方法，通过建立、实施、运行、监控、评审、保持和改进等活动，达到保障整体信息安全的目标。它不仅是直接管理活动的结果，也是一个涉及人、过程和信息技术的有机系统。

一个组织机构信息安全管理体系的构建，通常是结合自身特点，先明确构建目标，然后再通过参照和裁剪现行的信息安全管理标准来建立适用于自身的 ISMS。

3.1 构建目标

结合上一章节的现状分析，我院构建 ISMS 的目标主要有以下几个方面：

- 摸清家底，全面掌握情况。

通过 ISMS 的构建，借助其中的风险评估、差距分析等过程活动，准确掌握我院的信息安全现状，如：信息安全管理现状、制度建设与落实状况、现有信息资产存在的安全隐患和面临的安全风险等。

- 建立常态化机制，持续改进。

通过 ISMS 的构建和部署实施，对现有的各项信息安全管理流程进行梳理和规范，建立科学、有效、有序的常态化工作规程和管理机制，并进行持续性改进。

- 提高信息安全管理水平，保证适度安全。

通过 ISMS 的构建与部署实施，切实提高院内各级信息化管理部门的信息安全管理水平。同时借助其中的风险评估与分析等过程活动，落实信息系统等级保

护制度的适度安全要求。

3.2 构建依据

院内 ISMS 的构建主要依据的是现行的国际标准和国内标准。

3.2.1 国际标准

ISMS 的概念最初来源于 ISO/IEC 17799 的前身 BS 7799。BS 7799 是英国标准协会（British Standards Institute，简称 BSI）通过汇集各优秀企业的相关信息安全管理最佳实践而推出的信息安全管理标准，包括信息安全管理实施细则（BS 7799-1）和信息安全管理体系规范（BS 7799-2）两个部分。其中，BS 7799-1 于 2000 年 12 月为国际标准化组织所接受，形成国际标准 ISO/IEC 17799，而后历经几次改版和修订，2007 年的最新版本为 ISO/IEC 27002:2005；BS 7799-2 于 2005 年 10 月为国际标准化组织所接受，形成国际标准 ISO/IEC 27001:2005。

院内 ISMS 构建所参照的国际标准主要是 ISO/IEC 27000 标准族[3]，可参考的国际标准详见表 3-1 所示，其中的 ISO/IEC 27001 和 ISO/IEC 27002 为 ISMS 构建和实施的参考重点。

表 3-1 ISMS 主要参考的 ISO/IEC 27000 标准族

标准标号	说　明
ISO/IEC 27000	Information technology-Security techniques-Information security management systems-Overview and vocabulary （信息技术—安全技术—信息安全管理体系—概况与术语）
ISO/IEC 27001	Information technology-Security techniques-Information security management systems-Requirements （信息技术—安全技术—信息安全管理体系—要求）
ISO/IEC 27002	Information technology-Security techniques-Code of practice for information security management （信息技术—安全技术—信息安全管理实践规则）
ISO/IEC 27003	Information technology-Security techniques-Information security management systems implementation guidance （信息技术—安全技术—信息安全管理体系实施指南）

ISO/IEC 27004	Information technology-Security techniques-Information security management -Measurements （信息技术—安全技术—信息安全管理—度量）
ISO/IEC 27005	Information technology-Security techniques-Information security risk management （信息技术—安全技术—信息安全风险管理）

3.2.2 国内标准

院内 ISMS 构建所参照的国内标准主要是与信息系统安全等级保护、信息安全管理、应急响应和信息安全风险管理等相关的国家标准，详见表 3-2。

表 3-2 ISMS 主要参考的国内标准

类　别	标准标号	说　明
信息安全管理	GB/T 22080-2008	信息技术 安全技术 信息安全管理体系 要求 （为国际标准 ISO/IEC 27001 的等同转化）
	GB/T 22081-2008	信息技术 安全技术 信息安全管理使用规则 （为国际标准 ISO/IEC 27002 的等同转化）
等级保护	GB 17859-1999	计算机信息系统安全保护等级划分准则
	GB/T 22239-2008	信息安全技术 信息系统安全等级保护基本要求
	GB/T 22240-2008	信息安全技术 信息系统安全保护等级定级指南
	GB/T 24856-2009	信息安全技术 信息系统等级保护安全技术设计要求
应急响应	GB/T 20985-2007	信息技术 安全技术 信息安全事件管理指南
	GB/T 20986-2007	信息安全技术 信息安全事件分类分级
	GB/T 20988-2007	信息安全技术 信息系统灾难恢复规范
	GB/T 24363-2009	信息安全技术 信息安全应急响应计划规范
信息安全风险管理	GB/T 24364-2009	信息安全技术 信息安全风险管理指南
	GB/T 20984-2007	信息安全技术 信息安全风险评估规范

3.2.3 信息安全管理循环模型

为体现动态性和持续发展的特点，院内 ISMS 的构建与信息安全管理工作部署实施也将遵循管理的一般循环模式—PDCA（Plan-Do-Check-Act）循环模型。

PDCA 循环[3]又称「戴明环」(Deming Cycle)，来源于休哈特（Walter A Shewhart)于 19 世纪 30 年代提出的 PDS(Plan-Do-See)循环，后被戴明(Edwards Deming）所采纳并加于拓展，进而形成一个质量持续改进循环模型。该循环将一个过程抽象为 Plan（策划）、Do（实施）、Check（检查）、Act（处置）等四个阶段（如图 3-1 所示），每个阶段都有各自相应的任务和目标。每个 PDCA 循环都从 Plan 阶段为起始，以 Act 阶段为结束，每四个阶段形成一个闭合的循环。同时，上一个 PDCA 循环的产出物可以作为下一个 PDCA 循环的输入，如此循环往复，使得过程的目标可以进行持续性的发展和改进（如图 3-2 所示）。

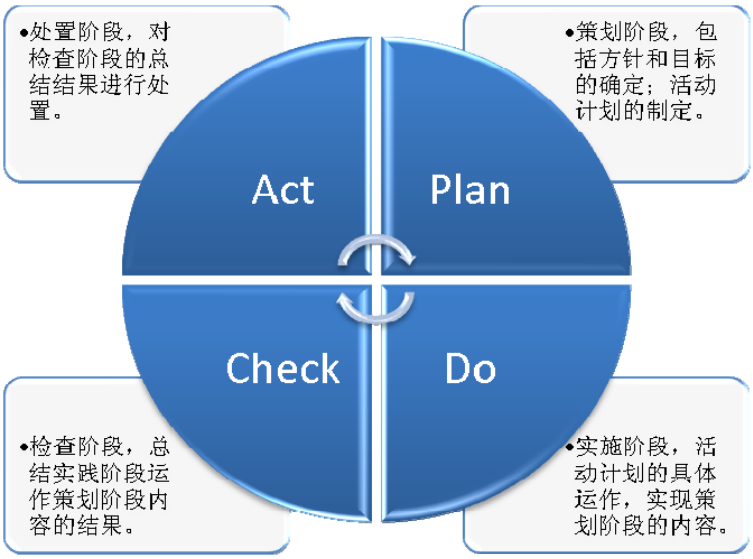

图 3-1 PDCA 循环

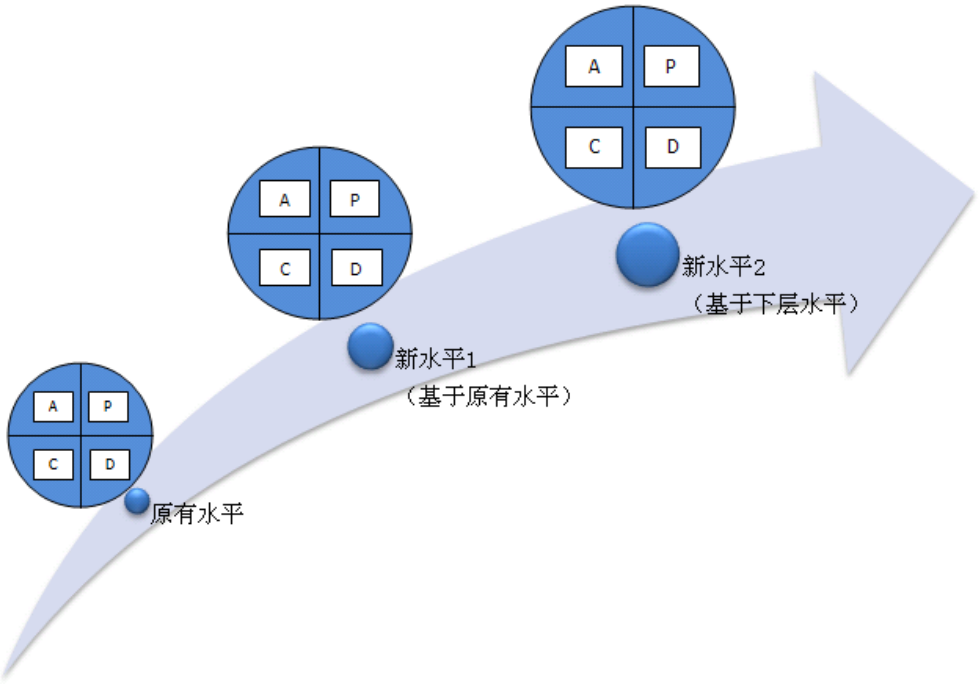

图 3-2 PDCA 循环持续改进示意图

应用到 ISMS 中的 PDCA 循环模型如图 3-3 所示，各阶段的工作内容详见表 3-3。

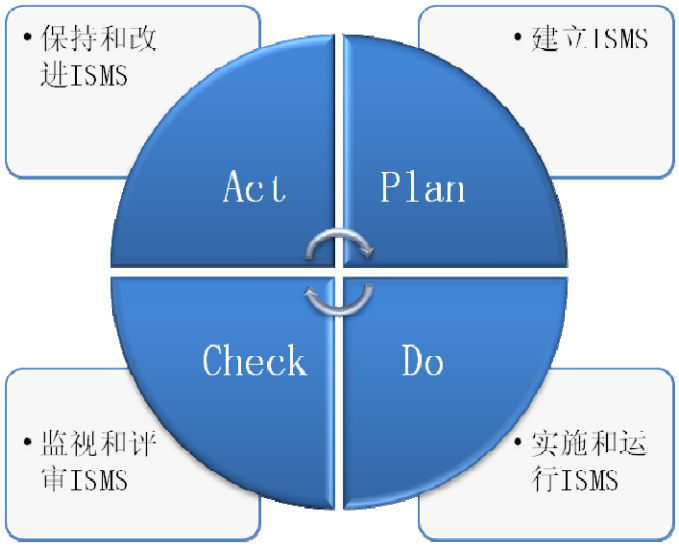

图 3-3 应用于 ISMS 的 PDCA 模型

表 3-3 应用于 ISMS 的 PDCA 模型各阶段工作内容

阶　段	目　标	工作内容
Plan	建立 ISMS	建立与管理风险和改进信息安全有关的ISMS 方针、目标、过程和程序，以提供与组织总方针和总目标相一致的结果。
Do	实施和运行 ISMS	实施和运行 ISMS 方针、控制措施、过程和程序。
Check	监视和评审 ISMS	对 ISMS 方针、目标和实践经验进行评估，在适当时候测量过程的执行情况，并将结果报告给管理者一共评审。
Act	保持和改进 ISMS	基于 ISMS 内部审核和管理评审的结果或者其它相关信息，采取纠正和预防措施，持续改进 ISMS。

3.3 构建原则

为了确保可行性、适用性和合规性，我院 ISMS 的构建过程将遵循以下原则：

- 先试点后推广原则

我院所属单位的数量较多，信息化程度和信息安全管理水平参差不齐，若一开始就在院内全面铺开 ISMS 的建设工作，不仅涉及面广，工作量大，而且容易造成建设进度的拖延。因此，我院 ISMS 的构建将在局部范围内进行试点，在总结实践经验后再在全院范围内的推广。

- 合规性原则

所构建的 ISMS 不仅要符合国内各项法律法规和规章制度的要求（如：等级保护制度的要求），而且还要符合各项合同的约定。

- 以业务为导向，以等级保护为判断点的原则

ISMS 在构建过程中要以业务流程梳理为导向，用等级保护制度要求为判断点来评判各项目标和策略的符合程度。

- 以信息系统为核心，以资产为操作对象的原则[4]

为了便于 ISMS 的操作，在设计伊始就要贯彻以信息系统保护为核心，以资产为操作对象的原则，将具体的目标和策略逐一分解到具体的信息资产中。

3.4 信息安全管理体系的设计与建立

3.4.1 信息安全管理体系设计

国际标准 ISO/IEC 27002:2005《信息安全管理实用规则》作为一个通用的信息安全控制措施集合，为我院 ISMS 的建立提供了控制措施的选择参考。该标准共包含 11 个安全域（如图 3-4 所示）、39 个安全类别和 133 条控制措施。

图 3-4 ISO/IEC 27002:2005 的安全域构成

针对现状分析中所表现出的不足之处，我院需要加强内部人员的安全意识教育；与外部合作伙伴的合作安全；信息系统的监管等方面的管理。基于此，我院的 ISMS 将在 ISO/IEC 27002:2005 原有的 11 个安全域上进行扩展，重点突出 3 个切实需要加强管理的安全域[5]：信息安全教育培训、服务外包安全和检查监督审计，扩展后的安全域构成如图 3-5 所示。

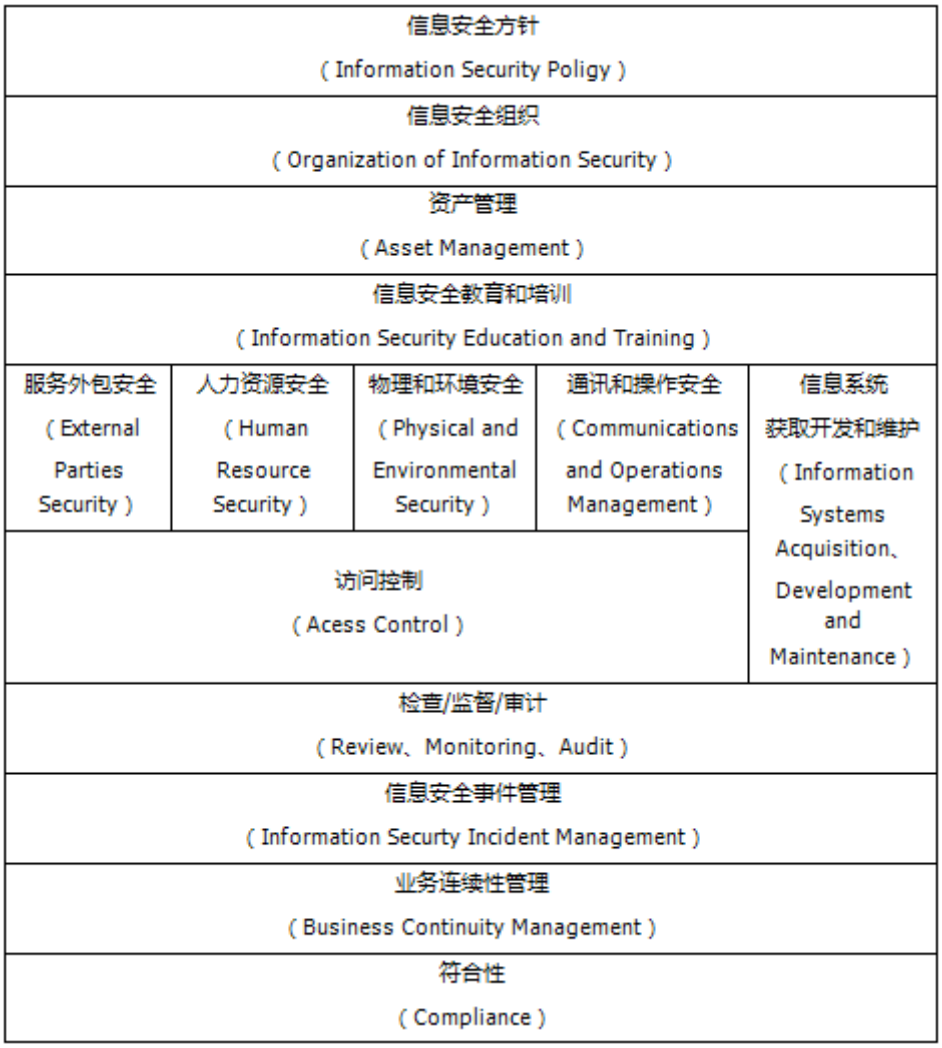

图 3-5 院内 ISMS 的安全域构成

3.4.2 信息安全管理体系建立

结合上述章节所阐述的 ISMS 构建原则和构建目标，参照国际标准 ISO/IEC 27001:2005 中 ISMS 的建立流程，我院此次的 ISMS 构建过程将按信息化项目的方式来进行管理，具体的建设阶段[6][7]为：前期准备、运行分析、现状调研、风险评估、体系编制和试运行。

（1） 前期准备阶段

前期准备阶段承担的是 ISMS 构建项目启动前的工作，主要包括：

- 成立 ISMS 建设项目组，明确责任人。
- 确定 ISMS 项目的项目范围，明确实施对象。

- 召开项目启动会并进行前期培训。
- 确定 ISMS 项目的总体实施方案。
- 确定项目的合作伙伴，含技术支持方和咨询服务方。

（2） 运行分析阶段

运行分析阶段是院内 ISMS 构建的第一步，一般以现场访谈和调查问卷的方式进行，其主要目的是使项目组成员初步了解我院的组织机构、信息安全管理目标、管理需求、业务流程以及现有信息资产等情况，阶段结束后将明确院内 ISMS 构建的范围和边界。

运行分析阶段的主要工作有：

- 明确运行分析阶段的工作范围。
- 收集所有已经得到确认的文档，如：法律法规、规章制度、标准规范、合同或协议、年度报表等，分类后将其进行文档化。
- 了解并确认工作范围内的组织架构。
- 分析并确认工作范围内组织所面临的特定环境和形势，如：通信网络、活动场所、IT 资源、信息处理、系统应用等。
- 了解工作范围内的业务流程，确认其实现的功能，并给出执行过程的流程图示。
- 通过业务流程的梳理，识别出流程中所涉及的信息系统，绘制并确认工作范围内的信息系统逻辑拓扑图。
- 了解并确认信息系统的主观重要性、所包含的信息资产明细和类别，初步排定其进行等级保护定级工作的优先级别。
- 了解并确认工作范围内的组织愿景，同时确认其对未来信息安全需求的影响度。

该阶段的关键产出物包括：

- ISMS 构建和实施的范围和边界。
- 工作域的划分以及优先级别的确认。
- 主要业务流程、功能、场所、信息系统、通信网络的确认。
- 核心业务流程、重要信息系统及信息资产的归类。
- 组织愿景和信息安全需求文档。
- 记录脆弱性的文档。

（3） 现状调研阶段

现状调研阶段一般采用调查问卷、技术手段和现场访谈的方式进行，其主要目的是使项目组成员全面了解我院现有的信息安全水平，阶段结束后将形成现状调研报告或差距分析报告。

现状调研阶段的主要工作有：

- 对信息系统和通信网络进行配置、操作、管理、运维等方面的现场调研。
- 确定信息系统的等级保护级别，完成信息系统的定级工作，修正工作范围内的重要信息资产列表。
- 收集与信息系统和通信网络相关的各类技术支持、操作规程和运维管理资料。
- 参照选定的各类国际国内信息安全管理标准，对比院内现有的信息安全管理现状，进行现状分析和差距分析。

该阶段的关键产出物包括：

- 现状调研报告或差距分析报告。
- 重要信息系统及信息资产的修正。
- 信息系统等级保护级别的确定与确认。

- 记录脆弱性或缺陷的文档

（4） 风险评估阶段

风险评估是对信息系统存在的风险进行确认的过程。信息系统的风险评估工作通常是以信息系统为核心，以资产为操作对象，同时参照相关信息安全技术标准的模式进行。

风险评估阶段将对信息系统的脆弱性、信息系统面临的威胁、威胁利用脆弱性后对信息系统所造成的实际负面影响、利用事件发生的可能性等方面进行风险评估和分析，操作的优先级别将取决于现状调研阶段形成的信息系统等级保护级别，阶段结束后将形成风险评估报告。

风险评估阶段的主要工作有：

- 风险评估的准备，包括取得高层的许可和支持；划定风险评估的范围；确定风险评估的具体对象；准备可能用到的技术手段或工具；制定风险评估工作计划等。
- 识别并评价资产，包括特定信息系统所涉及的资产的识别；已识别资产的界定与分类；核心资产的识别等。
- 识别威胁和威胁可以利用的脆弱性，包括参照相关信息安全技术标准建立威胁和脆弱性列表；对比威胁和脆弱性列表，识别信息系统可能存在的威胁和脆弱性；运用技术手段或工具，识别信息系统实际存在的漏洞以及防范攻击的能力等。
- 识别和评价现有控制措施，包括行政、技术、管理和法律法规等方面的安全控制措施的识别和评价。
- 分析威胁利用脆弱性的可能性和影响，包括识别每个脆弱性的控制措施部署程度；分析现有控制措施的有效性和符合度等。
- 分析风险的大小，包括确定风险计算方法；计算风险发生的可能性；评定风险等级等。

- 编写风险评估报告。
- 风险处置，包括风险降低；风险转移；风险接受等。进行风险处置时应优先考虑进行风险降低，当风险不可降低时，可以考虑风险转移的处理方式，当然也要考虑到风险被转移方的认可问题，而当风险既不可降低又不可转移时，要考虑风险接受问题。另外，在选择和部署安全控制措施降低风险的过程中要关注适度安全、投入产出比等要求。

该阶段的关键产出物包括：

- 风险评估程序。
- 风险评估报告。
- 风险处理计划。
- 风险评估表。

（5） 体系编制阶段

ISMS 的构建和部署实施非常注重文档化工作，体系编制阶段的主要目的是建立完整的 ISMS 体系文件，包括 ISMS 方针文件和适用性声明（SOA）的编制。

(a) ISMS 方针文件

虽然 ISMS 方针文件的长度没有强制性要求，一般依实际情况而定，但在编制时应概括全面，便于员工理解；同时应清晰精确，便于参考转化和贯彻落实。另外，编制定稿后的方针文件必须获得领导层的认可，并在 ISMS 范围内进行落实。

院内 ISMS 方针文件的编制至少包含以下方面的内容：

- 定义信息安全的内涵、信息安全管理的总体目标和范围，阐述以安全可靠方式进行信息共享的便利性和重要性。
- 宣布高层的愿景，以及为实施信息安全管理的目标和原则所承诺给予的支持。

- 简要陈述信息安全管理的方针、目标、原则、需求、安全策略。
- 定义信息安全事件的通报机制和责任认定。
- 列举需要遵守的其他相关文件，如：政策性文件、个人信息安全管理的常规性事务、其它信息安全管理方面的规则等。

(b) 适用性声明

ISMS 适用性声明的编制实际上就是对哪些控制措施适用于院内的信息安全管理进行声明，该文件的编制是强制性的。

院内 ISMS 适用性声明编制的主要工作包括：

- 选择的控制目标和控制措施，包括参照 ISO/IEC 27001:2005 的附录 A，选择用于进行风险处置的控制目标和控制措施；新增控制目标和控制措施等。
- 准备适用性声明，包括参照 ISO/IEC 27001:2005 的附录 A，记录选择控制目标和控制措施的理由；记录删减控制目标和控制措施的理由等。

（6） 试运行阶段

体系编制阶段的产出物按照文件控制要求进行审核批准后正式发布实施，此时将进入 ISMS 的试运行阶段。该阶段是 ISMS 正式运行前的磨合阶段，是 PDCA 循环模型后三个阶段的缩减，其主要目的是为了在实践中检验 ISMS 构建的全面性、充分性、适用性和有效性，同时通过适时适度的调整提高 ISMS 的契合度。

4 结束语

信息安全管理体系的建立和部署实施可以切实提高组织的信息安全管理水平，而基于先进信息安全管理标准，并进行适当地裁剪则是构建有效信息安全管理体系的快速途径。本文结合我院的信息安全管理实际，参照国内外信息安全管理标准，提出了院内信息安全管理体系的构建设想，并给出了具体的建设路线图。不足之处，希望大家给予指正。

参考文献

[1] 吴海燕，苗春雨，蒋东兴.美国高校信息安全管理情况分析与启示[J].实验技术与管理，2009，26（5）.

[2] 李天目.信息安全管理标准及综合应用[J].现代管理科学，2006，(6)：51-57.

[3] 吴昌伦，王毅刚.PDCA 过程模式在信息安全管理体系的应用[J].中国计算机用户，2003，(43)：42-43.

[4] 范怀炜.基于企业信息资产建立安全管理体系[J].中国计算机信息防护论文集，2008，258-262.

[5] 春增军.基于 ISO27001 的企业信息安全保障体系的构建设想[J].情报杂志，2009，28（5）：155-158.

[6] 谢宗晓，郭立生.信息安全管理体系应用手册[M].北京:中国标准出版社.2008.

[7] 于华欣.政府部门 ISMS 建设的体会与思考[J].通信技术，2009，42(8)：239-242.

【作者简介】

杨东娴 女

职　　称： 社科院 计算机网络中心 工程师

职　　务： 社科院 计算机网络中心「网络信息安全处」副处长

研究领域： 软件工程、信息安全与管理

个人简介： 2008 年毕业于中科院研究生院，获工程硕士学位；现任社科院计算机网络中心工程师，近年参与院综合地理信息服务平台系统和院社会调查数据支撑平台系统的建设，先后发表了《GIS 技术在哲学人文社会科学中的应用研究》、《社会调查数据平台中基本统计分析功能的 R 实现》、《数据共享与学科交叉研究—浅析社科领域的 GIS 系统应用》等文章；近期研究领域为软件工程、信息安全与管理。

联络电话： 86-85196461

联络邮箱： ydxian@cass.org.cn