文章编号:1671-8585(2008)06-0471-08

大型企业信息安全体系架构设计初探

罗革新,吕增江,崔广印,鲍天祥,王振欣,于普漪
(中国石油集团东方地球物理勘探有限责任公司信息技术中心,北京 100007)

摘要:随着信息技术的发展和应用的不断深入,信息安全日益受到国家、企业和社会公众的关注。中国政府已经提出了构建国家信息安全保障体系的设想,明确了政府、企业和公民各自应承担的责任与义务。企业的信息安全工作,主要关注点是如何保障信息技术应用和防止企业商业秘密泄露。同时,大型企业特别是地理位置分布广泛的企业集团,在信息安全方面存在很多难点。分析了国内、国际信息安全现状和发展趋势,概述了 Gartner 的企业信息安全体系架构设计思想和国内大型企业面临的信息安全需求;从管理、技术、控制三个视角和概念、逻辑、实现三个层面阐述了构建企业信息安全体系架构的概念、内容和方法,提出了一种大型企业信息安全体系架构模型——MCT(管理-控制-技术)模型;针对大型企业实际情况,陈述了如何应用 MCT 模型进行信息安全体系架构设计;最后给出了一套可实施的从设计层到实现层的转换方法,即以项目为单位来组织具体的信息安全体系建设工作。

关键词: 信息技术;信息安全;信息系统;信息技术基础设施;信息安全体系架构
中图分类号:TP393.08 **文献标识码**:A

随着信息技术的发展及信息技术在企业生产和经营管理等方面的广泛、深入应用,企业越来越依赖网络和信息系统。而不时发生的病毒侵袭、黑客攻入和敏感机密信息被窃取事件,使得信息安全保障工作日益重要并倍受人们关注。中国信息化办公室专家委员会常务委员曲成义指出,我国网络信息安全入侵事件态势严峻,互联网信息安全威胁的新动向值得关注,比如谍件泛滥值得严重关注,网络钓鱼的获利动机明显,DDoS 开始用于敲诈,木马潜伏孕育着杀机,获利和窃信倾向正在成为信息安全事件的主流,等等。归结原因,包括:内控机制尚显脆弱,强审计机制不够落实,风险评估意识不够强,高危漏洞潜在,信息安全域界定与等级保护待探索,灾难恢复尚不到位,缺少对"分发式威胁"的警惕和治理,信息安全集成管理有待加强,等等。

随着美国萨班斯法案的发布和内控要求的提升,对在美上市公司财务风险控制提出了更高要求,促使全球各大企业近年来纷纷加大信息安全建设力度以满足合规性要求。中国政府也非常重视信息安全保障工作,政府有关部门从国家安全和行政监管角度正在抓紧立法和标准制定工作,并明确提出了建设国家信息安全保障体系的构想,政府、企业和公民在建设国家信息安全保障体系中各自承担不同的责任。构建国家信息安全保障体系已经提高到国家信息化发展战略层面,大型企业设计合理的信息安全体系架构,建立完整的信息安全保障体系不但必要,而且非常紧迫。本文基于笔者参加中国石油"十一五"信息技术总体规划和信息安全总体规划编制工作的经验,以及工作期间与 IBM、毕博、埃森哲和 Gartner 等公司资深信息安全专家进行交流的心得,初步探讨了大型企业信息安全体系架构的设计问题。

1 国家信息安全保障体系相关工作情况

中国政府高度重视国家信息安全保障体系建设工作。国家信息化领导小组 2003 年发布的《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发 27 号文)提出:"立足国情,以我为主,坚持管理与技术并重;正确处理安全与发展的关系,以安全保发展,在发展中求安全;统筹规划,突出重点,强化基础性工作;明确国家、企业、个人的责任和义务,充分发挥各方面的积极性,共同构筑国家信息安全保障体系",并从"实行信息安全等级保护"和"加强信息安全法制建设和标准化建设"等方面对信息安全保障工作提出了指导意见。中共中央办公厅、国务院办公厅 2006 年发布的《2006—2020 年国家信息化发展战略》提出要提升信息安全保障水平的战略目标,使我国在这个时期

收稿日期:2008-09-20;**改回日期**:2008-10-12。
第一作者简介:罗革新(1966—),男,高级工程师,从事企业信息化、信息系统与信息安全体系建设、知识管理,及石油勘探开发软件平台、软件体系结构与模式、软件工程与 IT 项目管理等工作。

内信息安全的长效机制基本形成，国家信息安全保障体系较为完善，信息安全保障能力显著增强。

在标准与立法方面，国家先后出台了一系列法律法规，包括《中华人民共和国计算机信息系统安全保护条例》[1]、《中华人民共和国电子签名法》等，也包括国务院颁布的行政法规，公安部、国信办等中央部委颁布的部门规章以及由地方人民政府发布的地方性行政规章。这些法律法规对信息安全涉及的内容和法律措施等作出了明确的界定。

近年来，国家大力推动信息安全等级保护工作，陆续出台了《计算机信息系统安全保护等级划分准则》(GB17859—1999)等标准[2]，2007 年国家四部委下发《关于印发〈信息安全等级保护管理办法〉的通知》(公通字[2007]43 号)[3]明确指出："国家通过制定统一的信息安全等级保护管理规范和技术标准，组织公民、法人和其他组织对信息系统分等级实行安全保护，对等级保护工作的实施进行监督、管理"，在提高信息安全意识、落实信息安全责任、提高信息安全保障能力等方面起到了积极作用。同时，国家还设立了一批信息安全专业机构，如"国家计算机网络应急技术处理协调中心"、"中国信息安全产品测评认证中心"、"公安部计算机信息系统安全产品质量监督检验中心"等，我国信息安全组织保障体系正在逐步完善。

在信息安全技术研究方面，《信息产业科技发展"十一五"规划和 2020 年中长期规划纲要》中明确把信息安全技术作为未来优先发展的重点技术之一，主要包括：密码技术、安全处理芯片技术、电子认证、应急响应和灾难恢复技术、信息安全测评技术等。在信息安全人才体系建设上，相关的高校和科研院所陆续开设了信息安全专业，一些高校还拥有密码学专业和信息安全专业的博士点和硕士点。目前，我国信息安全专业教育已基本形成了正规高等教育人才培养体系。

对于构建国家信息安全保障体系，曲成义研究员提出了中国国家信息安全保障体系框架(图 1)

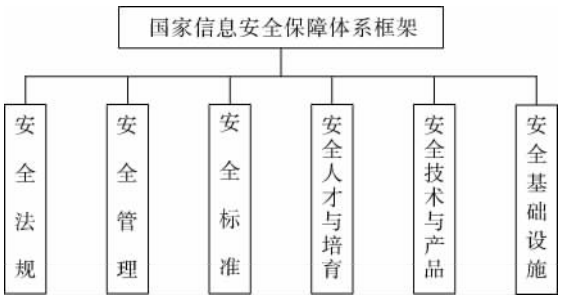

图 1 国家信息安全保障体系框架

和行业信息安全保障体系框架(图 2)。国家层面涵盖了信息安全立法、行政监管、产品与技术研发、人才培养和基础设施建设等方面，行业层面应关注安全工程和服务。

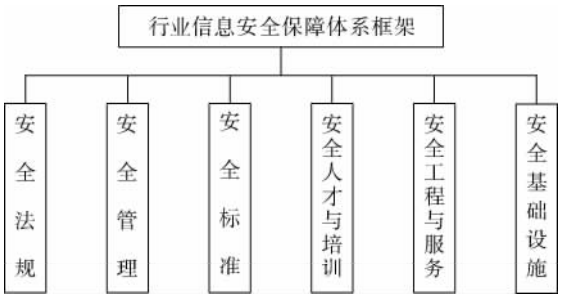

图 2 行业信息安全保障体系框架

总体上看，国家信息安全保障体系已经开始建立，但在信息安全法律、标准、技术和人才体系建设等方面还存在一些亟待解决的问题，如缺乏专门的信息安全基本法，信息安全标准制定工作依然落后，信息安全关键技术和产品受制于人等。此外，国内各大企业的信息安全工作水平参差不齐，绝大多数企业没有确立完整的信息安全体系架构，在国家政策落实和主动防御方面也较国外有较大差距。

2 大型企业信息安全体系建设需求

我国大型企业为突出发展主营业务，全面增强市场竞争和可持续发展能力，都不断加大对信息化建设的投入力度，也取得了显著成效，基本建成了企业网络系统和电子邮件、企业门户、视频会议等基础应用，并实施了 ERP，CRM 等管理应用系统和生产过程控制的专业应用系统。在信息安全方面，各企业也做了很多基础性工作，包括：①采用成熟、实用、可靠的技术，建立一系列保障信息网络安全的设施和系统，如防火墙、入侵检测、防病毒系统等；②适时制定信息安全方面的规章制度，并通过规章制度的贯彻执行，落实信息安全责任制等。

随着信息技术的广泛应用，信息系统集中化程度不断提高，对业务的支撑作用越来越显著，一旦发生信息安全事件对企业造成的经济损失和社会影响都将非常巨大。但各大型企业大都具有规模庞大、分支机构地域分布广、业务复杂多样等特点，企业信息系统存在较多安全隐患，易遭受攻击，信息安全风险与日俱增，单靠采用一些独立、分散的信息安全措施已经无法满足其实现综合、纵深安全防护的迫切需求。因此，大型企业亟需制定完善的信息安全政策方针，规划并建立符合企业实际情况

的信息安全体系架构，完善信息安全相关管理制度与规范，采用先进的技术手段，加强信息安全风险控制能力，提高员工信息安全意识，全面提高信息安全保障能力，支撑企业核心业务的健康发展。

3　国际信息安全领域进展情况

3.1　国际信息安全发展趋势

进入 21 世纪以来，世界各个国家和地区高度重视信息安全的发展，美国、俄罗斯、欧盟、日本等相继制定了信息安全的法律法规，明确关键基础设施面临的威胁，确定信息安全目标和范围，制定信息安全基础设施保障框架，加紧关键技术研究，加强技术标准制定与立法管理等相关工作。信息安全已成为世界发达国家安全战略的重要组成部分。

据 Gartner 分析，当前国际大型企业在信息安全领域主要有如下发展趋势：

1）信息安全投资从基础架构向应用系统转移；

2）信息安全的重心从技术向管理转移；

3）信息安全管理与企业风险管理、内控体系建设的结合日益紧密；

4）信息技术逐步向信息安全管理渗透。

结合大型企业信息安全发展趋势，国际各大咨询公司、厂商等机构纷纷提出了符合大型企业业务和信息化发展需要的信息安全体系架构模型，着力建立全面的企业信息安全体系架构，使企业的信息安全保护模式从较为单一的保护模式发展成为系统、全面的保护模式。

3.2　Gartner 企业信息安全体系架构[4]

Gartner 将企业信息安全体系架构视为企业进行信息安全管理的指南，用于在企业内部以一致的方式记载和交流信息安全管理成果。Gartner 基于其企业信息安全体系架构实践和对信息安全管理的深入理解，提出了企业信息安全体系架构（EISA）模型（图 3）[5]。Gartner 认为，要建立 EISA，必须给组织提供某种机制，使得组织能够充分利用通用的原则和最佳实践，将信息安全的业务需求转换成可操作的信息安全和风险管理解决方案。

Gartner 建议 EISA 架构应包括业务、信息和技术三个视角和概念层、逻辑层和实现层三个层面。其中业务视角包括信息安全组织和流程，信息视角包括执行信息安全职能所需要的各类信息，技术视角包括基础设施的安全架构、安全服务架构和应用安全架构，定义了实现安全需求的软硬件配置。概念层描述相对抽象的意图、目标、特性和模型，在相当长的时期内保持稳定；逻辑层详细描述在对环境、资源等进行各种可能的选择分析和权衡基础上确定的实现概念层目标的各种思想、方法、技术、设计；实现层描述实现概念层目标和逻辑层设计的具体模型。

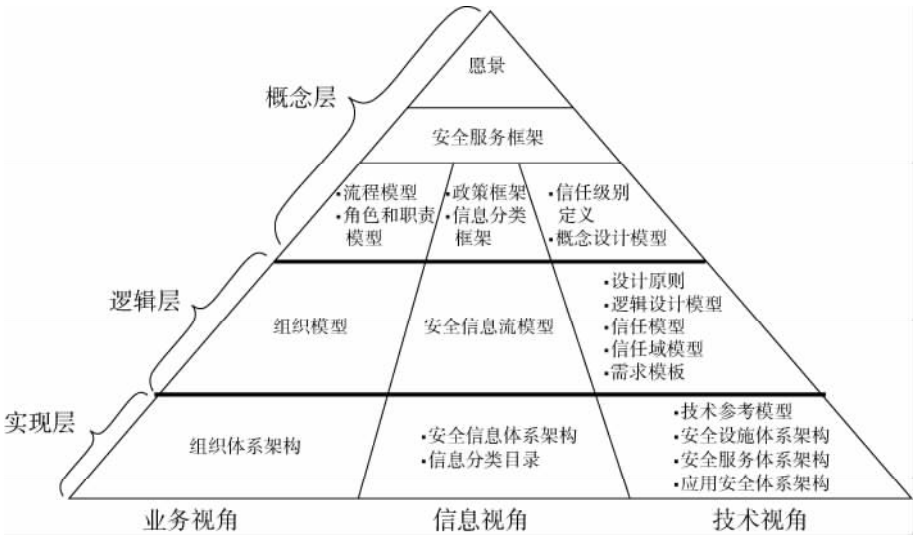

图 3　Gartner 企业信息安全体系架构

4　企业信息安全体系架构模型

Gartner 从业务、信息和技术三个视角来阐述企业信息安全体系架构模型，并从概念、逻辑和实现层三个层次来展现不同视角的关注点，以体系架构的方式展现了一个企业信息安全体系架构模型。中国企业尤其是大型企业信息安全体系架构的建

立，在借鉴国际先进经验的同时，须结合企业的实际需求，严格落实国家在信息安全保障体系方面的相关规定，落实国家信息安全等级保护中提出的从管理和技术两个方面提高信息安全保障能力的要求。因此，我们提出从管理、技术和控制三个视角与概念层、逻辑层和实现层三个层次构建企业信息安全体系架构模型。

4.1 企业信息安全体系架构的三个视角

企业信息安全体系的建立是为了保障业务运作。我们从企业的可实施角度，在企业信息安全体系架构实践的基础上，结合对信息安全管理的理解，提出从管理、技术和控制三个视角来综合考虑企业信息安全体系的构建，如图 4 所示。

1）管理视角，关注企业的信息安全管理架构。信息安全管理架构描述企业信息安全工作如何开展，信息安全管理职能如何与企业内的其他业务职能沟通协作，实现对信息安全的有效管理。如同企业内的其它业务管理架构一样，信息安全管理架构应包括组织、流程、管理制度三个要素。

2）控制视角，关注企业的信息安全控制架构。信息安全控制架构全面描述了企业信息安全对业务运作过程的要求，业务运作对信息安全技术的要求，以及网络和信息系统所采用的保护方式。

3）技术视角，关注企业的信息安全技术架构。信息安全技术架构从技术角度描述了企业信息技术基础设施和应用系统的安全保护措施，包括应用安全架构、信息安全服务架构、信息技术基础设施安全架构 3 个方面。

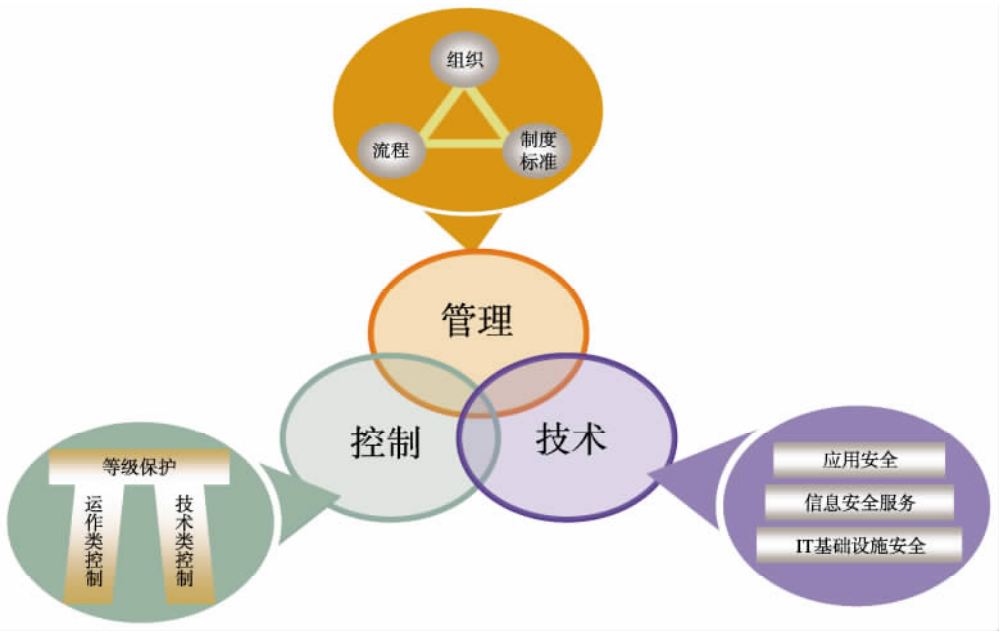

图 4 企业信息安全体系架构的三个视角

企业信息安全体系架构的三个视角是相互联系、相互合作的，由此构成一个有机融合的整体。信息安全管理架构包含信息安全风险管理的流程、信息安全管理的职责和相应的信息安全制度，使企业能够正确地评价信息系统所面临的安全风险，并根据等级保护的基本要求，选择和实施合理的安全控制，从而实现对信息系统的等级保护。信息安全控制架构规范了对企业信息系统的基本保护要求，包括两个方面：一方面，该架构建立在对风险合理预期基础之上，同时也是信息安全风险管理的成果；另一方面，该架构是企业进行信息安全需求分析并确定安全控制的重要工具，是信息安全风险管理的输入。信息安全技术架构描绘了企业基础设施和应用的信息安全架构，以及信息安全服务的架构，是控制架构中技术控制要求的实际实现。

4.2 企业信息安全体系架构的三个层次

企业信息安全体系架构必须能够指导企业将信息安全的战略和业务的要求转换成可操作的信息安全风险管理实践。在实现信息安全目标的过程中，不同层级的管理和实施者关心不同详细程度的信息。因此从概念层，逻辑层和实现层三个层次来考虑企业信息安全体系架构就显得更加重要并具有可操作性，如图 5 所示。

1）概念层，定义了信息安全体系架构的概念模型。概念模型由概念要素组成，包含目标和特征，是高度抽象的模型，在较长的时间内保持稳定。

概念模型为规划者所关心，阐述了实现企业信息安全战略目标所需要的管理、控制和技术组件。

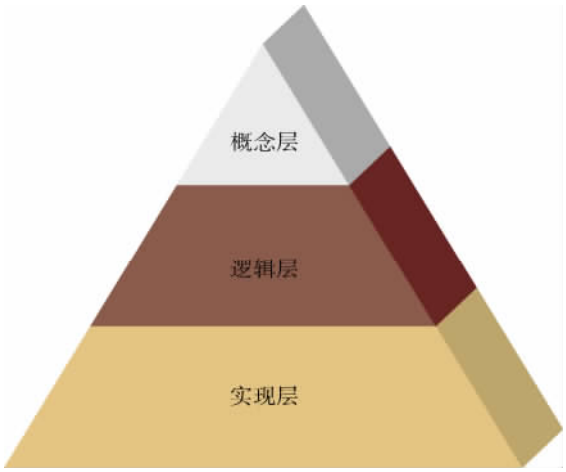

图 5　企业信息安全体系架构的三个层次

2）逻辑层，定义了信息安全体系架构的逻辑模型。逻辑模型由功能逻辑元素组成，描述了如何通过功能逻辑元素及元素间的合作关系来实现概念模型要求的目标和特征，与具体的资源和产品无关。逻辑模型为设计者所关心，是在环境、资源、各种可能选择分析和权衡基础上确定的实现概念层目标的各种思想、方法、技术和设计。

3）实现层，定义了信息安全体系架构的实施模型。实施模型由具体的物理实现元素组成，描述用什么资源和产品来实现逻辑设计方案，解决部署和配置等方面问题。实施模型涉及具体的资源、产品，为构建者所关心，是概念层目标和逻辑层设计的具体实现。

概念层、逻辑层和实现层之间的关系是：上层模型指导下层模型，下层模型是上层模型的细化和实现。通过这种内在的指导和实现关系，信息安全体系架构提供了将业务对信息安全的要求转换成具体的信息安全控制方案的工具。

4.3　企业信息安全体系架构模型

信息安全体系架构是企业信息安全建设和运作的蓝图，是企业构建信息安全保障体系的核心内容。通过对企业信息安全体系架构的描述，以及在企业内部进行广泛的宣传与推广，可以帮助企业规范信息安全的管理、建设和运作，提高信息安全的整体保障水平。最重要的是，企业信息安全体系架构提供了一种将业务对信息安全的需求转换成可操作的信息安全和风险管理解决方案的机制。因此，我们根据上述三个视角、三个层次的建设理念，提出 MCT（管理、控制和技术）企业信息安全体系架构模型，如图 6 所示。

该信息安全体系架构模型从企业信息安全风险管理的角度出发，构建了组织、人员、信息安全流程、制度和标准规范、基于等级保护的安全控制基本要求体系、基础设施与应用的安全架构、共享信

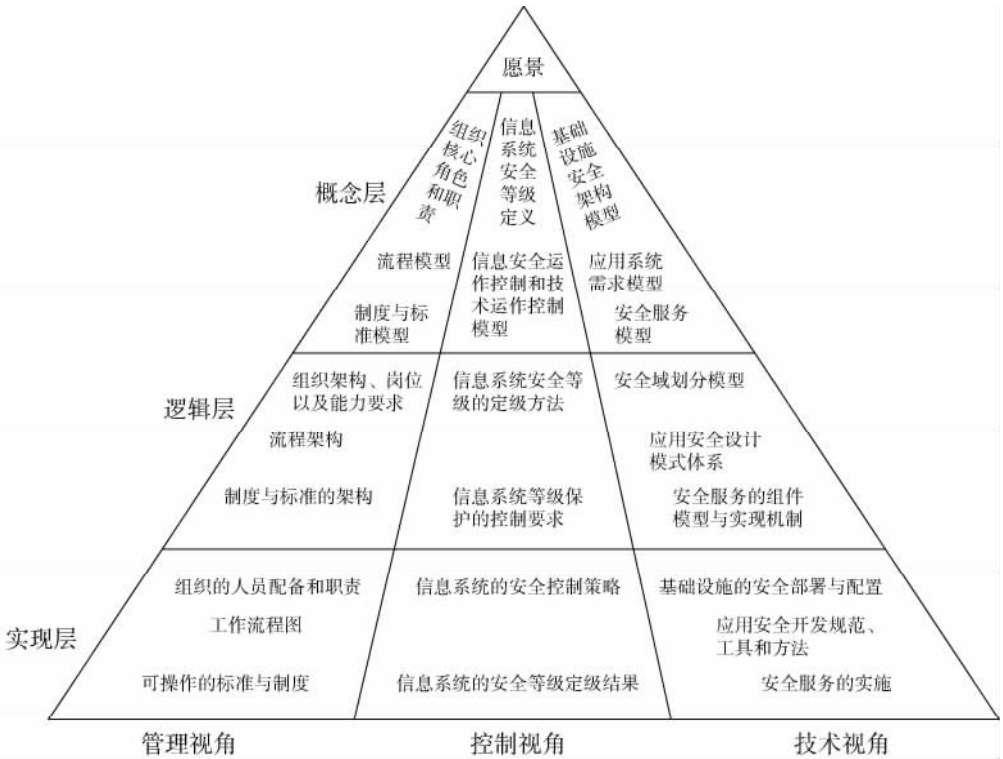

图 6　MCT 企业信息安全体系架构模型

息安全服务等关键要素，强调从组织、人员技能、流程、基础设施、标准规范等5个方面实现信息安全体系的核心功能，规划了以等级保护为基础的控制架构，以符合国家关于信息安全保障体系与等级保护的要求。

5 企业信息安全体系架构设计

MCT模型提出了企业信息安全体系架构的设计思想，对体系架构的管理、控制和技术三个视角，概念、逻辑和实现三个抽象层次，以及对应的架构内容进行了描述和论证，并说明了企业在信息安全建设中如何应用和不断完善信息安全体系架构的基本思路。我们通过分析MCT模型中的管理架构(M)、控制架构(C)和技术架构(T)，来设计适合企业应用的信息安全体系架构。

5.1 信息安全管理架构设计

随着信息技术与企业管理结合的日益紧密，人在信息技术应用中的作用越来越重要，信息安全工作的重点开始从传统的侧重技术向关注管理转变，并有信息安全“三分技术、七分管理”的说法，因此信息安全管理架构的设计和实施就显得尤为重要，企业信息安全管理架构的设计可以从组织、流程和制度三个方面开展[5,6]。

1) 信息安全组织。信息安全组织的核心是信息安全角色职责，它定义和明确了信息安全专业团队核心职能角色及其相关的职责，并以此指导未来信息安全组织建设、团队建设和能力培养。信息安全组织设计具体是指根据企业信息安全战略、信息技术组织结构及组织分布特点进行信息安全专业组织架构的设计，包括设计信息安全组织架构，明确各级信息安全组织的职责与汇报关系，同时设计在各级信息安全组织中承担各项信息安全工作的岗位及其职责，并定义适合其岗位职责的能力要求等。

2) 信息安全流程。信息安全流程描述企业信息安全职能的所有业务流程及其关系，它识别和定义了信息安全管理的主要流程以及它们之间的关系。通过这些流程的设计，企业的信息安全职能可以实现对信息安全风险的识别、减少、监控和响应，进行有效的全生命周期管理，实现业务对信息安全的要求。信息安全流程的设计可以包括信息安全风险管理，信息安全检查监督以及信息安全意识、培训和教育等内容。

3) 信息安全制度。信息安全制度描述与企业信息安全相关的管理和技术制度的层次结构，以及不同层次的信息安全制度涉及的内容和解决的问题。信息安全制度设计除应考虑体系的完整性外，还应考虑制度体系本身能满足两方面要求：①灵活地更新、修订信息安全制度，及时反映信息安全风险环境动态；②方便与制度使用者之间的沟通，确保信息安全管理和技术人员及用户能够方便地了解哪些是必须做的，哪些是禁止做的。

信息安全制度是规范信息安全管理的基本手段，离开了信息安全制度，就缺乏落实信息安全管理各项要求以及实现信息安全管理目标的手段。因此，信息安全制度设计必须有利于制度的及时更新，反映风险环境和业务需求的变化。一个缺乏更新的、陈旧的信息安全制度是无法落实的，也不能起到保障企业信息安全目标实现的作用。

信息安全制度是整个企业信息安全体系架构核心内容在制度、文件形式上的体现，其设计可以从信息安全管理办法、信息安全标准规范以及信息安全实施细则和操作规程等方面开展。

5.2 信息安全控制架构设计

MCT模型的管理、控制和技术三个视角是相互联系、相互合作的一个有机整体，而信息安全控制则是管理和技术架构能否成功衔接的关键环节。信息安全控制架构设计可以从信息系统等级划分、信息安全运作控制和信息安全技术控制三方面来阐述。

1) 信息系统等级划分。信息系统等级划分描述了企业信息系统安全等级的划分框架和各安全等级的正式定义。信息系统安全等级划分包括信息资产等级、应用系统等级和网络系统等级三个方面，可以分系统识别与划分和等级确定两个阶段来实施。

2) 信息安全运作控制。信息安全运作控制描述为了达到不同安全等级的信息系统和信息的安全目标，在企业的业务运作和信息技术运作过程中需要实施的运作类安全控制的架构，包括控制的分类和控制针对的主要信息安全风险。信息安全运作控制是相对于技术控制而言的，是指主要由人来执行的那些控制。安全控制的强度应该与被保护信息系统的安全等级相适应。

3) 信息安全技术控制。信息安全技术控制描述为了达到各安全等级的信息系统和信息的安全目标，对通用信息技术和信息安全技术需要实施的技术类安全控制的架构，包括控制的分类和控制针对的主要信息安全风险[7]。信息安全技术控制是

相对于运作控制而言的，是指主要由系统自动完成的那些安全控制。在信息系统网络层、系统层、应用层的信息安全技术控制中，都包含标识与鉴别、访问控制等五大类通用技术控制。信息安全技术控制对必须具备的技术手段、实现机制、控制强度都作了要求，其中控制强度还必须与被保护信息系统的安全等级相适应。

5.3　信息安全技术架构设计

信息安全技术架构作为企业信息安全体系架构的一部分，同时也是企业的应用系统架构和信息技术基础设施架构的组成部分。它包括：信息技术基础设施安全架构、信息安全服务架构和应用安全架构。

信息安全技术架构与应用系统架构、信息技术基础设施架构的关系如图 7 所示。

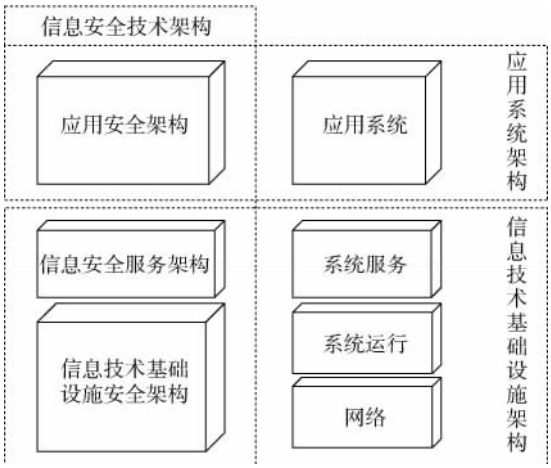

图 7　信息安全技术架构与应用系统架构、信息技术基础设施架构的关系

1）信息技术基础设施安全架构。信息技术基础设施是信息传递和系统运行的基础平台，信息技术基础设施安全架构是信息技术基础设施架构的一部分，描述了如何在网络和系统软硬件构成的系统运行技术架构上建立安全的信息技术环境，成为保障信息安全的基础。

信息技术基础设施安全架构应该以网络安全架构作为主体，并在此基础上结合相应的系统软硬件进行安全部署和配置。网络安全架构的规划应该采用功能区域划分的方法，根据网络所承载业务系统的特性与所面临的风险，划分不同的网络功能区域，并根据业务的安全需求以及等级保护的要求，结合纵深防御的原则，对不同区域之间的信息访问作出限制。网络功能区域的划分能够对安全架构的设计起到指导作用，而区域间的信息访问限制也能够成为制定网络安全控制策略的依据。

2）信息安全服务架构。信息安全服务架构定义了信息安全体系架构中的安全服务以及各服务之间的关系。在信息安全技术架构中，信息安全服务定义为保证信息和信息系统安全的一系列技术功能。信息安全服务架构的设计将参考 PDRR 模型。在信息保障的概念下，PDRR 模型把信息安全分成保护、检测、反应和恢复四个环节，以实现对信息机密性、完整性和可用性的保护，检查并监控系统仍然存在的安全漏洞，对危及安全的事件和行为及时做出响应和处理，当发生安全事故时可以在短时间内恢复正常运营。

3）应用安全架构。应用安全架构既是信息安全技术架构的一部分，又是应用系统架构的一部分。应用安全架构是应用系统的信息安全视角的体现，解决了如何保障应用系统安全的问题。应用系统建立在信息技术基础设施的基础之上，所以应用系统的信息安全保障更关注已有的信息安全服务的充分利用，并在信息技术基础设施安全架构上，通过在应用系统中实现、集成保障信息安全的机制，满足应用系统的业务流程对信息安全的需求，达到信息安全技术控制的要求，从而全方位、全过程地保障信息安全。

5.4　信息安全项目设计方法

为了完成信息安全体系架构从设计层到实现层的转换，我们针对上述三个视角的架构给出一套可实施的方法，即以项目为单位来描述具体的信息安全工作。

5.4.1　信息安全项目设计

信息安全项目设计采用基于差距分析的方法，通过从管理、控制与技术三个视角分析信息安全现状与总体架构的差距，识别出改进需求，并针对改进需求提出具体的改进措施，最终将改进措施归纳形成项目，如图 8 所示。

项目设计方法所依据的信息安全现状来自于企业在各个信息安全领域的主要发现，总体架构则来自于管理、控制与技术架构的设计。在设计改进措施的过程中，需要考虑到改进措施覆盖的范围、时间跨度、实施条件的成熟度等，遵循全面覆盖、相对独立和远近结合等原则。项目群实施蓝图设计方法是基于依赖性关系与优先级分析的方法，通过分析项目间的依赖关系与各项目的优先级顺序确定最终的项目群实施蓝图，如图 9 所示。根据项目间的输出输入关系与项目实施的前提条件确定项目间的依赖关系，根据项目实施的紧迫性与重要性确定项目实施优先级顺序。

图 8 信息安全项目设计方法

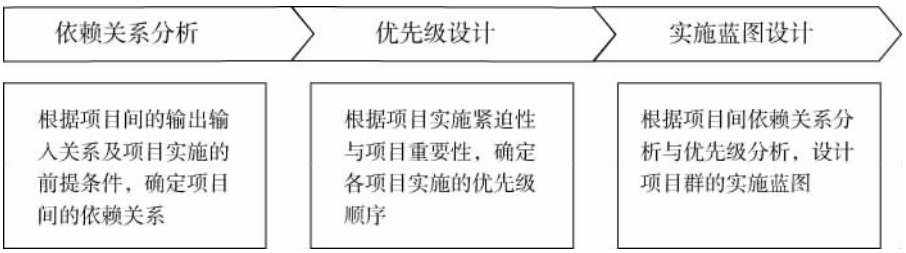

图 9 实施蓝图设计方法

5.4.2 项目设计思路与原则

项目设计的基本思路是将改进措施按一定的原则归类组合成可实施的项目。为了确保项目的可实施性，在设计项目时应遵循范围清晰、同类合并和依赖简化等原则。

6 结论

综上所述，信息安全是企业信息化发展到一定程度后都会面临的问题，而建立信息安全体系架构则可以尽可能多地帮助企业降低信息安全问题带来的损失。但是，即使采取了一定的措施，企业内各种信息安全问题仍然可能发生，所以建立信息安全体系将会是一个长期的过程，而不是单纯通过建立一些制度、规范或采用某些新技术就可以完成的过程。因此，企业信息安全体系建设应该与企业业务和信息化建设协调发展，企业信息安全体系必须针对其自身业务发展和信息化建设的需要而建立。同时，信息安全体系应该是一个开放的体系，具有持续改进的能力，能够随着业务和信息技术的发展不断自我完善。

参 考 文 献

1 中华人民共和国国务院 147 号令. 中华人民共和国计算机信息系统安全保护条例[EB/OL]. (1994 - 02 - 18)[2008 - 10 - 04]. http://www.tc260.org.cn/infoViewF.jsp

2 国家质量技术监督局. GB 17859—1999 计算机信息系统安全保护等级划分准则[EB/OL]. (1999 - 09 - 13)[2008 - 10 - 04]. http://www.ga.dl.gov.cn/djbh/GB17859—1999.doc

3 公安部，国家保密局，国家密码管理局，等. 关于印发《信息安全等级保护管理办法》的通知[EB/OL]. (2007 - 06 - 22)[2008 - 09 - 17]. http://www.gov.cn/gzdt/2007 - 07/24/content_694380.htm

4 Gartner Inc. Structure and content of an enterprise information security architecture: Gartner research[EB/OL]. (2006 - 01 - 26)[2008 - 09 - 18]. http://egovstandards.gov.in/egs/eswg5/enterprise-architecture-working-group-folder/gartners-reports/structure_and_content_of_an__136867.pdf

5 ISO/IEC 27001:2005. Information technology—Security techniques—Information security management systems[EB/OL]. (2005 - 10 - 14)[2008 - 10 - 04]. http://www.iso.org/iso/catalogue_detail? csnumber=42103

6 ISO/IEC 27002:2005. Information technology—Security techniques—Code of practice for information security management[EB/OL]. [2008 - 10 - 04]. http://www.iso.org/iso/search.htm? qt=27002&published=on&active_tab=standards

7 ISO/IEC 27005:2008. Information technology—Security techniques—Information security risk management[EB/OL]. (2008 - 06 - 04)[2008 - 10 - 04]. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm? csnumber=42107

（编辑：戴春秋）