网络安全实施框架指南

ISACA®

关于 ISACA

ISACA®是享誉全球的信息安全专业机构，在其近50年历史中，致力于帮助专业人员和企业实现技术的最大潜力。当今世界为技术所驱动，ISACA为全球专业人员提供知识、职业认证并打造社群网络，助力其职业进阶，推动他们所在的机构转型，通过技术实现创新。ISACA全球社区中有50多万名从事信息与网络安全、治理、审计与鉴证、风险与创新工作的人员。ISACA旗下的CMMI则专注于企业能力成熟度的评估与改进。ISACA在全球188个国家设有215个分支机构，并在美国和中国开设办公室。

免责声明

ISACA设计并编制了*网络安全实施框架指南*（下称“作品”），主要用作专业人员的学习资料。ISACA无法保证使用本作品就一定能够实现成功的结果。本作品不应被视为包含所有适用的信息、程序和测试，不排除在其它信息、程序和测试的合理指导下获得同样结果的可能。在确定任何具体信息、程序或测试的适宜性时，专业人员应就具体的情况（特定的系统或信息技术环境）做出自己专业性的判断。

保留权利

ISACA中国

北京朝阳区东三环中路20号乐成中心A座5层578室
电话：010-58783078

目录

本页为空白页

图表列表

本页为空白页

一、背景概述

2016年7月6日起中国的《国家网络安全法》 向社会公开征求意见，2017年6月1日正式实施。《网络安全法》是中国网络安全领域的基础性法律，具有里程碑式的意义。这次发布的国家网络安全法第一次把网络安全的要求以专门法律的形式发布出来，明确了国家、主管部门、网络所有者、运营者及普通用户各自的责任，规定了违规相关的罚则，比任何一部安全规范具有更强的执行力。

《国家网络安全法》正式实施后，国家主管部门将开展全面的网络安全检查工作，以期推进《网络安全法》实施，提升全员信息安全意识，加强对关键基础设施和个人敏感数据的保护，促进网络安全实践的常态化与制度化。此法的实施将对中国信息安全领域有着深远的影响。

在正确理解此法要旨的基础上，如何正确有效地落实此法将是全社会即将面临的问题。目前各机构纷纷解读此法内容，各厂商围绕网络安全法制定各自的产品与服务推进计划。

今年是ISACA中国大陆正式建立运营机构的开局之年，希望通过开展一些有影响的活动来为中国的信息安全实践与IT风险控制做出自己的贡献。ISACA在IT控制与信息安全领域积累四十多年的经验，为全球IT控制与信息安全专业人士提供创新和世界一流的知识、标准、认证以及最佳实践。

ISACA在美国网络安全法律的实施推广过程中积累了丰富的经验。美国总统奥巴马于2013年2月签署并发布了13636法案《增强关键基础设施网络安全》，2014年2月美国国家标准与技术研究所NIST针对《增强关键基础设施网络安全》提出了《美国增强关键基础设施网络安全框架》（简称CSF），ISACA参与了NIST牵头的CSF研究与制定过程，并提出了基于COBIT5的网络安全实施框架，为美国的政府部门及重要机构实施13636法案提供了宝贵的经验。

ISACA认为CSF的制定及推进的思路及方法适合于中国在当前网络安全法的实施过程中加以借鉴。ISACA希望借鉴其知识及经验为中国网络安全法的实施建立一个可以参考的框架，为各行各业落实网络安全法的要求提供可行的参考方法。

本页为空白页

二、ISACA网络安全实施方法论

（一）网络安全法的内容分析

网络安全法结构与内容

图1—国家网络安全法的结构和内容		
法律章节	条款数量	内容简介
第一章总则	14条	简述法律目的、范围、总则、部门职责、总体要求等
第二章网络安全支持与促进	6条	定义国家直属部门和政府在推动网络安全工作上的职责
第三章网络运行安全	19条	定义网络运营者与关键信息基础设施的运行安全规定
第一节一般规定	10条	针对网络运营者的网络运行安全要求与职责规定
第二节关键信息基础的运行安全	9条	针对关键信息基础设施的安全规定与保护措施要求
第四章网络信息安全	11条	定义个人信息保护的保护规定
第五章监测预警与应急处置	8条	定义国家网络安全监测预警与汇报机制
第六章法律责任	17条	定义处罚规定
第七章附则	4条	相关名词释义与其他附则

网络安全法的特点分析

- 明确提出了国家网络主权的概念，网络空间主权是国家主权在网络空间的延伸和表现；
- 明确了网络安全和信息化发展并重原则，提出要促进网络基础设施建设的互联互通，鼓励新技术应用和创新，鼓励应用新技术来改善网络安全。
- 专门强调了保障关键信息基础设施的运行安全，在强调网络安全等级保护制度的基础上，对关键信息基础设施实施重点保护，并且规定了关键信息基础设施的运营者在采购网络安全产品和服务可能影响国家安全的应当通过国家网络安全审查。
- 明确加强了对个人信息的保护，对网络运营者的主体的法律责任和义务做出了全面的规定，公民个人信息保护将进入新的起点和转折点，网民从道德自觉将走向法律规范，用法律武器维护自己的合法权益。

网络安全法的实施重点

各机构在落实网络安全法时，要重点关注保护对象和保护的方法。网络安全法提出了保护内容涉及了网络运行安全、敏感信息保护及监控应急机制三个方面的内容，网络运行安全又根据是否一般性网络运营者、关键信息基础设施运营者实施不同保障要求；保护的方法涉及了等级保护体系实施、网络安全评估监测及预警、网络安全技术防护、网络安全应急管理、安全职责落实与违规处罚、网络安全意识宣传、网络安全人才培养等方面的内容。

一般性网络系统是指组织实现信息化应用的基本硬件系统和软件系统，由网络系统、应用系统及周边辅助系统组成的信息系统。网络安全法所指的网络运营者泛指网络的所有者、管理者和网络服务提供者，这些系统一旦发生网络安全事故，会影响局部机构及个人的网络安全，造成一定的损失。

关键信息基础设施是指面向公众提供网络信息服务或支撑能源、通信、金融、交通、公用事业等重要行业运行的信息系统或工业控制系统，且这些系统一旦发生网络安全事故，会影响重要行业正常运行，对国家政治、经济、科技、社会、文化、国防、环境以及人民生命财产造成严重损失。

（二）ISACA网络安全框架实施方法论

ISACA认为面对日趋严重的网络威胁时，无论是一般性网络系统还是关键信息基础设施，都需要充分了解当前威胁环境、存在的脆弱性及自身业务特征，分析与安全法要求之间存在的差距和面临的风险；但在具体实施时，要根据组织的规模、投入资源及监管要求的不同，采用合规性应对及精细化应对两种不同的实施方法。

图2—确定实施方法

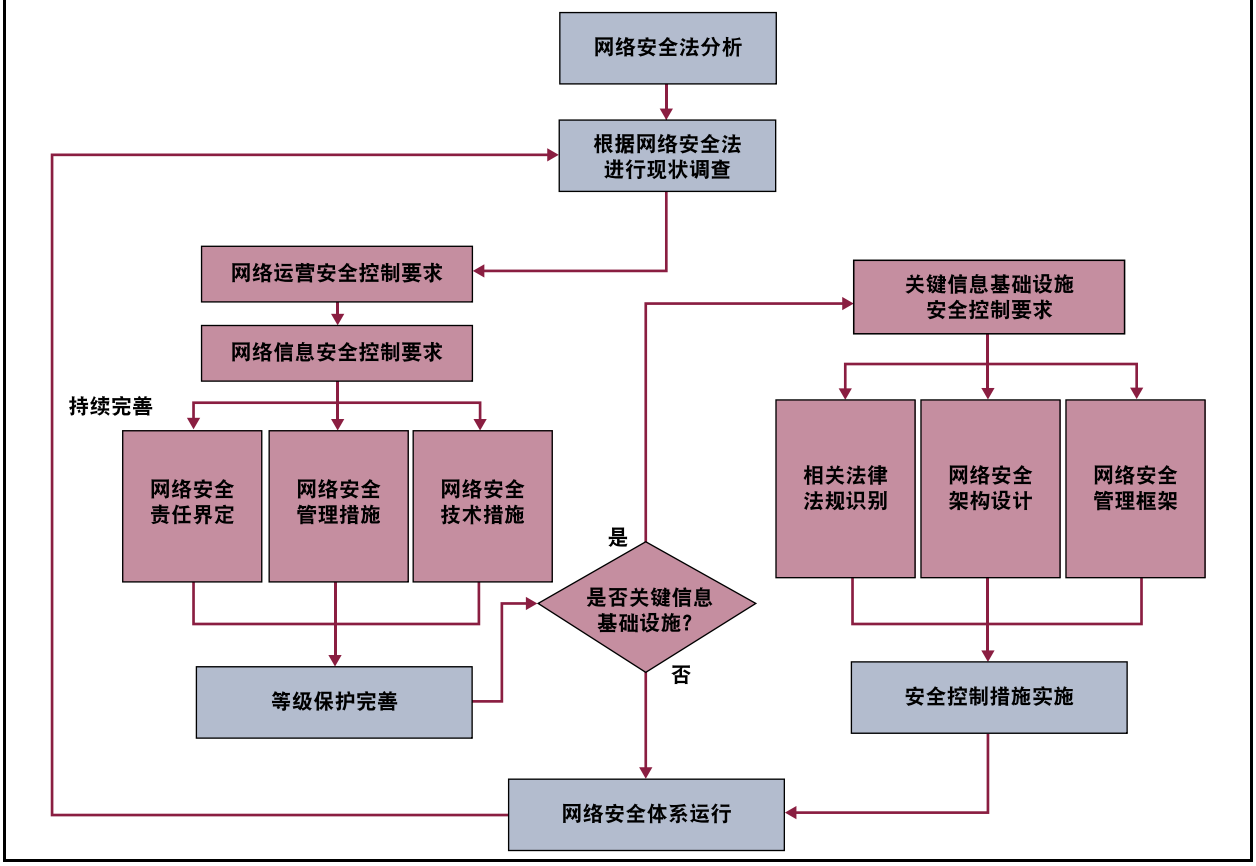


图1-网络安全实施框架（根据网络安全法与相关指引进行分析与实施）

ISACA网络安全框架实施方法论描述如下：

- 对网络安全法进行充分的分析，了解网络安全法出台的背景、主要内容、关键举措、责任主体、检查办法等。
- 根据网络安全法的具体要求，分析组织当前的实际情况，从管理要求、技术要求及敏感数据保护等方面进行差距分析。
- 根据组织所在行业的重要程度，分析组织对支撑关键业务的信息系统的依赖性及信息系统发生网络安全事件后可能造成的损失来分析判断是否是关键业务；
- 针对一般性的网络运营者，需要从网络运营安全、网络信息安全二个层面对网络安全法的相应条款进行分析，在责任方界定、管理措施及技术措施三个方面分析组织应当采取的措施。
- 针对关键信息基础设施的网络运营者，在落实一般性的网络运营基本要求的基础上，还需要增加关键信息基础设施相关的控制要求，利用体系化、精细化的方法来实施网络安全法。具体措施有：识别适用的法律法规和行业最佳实践；对网络安全进行架构设计；建设综合的网络安全管控框架。
- 为网络安全管控体系的有效运行建立保障体系。具体措施有：网络安全制度与流程的建立，网络安全的监测与预警，网络安全应急管理，网络安全审计与持续完善。

三、法律所要求的网络安全差距分析

在对网络安全解读与特征分析的基础上，结合实施单位的具体情况，从网络安全的管理体系、技术体系及敏感数据保护三个方面进行差距分析，以了解组织当前的现状及与合规要求之间的存在的差距和所面临的风险，为后续的整改规划奠定基础。

（注：以下三个方面是为用户建议的重点差距分析的内容，用户可以根据此示例模板，细化符合自身需要的更加细化的差距分析内容。）

（一）网络安全管理方面的差距分析

图3—现状与监管要求之间的差距分析方法

安全领域	合规要求	参考对应条款	差距分析结果
1.1 制度与组织	实行网络安全等级保护制度，严格按照法案要求确定网络安全管理负责人，涉及关键信息基础设施运营的机构还要依法设置专门安全管理机构和安全管理负责人。	第21条	
1.2 风险评估	关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估。	第38条	
1.3 应急管理	企业制定应急预案应覆盖所有网络安全场景，包括网络扫描攻击、拒绝服务攻击等，系统方面有恶意代码、后门程序等；另外，根据应急预案涉及的各方面内容，建议由负责应急预案工作的部门组织预案中各角色相关人员开展应急预案培训和应急演练工作。	第25条、第53条	
1.4 事件通报	企业应建立健全本机构的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息，杜绝发生信息安全事件后企图瞒报、少报的事件。	第51条	
1.5 IT审计	企业需明确制定内部审计检查方法、标准、检查项，开展信息内审工作，以验证措施有效性，避免违规而承担法律责任。	第59—第75条	

（二）网络安全技术方面的差距分析

图4—现状与监管要求之间的网络安全差距分析方法

安全领域	法规要求	对应条款	差距分析结果
2.1 系统建设	企业网络和重要信息系统建设应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施要同步规划、同步建设、同步使用。	第33条	
2.2 安全防护	企业除了持续加强对传统攻击的防范和应对，做好网络边界防御、应用安全防护、终端安全防护等边界防护工作外，还应持续加强安全风险事中监控和处置，加快安全风险态势感知平台的建设，通过将大数据技术和信息安全技术充分结合，将海量数据集中进行关联和实时分析，识别潜在风险活动，由被动防护转变为主动防护。	第10条、第21条	
2.3 采购产品与服务	企业所需的网络关键设备和网络安全专用产品需经安全认证或检测，并且网络产品和服务的采购可能需通过国家安全审查。	第35条	
2.4 网络运营	对关键信息基础设施的运营者要求一系列安全保护义务，如监测记录网络运行状态并留存相关的网络日志不少于六个月。	第21条	

（三）敏感数据保护方面的差距分析

图5—现状与保护敏感数据相关监管要求之间的差距分析方法

安全领域	法规要求	对应条款	差距分析结果
3.1 业务敏感数据的识别与保护	企业应当对其业务数据进行识别和敏感性分类，对敏感数据的生命周期过程进行风险评估，对技术环境及业务流程中薄弱环节进行整改与加固，以防止组织重要信息和数据的泄露或者被窃取、篡改。	第21条、第45条、第47条、第48条、第50条	
3.2 个人信息使用公示	企业对于个人信息收集或使用环节应以明确、易懂和合理的方式如实公示其收集或使用个人信息的目的、个人信息的收集和使用范围、个人信息安全保护措施等信息，接受公共监督。	第22条、第41条、第43—48条	
3.3 个人信息的保护	企业应采取安全措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失，做好自有信息系统的前台和后台数据访问控制，采取合理、有效措施，如业务流程评估、账号和权限管理、数据库审计等，降低个人信息泄露、毁损、丢失风险。	第42条	
3.4 信息跨境流动	企业在业务中涉及的个人信息和重要业务数据需在中国境内存储、处理和分析，且未经安全评估不得向境外提供，除非法律、行政法规另有规定。	第37条	

本页为空白页

四、网络关键信息基础设施的识别

（一）关键信息基础设施的定义*

由于关键信息基础设施在国家网络安全中有着举足轻重的作用，因此，国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。

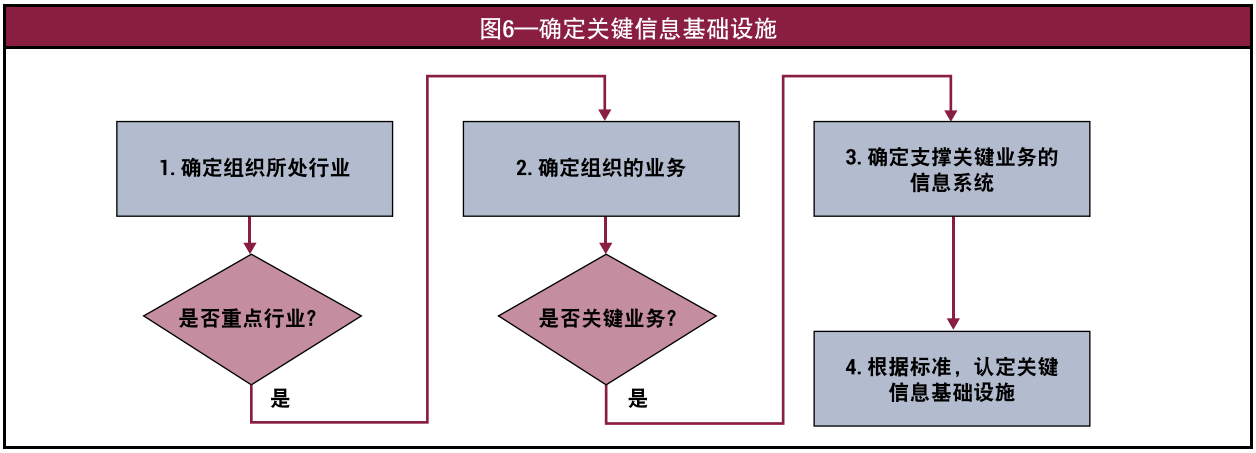
各行各业负责关键信息基础设施安全保护工作的部门要编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作。

* 本文中关于关键基础设施的定义参照了中央网信办2016年发布的《关键信息基础设施确定指南（试行）》相关规定。

（二）关键信息基础设施的识别

关键信息基础设施的确定，通常包括四个步骤，一是确定所属行业，国家有关跨部门有重点行业有相关认定标准；二是确定组织的业务价值链的组成与分布，识别关键业务；三是根据关键业务，逐一梳理出支撑关键业务运行或与关键业务相关的信息系统或工业控制系统；四是根据关键业务对信息系统或工业控制系统的依赖程度，以及信息系统发生网络安全事件后可能造成的损失认定关键信息基础设施。如下图所示：

图6—确定关键信息基础设施



重点行业

根据国家有关部门（公安部、国资委）的认定，一般把能源、金融、交通、水利、医疗卫生、环境保护、工业制造、市政、电信与互联网、广播电视、政府部门等部门认定为国家重点行业和部门。

关键业务

图7—业内关键业务		
行业		关键业务
能源	电力	• 电力生产（含火电、水电、核电等） • 电力传输 • 电力配送
	石油石化	• 油气开采 • 炼化加工 • 油气输送 • 油气储存
	煤炭	• 煤炭开采 • 煤化工
金融		• 银行运营 • 证券期货交易 • 清算支付 • 保险运营
交通	铁路	• 客运服务 • 货运服务 • 运输生产 • 车站运行
	民航	• 空运交通管控 • 机场运行 • 订票、离港及飞行调度检查安排 • 航空公司运营
	公路	• 公路交通管控 • 智能交通系统（一卡通、ETC收费等）
	水运	• 水运公司运营（含客运、货运） • 港口管理运营 • 航运交通管控
水利		• 水利枢纽运行及管控 • 长距离输水管控 • 城市水源地管控
医疗卫生		• 医院等卫生机构运行 • 疾病控制 • 急救中心运行
环境保护		• 环境监测及预警（水、空气、土壤、核辐射等）
工业制造 （原材料、装备、消费品、电子制造）		• 企业运营管理 • 智能制造系统（工业互联网、物联网、智能装备等） • 危化品生产加工和存储管控（化学、核等） • 高风险工业设施运行管控
市政		• 水、暖、气供应管理 • 城市轨道交通 • 污水处理 • 智慧城市运行及管控

图7—业内关键业务	
行业	关键业务
电信与互联网	• 语音、数据、互联网基础网络及枢纽 • 域名解析服务和国家顶级域注册管理 • 数据中心/云服务
广播电视	• 电视播出管控 • 广播播出管控
政府部门	• 信息公开 • 面向公众服务 • 办公业务系统

关键信息基础设施的类型

关键信息基础设施一般三大类，第一类是网站类，如党政机关网站、企事业单位网站、新闻网站等；第二类是平台类，如即时通信、网上购物、网上支付、搜索引擎、电子邮件、论坛、地图、音视频等网络服务平台；第三类是生产业务类，如办公和业务系统、工业控制系统、大型数据中心、云计算平台、电视转播系统等。

关键信息基础设施的认定

针对不同基础设施类型，从关键业务对信息系统或工业控制系统的依赖程度，以及信息系统发生网络安全事件后可能造成的损失认定关键信息基础设施。

图8—评估关键信息基础设施			
关键信息基础设施分类	判断标准	网络安全事件影响	举例
网站类	1. 县级（含）以上党政机关网站。 2. 重点新闻网站。 3. 日均访问量超过100万人次的网站。 4. 一旦发生网络安全事故，可能造成右边列影响之一的。 5. 其他应该认定为关键信息基础设施。	• 影响超过100万人工作、生活； • 影响单个地市级行政区30%以上人口的工作、生活； • 造成超过100万人个人信息泄露； • 造成大量机构、企业敏感信息泄露； • 造成大量地理、人口、资源等国家基础数据泄露； • 严重损害政府形象、社会秩序，或危害国家安全。	如：党政机关网站、企事业单位网站、新闻网站等。
平台类	1. 注册用户数超过1000万，或活跃用户（每日至少登陆一次）数超过100万。 2. 日均成交订单额或交易额超过1000万元。 3. 一旦发生网络安全事故，可能造成右边列影响之一的。 4. 其他应该认定为关键信息基础设施。	• 造成1000万元以上的直接经济损失； • 直接影响超过1000万人工作、生活； • 造成超过100万人个人信息泄露； • 造成大量机构、企业敏感信息泄露； • 造成大量地理、人口、资源等国家基础数据泄露； • 严重损害社会和经济秩序，或危害国家安全。	如：即时通信、网上购物、网上支付、搜索引擎、电子邮件、论坛、地图、音视频等网络服务平台。
生产业务类	1. 地市级以上政府机关面向公众服务的业务系统，或与医疗、安防、消防、应急指挥、生产调度、交通指挥等相关的城市管理系统。 2. 规模超过1500个标准机架的数据中心。 3. 一旦发生网络安全事故，可能造成右边列影响之一的。 4. 其他应该认定为关键信息基础设施。	• 影响单个地市级行政区30%以上人口的工作、生活； • 影响10万人用水、用电、用气、用油、取暖或交通出行等； • 导致5人以上死亡或50人以上重伤； • 直接造成5000万元以上经济损失； • 造成超过100万人个人信息泄露； • 造成大量机构、企业敏感信息泄露； • 造成大量地理、人口、资源等国家基础数据泄露； • 严重损害社会和经济秩序，或危害国家安全。	如：办公和业务系统、工业控制系统、大型数据中心、云计算平台、电视转播系统等。

五、一般性网络运营所需要网络安全控制措施

网络安全法对一般性网络系统及关键信息基础设施合规要求进行了区分对待，机构在实施网络安全法要找准两类对象的不同要求，有重点的加以实施。针对一般性网络系统的安全控制要求主要是从网络运营安全与网络信息安全二个方面，促进相关责任方落实管理措施与技术措施。

（一）网络运营安全控制措施

图9—网络运行安全要求和控制

保护要求	对应条款	责任方	建议的管理措施	建议的技术措施
1.1 制定安全制度，落实安全职责	第21条（1）	信息安全管理委员会、信息安全主管领导、信息安全管理团队及各部门信息安全负责人	1. 根据等级保护的要求，建立信息安全相关组织、制度和流程。 2. 建立负责网络安全管理的部门，明确网络安全负责人，并把安全职责落实到所有重要岗位中。 3. 确保信息安全制度落实执行，并对制度进行及时更新。 4. 在信息安全管理制度完善的基础上，逐步建立信息安全管理流程及度量指标体系。 5. 对全部员工进行信息安全规范和意识的教育。	在信息安全管理体系逐步完善的基础上，机构可以考虑开发部署信息安全管理软件平台，把制度管理、风险评估、安全规划、控制执行、绩效评价、威胁情报、日常工作流程等进行统一管理，以提高信息安全管理效率。（详细技术请参见本章（三）之“信息安全技术与管理措施的具体要求”）
1.2 部署安全技术措施，防范网络攻击	第21条（2）	信息安全主管领导、信息安全管理部门、信息技术部门、业务部门	1. 在现状调研与安全风险评估的基础上，结合业务战略要求，进行信息安全愿景规划。 2. 结合安全规划要求及技术市场动态，进行安全防护技术体系设计。 3. 对网络安全专业人员及IT专业人员进行相应的信息安全知识与技能培训。	从以下领域考虑安全防护技术措施的设计与部署：物理安全、网络安全、主机安全、应用安全、数据安全及云安全等。(详细技术请参见本章（三）之“信息安全技术与管理措施的具体要求”)

图9—网络运行安全要求和控制（续）				
保护要求	对应条款	责任方	建议的管理措施	建议的技术措施
1.3 建立网络监控和日志	第21条（3）	信息安全管理部门、信息技术部门	1. 制定网络系统监控管理制度，明确对网络、主机及应用系统进行监控的要求。 2. 制定系统日志管理相关流程，确保日志统一收集、备份及分析的方法与步骤。	1. 结合网络系统及应用系统运行需要，开启重要系统的日志记录功能。 2. 逐步部署日志的统一收集与监控分析设备，确保日志留存下限不少于6个月。 3. 定期对系统的重要日志进行检查和分析并形成记录。 4. 根据日志分析结果，进行安全态势感知和控制措施调整。
1.4 数据分类和备份加密	第21条（4）	安全管理团队、信息技术部门、业务部门	1. 制定数据分级分类、数据备份及数据安全控制相关规范 2. 数据安全管理相关要求落实到重要岗位的职责要求中。 3. 推进信息技术部门和业务部门对所管理的数据实施安全管理。	1. 根据组织业务特征，分析组织的静态数据与动态数据的现状，评价面临的控制风险，制定管控策略。 2. 根据数据的分类分级，对组织的敏感进行全生命周期管理，选用适当的技术措施对数据的使用、传输、存储及销毁过程进行安全防护。 3. 对于重要数据按照规范要求，在可用性方面，采取适宜的备份策略进行数据冗余备份；在机密性方面，采用符合国家要求的加密算法对其进行加密处理和访问控制。
1.5 确保网络产品和服务的安全性和合规性	第22条	安全管理团队、信息技术部门、采购部门、法律合规部门	1. 识别国家和行业有关网络产品与服务的基本要求； 2. 组织建立网络安全产品与服务供应商的准入、退出和安全考评机制，要求安全厂商提供持续的安全运维服务。 3. 建立威胁情报管理管理制度，形成威胁与漏洞通报预警机制。 4. 与厂商、上级监管及专业安全机构保持密切联系，制定安全漏洞的对外公布机制和上报机制。	1. 在合同中要求厂商对其提供的产品及服务确保安全要求，并在约定期限内持续提供安全维护服务。 2. 部署恶意代码毒查杀工具，对系统持续进行安全检测。 3. 部署漏洞扫描工具，进行安全漏洞检测、验证和补丁修补。 4. 对网络产品和服务进行渗透测试，对发现的安全问题及时进行整改。 5. 对于重大安全事件要向上级主管部门及时上报。

图9—网络运行安全要求和控制（续）				
保护要求	对应条款	责任方	建议的管理措施	建议的技术措施
1.6 网络关键设备和网络安全专用产品的安全认证和安全检测	第23条	安全管理团队、信息技术部门、采购部门	1. 建立组织范围内的网络关键设备和网络安全专用产品清单。 2. 了解国家有关网络关键设备和网络安全专用产品目录及相关安全认证和安全检测管理办法。 3. 在IT产品及服务的采购管理制度中明确网络产品和服务的安全认证与安全检测要求，并在合同中加以落实。	1. 组织应把网络关键设备和网络安全专用产品的安全与合规要求嵌入到项目审批和项目后评价的流程中。 2. 组织应重点关注主管部门出台的相关管理规范，包括但不限于以下内容： • 2017年5月国家网信办发布*《网络产品和服务安全审查办法（试行）》* • 2017年6月国家网信办、工信部、公安部和国家认可委共同发布*《网络关键设备和网络安全专用产品目录（第一批）》*
1.7 网络运营者应要求用户提供真实身份信息	第24条	安全管理团队、信息技术部门、业务部门、法律合规部门	1. 严格落实“实名制”工作，将用户身份识别和录入作为业务发展的首要环节和先决条件。 2. 在提供相应服务过程中对客户进行实名信息提供的要求，若有能力应对信息进行核实。	1. 使用二代身份证校验设备。 2. 将校验结果贯穿到业务受理的IT流程环节中。 3. 采用国家认可的电子身份认证技术。
1.8 建立网络安全事件处置流程，及时启动应急预案	第25条	安全管理团队、信息技术部门、业务部门	1. 建立信息安全事件管理制度与流程。 2. 建立网络安全应急管理制度与流程。 3. 编写应急预案与演练指南。 4. 实施网络安全应急演练，并对预案与演练进行总结与改进。	1. 对于发生的一般性安全事件，通过服务台启动安全响应程序。 2. 对于发生的较大的安全事件，需要启动相应的应急预案。 3. 对于发生的灾难性事件，需要启动灾难恢复和业务连续计划。
1.9 不得从事危害网络安全的活动或者为入侵者提供支持和帮助	第27条	安全管理团队、信息技术部门、法律合规部门	1. 在信息安全制度和员工行为准则中明确要求机构和员工不得从事任何危害网络安全的活动。 2. 不得为网络入侵者提供工具、支持和帮助。 3. 明确规定违反规定所面临的处罚。	1. 通过部署物理隔离、身份认证、访问控制、安全审计等技术手段对非法网络活动加以预防。 2. 通过对内部人员的终端操作、网络流量及系统日志的监测与分析，可以对非法的网络活动加以检测与响应。

图9—网络运行安全要求和控制（续）				
保护要求	对应条款	责任方	建议的管理措施	建议的技术措施
1.10 网络运营者在发布信息和配合安全调查方面要遵守国家规定，鼓励网络运营者开展信息安全行业协作	第26、28、29、30条	信息安全管理委员会、信息安全主管领导、信息安全管理团队	1. 在信息安全制度明确要求不得随意向社会发布系统漏洞和计算机病毒等网络安全信息，全力配合执法机构的安全调查活动。 2. 加强与社会机构在威胁情报和应急处置等方面进行合作。 3. 推进和响应建立行业协作机制，定期向会员进行风险警示，协助会员应对网络安全风险。	1. 与国家级和行业级的信息安全监测与响应中心进行联网，获取及时的信息安全威胁情报信息和行业最佳实践。 2. 建立组织内部的安全运行中心(SOC)，结合外部大数据进行集中式安全大数据分析与态势感知，做到安全风险事前预警，防患于未然。

（二）网络信息安全控制措施

图10—网络安全控制要求和措施				
保护要求	条款对应	责任方	建议的管理措施	建议的技术措施
2.1 组织应制定敏感信息保护制度	第21(4)、40、45、47、48、50条	信息安全管理委员会、信息安全主管领导、信息安全管理团队及各部门信息安全负责人。	1. 组织应建立健全组织内部敏感信息保护管理制度与职责体系。 2. 组织应当对其业务数据和个人信息进行分类识别和敏感性分级。 3. 对敏感数据的生命周期过程中各类系统环境及业务场景的静态数据和动态数据进行安全风险评估。 4. 对技术环境及业务流程中薄弱环节进行整改与加固，以防止组织和个人的重要信息和数据免受泄露、窃取、篡改。	1. 把敏感数据保护纳入到组织安全架构设计之中。 2. 使用数据脱敏、数据加密、访问控制、数据销毁等技术与产品来保护敏感信息，防止敏感的泄露、窃取和篡改。 3. 通过内部信息安全技术手段（如堡垒机、数据防泄露、终端安全管理、PKI加密体系的应用等）来加强数据安全体系建设。 4.从事后追责、溯源向事前感知、预警转变。

图10—网络安全控制要求和措施（续）				
保护要求	条款对应	责任方	建议的管理措施	建议的技术措施
2.2 网络运营者收集、使用个人信息时，要向用户明示并取得同意，不得超范围滥用个人信息，不得以非法方式获取、提供和出售个人信息	第22、41、44、45条	信息安全主管领导、信息安全管理团队、信息技术部门及各业务部门	1. 建立个人敏感信息收集的规范。 2. 梳理、修订现有各类业务合同、用户协议等格式文档，增加收集、使用用户个人信息的征询或告知类内容(包括网站页面)。 3. （补充）签订相应授权或许可协议。 4. 对可能涉及敏感个人信息的复杂业务应用场景，信息安全管理团队要与信息技术部门、业务部门、合规部门一起研究制定风险应对措施。	1. 在个人信息敏感性分类分级的基础上，在元数据及数据集标准层次上建立敏感数据的约束机制。 2. 在数据库、应用系统及网络流量及数据文件等层次上，使用相应的技术手段与产品保护保护个人敏感信息，防止对收集的敏感信息的误用与滥用。 3. 利用威胁情报及网络舆情大数据分析与组织相关的个人敏感信息的误用和滥用情况。
2.3 网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全	第42条	信息安全管理团队、信息技术部门及各业务部门	1. 建立个人敏感信息保护相应的制度与流程。 2. 建立个人敏感信息的保护机制：个人敏感信息的识别与分类分级、安全控制机制的建立、个人敏感信息全生命周期的管理、安全技术手段控制、检查审计持续改进。 3. 加强全员网络信息安全意识和职业素养的教育培训。	1. 对需要提供的个人信息，采用技术手段对个人信息进行脱敏处理。 2. 采取包括加密在内的技术手段对个人信息进行安全管理，并制定信息泄露的补救措施和汇报机制。
2.4 个人有权要求网络运营者删除和更改其个人信息	第43条	信息安全管理团队、信息技术部门及各业务部门	1. 建立个人敏感信息保护相应的制度与流程。 2. 制定个人信息所有者就其信息处置的投诉渠道和操作方法。	为用户提供访问通道，使用户能对其个人信息进行监控、修改与销毁的操作。

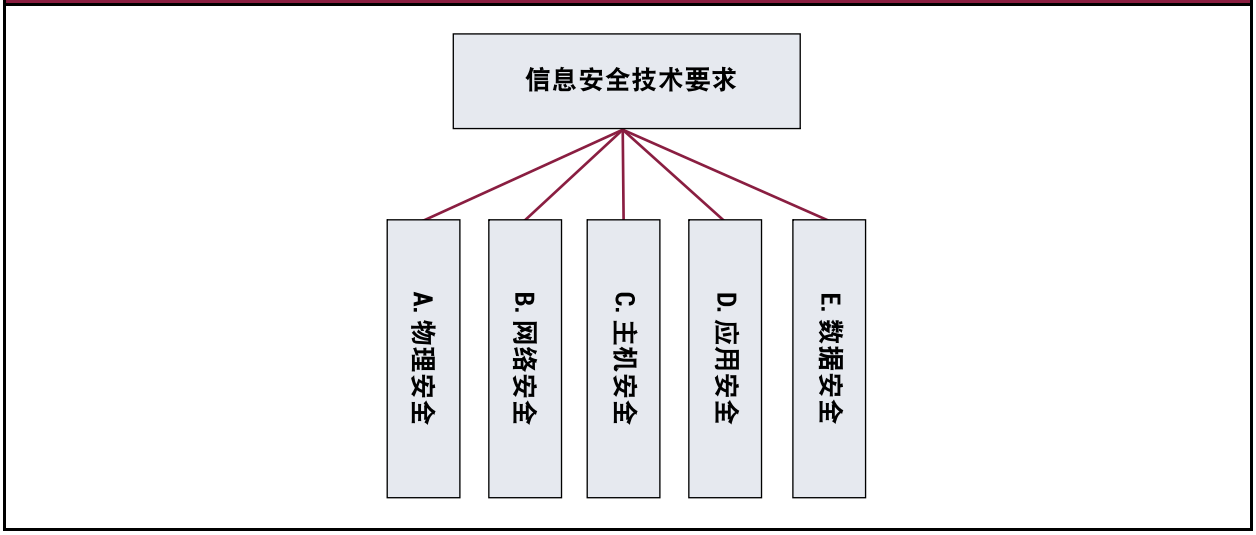
图10—网络安全控制要求和措施（续）				
保护要求	条款对应	责任方	建议的管理措施	建议的技术措施
2.5 网络运营者要其内部及外部用户使用网络行为进行监督，任何组织与个人不得设置恶意程序和散布非法信息	第46、47、48条	信息安全管理团队、信息技术部门及各业务部门	1. 根据公安部、工信部等主管部门的要求，建立管理与技术措施，防范打击网络诈骗、通讯信息诈骗、金融诈骗、信息窃取等非法活动。 2. 严格按照“谁接入谁负责，谁运营谁负责，谁收费谁负责”的总体原则，加强内容监管。 3. 在合同中添加相应条款（免责条款，授权使用说明），为内部及外部用户建立系统安全和内部和外部信息安全可接受策略。 4. 对内部及外部用户进行个人敏感信息保护的安全意识教育。	1. 使用相应技术手段，对用户信息进行管理（违法信息的监控、抑制与删除）。 2. 通过技术手段禁止恶意程序与违法信息的使用。 3. 进行完整性的检测（软件完整性与内容完整性）和敏感字段的识别与屏蔽。
2.6 网络运营者应当建立网络信息安全投诉、举报制度，配合主管部门的调查与处置	第49、50条	信息安全管理团队、信息技术部门及各业务部门	1 建立投诉举报相关制度与处理流程，明确要求； 2. 对网信部门和有关部门依法实施的监督检查，应当予以配合。	1. 设置专门的投诉举报热线电话或网络投诉渠道。 2. 根据主管部门的要求，对非法信息应当配合采取技术措施和其他必要措施阻断传播。

（三）网络安全技术与管理措施的具体要求

信息安全技术措施的具体要求描述

网络安全法所要求的安全技术可以从等级保护基本要求中的物理安全、网络安全、主机安全、应用安全、数据安全五个层次进行安全防护设计，以体现层层递进，纵深防御的设计思想。未来还可以考虑等级保护扩展要求中的云计算安全、工业控制安全、移动互联安全、物联网安全的相关要求。（以下以等级保护三级中的信息安全技术要求为例）

图11—安全保护等级设计



A. 物理安全

<table>
<tr><th colspan="4">图12—物理安全保护</th></tr>
<tr><td>1、概述</td><td colspan="3">• 保护组织的物理场所和信息免受未授权物理访问、损坏和干扰，防止资产的丢失、损坏、失窃或危及资产安全以及组织活动的中断。</td></tr>
<tr><td>2、防护目标</td><td colspan="3">• 确保组织的关键或敏感的信息处理设施要放置在安全区域内，并受到确定的安全边界的保护，包括适当的安全屏障和入口控制。
• 防止信息资产的丢失、损坏、失窃或危及资产安全以及组织活动的中断。应保护设备免受物理的和环境的威胁。</td></tr>
<tr><td rowspan="11">3、控制要点</td><td>编号</td><td>控制要点</td><td>控制项说明</td></tr>
<tr><td>A.1</td><td>物理位置的选择</td><td>机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内，机房场地应避免设在用水设备的下层或隔壁。</td></tr>
<tr><td>A.2</td><td>物理访问控制</td><td>要对进入机房的来访人员控制、鉴别和记录；对机房划分区域进行物理隔离，重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。</td></tr>
<tr><td>A.3</td><td>防盗窃和防破坏</td><td>应将主要设备放置在机房内，进行固定和标记；利用光、电等技术设置机房防盗报警系统。</td></tr>
<tr><td>A.4</td><td>防雷击</td><td>机房建筑应设置避雷装置和交流电源地线。</td></tr>
<tr><td>A.5</td><td>防火</td><td>机房应采用具有耐火等级的建筑材料，设置火灾自动消防系统，采取区域隔离防火措施，将重要设备与其他设备隔离开。</td></tr>
<tr><td>A.6</td><td>防水和防潮</td><td>应采取措施防止机房中水管渗透、窗户墙壁渗透、水蒸气结露、地下积水渗透；应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。</td></tr>
<tr><td>A.7</td><td>防静电</td><td>机房应采用防静电地板，主要设备应采用必要的接地防静电措施。</td></tr>
<tr><td>A.8</td><td>温湿度控制</td><td>机房应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内。</td></tr>
<tr><td>A.9</td><td>电力供应</td><td>应在机房供电线路上配置稳压器和过电压防护设备；应提供短期的备用电力供应；应设置冗余或并行的电力电缆线路为计算机系统供电；应建立备用供电系统。</td></tr>
<tr><td>A.10</td><td>电磁防护</td><td>应采用接地方式防止电磁干扰；电源线和通信线缆应隔离铺设，避免互相干扰；对关键设备和磁介质实施电磁屏蔽。</td></tr>
</table>

B. 网络安全

<table>
<tr><th colspan="4">图13—网络安全保护</th></tr>
<tr><td>1、概述</td><td colspan="3">• 通过网络处理能力、边界访问控制、网络攻击防护、设备安全防护等措施来保护网络系统安全，防止网络服务可用性不足和遭受未授权访问</td></tr>
<tr><td>2、防护目标</td><td colspan="3">• 通过网络结构设计来确保网络设备处理和流量带宽具备一定的冗余能力，划分安全域进行网络边界安全隔离，通过建立访问控制，防止网络资源的非授权使用。
• 防范恶意人员通过网络对应用系统进行攻击，同时阻止恶意人员对网络设备发动的攻击。
• 在安全事件发生前可以通过恶意代码防护、入侵检测事件等手段发现攻击意图，在安全事件发生后可以通过集中的事件审计来进行事件追踪、事件源定位。</td></tr>
<tr><td rowspan="8">3、防护要点</td><td>编号</td><td>控制要点</td><td>控制说明</td></tr>
<tr><td>B.1</td><td>结构安全</td><td>确保主要网络设备的处理能力和流量带宽具备冗余空间，满足业务高峰期需要；业务终端与业务服务器之间进行路由控制，以建立安全的访问路径；应根据工作性质和所涉及信息重要程度等因素，划分不同的子网或网段，并建立网络带宽优先级别；应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段。</td></tr>
<tr><td>B.2</td><td>访问控制</td><td>应在网络边界部署访问控制设备，启用访问控制功能；对进出网络的信息内容进行过滤；在会话处于非活跃一定时间或会话结束后要终止网络连接；要限制网络最大流量数及网络连接数；对重要网段应采取技术手段防止地址欺骗；可以设置允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户。</td></tr>
<tr><td>B.3</td><td>安全审计</td><td>应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录；应能够根据记录数据进行分析，并生成审计报表；应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。</td></tr>
<tr><td>B.4</td><td>非法接入检查</td><td>应能够对非授权设备联到内部网络，以及内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断；</td></tr>
<tr><td>B.5</td><td>入侵防范</td><td>应在网络边界处监视网络攻击行为，当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。</td></tr>
<tr><td>B.6</td><td>恶意代码防范</td><td>应在网络边界处对恶意代码进行检测和清除，同时要维护恶意代码库的升级和检测系统的更新。</td></tr>
<tr><td>B.7</td><td>网络设备防护</td><td>应对登录网络设备的用户进行身份鉴别，对网络设备的管理员登录地址进行限制，确保网络设备用户的标识应唯一；主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别；应实现设备特权用户的权限分离。</td></tr>
</table>

C. 主机安全

<table>
<tr><th colspan="4">图14—主机安全保护</th></tr>
<tr><td>1、概述</td><td colspan="3">• 采用安全保护技术确保业务数据在进入、离开或驻留服务器与桌面主机时保持可用性、完整性和保密性。</td></tr>
<tr><td>2、防护目标</td><td colspan="3">• 采用相应的身份鉴别、访问控制等手段阻止针对主机系统的非授权访问，对主机资源的可用性进行管理；
• 采用主机防火墙、恶意代码防护、入侵检测、剩余信息保护等手段来保护主机系统的安全；
• 在安全事件发生后通过对事件日志的分析进行审计追踪，确认事件对主机的影响以进行后续处理。</td></tr>
<tr><td rowspan="9">3、防护要点</td><td>序号</td><td>控制要求</td><td>控制说明</td></tr>
<tr><td>C.1</td><td>身份鉴别</td><td>应对登录主机系统的用户进行身份标识和鉴别；系统用户的身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换；应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；对服务器进行远程管理时，应防止鉴别信息在网络传输过程中被窃听；应为不同系统用户分配不同的用户名，确保用户名具有唯一性；应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。</td></tr>
<tr><td>C.2</td><td>访问控制</td><td>应根据角色的职责，按照最小授权原则来分配权限；实现管理用户、特权用户的权限分离；应重命名系统默认帐户，修改这些帐户的默认口令；及时删除多余的、过期的帐户，避免共享帐户的存在；应对重要信息资源设置敏感标记，依据安全策略严格控制用户对有敏感标记重要信息资源的操作。</td></tr>
<tr><td>C.3</td><td>安全审计</td><td>审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户；能够根据审计记录数据进行分析，并生成审计报表；应保护审计进程和审计记录，避免受到未预期的中断、删除和修改。</td></tr>
<tr><td>C.4</td><td>剩余信息保护</td><td>应保证系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除；应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。</td></tr>
<tr><td>C.5</td><td>入侵防范</td><td>应能够检测到对重要服务器进行入侵的行为并进行特征记录；应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施；操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序。</td></tr>
<tr><td>C.6</td><td>恶意代码防范</td><td>应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库；主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库；应支持防恶意代码的统一管理。</td></tr>
<tr><td>C.7</td><td>资源控制</td><td>应对重要服务器的CPU、硬盘、内存、网络等资源的使用情况；限制单个用户对系统资源的最大或最小使用限度；应能够对系统的服务水平降低到预先规定的最小值进行检测和报警；应可以按照规则限制终端登录方式和登录时间。</td></tr>
</table>

D. 应用安全

<table>
<tr><th colspan="4">图15—应用安全保护</th></tr>
<tr><td>1、概述</td><td colspan="3">• 采用安全保护技术确保应用系统本身的防护，以及对于应用间数据接口、远程终端数据访问的安全防护。</td></tr>
<tr><td>2、防护目标</td><td colspan="3">• 通过采取身份认证、访问控制等安全措施，保证应用系统自身的安全性，以及与其他系统进行数据交互时所传输数据的安全性。
• 建立软件的输入控制，确保输入数据符合系统设定要求。提供软件自动保护功能，当故障发生时自动保护当前所有状态。
• 采取审计措施在安全事件发生前发现入侵企图或在安全事件发生后进行审计追踪。</td></tr>
<tr><td rowspan="11">3、防护要点</td><td>序号</td><td>控制要求</td><td>控制说明</td></tr>
<tr><td>D.1</td><td>身份鉴别</td><td>应提供专用的登录控制模块对登录用户进行身份标识和鉴别；应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别；提供用户身份标识唯一和鉴别信息复杂度检查功能；应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；应启用应用软件中的安全功能，并根据安全策略配置相关参数。</td></tr>
<tr><td>D.2</td><td>访问控制</td><td>应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；应由授权主体配置访问控制策略，并严格限制默认帐户的访问权限；应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系；应具有对重要信息资源设置敏感标记的功能，应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。</td></tr>
<tr><td>D.3</td><td>安全审计</td><td>应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计；应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录；应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。</td></tr>
<tr><td>D.4</td><td>剩余信息保护</td><td>应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。</td></tr>
<tr><td>D.5</td><td>通信完整性</td><td>应采用密码技术保证通信过程中数据的完整性。</td></tr>
<tr><td>D.6</td><td>通信保密性</td><td>在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证；应对通信过程中的整个报文或会话过程进行加密。</td></tr>
<tr><td>D.7</td><td>抗抵赖</td><td>应具有在请求的情况下为数据原发者或接收者提供数据原发证据和数据接收证据的功能。</td></tr>
<tr><td>D.8</td><td>软件容错</td><td>应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求；应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。</td></tr>
<tr><td>D.9</td><td>资源控制</td><td>当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；应能够对系统的最大并发会话连接数和单个帐户的多重并发会话进行限制；应能够对一个时间段内可能的并发会话连接数进行限制；应能够对一个访问帐户或一个请求进程占用的资源分配最大限额和最小限额；应能够对系统服务水平降低到预先规定的最小值进行检测和报警。</td></tr>
</table>

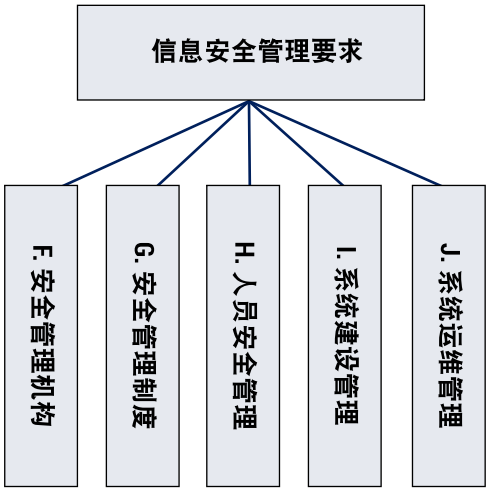
E. 数据安全

图16—数据安全保护			
1、概述	• 确保对数据完整性和机密性的保护，以及确保数据可以得到有效的备份与恢复。		
2、防护目标	• 通过采取身份认证、访问控制等安全措施，保证数据的传输数据性和存储机密性； • 确保重要数据得到有效备份，备份得到有效存放与维护，确保备份数据能够有效恢复。		
3、防护要点	序号	控制要求	控制说明
	E.1	数据完整性	应能够检测到系统管理数据、鉴别信息和重要业务数据在传输、存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。
	E.2	数据保密性	应采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据传输保密性；应采用加密或其他保护措施实现系统管理数据、鉴别信息和重要业务数据存储保密性。
	E.3	备份和恢复	应提供本地数据备份与恢复功能，完全数据备份至少每天一次，备份介质场外存放；应提供异地数据备份功能，利用通信网络将关键数据定时批量传送至备用场地；应采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障；应提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性。

信息安全管理措施的具体要求描述

网络安全法所要求的安全管理可以从安全管理机构、安全管理制度、人员安全管理、系统建设管理及系统运维管理五个方面来设计。（以下以等级保护三级中的信息安全管理要求为例）

图17—安全管理等级设计



F. 安全管理机构

图18—安全管理机构	
管理内容	内容描述
概述	建立配套的安全管理职能部门，通过管理机构的岗位设置、人员的分工以及各种资源的配备，为信息系统的安全管理提供组织上的保障。
控制要求	F.1 岗位设置、F.2 人员配置、F.3 授权与审批、F.4 沟通与合作、F.5 审核与检查。
参与角色	信息系统主管部门，信息系统运营、使用单位，信息安全服务机构。
活动输入	安全组织结构表，安全成员及角色说明书，安全详细设计方案。

G. 安全管理制度

图19—安全管理系统	
管理内容	内容描述
概述	指建设或修订与信息系统安全管理相配套的、包括所有信息系统的建设、开发、运维、升级和改造等各个阶段和环节所应当遵循的行为规范和操作规程。
控制要求	G.1 安全管理制度、G.2 制度的制定与发布、G.3 制度的评审与修改。
参与角色	信息系统运营、使用单位，信息安全服务机构。
活动输入	机构现有相关管理制度和政策，安全详细设计方案。

H. 人员安全管理

图20—人员安全管理	
管理内容	内容描述
概述	对人员的职责、素质、技能、意识等方面进行培训，保证人员具有与其岗位职责相适应的技术能力、管理能力和基本的安全意识，以减少人为因素给系统带来的安全风险。
控制要求	H.1 人员录用、H.2 人员离岗、H.3 人员考核、H.4 安全意识与培训、H.5 外部访问人员。
参与角色	信息系统主管部门，信息系统运营、使用单位，信息安全服务机构。
活动输入	各项管理制度和操作规范，系统/产品使用说明书，基本的安全意识。

I. 系统建设管理

图21—系统构建管理	
管理内容	内容描述
概述	在系统定级、规划设计、实施过程中，对工程的质量、进度、文档和变更等方面的工作进行监督控制和科学管理。
控制要求	I.1 系统定级、I.2 安全方案设计、I.3 产品采购与使用、I.4 自行软件开发、I.5 外包软件开发、I.6 工程实施、I.7 测试验收、I.8 系统交付、I.9 系统备案、I.10 等级测评、I.11 服务商选择。
参与角色	信息系统运营、使用单位，信息安全服务机构，信息安全产品供应商。
活动输入	安全设计与实施阶段参与各方相关进度控制和质量监督要求文档。

J. 系统运维管理

图22—系统运行和维护管理	
管理内容	内容描述
概述	通过制定运行管理操作规程，确定运行管理人员的操作目的、操作内容、操作时间和地点、操作方法和流程等，并进行操作过程记录，确保对操作过程进行控制。
控制要求	J.1 环境管理、J.2 资产管理、J.3 介质管理、J.4 设备管理、J.5 监控和安全管理、J.6 网络安全管理、J.7 系统安全管理、J.8 恶意代码防范管理、J.9 密码管理、J.10 变更管理、J.11 备份与恢复管理、J.12 安全事件管理、J.13 应急预案管理。
参与角色	信息系统运营、使用单位。
活动输入	运行管理需求，运行管理人员角色和职责表。

六、关键信息基础设施所需要的安全控制

针对关键信息基础设施的网络运营者，在落实一般性的网络运营基本要求的基础上，还需要增加关键信息基础设施相关的控制要求，利用体系化、精细化的方法来实施网络安全法。具体措施有：识别适用的法律法规和行业最佳实践；对网络安全进行架构设计；建设综合的网络安全管控框架。

（一）关键信息基础设计安全控制要求

图23—关键信息基础设施设计要求和措施

保护要求	条款对应	责任方	建议的管理措施	建议的技术措施
3.1 关键信息基础设施的定义与行业规划	第31、32条	国家主管部门、行业主管部门	1. 国家统一制定针对关键信息基础设施的具体范围和安全保护办法。 2. 国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。	1. 国家和行业分别建立针对关键信息基础设施的网络安全监控平台。 2. 组织与国家和行业网络安全监控平台对接后获取相关信息。 3. 参见2017年7月网信办发布的*《关键信息基础设施安全保护条例（征求意见稿）》*。
3.2 关键信息基础设施的网络安全与信息化应做到“三同步”	第33条	信息安全管理委员会、信息安全主管领导、信息安全管理团队、信息技术部门	1. 在组织的信息化管理制度中明确信息化要与信息安全“同步规划、同步建设、同步使用”。 2. 在信息安全管理制度中明确信息安全要与信息化“同步规划、同步建设、同步使用”。	组织的信息化规划与架构管理部门与信息安全管理团队一起研究“三同步”的架构框架、概念模型和技术方法。
3.3 设立信息安全专门机构和负责人	第39条（1）	信息安全管理委员会、信息安全主管领导、信息安全管理团队	1. 建立、健全专职的网络信息安全管理组织，设立信息安全负责人，指导协调组织的整体信息安全工作。 2. 对信息安全负责人及关键岗位人员进行背景调查。	
3.4 定期培训考核	第39条（2）	信息安全主管领导、信息安全管理团队、各部门信息安全负责人	1. 编制年度信息安全培训计划定期举行全员网络信息安全意识教育。 2. 针对关键岗位人员举行信息安全专业知识与技能培训。 3. 通过丰富多彩形式，营造企业信息安全文化。	1. 开展信息安全专业认证培训（例如CISP、CISSP、CISA、CISM等）。 2. 开展信息安全知识与技能培训(安全风险评估、安全架构设计、网络监控检测、网络攻防、Web开发安全、数据防泄露等)。 3. 通过课堂培训、视频动画、海报宣传、情景电影、移动APP、电子课件、有奖竞赛等形式开展信息安全意识宣传与教育。

图23—关键信息基础设施设计要求和措施（续）				
保护要求	条款对应	责任方	建议的管理措施	建议的技术措施
3.5 系统与数据容灾备份	第39条（3）	信息安全主管领导、信息安全管理团队、信息技术部门	1. 根据系统可用性及数据管理的策略规划组织的灾难备份策略，制定系统与数据容灾备份管理制度 2. 根据灾难恢复策略的需求明确定义灾难恢复资源,包括数据备份系统、备用数据处理系统、备用网络系统、备用基础设施、专业技术支持能力、运行维护管理能力。 3. 根据组织自身的特点，进行容灾备份系统建设。对于业务连续性有较高要求的组织，甚至需要建立专门的本地和异地灾备中心，同时并把业务部门的相关业务恢复纳入其中，形成全组织范围内业务连续性计划。	1. 从其对系统的保护程度来分，可以将容灾系统分为:数据容灾和应用容灾两种类型。数据容灾是指指建立一个异地的数据系统，该系统是本地关键应用数据的一个实时复制或延迟复制；应用容灾是指在数据容灾的基础上，在异地建立一套完整的与本地生产系统相当的备份应用系统（可以是互为备份），在灾难情况下，远程系统迅速接管业务运行。数据容灾是抗御灾难的保障，而应用容灾则是容灾系统建设的目标。 2. 备份分为同城备份、异地备份和云备份。同城备份，是指将生产中心的数据备份在本地数十公里以外的同城容灾备份机房中，它的特点是速度相对较快；异地备份，通过互联网TCP/IP协议，将生产中心的数据备份到异地。对容灾要求相高的企业，一般把同城与异地相结合形成“两地三中心”模式；云备份就是通过云存储的方式把数据和系统备份到公有云或私有云上。云备份已经成为云计算最重要的落地表现形式之一，在企业市场中获得了快速的发展。

图23—关键信息基础设施设计要求和措施（续）				
保护要求	条款对应	责任方	建议的管理措施	建议的技术措施
3.6 应急预案并定期演练	第39条（4）	信息安全管理团队、信息技术部门、业务部门	1. 编写应急灾备与业务连续性管理制度，明确相关职责，对应急管理、应急准备、应急处置、应急保障以及有关奖惩措施等做出明确规定。 2. 建立应急管理组织机构，该机构至少包括应急领导小组、应急执行小组和应急保障小组。 3. 组织应制订总体应急预案和分类应急预案，分类应急预案至少包括基础设施、网络通讯、信息系统和业务流程等。 4. 组织应将支撑重要信息系统运行的外包服务应急管理纳入预案范围，建立重要外包服务的专项应急预案。 5. 组织要对应急预案进行及时的更新，要专门组织对技术人员、业务人员及相关人员进行应急预案有关培训。 6. 组织应制定应急演练计划，明确应急演练时间、内容、依据、目的、负责人和相关部门。开展演练时要对照应急预案进行。通过演练验证应急预案各个环节是否有效，应急资源是否完备，应急人员是否胜任。全面演练至少每年进行一次，专项演练的频度根据需要进行设定。	1. 应急预案的内容一般包括以下内容： • 明确有关各方的分工和责任； • 说明重要信息系统的业务影响范围、恢复时间目标、恢复点目标、以及信息系统包括的系统资源，明确资源的物理位置、设备型号、软件资源、网络配置等关键信息； • 明确各类事件的应急处置方法和流程；应急场景应至少覆盖电力故障、通信线路故障、火情水灾、治安、病毒爆发、网络攻击、人为破坏、不可抗力、计算机硬件故障、网络故障、操作系统故障、漏洞、应用系统故障以及其他各类与信息系统相关的故障； • 制定系统恢复流程和应急处置操作手册，应尽可能将操作代码化、自动化，降低应急处置过程中产生的操作风险； • 明确应急恢复过程中的关键状态，并明确不同状态的沟通和报告内容及等级； • 明确应急人员的协调内容和沟通方式； • 明确系统重建步骤，确保信息系统恢复正常业务处理能力。 2. 参见2017年1月网信办发布的《国家网络安全事件应急预案》。

图23—关键信息基础设施设计要求和措施（续）				
保护要求	条款对应	责任方	建议的管理措施	建议的技术措施
3.7 采购安全产品与服务要接受主管部门的安全审查	第35条	信息安全管理团队、信息技术部门、业务部门、采购部门	1. 针对网络关键设备和网络安全专用产品的采购，组织应建立相应的管理制度与规范，要求组织中的网络关键设备和网络安全专用产品需经安全认证或检测，并且要求网络产品和服务的供应和采购双方都要遵守国家和行业主管部门的要求，随时接受安全审查。 2. 组织应建立网络安全产品与服务供应商的准入、退出和安全考评机制，在合同中加以明确要求，并在安全产品与服务实施过程中进行评估与考核。	对网络关键设备和网络安全专用产品与服务的安全审查是网信部门实施安全监督的重要抓手，组织要重点关注主管部门出台的相关管理规范，包括但不限于以下内容： • 2017年5月国家网信办发布*《网络产品和服务安全审查办法（试行）》* • 2017年6月国家网信办、工信部、公安部和国家认可委共同发布*《网络关键设备和网络安全专用产品目录（第一批）》*
3.8 要与安全产品与服务方签订保密协议。	第36条	信息安全管理团队、采购部门、各业务部门	在合同中添加相应条款，要求网络关键设备和网络安全专用产品与服务的供应商承担安全和保密义务与责任。	组织可以与供应商签订组织与组织之间的保密协议，同时也可以与供应商派出的实施人员签订组织与个人之间的保密协议。
3.9 重要数据和个人信息跨境传输	第37条	信息安全主管领导、信息安全管理团队、信息技术部门和相关业务部门	1. 对组织业务范围内的个人敏感信息进行识别并进行分类分级。 2. 开展对敏感信息的跨境传输的场景及数据类型进行识别与风险评估。 3. 根据评估结果，设计并实施数据本地存储或跨境传输安全控制措施改造。	1. 组织应密切关注国家及行业及行业主管部门对个人信息跨境传输的相关的后续规定。例如： 2. 参见2017年4月网信办发布了*《个人信息和重要数据出境安全评估办法（征求意见稿）》*。 3. 参见2017年5月全国信息安全标准化技术委员会发布的*《信息安全技术数据出境安全评估指南（草案）（征求意见稿）》*。

图23—关键信息基础设施设计要求和措施（续）				
保护要求	条款对应	责任方	建议的管理措施	建议的技术措施
3.10 至少每年进行一次安全评估，并向主管部门上报评估结果；主管部门对关键信息基础设施进行抽查检测与评估	第38、39条	国家和行来信息安全主管部门，信息安全管理团队、信息技术部门和业务部门	1. 组织应建立对关键信息基础设施持续进行安全评估的制度与流程。 2. 通过安全风险评估与上级的监督性检查，促进信息安全保障体系的不断完善。 3. 把开展安全评估，及对评估结果的整改作为考核单位和员工安全绩效的重要内容。	信息安全风险评估方法一般有以下几种类型： 1. 基于信息安全法规的合规性评估，根据法规条款的要求进行差距分析，以发现安全管理体系方面的风险。 2. 基于信息资产的风险评估，利用ISO27005及GB20984规定的方法来进行风险评估，以发现信息资产的总体性风险。 3. 针对IT资产进行人工检查、工具扫描、渗透测试的技术性评估，以发现信息资产的技术性风险。 4. 根据业务场景建模，分析业务操作流程中的数据流转有关系，分析关键环节中安全控制的存在性和有效性，以发现业务场景中的安全风险。 5. 利用外部威胁情报大数据，对组织面临的域名劫持、邮箱被封、漏洞披露、帐号信息泄露、恶意代码、僵尸网络、公有云风险等进行评估，通过外部视野发现组织面临的互联网安全风险。

（二）网络安全法相关法律法规的识别

本次网络安全法的实施虽然是中国第一部全面规范网络空间安全管理方面问题的基础性法律，但从1994年国务院发布计算机信息系统安全保护条例以来，已经出台了多个行业及部门的法规，刑法及民法的修正案也在逐步体现对信息安全的要求。特别是2004年国家信息化领导小组发布27号文要求在全国范围内实施等级保护以来，信息安全工作开始得到了广泛的重视，一些领先的行业也纷纷发布有自身特点的信息安全规范及标准，有力地推动了信息安全在中国的前进步伐。

西方发达国家无论是从国家战略、安全标准、最佳实践层面来看，还是从安全研究、技术产品、产业发展层面来看，在网络安全方面积累的许多知识与经验可以为中国的网络安全实践提供借鉴。

参照NIST发布的CSF的做法，当前中国各机构实施网络安全法所需的方法并不需要完全重新设计与制定，我们需要对国内外适用的法律法规、标准规范及最佳进行识别，并与建立的网络安全框架建立映射，以指导各行各业的人们在落实网络安全法有所参考，同时也是避免重复性的工作，更好地整合现有的各类规范与标准。

国内相关法律法规的识别

序号	法案名称	颁布机构	发布时间	类型
1	中华人民共和国网络安全法	全国人民代表大会常务委员会	2016年11月7日	法律
2	“十三五”国家信息化规划	国务院	2016年12月15日	行业意见
3	网络产品和服务安全审查办法（试行）	国家互联网信息办公室	2017年5月2日	管理规定
4	工业控制系统信息安全防护指南	工信部	2016年10月17日	管理规定
5	中央企业商业秘密信息系统安全技术指引	国资委	2012年5月	技术指引
6	等级保护基本要求	全国信息安全标准化技术委员会	2008年6月19日	制度规范
6.1	等级保护-物联网安全扩展要求		意见征求阶段	
6.2	等级保护-移动互联安全扩展要求			
6.3	等级保护-云计算安全扩展要求			
6.4	等级保护-工业控制安全扩展要求			
7	个人信息安全规范			

详细介绍请参见附件一（一）。

国际相关法律法规的识别

序号	法案名称（CN）	法案名称（EN）	颁布机构	发布时间	技术领域
1	欧洲议会和理事会（EU）2016年第1148号指令2017-01-04	(EU) 2016/1148---Directive on Security of Network and Information Systems (the NIS Directive)	欧洲议会和理事会	2016年7月6日	网络安全基础框架
2	关于个人数据处理和数据自由流动保护条例（一般数据保护条例）的提案	General Data Protection Regulation，GDPR	欧洲议会和欧盟委员会	2012年	隐私保护
3	2014年联邦信息安全管理法案	US Congress Federal Information Security Management Act 3554,or, Federal Information Security Modernization Act of 2014 (FISMA)	美国国会	2014年12月	网络安全
4	网络空间安全信息共享法（2015）	US Congress Cybersecurity Information Sharing Act of 2015 (CISA)		2015年12月18日	网络安全基础框架
5	萨班斯法案	Sarbanes–Oxley Act (SOX)	美国政府	2002年	安全管理、数据安全

序号	法案名称（CN）	法案名称（EN）	颁布机构	发布时间	技术领域
6	国家基础设施保护计划	National Infrastructure Protection Plan (NIPP)	美国国土安全部	2006年	关键基础设施安全
7	网络空间国际战略	US Government National Strategy to Secure Cyberspace – Critical priorities	美国政府	2011年	关键基础设施安全、网络安全
8	网络安全基本法&信息处理促进法	Japan Congress Cyber Security Basic Act & Information Processing Promotion Act	日本国会	2014年11月6日	网络安全基础框架
9	保卫国家信息安全战略	Japan Congress Information Security Strategy for Protecting the Nation	日本国会	2010年	关键基础设施安全、数据安全
10	个人数据保护法	Singapore Congress Personal Data Protection Act (PDPA)	新加坡国会	2012年	隐私保护
11	信息安全法	Security of Canada Information Sharing Act	加拿大政府	2001年12月18日	数据安全
12	香港隐私保护条例	Personal Data (Privacy) Ordinance	香港特区	2013年4月25日	隐私保护

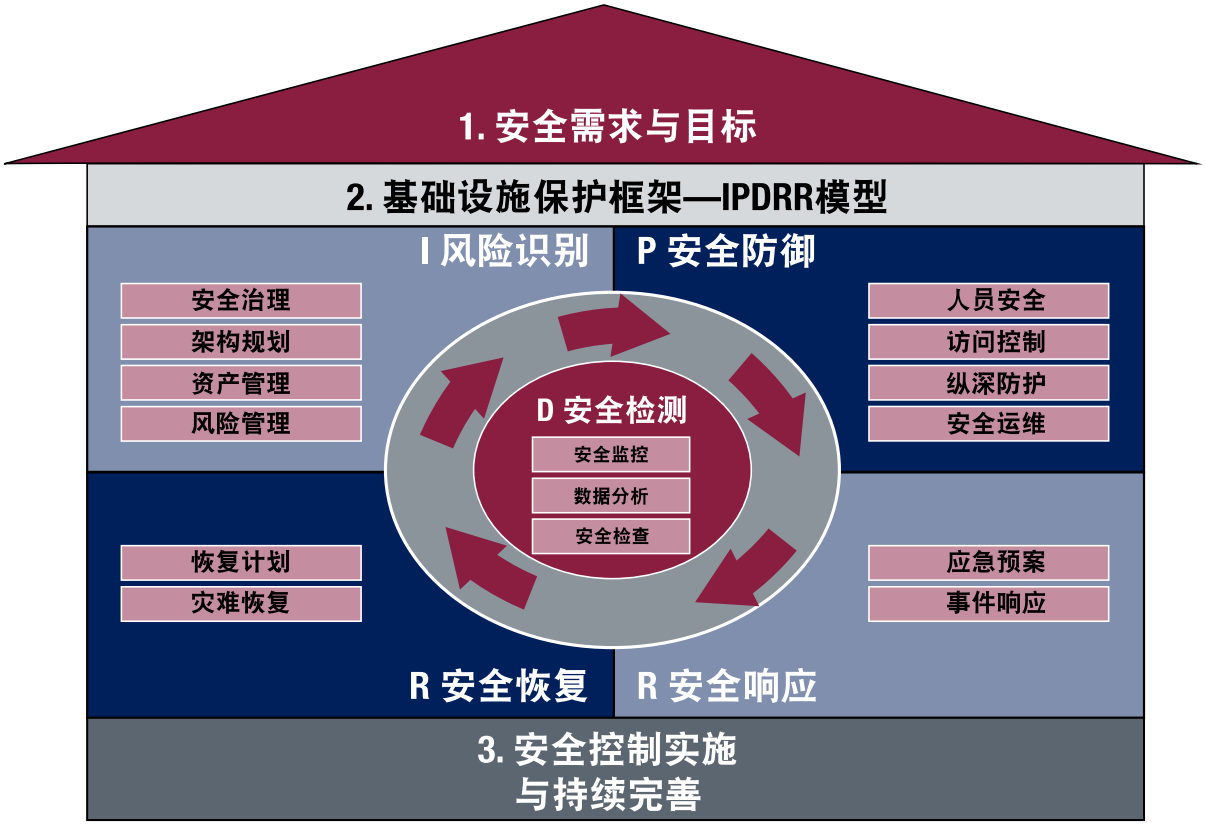
详细介绍请参见附件一（二）。

（三）网络安全架构设计

网络安全法是从国家法律的层面对网络安全所提出的最基本的要求，各类机构及人员的遵照执行的过程中，参照条款的要求逐条解读并落实执行是必要的。但网络安全法所要求的安全结果是需要通过体系和过程来保证的，否则安全控制措施很难确保一致性、持续性。因此应当设计有效的网络安全体系框架来为法规的执行奠定基础，提供保障。

网络安全体系架构包括安全需求与目标、安全保护基本架构、安全控制实施三个过程。企业的网络安全体系首先要从安全需求出发，设定可实现的目标；根据信息安全最佳实践，规划信息保护框架，在框架基础上，映射网络相应的信息安全标准与规范；根据标准与规范的要求，把网络安全相关落实具体控制要求，以项目或任务方式推进实施，通过持续的监测与测量，保证安全体系的持续完善。

图24—网络安全系统框架的组成部分



安全需求

- **业务发展规划**—网络安全体系设计需要与企业业务的发展保持一致，要充分了解企业未来几年的业务规划，并根据业务特点，分析未来业务的安全需求。
- **信息技术规划**—网络安全体系是企业的信息技术体系的一部分，需要根据企业总体的信息技术规划来设计安全体系。
- **网络安全风险**—网络安全风险评估是安全体系设计和建设的基础，企业需要充分了解自身业务和信息系统的安全风险。
- **合规管理要求**—企业面临国家、行业、监管机构的各类安全监管要求，安全体系设计需要考虑企业需要满足的各类合规要求。

安全目标

- **总体目标**—信息资产的机密性C、完整性I及可用性A。
- **过程目标**—风险可视化、防御主动化、运行自动化。
  - **风险可见化**—Visibility 未知攻，焉知防，看见风险才能防范风险；
  - **防御主动化**—Proactive 最好的防守是进攻，主动防御，纵深防御是设计的目标；
  - **运行自动化**—Automotive自动化的安全运营才能保障安全体系的落实；

由于每个组织的业务需求和特点不同，发展成熟度也不同，企业可以根据发展情况制定不同时期的安全目标，逐步实现比较高的安全目标。

（四）网络基础设施保护框架

框架的内容

建立网络基础设施保护框架可参考了NIST Cybersecurity Framework(CSF)的核心内容，简称为IPDRR模型。此框架模型包括风险识别（Identify）、安全防御（Protect）、安全检测（Detect）、安全响应（Response）和安全恢复（Recovery）五大能力。

图25—IPDRR模型

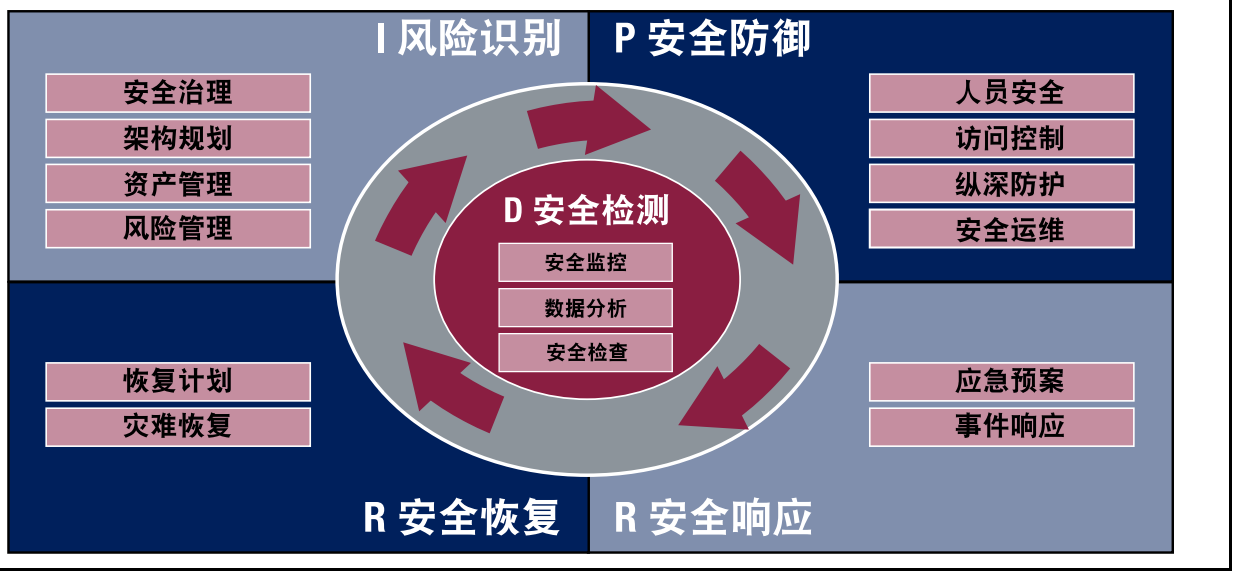


图26—IPDRR模型的详细组成部分

功能标识	功能	类别标识	类别
ID	识别	ID.AM	资产管理
		ID.BE	业务环境
		ID.GV	治理
		ID.RA	风险管理
		ID.RM	风险管理战略
		PR.AC	访问控制
		PR.AT	意识与培训
PR	防护	PR.DS	数据安全
		PR.IP	信息防护流程与程序
		PR.MA	维护
		PR.PT	防护技术
		DE.AE	异常与事件
DE	检测	DE.CM	持续性安全监控
		DE.DP	检测流程
		RS.RP	响应计划
		RS.CO	通信

图26—IPDRR模型的详细组成部分（续）			
功能标识	功能	类别标识	类别
RS	响应	RS.AN	分析
		RS.MI	缓解
		RS.IM	提升
		RC.RP	恢复计划
RC	恢复	RC.IM	提升
		RC.CO	通信

- **ID风险识别**—通过对组织信息化环境全面分析，识别可能产生网络安全风险的系统、资产、数据。此过程包括：资产管理、业务环境、治理机制、风险评估以及风险管理策略。
- **PR安全防御**—制定并实施相应的网络安全保障措施，以确保提供重要的基础设施服务。此过程包括：访问控制、意识和培训、数据安全、信息保护流程和程序、安全运维和保护技术。
- **DE安全检测**—制定并实施适当的活动，以识别网络安全事件的发生。此过程包括：异常和事件、安全持续监测以及检测过程。
- **RS安全响应**—制定并实施适当的活动，以采取有关检测到的网络安全事件的行动。此过程包括：响应计划、事件沟通、风险分析、风险控制和持续改进。
- **RC安全恢复**—制定并实施适当的活动，对网络安全事件受损的任何功能或服务进行还原操作，以保持业务的连续性。此过程包括：恢复规划、恢复与改进和沟通。

IPDRR能力框架实现了“事前、事中、事后”的全过程覆盖，从原来以防护能力为核心的模型，转向以检测能力为核心的模型，支撑识别、预防、发现、响应等，变被动为主动，直至自适应（Adaptive）的安全能力。

CSF框架与法律法则及最佳实践的映射

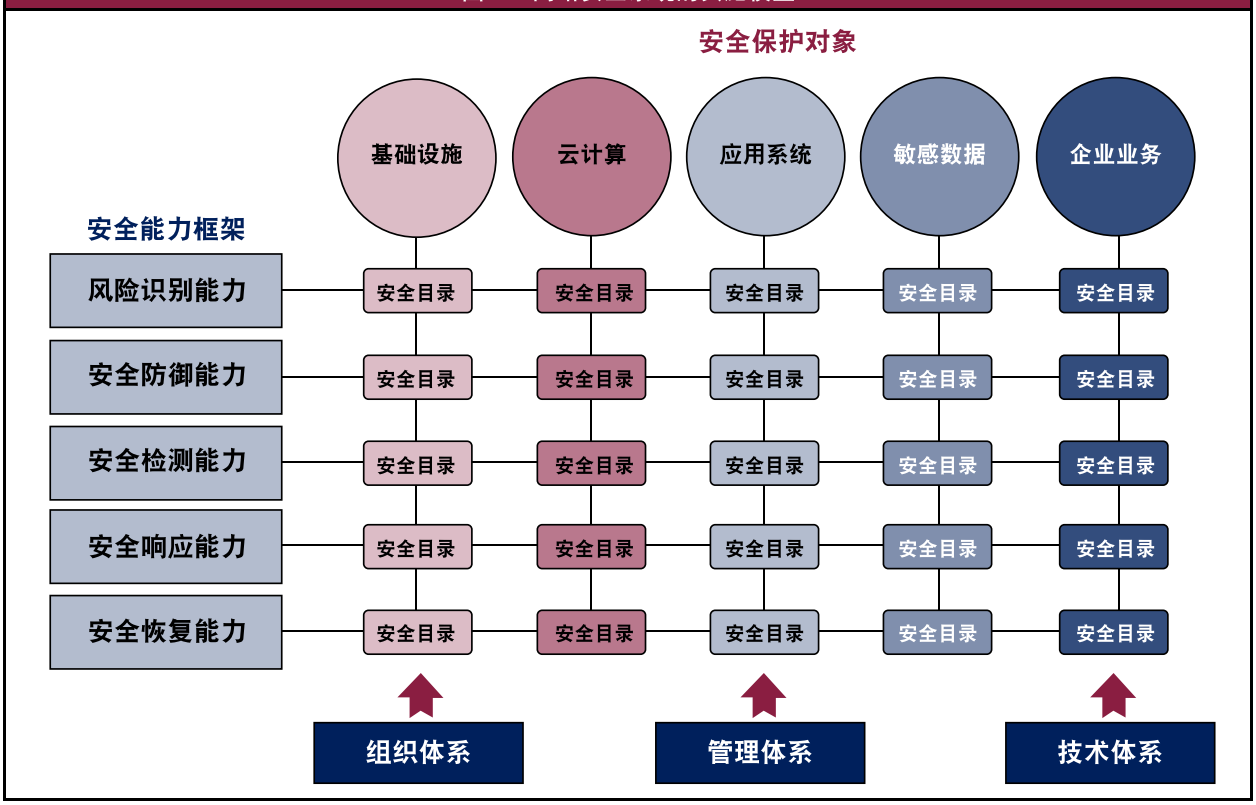
功能	分类	子类	网络安全规范
识别	**资产管理（ID.AM）：识别能使组织达到商业目的的数据、人员、设备、系统和设施，并使其业务目标与企业风险战略保持一致。**	ID.AM-1：组织内的物理设备和系统的盘点	• 等级保护5.2.5.2，5.2.5.3，5.2.5.4，6.2.5.2，6.2.5.3，6.2.5.4，7.2.5.2，7.2.5.3，7.2.5.4，
			• 工业控制系统信息安全防护指南第八条（一）
		ID.AM-2：组织内的软件平台和应用的盘点	• 等级保护5.2.5.2，6.2.5.2，7.2.5.2
		ID.AM-3：组织通信和数据流的映射	• 等级保护5.1.4.3，5.1.5，6.1.4.4，6.1.5，7.1.4.4，7.1.5
		ID.AM-4：外部信息系统的编目	• 等级保护5.2.4，6.2.4，7.2.4
		ID.AM-5：资源（例如，硬件、设备、数据和软件）基于其分类、临界性和商业价值优先次序的划分	• 等级保护4.1，4.2
		ID.AM-6：为全体员工和第三方利益相关者（如供应商、客户、合作伙伴）网络安全的角色和责任的建立	• 网络安全法第二十九条、网络安全法第三十六条
			• 等级保护5.1.2，6.1.2，7.1.2
			• 中央企业商业秘密信息系统安全技术指引11.4.4
			• 工业控制系统信息安全防护指南第十条（二）、第十一条
			• 个人信息安全规范1a、2.1b
			• 网络产品和服务安全审查办法第三条
		ID. BE-1：该组织的在供应链中的作用是识别和沟通	• 工业控制系统信息安全防护指南第十条（一）

详细请参见附件二：《NIST控制框架与国内外法律法规及最佳实践的对应关系》

（五）企业网络安全体系的实施模型

企业安全体系的实施模型如下：

图27—网络安全系统的实施模型



建立企业安全保护对象框架

每个企业的业务和架构是不同的，企业需要识别自身的安全保护对象框架，包括不限于：基础设施（机房、网络、主机、数据库、终端等）、云平台、移动平台、大数据平台、应用系统、敏感数据、企业业务（金融、电商、智能制造、可穿戴设备……）等。

建立企业安全能力框架

每个企业的成熟度是不同的，企业需要根据自身业务发展的成熟度，在不同阶段重点选择建设不同的安全能力，可以从IPDRR模型中的子能力中选取。

建立安全能力目录矩阵

横向的安全能力结合纵向的安全保护对象，将组合成每个节点的安全能力目录。安全目录包括不限于：安全产品、安全技术、安全工具、安全服务、安全方法论等。安全目录的选择将根据企业自身的安全预算、技术架构、安全技术趋势等来确定；安全目录对应的工作内容必须通过组织、流程和技术来支撑才能实现。

建立安全支撑体系

最终所有安全能力的落实都依赖于三大体系的建设，包括组织体系、管理体系和技术体系。每个安全能力目录都应对应上相关的组织职责、管理流程和技术支撑。

- **安全组织体系**—明确企业安全组织体系及其运作模式，建立企业安全的决策、管理、执行、监督组织架构，同时明确关键角色/职责，是网络安全能力建设的基础与保障。
- **安全管理体系**—在组织体系的基础上，建立完善的管理体系，明确组织网络安全工作的策略、方法和体系，是网络安全工作开展的规范。
- **安全技术体系**—明确了企业网络安全建设过程中所需的技术手段，是网络安全工作开展的有力支撑。
- **网络安全专题规划**—依据上述的安全体系架构模型和技术成熟度模型，企业在落实某个领域具体工作时，可以按照专题规划的方式来落实安全体系。专题内容可以按照体系架构中纵向的每类防护对象来开展。

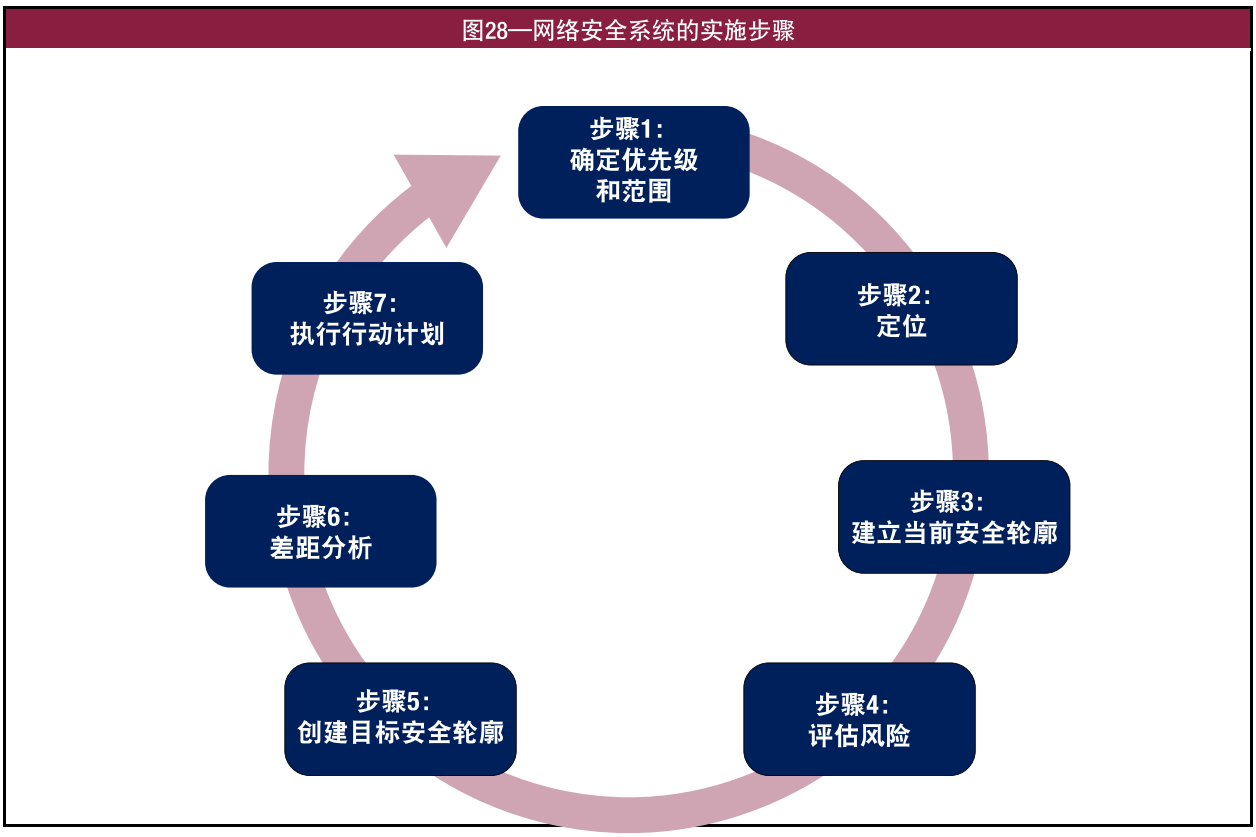
七、参考CSF框架的网络安全体系实施过程

由于NIST及ISACA在围绕推进CSF实施过程中积累了丰富的经验，我们在这里引入NIST的CSF实施过程及ISACA基于COBIT5的CSF实施过程作为实施网络安全体系的参考。

（一）网络安全体系推进实施的步骤

以下步骤说明了组织在实施网络安全法时，如何参考利用CSF框架来创建新的网络安全计划或改进现有计划。为建立健全网络安全体系，确保网络安全水平的持续提升，组织可根据自身的特点和安全需要，重复执行以下步骤：

图28—网络安全系统的实施步骤



上图中的7个实施步骤说明如下：

- **步骤1**—确定优先级和范围。组织确定其业务或任务目标的优先级，制定与网络安全实施相关的战略决策，并确定哪些系统和资产需支持所选业务线或流程。
- **步骤2**—定位。组织在明确了需纳入网络安全计划的业务线和流程之后，需确定相关系统和资产、监管要求和整体风险管理方案。此外，组织还需识别这些系统和资产面临的威胁及存在的漏洞。
- **步骤3**—建立当前安全轮廓。组织可根据安全现状调研，建立当前安全轮廓，并与框架核心中的类别和子类别建立对应关系。
- **步骤4**—评估风险。组织可依据整体风险管理流程或之前的风险管理活动进行风险评估。评估时，组织需分析运营环境，判断是否有网络安全事件发生，并评估事件对组织的影响。
- **步骤5**—创建目标安全轮廓。组织为未来期望的安全结果建立一个目标轮廓，通过框架类别和子类别来展现其期望的网络安全结果。并且，组织还可以开发自己的类别和子类别，以呈现其独特的安全风险。
- **步骤6**—确定当前的风险管理结果与期望目标之间的差距，分析这些差距，并对其进行优先级排序；然后制定一份优先执行的行动计划消除这些差距。该计划依据任务驱动、成本收益分析和对风险的理解，规划如何实现目标安全轮廓中的目标。最后，组织需确定消除这些差距所需的资源。
- **步骤7**—执行行动计划。组织决定应执行哪些行动以消除差距（如果步骤6说明了差距）。之后，组织基于目标安全轮廓的要求来监控当前的网络安全实践。为提供进一步指导，该框架识别出有关类别和子类别的参考资料实例，而组织应确定哪些标准、指导方针、实践以及部门标准能够最为有效地满足自身的需求。

组织可能会视需要重复执行以上步骤，持续评估和提升其网络安全。例如，组织可能会发现多次执行步骤2提升了风险评估质量。此外，组织可通过持续的差距分析来迭代更新监控风险评估进度。使用这一流程，组织的网络安全计划将更加贴近框架实施层级。

详细的CSF实施过程可参考：
https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

附件二详细解释了NIST的CSF框架中各种控制类与国内外相关法规标准的对应关系，组织在建立网络安全体系中可根据自身的特点进行剪裁利用。

（二）利用COBIT为网络安全体系的建立提升IT治理环境

COBIT(Control Objectives for Information and related Technology) 是ISACA制定的、在国际上得到公认的、权威的信息技术控制标准，目前已经更新至5.0版。它在商业风险、控制需要和技术问题之间架起了一座桥梁以满足管理的多方面需要。该标准体系已在世界一百多个国家的重要组织与企业中得到了广泛运用，指导了这些组织有效利用信息资源并有效地管理信息系统风险。

ISACA参与了NIST牵头的CSF研究与制定过程，并提出了基于COBIT5的网络安全实施框架，为美国的政府部门及重要机构实施13636法案提供了宝贵的经验。利用于COBIT可以为CSF的实施提供可靠的IT治理环境与IT管理流程。

组织需要根据安全架构的基本要求，结合网络安全架构设计与COBIT实施指南，分步骤列出每一个环节的最佳实践。

图29—CSF实施步骤与COBIT的映射			
CSF步骤	主要内容	与安全架构的关系	COBIT 针对CSF的实施指南
1. 确定优先级和范围	用户要识别其所在行业，选择适用的安全相关规范，分析自身的业务特点，列出要保护的关键基础设施与其上的重要信息类型。	网络安全的驱动力—来自合规管理要求、网络安全风险、业务发展规划、信息技术规划等方面的安全需求。	**COBIT Phase 1 —What Are the Drivers?** **选择COBIT5最佳实践和流程支持。**
2. 定位 3. 建立当前安全轮廓	列出基础设施的保护等级（可参考等保定级清单）和重要信息类型敏感程度（可参考“附件一：信息安全相关法律法规”所列出的相关指引。 列出组织安全需求与保护框架IPDRR中控制大类和子类的对应关系。	明确组织的安全目标总体，并对安全结果目标与过程目标进行描述；在IPDRR框架选择必要的安全控制大类和子类作为其安全能力；分析组织当前安全能力存在的薄弱环节和面临的威胁，分析总结组织的信息安全现状。	**COBIT Phase 2 —Where Are We Now?** **选择COBIT5最佳实践和流程支持。**
4. 评估风险 5. 创建目标安全轮廓	参考在IPDRR框架映射中“网络安全法”所对应的基础控制要求；参考“附件一：信息安全相关法律法规”所提出的法律条款最佳实践建议。	分析组织的未来的网络安全目标需求，在保护框架IPDRR中控制大类和子类中列出未来的安全要求。	**COBIT Phase 3 —Where Do We Want To Be?** **选择COBIT5最佳实践和流程支持。**
6. 确定当前的风险管理结果与期望目标之间的差距	针对COBIT Phase 3所列出的IPDRR框架中进行多维度的差距分析，找着未来的努力方向。	根据IPDRR框架中大类与子类的差距分析，得出组织的安全能力存在的差距，形成风险评估报告和整改建议。	**COBIT Phase 4 —What Needs To Be Done?** **选择COBIT5最佳实践和流程支持。**
7. 执行行动计划	根据风险评估与整改建议，组织要设计未来的行动计划与实施方案。	设计未来行动计划与实施方案时，可考虑企业安全体系架构模型和网络安全专题规划的方法。	**COBIT Phase 5 —How Do We Get There?** **选择COBIT5最佳实践和流程支持。**

COBIT的CSF实施框架指南请参见：
http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/implementing-the-nist-cybersecurity-framework.aspx

本页为空白页

附件一：信息安全相关的法律法规

（一）国内相关法律法规

序号	法案名称	颁布机构	发布时间	类型	技术领域	概况介绍
1	中华人民共和国网络安全法	全国人民代表大会常务委员会	2016年11月7日	法律	网络安全基础架构、数据安全、业务连续性	本法律明确了部门、企业、社会组织和个人的权利、义务和责任，确立了对国家关键信息基础设施的保护制度，并对个人信息保护和数据安全提出了管理要求，同时强调了为确保网络安全应采取的监测预警、应急处置和涉及关键信息网络基础设施的产品与服务审查。
2	“十三五”国家信息化规划	国务院	2016年12月15日	行业意见	网络安全基础架构、数据安全、业务连续性、云安全、数据安全	1. 关键信息基础设施安全防护。组织实施信息安全专项，建立关键信息基础设施安全防护平台，支持关键基础设施和重要信息系统，整体提升安全防御能力。强化安全监管、综合防护的技术手段支撑，提升我国域名体系的网络安全和应急处置能力。 2. 网络安全审查能力建设。开展网络安全审查关键技术研究，统筹建立网络设备、大数据、云计算等重点实验室。 3. 网络安全标准能力提升。加强我国网络安全标准专业队伍建设，建设网络安全标准验证和检测平台，重点构建基于芯片和操作系统的安全评测，完善网络安全标准信息共享和实施情况跟踪评估机制。
3	网络产品和服务安全审查办法（试行）	国家互联网信息办公室	2017年5月2日	管理规定	准入控制	该办法为提高网络产品和服务安全可控水平，防范网络安全风险，维护国家安全而制定。办法要求关系国家安全和公共利益的信息系统使用的重要网络产品和服务，应当经过网络安全审查，审查重点审查网络产品和服务的安全性、可控性。同时，对审查相关的监管方、发起方和审查方提出了相关要求。
4	工业控制系统信息安全防护指南	工信部	2016年10月17日	管理规定	工控安全、数据安全	该指南为提升工业企业工业控制系统信息安全防护水平，保障工业控制系统安全而制定，适用于工业控制系统应用企业以及从事工业控制系统规划、设计、建设、运维、评估的企事业单位。指南对安全软件选择与管理、配置和补丁管理、边界安全防护、物理和环境安全防护、身份认证、远程访问安全、安全监测和应急预案演练、资产安全、数据安全、供应链管理以及落实责任等方面提出了管理要求，从而进一步完善网络与信息安全管理制度和机制，加强大数据场景下的网络数据保护，动信息安全技术和产业发展并提升工业信息安全保障能力。

（一）国内相关法律法规（续）

序号	法案名称	颁布机构	发布时间	类型	技术领域	概况介绍
5	中央企业商业秘密信息系统安全技术指引	国资委	2012年5月	技术指引	商业秘密	该指引是为进一步增强中央企业商业秘密保护技术防范能力，提高商业秘密保护水平而制定，涉及普通商密和核心商密两个级别的信息系统采取不同的技术规范。核心是数据安全保护，还包括网络安全、服务器与应用安全、终端安全、移动介质安全以及制度的安全，以期建立一个相对完善的防护体系。
6	等级保护基本要求	全国信息安全标准化技术委员会	2008年6月19日	制度规范	物理安全、网络安全、主机安全、应用安全和数据安全及日常管理（制度、机构、人员、系统建设和运维）	该要求提出和规定了不同安全保护等级信息系统的最低保护要求，即基本安全要求，基本安全要求包括基本技术要求和基本管理要求，适用于指导不同安全保护等级信息系统的安全建设和监督管理。
6.1	等级保护—物联网安全扩展要求		意见征求阶段		物理和环境、网络与通信、应用和数据、开发和运维	该扩展要求针对《网络安全等级保护基本要求》修订的思路和方法，成为其组织部分之一。分别从管理和技术两方面对物联网、移动互联网、云计算和工控的物理和环境安全、通信安全、应用和数据安全及管理和开发运维提出要求。
6.2	等级保护—移动互联安全扩展要求					
6.3	等级保护—云计算安全扩展要求					
6.4	等级保护—工业控制安全扩展要求					
7	个人信息安全规范				个人隐私	该标准 将针对处理个人信息的各类组织（包括机构、企业等），提出具体的保护要求，定位为我国个人信息保护工作的基础性标准文件，为今后开展与个人信息保护相关的各类活动提供参考，为制定和实施个人信息保护相关法律法规奠定基础，为国家主管部门、第三方测评机构等开展个人信息安全管理、评估工作提供指导和依据。内容主要包括：个人信息使用、个人信息存储、个人信息收集以及个人信息的转让和披露。

（二）其他国家及地区法律法规

序号	法案名称（CN）	法案名称（EN）	颁布机构	发布时间	技术领域	概况介绍
1	欧洲议会和理事会（EU）2016年第1148号指令2017-01-04	(EU) 2016/1148—Directive on Security of Network and Information Systems (the NIS Directive)	欧洲议会和理事会	2016年7月6日	网络安全基础框架	本指令为欧盟内部在网络安全方面的首部指令，其目的是为了通过提高网络安全能力、增加成员国间协作以及关键服务和数字服务提供者的风险管理、事件报告等手段和措施，实现欧盟高水平的网络和信息系统安全水平，保证公共信息安全。
2	关于个人数据处理和数据自由流动保护条例（一般数据保护条例）的提案	General Data Protection Regulation, GDPR	欧洲议会和欧盟委员会	2012年	隐私保护	该指令是欧盟为加强其居民的数据保护，提供更加坚实的框架，指导跨欧盟个人数据的商业使用而设计的。GDPR包括广泛的与隐私相关的要求，其将对组织的立法、合规、信息安全、市场、工程和人力资源管理产生巨大的影响。 指令规定了控制者和处理者应实施适当的措施保护数据处理安全的义务，以及应采用适当的技术和组织措施；同时，对处理过程中根据受保护的个人数据的性质所产生的风险提供适当的安全等级。控制者和处理者应当在风险评估后，实施前述规定的措施，保护个人数据免受意外或非法的破坏、意外丢失，预防任何非法形式的处理，特别是任何对个人数据未经授权的披露、传播、访问或更改。 此外，该指令对包括国际间数据传输、数据可移植性、隐私影响评估等诸多方面也提出了要求。

（二）其他国家及地区法律法规（续）

序号	法案名称（CN）	法案名称（EN）	颁布机构	发布时间	技术领域	概况介绍
3	2014年联邦信息安全管理法案	US Congress Federal Information Security Management Act 3554, or, Federal Information Security Modernization Act of 2014 (FISMA)	美国国会	2014年12月	网络安全	FISMA作为美国信息安全领域的一项重要法律，对于确保美国联邦信息系统安全，发挥了重要作用。FISMA规定了信息安全计划的主要内容，明确了联邦机构保障联邦信息与信息系统安全的主要职责，并提出了制定标准、监督检查、应急处理等保障措施。FISMA要求各联邦机构制定并实施适用于本机构的信息安全计划，为联邦信息和信息系统提供安全保障。该法案明确指出，信息安全计划应当包含：定期实施风险评估、制定有关政策和流程、制定安全保障计划、实施信息安全培训、检测评估策略有效性、明确整改措施制定流程、制定安全事件处理策略以及制定确保联邦信息系统持续运行的有关计划和流程等内容。
4	网络空间安全信息共享法（2015）	US Congress Cybersecurity Information Sharing Act of 2015 (CISA)	美国国会	2015年12月18日	网络安全基础框架	该法案旨在实现关于网络安全漏洞的信息分享，其内容是对企业的信息共享行为增加法律上的照顾，以鼓励美国企业把信息安全漏洞信息共享给其它企业以及政府部门。法案首次明确了网络安全信息共享的范围包括：“网络威胁指标”（Cyber Threat Indicator, CTI）和“防御性措施”（Defensive Measure）两大类，重点关注网络安全信息共享的参与主体、共享方式、实施和审查监督程序、组织机构、责任豁免及隐私保护规定等。
5	萨班斯法案	Sarbanes–Oxley Act（SOX）	美国政府	2002年	安全管理、数据安全	该法案是美国政府出台的一部涉及会计职业监管、公司治理、证券市场监管等方面改革的重要法律。针对信息安全管理，对安全技术的保护、加密密钥管理、敏感数据的交换和数据管理提出了安全要求，从而护有关上市公司财务报告的敏感数据，为上市公司制定和报告保护金融信息的控制措施提供指导。

（二）其他国家及地区法律法规（续）

序号	法案名称（CN）	法案名称（EN）	颁布机构	发布时间	技术领域	概况介绍
6	国家基础设施保护计划	National Infrastructure Protection Plan (NIPP)	美国国土安全部	2006年	关键基础设施安全	该计划由美国国土安全部发布，为现行和未来的保护关键基础设施和重要资源方案和活动提供了一个总体框架，其定义了3种不同的保护政策：阻止恐怖威胁、减少脆弱性和减轻潜在后果，为关键基础设施提供了一个风险管理框架，并促进公共和私营部门在关键基础设施和关键信息基础设施领域的合作伙伴关系的制度化。
7	网络空间国际战略	US Government National Strategy to Secure Cyberspace – Critical priorities	美国政府	2011年	关键基础设施安全、网络安全	该战略是美国政府出台的首份关于网络空间的战略，宣称要建立一个“开放、互通、安全和可靠”的网络空间，并为实现这一构想勾勒出了政策路线图，内容涵盖经济、国防、执法和外交等多个领域，“基本概括了美国所追求的目标”。“战略”列出了七个政策重点，即：通过制定国际标准、鼓励创新和开放市场，加强知识产权保护；确保网络的安全、可靠和韧性；深化执法合作并积极推出国际规则；强化“网军”以应对21世纪的安全挑战；建立有效且多方参与的国际互联网治理架构；展开“网络援外”以及保障互联网自由。
8	网络安全基本法&信息处理促进法	Japan Congress Cyber Security Basic Act & Information Processing Promotion Act	日本国会	2014年11月6日	网络安全基础框架	《网络安全基本法》旨在加强日本政府与民间在网络安全领域的协调和运用，更好地应对网络攻击。根据这项立法，日本政府将新设以内阁官房长官为首的“网络安全战略本部”，其将与日本国家安全保障会议、IT综合战略本部等其他相关机构加强合作，协调各政府部门的网络安全对策。该法还规定电力、金融等重要社会基础设施运营商、网络相关企业、地方自治体等有义务配合网络安全相关举措或提供相关情报。此外，该法提出将协助中小企业制定网络安全措施。

（二）其他国家及地区法律法规（续）

序号	法案名称（CN）	法案名称（EN）	颁布机构	发布时间	技术领域	概况介绍
9	保卫国家信息安全战略	Japan Congress Information Security Strategy for Protecting the Nation	日本国会	2010年	关键基础设施安全、数据安全	该战略为适用于日本第二个信息安全战略（FY 2010~FY 2013）而制定，从而确保每年的安全计划将被实施，包括：巩固政府基础设施的措施、巩固关键基础设施的措施和巩固其他基础设施的措施的内容。
10	个人数据保护法	Singapore Congress Personal Data Protection Act（PDPA）	新加坡国会	2012年	隐私保护	该法律确立了对于个人数据的收集、使用、披露和管理的各项治理规则。它认可了个人保护自身数据的权利，包括访问、修改等内容，保护个人资料不被滥用，特别在营销领域，组织必须在获得消费者允许后，才能收集和使用消费者的个人信息；组织也需向消费者解释他们收集和披露消费者个人信息的原因。该法中的“个人数据”是指所有可以用于识别其身份的数据或资料，无论是否真实；而个人是指自然人，无论其是否尚在人世。
11	信息安全法	Security of Canada Information Sharing Act	加拿大政府	2001年12月18日	数据安全	该法律没有采用传统的秘密信息概念，而是采用特别业务信息概念。《信息安全法》明确界定，所谓特别业务信息是指为保卫国家，加拿大政府在采取措施时所揭示的或从其保护措施可以推知的下列信息：有意成为、已经提议成为、提出要求或同意成为加拿大政府信息、谍报秘密来源或向其提供援助的个人、代理机构、团体、机关或组织的情况；为了暗中收集或获取解密、评估、分析、加工、处理、报告、传达或应对信息及谍报，加拿大政府曾使用、目前使用、打算使用或能够使用的手段以及该手段的限制或缺陷等7种具体情况。从特别业务信息的具体规定来看，其范围远远超出秘密信息的范围，可以说，《信息安全法》扩大了对政府信息的保护。
12	香港隐私保护条例		香港特区	2013年4月25日	隐私保护	该条例规定了个人资料收集的原则、使用及披露的一般原则、违反个人资料的收集和使用原则的行政救济和民事救济，并设立了个人资料隐私专员公署。为了保障公众利益，包括保安、罪案的防止或侦查、税收及健康方面的利益资料使用者可获豁免不受条例所管限。

附件二：NIST控制措施与国内外法律法规的对应关系

（一）NIST控制框架与国内法律法规的对应关系

功能	分类	子类	网络安全规范
识别	**资产管理（ID.AM）：识别能使组织达到商业目的的数据、人员、设备、系统和设施，并使其业务目标与企业风险战略保持一致。**	ID.AM-1：组织内的物理设备和系统的盘点	• 等级保护5.2.5.2，5.2.5.3，5.2.5.4，6.2.5.2，6.2.5.3，6.2.5.4，7.2.5.2，7.2.5.3，7.2.5.4，
			• 工业控制系统信息安全防护指南第八条（一）
		ID.AM-2：组织内的软件平台和应用的盘点	• 等级保护5.2.5.2，6.2.5.2，7.2.5.2
		ID.AM-3：组织通信和数据流的映射	• 等级保护5.1.4.3，5.1.5，6.1.4.4，6.1.5，7.1.4.4，7.1.5
		ID.AM-4：外部信息系统的编目	• 等级保护5.2.4，6.2.4，7.2.4
		ID.AM-5：资源（例如，硬件、设备、数据和软件）基于其分类、临界性和商业价值优先次序的划分。	• 等级保护4.1，4.2
		ID.AM-6：为全体员工和第三方利益相关者（如供应商、客户、合作伙伴）网络安全的角色和责任的建立。	• 网络安全法第二十九条、网络安全法第三十六条
			• 等级保护5.1.2，6.1.2，7.1.2
			• 中央企业商业秘密信息系统安全技术指引11.4.4
			• 工业控制系统信息安全防护指南第十条（二）、第十一条
			• 个人信息安全规范1a、2.1b
			• 网络产品和服务安全审查办法第三条

（一）NIST控制框架与国内法律法规的对应关系（续）

功能	分类	子类	网络安全规范
I识别（续）	**业务环境（ID.BE）：该组织优先考虑和易被接受的使命，目标，利益相关者和行动；并且这些信息被协助用于网络安全角色、责任和风险的管理决策。**	ID.BE-1：该组织的在供应链中的作用是识别和沟通	• 工业控制系统信息安全防护指南第十条（一）
		ID.BE-2：组织重要基础设施和工业部门的地点的确定与通知	• 网络安全法第三十一条、三十二条、三十三条
			• 等级保护5.1.1.1，5.1.1.2，6.1.1.1，6.1.1.2，7.1.1.1，7.1.1.2
		ID.BE-3：组织使命、目标和活动的优先次序的建立和沟通	• 中央企业商业秘密信息系统安全技术指引11.1.1（1）
		ID.BE-4：关键业务提供的依赖关系和关键功能的建立	
		ID.BE-5：对于支持提供关键业务的韧性要求的建立	• 等级保护5.2.5.8，6.2.5.10，6.2.5.12，7.2.5.11，7.2.5.13
	治理（ID.GV）：管理和监控组织的监管，法律，风险，环境和业务要求的政策，程序和流程的意识；以及网络安全风险管理的通报。	ID.GV-1：组织信息安全策略的建立	• 中央企业商业秘密信息系统安全技术指引11.1.1（1）（2）
			• 个人信息安全规范2.3a
		ID.GV-2：信息安全角色和职责的协调，内部角色和外部合作伙伴的一致	• 网络安全法第二十九条
			• 等级保护5.2.2，5.2.3，6.2.2，6.2.3，7.2.2，7.2.3
			• 中央企业商业秘密信息系统安全技术指引11.1.1（3）
		ID.GV-3：关于网络安全的法律和监管要求，包括隐私和公民自由的义务的意识和管理	• 网络安全法第三十条、网络安全法第三十六条、网络安全法第三十七条、网络安全法第四十条至四十五条
			• 等级保护5.2.3.3，6.2.3.4，7.2.3.4
			• 网络产品和服务安全审查办法第四条（三）、网络产品和服务安全审查办法第十三条
		ID.GV-4：应对网络安全风险的治理与风险的管理流程	• 网络安全法第二十一条（一）、网络安全法第三十八条、网络安全法第三十九条（一）
			• 等级保护5.2.5.5，6.2.5.5，7.2.5.6
			• 网络产品和服务安全审查办法第四条（二）

（一）NIST控制框架与国内法律法规的对应关系（续）

功能	分类	子类	网络安全规范
I识别（续）	**风险评估（ID.RA）：组织对组织业务（包括使命，功能，形象，声誉或）、企业资产和个人关于网络安全风险方面的意识。**	D.RA-1：资产漏洞的确定和记录	• 等级保护5.2.5.5，5.2.5.6，6.2.5.5，6.2.5.6，7.2.5.6，7.2.5.7
			• 工业控制系统信息安全防护指南第二条（三）
		ID.RA-2：从信息共享论坛和渠道关于威胁和漏洞信息的获得	• 网络安全法第二十九条、网络安全法第三十九条（三）
		ID.RA-3：内部和外部威胁的确定和记录	• 等级保护5.2.5.5，5.2.5.6，6.2.5.5，6.2.5.6，7.2.5.6，7.2.5.7
		ID.RA-4：潜在的业务影响和可能性的确定	• 个人信息安全规范2.1d
			• 网络产品和服务安全审查办法第四条（一）、网络产品和服务安全审查办法第四条（二）、网络产品和服务安全审查办法第六条
		ID.RA-5：威胁、脆弱性、可能性和影响来确定风险	• 网络产品和服务安全审查办法第四条（一）、网络产品和服务安全审查办法第四条（二）、网络产品和服务安全审查办法第六条
		ID.RA-6：风险响应识别并优先级区分	
	风险管理战略(ID.RM)：组织的优先事项、约束、风险承受力与设想的建立，并用于支持操作风险决策。	ID.RM-1：由组织利益攸关者进行风险管理流程的建立、管理和商定	• 网络安全法第三十八条
		ID.RM-2：组织风险承受能力的确定，并明确表示	• 网络安全法第三十九条（一）
		ID.RM-3：通过对组织在重要基础设施中扮演的角色及行业特定风险分析展示的对风险承受能力的决心	• 网络安全法第三十一条、三十二条、三十三条、网络安全法第三十九条（一）

（一）NIST控制框架与国内法律法规的对应关系（续）

功能	分类	子类	网络安全规范
P保护	**访问控制（PR.AC）：授权的用户、进程或设备、授权的活动和交易对于获得资产和相关的设施是有限制的。**	PR.AC-1：对经授权的设备和用户的身份的凭据管理	• 网络安全法第二十二条、网络安全法第二十三条
			• 等级保护5.1.1.1，5.1.2.2，5.1.2.4,5.1.3.1，5.1.3.2，5.1.4.1，5.1.4.2，5.2.5.5，5.2.4.5，6.1.1.2，6.1.2.2，6.1.3.1，6.1.3.2，6.1.4.1，6.1.4.2，6.2.5.5，6.2.5.6，7.1.1.2，7.1.2.2，7.1.3.1，7.1.3.2，7.1.4.1，7.1.4.2，7.2.2.3，7.2.3.5，7.2.5.6，7.2.5.7
			• 中央企业商业秘密信息系统安全技术指引5.4.1核心商密（4） 中央企业商业秘密信息系统安全技术指引5.4.3核心商密（1） 中央企业商业秘密信息系统安全技术指引5.4.3核心商密（4） 中央企业商业秘密信息系统安全技术指引7.1普通商密（1） 中央企业商业秘密信息系统安全技术指引8.1 中央企业商业秘密信息系统安全技术指引8.2普通商密（1） 中央企业商业秘密信息系统安全技术指引9.1普通商密（1） 中央企业商业秘密信息系统安全技术指引9.1核心商密（3） 中央企业商业秘密信息系统安全技术指引10.2普通商密（1）（2）
			• 工业控制系统信息安全防护指南第一条（一） 工业控制系统信息安全防护指南第五条（一） 工业控制系统信息安全防护指南第五条（三）
			• 网络产品和服务安全审查办法第二条、第十条、第十一条
		PR.AC-2：对资产的物理访问的管理和保护	• 等级保护5.1.1.1，5.1.2.3，5.2.5.4，5.2.5.5，6.1.1.2，6.1.2.6，6.2.5.4，6.2.5.5，7.1.1.2，7.1.2.7，7.2.5.4，7.2.5.6
			• 中央企业商业秘密信息系统安全技术指引5.4.3核心商密（6） 中央企业商业秘密信息系统安全技术指引6.2 中央企业商业秘密信息系统安全技术指引9.1普通商密（8）
			• 工业控制系统信息安全防护指南第四条（一）（二）
		PR.AC-3：远程访问管理	• 等级保护5.1.2.3，6.1.2.6，6.1.3.1，7.1.2.7，7.1.3.1
			• 工业控制系统信息安全防护指南第四条（一）（二）（三）（四）

（一）NIST控制框架与国内法律法规的对应关系（续）

功能	分类	子类	网络安全规范
P保护（续）	**访问控制（PR.AC）：授权的用户、进程或设备、授权的活动和交易对于获得资产和相关的设施是有限制的。（续）**	PR.AC-4：结合最小特权原则和职责分工管理访问权限	• 网络安全法第三十四条（一）
			• 等级保护5.2.2.1，5.2.2.3，5.2.3.4，6.2.2.1，6.2.2.3，6.2.3.5，7.2.2.1，7.2.2.3，7.2.3.5
			• 中央企业商业秘密信息系统安全技术指引5.2普通商密（1） 中央企业商业秘密信息系统安全技术指引7.3普通商密 中央企业商业秘密信息系统安全技术指引8.2普通商密（2）（5）
			• 个人信息安全规范2.4b
			• 工业控制系统信息安全防护指南第五条（二）
		PR.AC-5：网络完整性的保护，酌情结合网络隔离	• 等级保护5.1.2.1，5.1.2.2，6.1.2.1，6.1.2.2，6.1.2.4，7.1.2.1，7.1.2.2，7.1.2.4，7.1.2.5
			• 中央企业商业秘密信息系统安全技术指引6.1核心商密 中央企业商业秘密信息系统安全技术指引7.2普通商密（1）
			• 工业控制系统信息安全防护指南第三条（一）（二）（三）
	意识和培训（PR.AT）：按照相关的政策、程序和协议，组织对工作人员和合作伙伴提供网络安全意识教育和使其得到充分的培训，以执行其信息安全相关的职务及职责。	PR.AT-1：对全体员工的安全意识教育与培训	• 网络安全法第三十四条（二）
			• 等级保护5.2.3.3，5.2.5.7，6.2.3.4，6.2.5.7，7.2.3.4，7.2.5.8
			• 中央企业商业秘密信息系统安全技术指引11.3.2
			• 个人信息安全规范2.1j
		PR.AT-2：特权用户了解角色和职责	• 网络安全法第三十四条（一）
			• 等级保护6.1.3.2，7.1.2.7，7.1.3.2
		PR.AT-3：第三方的利益相关者（如供应商，客户，合作伙伴）了解角色和职责	• 网络安全法第二十二条、网络安全法第二十三条、网络安全法第二十四条、网络安全法第二十九条
			• 等级保护5.2.2.4，5.2.3.4，5.2.4.9，6.2.2.4，6.2.3.5，6.2.4.9，7.2.2.4，7.2.3.5，7.2.4.11
			• 中央企业商业秘密信息系统安全技术指引11.4.4
			• 网络产品和服务安全审查办法第七条

（一）NIST控制框架与国内法律法规的对应关系（续）

功能	分类	子类	网络安全规范
P保护（续）	**意识和培训（PR.AT）：按照相关的政策、程序和协议，组织对工作人员和合作伙伴提供网络安全意识教育和使其得到充分的培训，以执行其信息安全相关的职务及职责。（续）**	PR.AT-4：高级管理人员了解角色和职责	• 网络安全法第三十四条（一）
		PR.AT-5：物理和信息安全人员了解角色和职责	• 网络安全法第三十四条（一）
			• 等级保护5.2.2.1，5.2.2.2，5.2.3.3，5.2.3.4，6.2.2.1，6.2.2.2，6.2.3.3，6.2.3.4，7.2.2.1，7.2.2.2，7.2.3.3，7.2.3.4
			• 中央企业商业秘密信息系统安全技术指引5.2普通商密（3） 中央企业商业秘密信息系统安全技术指引5.4.1普通商密（1）（2）核心商密（3）
	数据安全（PR.DS）：信息和记录（数据）的管理与用以保护信息机密性、完整性和可用性的组织风险战略一致。	PR.DS-1：静态数据的保护	• 网络安全法第二十一条（四）
			• 等级保护 5.1.5，6.1.5，7.1.5
			• 中央企业商业秘密信息系统安全技术指引5.4.3核心商密（2）
			• 个人信息安全规范1f
			• 工业控制系统信息安全防护指南第九条（一）
		PR.DS-2：传输过程中数据的保护	• 等级保护 5.1.4.3，5.1.5，6.1.4.4，6.1.4.5，6.1.5，7.1.3.4，7.1.4.4，7.1.4.5，7.1.4.6，7.1.4.7，7.1.4.8，7.1.5
			• 中央企业商业秘密信息系统安全技术指引5.2核心商密（1）（2） 中央企业商业秘密信息系统安全技术指引5.3 中央企业商业秘密信息系统安全技术指引5.4.3核心商密（3）（4）
			• 个人信息安全规范1f、个人信息安全规范2.4d、个人信息安全规范4.1c
		PR.DS-3：资产在整个迁移、转让和处置中的正式管理	• 等级保护 5.2.5.3，6.2.5.3，7.2.5.3
			• 中央企业商业秘密信息系统安全技术指引5.2核心商密（3）（4） 中央企业商业秘密信息系统安全技术指引5.4.3普通商密（2） 中央企业商业秘密信息系统安全技术指引5.5普通商密（1）、（2）
			• 个人信息安全规范2.4f
		PR.DS-4：以确保有效性的足够的能力的维护	• 等级保护 5.1.5，5.2.5.3，5.2.5.8，6.1.5，6.2.5.3，6.2.5.10，7.1.5，7.2.5.4，7.2.5.11
			• 个人信息安全规范1e

（一）NIST控制框架与国内法律法规的对应关系（续）

功能	分类	子类	网络安全规范
P保护（续）	**数据安全（PR.DS）：信息和记录（数据）的管理与用以保护信息机密性、完整性和可用性的组织风险战略一致。（续）**	PR.DS-5：防止数据泄漏的保护功能的实现	• 网络安全法第二十一条（四）
			• 等级保护 5.1.2.2，5.1.3.2，5.1.3.3，5.1.4，5.1.5，6.1.2.2，6.1.3.2，6.1.3.4，6.1.4，6.1.5，7.1.2.2，7.1.3.2，7.1.3.4，7,1,4，7.1.5
			• 中央企业商业秘密信息系统安全技术指引5.1（3） 中央企业商业秘密信息系统安全技术指引5.3
		PR.DS-6：用于验证软件、固件和信息完整性的完整性检查机制	• 等级保护 5.1.4.3，5.1.4.4，5.1.5，6.1.4.4，6.1.4.6，6.1.5，7.1.4.5，7.1.4.7，7.1.5
			• 中央企业商业秘密信息系统安全技术指引5.5普通商密（3） 中央企业商业秘密信息系统安全技术指引5.5核心商密（2）
			• 个人信息安全规范1e
		PR.DS-7：开发和测试环境与生产环境互相独立	• 等级保护 5.2.4.4，6.2.4.4，7.2.4.4
	信息保护流程和程序（PR.IP）：安全策略（目的地址，范围，角色，职责，管理承诺和组织机构之间的协调）、流程和程序的维护，并用于管理信息系统和资产的保护。	PR.IP-1：信息技术/工业控制系统的基本配置的创建和维护	• 等级保护5.2.5.2，6.2.5.2，6.2.5.5，6.2.5.9，7.2.5.2，7.2.5.6，7.2.5.10
			• 工业控制系统信息安全防护指南第二条（一）
		PR.IP-2：管理系统的系统开发生命周期的实施	• 等级保护5.2.4，6.2.4，7.2.4
		PR.IP-3：配置变更控制流程的到位	• 等级保护6.2.5.9，7.2.5.10
			• 个人信息安全规范2.3b
			• 工业控制系统信息安全防护指南第二条（二）
		PR.IP-4：运行、维护、并定期测试的信息备份	• 网络安全法第三十四条（三）
			• 等级保护5.2.5.8，6.2.5.10，7.2.5.11
			• 中央企业商业秘密信息系统安全技术指引5.5普通商密（4） 中央企业商业秘密信息系统安全技术指引8.6普通商密（1） 中央企业商业秘密信息系统安全技术指引11.4.1
			• 工业控制系统信息安全防护指南第八条（二）第九条（二）
		PR.IP-5：关于满足组织资产的物理运行环境的政策和法规	• 网络安全法第三十条、网络安全法第三十五条
			• 等级保护5.2.5.8，6.2.5.10，7.2.5.11

（一）NIST控制框架与国内法律法规的对应关系（续）

功能	分类	子类	网络安全规范
P保护（续）	**信息保护流程和程序（PR.IP）：安全策略（目的地址，范围，角色，职责，管理承诺和组织机构之间的协调）、流程和程序的维护，并用于管理信息系统和资产的保护。（续）**	PR.IP-6：根据策略销毁的数据	• 等级保护5.2.5.8，6.2.5.10，7.2.5.11
			• 中央企业商业秘密信息系统安全技术指引5.2普通商密（4） 中央企业商业秘密信息系统安全技术指引5.4.1核心商密（3） 中央企业商业秘密信息系统安全技术指引5.4.3普通商密（3）（4） 中央企业商业秘密信息系统安全技术指引8.3核心商密（4）（5） 中央企业商业秘密信息系统安全技术指引10.2核心商密（2） 中央企业商业秘密信息系统安全技术指引11.3.3（1）（2）
			• 个人信息安全规范2.4f（3）、个人信息安全规范5.6
		PR.IP-7：不断完善的保护程序	• 等级保护5.2.5.6，5.2.5.7，6.2.5.6，6.2.5.7，7.2.5.5，7.2.5.7，7.2.5.8
		PR.IP-8：与相关各方共享的保护技术的有效性	• 网络安全法第二十九条、网络安全法第三十九条（三）
			• 等级保护5.2.5.9，6.2.5.11，6.2.5.7，7.2.5.12
			• 网络产品和服务安全审查办法第十四条
		PR.IP-9：响应计划（事件响应和业务连续性）和恢复计划（事故恢复和灾难恢复）的到位与管理	• 等级保护5.2.5.9，6.2.5.11，6.2.5.12，7.2.5.12，7.2.5.13
		PR.IP-10：响应和恢复计划的测试	• 等级保护6.2.5.12，7.2.5.13
		PR.IP-11：在人力资源方面的做法（如撤销服务，人员筛选）的网络安全	• 等级保护5.2.2.1，5.2.2.2，5.2.3.1，6.2.2.1，6.2.2.2，6.2.3.1，7.2.2.1，7.2.2.2，7.2.3.1
			• 中央企业商业秘密信息系统安全技术指引11.2.1 中央企业商业秘密信息系统安全技术指引11.2.2 中央企业商业秘密信息系统安全技术指引11.3.1 中央企业商业秘密信息系统安全技术指引11.3.3（3）
			• 个人信息安全规范2.1f、个人信息安全规范2.1h、个人信息安全规范2.1i
		PR.IP-12：漏洞管理计划的制定和实施	• 等级保护5.2.5.5，5.2.5.6，6.2.5.5，6.2.5.6，7.2.5.6，7.2.5.7
			• 中央企业商业秘密信息系统安全技术指引9.2普通商密（5）、中央企业商业秘密信息系统安全技术指引9.2核心商密（4）
			• 工业控制系统信息安全防护指南第二条（三）

（一）NIST控制框架与国内法律法规的对应关系（续）

功能	分类	子类	网络安全规范
P保护（续）	**维护（PR.MA）：符合政策和程序的工业控制与信息系统组件的维护和维修的执行。**	PR.MA-1：组织资产维护与维修的及时执行与记录，需使用已获批准和管控的工具	• 网络安全法第二十三条
			• 等级保护5.2.5.3，5.2.5.4，6.2.5.3，6.2.5.4，7.2.5.3，7.2.5.4
		PR.MA-2：组织资产的远程维护被批准、记录与执行，并防止以未经授权的访问的方式进行	• 等级保护5.2.5.3，5.2.5.4，6.2.5.3，6.2.5.4，7.2.5.3，7.2.5.4
	防护技术（PR.PT）：技术安全解决方案的管理，以确保系统和资产的安全性和弹性符合相关的政策、程序和协定。	PR.PT-1：根据政策对审核/日志记录的确定、记载、实施、审查	• 网络安全法第二十一条（三）
			• 等级保护5.2.5.5，5.2.5.6，6.1.2.3，6.1.3.3，6.1.4.3，6.2.5.5，6.2.5.6，7.1.2.3，7.1.3.3，7.1.4.3，7.2.5.6，7.2.5.7
			• 中央企业商业秘密信息系统安全技术指引|5.4.1核心商密（2） 中央企业商业秘密信息系统安全技术指引|7.3普通商密 中央企业商业秘密信息系统安全技术指引|8.2核心商密（1）（2） 中央企业商业秘密信息系统安全技术指引|8.4 中央企业商业秘密信息系统安全技术指引|9.1普通商密（7） 中央企业商业秘密信息系统安全技术指引|10.3普通商密（1）（2）核心商密 中央企业商业秘密信息系统安全技术指引|11.2.3
			• 个人信息安全规范2.5a
		PR.PT-2：根据限制使用政策对移动媒体的保护	• 网络安全法第二十四条、网络安全法第五十八条
			• 等级保护5.2.5.3，5.2.5.4，6.2.5.3，6.2.5.4，7.2.5.3，7.2.5.4
			• 中央企业商业秘密信息系统安全技术指引|10.1
		PR.PT-3：结合功能最少的原则对系统和资产访问的控制	• 等级保护5.1.1.1，5.1.2.2，5.1.3.2，5.1.4.2，5.2.5.5，5.2.5.6，6.1.1.2，6.1.2.2，6.1.3.2，6.1.4.2，6.2.5.5，6.2.5.6，7.1.1.2，7.2.2.2，7.1.3.2，7.1.4.2，7.2.5.6，7.2.5.7
			• 个人信息安全规范1c
		PR.PT-4：通信和控制网络的保护	• 网络安全法第二十一条（二）
			• 等级保护5.1.2，5.2.5.5，6.1.2，6.2.5.5，7.1.2，7.2.5.6

（一）NIST控制框架与国内法律法规的对应关系（续）

功能	分类	子类	网络安全规范
D检测	**异常和事件（DE.AE）：及时检测到异常活动和事件的潜在影响的理解。**	DE.AE-1：用户和系统的预期数据流和网络运营的基线的建立和管理	• 网络安全法第三十条
			• 等级保护6.2.5.11，7.2.5.12
		DE.AE-2：分析检测到的事件，以了解攻击目标和方法	• 等级保护6.2.5.11，7.2.5.12
		DE.AE-3：聚合和关联来自多个源和传感器的事件数据	• 网络安全法第五十一条
			• 等级保护6.2.5.11，7.2.5.12
		DU.AE-4：事件影响的确定	• 等级保护6.2.5.11，7.2.5.12
		DE.AE-5：事件警报阈值的建立	• 等级保护6.2.5.11，7.2.5.12
			• 中央企业商业秘密信息系统安全技术指引8.3核心商密（3） 中央企业商业秘密信息系统安全技术指引8.5普通商密（4）
			• 网络安全法第二十一条（三）
	安全连续监测（DE.CM）：不定时监测信息系统和资产，确保网络安全的落实和保护措施的有效性。	DE.CM-1：监测网络，以发现潜在的网络安全事件	• 等级保护5.2.5.5，6.2.5.5，7.2.5.5，7.2.5.6
			• 中央企业商业秘密信息系统安全技术指引7.1核心商密（1） 中央企业商业秘密信息系统安全技术指引7.2普通商密（2）
			• 工业控制系统信息安全防护指南第七条（一）（二）
		DE.CM-2：监测物理环境，以发现潜在的网络安全事件	• 网络安全法第二十一条（三）、网络安全法第五十一条
			• 等级保护5.1.1.1，5.1.1.2，5.1.1.3，5.1.1.4，5.1.1.5，5.1.1.6，5.1.1.7，6.1.1.1，6.1.1.2，6.1.1.3，6.1.1.3，6.1.1.4，6.1.1.5，6.1.1.6，6.1.1.7，6.1.1.8，6.1.1.9，6.1.1.10，7.1.1.1，7.1.1.2，7.1.1.3，7.1.1.4，7.1.1.5，7.1.1.6，7.1.1.7，7.1.1.8，7.1.1.10
		DE.CM-3：监视人员的活动，以发现潜在的网络安全事件	• 网络安全法第三十四条（一）、网络安全法第五十一条
			• 中央企业商业秘密信息系统安全技术指引7.1普通商密（2）（3）

（一）NIST控制框架与国内法律法规的对应关系（续）

功能	分类	子类	网络安全规范
D检测（续）	**安全连续监测（DE.CM）：不定时监测信息系统和资产，确保网络安全的落实和保护措施的有效性。（续）**	DE.CM-4：恶意代码的检测	• 等级保护5.1.3.4，6.1.3.5，7.1.3.6
			• 中央企业商业秘密信息系统安全技术指引7.1核心商密（1）（2） 中央企业商业秘密信息系统安全技术指引8.3普通商密（2） 中央企业商业秘密信息系统安全技术指引9.2普通商密（3）
			• 工业控制系统信息安全防护指南第一条（二）
		DE.CM-5：未经授权的移动代码的检测	
		DE.CM-6：监测外部服务提供者的活动，以发现潜在的网络安全事件	• 网络安全法第二十七条、网络安全法第五十一条
			• 等级保护5.2.3.4，6.2.3.5，6.2.4.9，6.2.5.1，7.2.3.5
		DE.CM-7：对未经授权的人员、连接、设备和软件进行监控的执行	• 网络安全法第二十二条、网络安全法第二十三条、网络安全法第五十一条
			• 等级保护5.1.2.2，6.1.3.6，7.1.3.2
			• 中央企业商业秘密信息系统安全技术指引7.1普通商密（2）
		DE.CM-8：漏洞扫描的执行	• 等级保护5.2.5.5，5.2.5.6，6.2.5.5，6.2.5.6，7.2.5.6，7.2.5.7
			• 中央企业商业秘密信息系统安全技术指引9.2 普通商密（5）
			• 工业控制系统信息安全防护指南第二条（三）
	检测过程（DE.DP）：维护和测试过程和程序的检测，以确保对异常事件及时和充分的认识。	DE.DP-1：角色和责任检测的明确界定，以确保问责制	• 网络安全法第三十条
			• 等级保护5.2.2.，5.2.3.1，5.2.3.2，6.2.3.1，6.2.3.2，7.2.3.1，7.2.3.2，7.2.3.3
			• 工业控制系统信息安全防护指南第十一条
		DE.DP-2：检测活动符合所有相应要求	• 网络安全法第二十六条
		DE.DP-3：检测过程的测试	• 等级保护5.2.4.7，6.2.4.7，6.2.5.6，7.2.4.7，7.2.5.7
		DE.DP-4：事件检测信息传达给相关方	• 网络安全法第五十二条
			• 等级保护5.2.5.9，6.2.5.11，7.2.5.12
		DE.DP-5：检测过程的不断完善	

（一）NIST控制框架与国内法律法规的对应关系（续）

功能	分类	子类	网络安全规范
R应急	**应急预案（RS.RP）：流程和程序应急的执行和维护，以确保网络安全检测事件的及时响应。**	RS.RP-1：事件期间或之后执行应急预案	• 网络安全法第二十五条、网络安全法第三十四条（四）、网络安全法第三十九条（二）、网络安全法第五十一三条
			• 等级保护 6.2.5.12，7.2.5.13
			• 中央企业商业秘密信息系统安全技术指引8.6普通商密（2） 中央企业商业秘密信息系统安全技术指引11.4.3（1）
			• 个人信息安全规范2.7a、个人信息安全规范2.7b
			• 工业控制系统信息安全防护指南第七条（三）（四）
	沟通（RS.CO）：应急措施与内外部利益相关者（酌情包括来自执法机关的外部支持）保持协调。	RS.CO-1：需要应急时职员知道自己的角色和操作流程	• 网络安全法第三十九条（二）
			• 等级保护6.2.5.12，7.2.5.13
			• 个人信息安全规范2.7b
		RS.CO-2：事件报告与既定标准一致	• 等级保护6.2.5.12，7.2.5.13
		RS.CO-3：信息共享符合应急预案	• 网络安全法第三十九条（三）
			• 等级保护6.2.5.12，7.2.5.13
		RS.CO-4：利益相关者与应急预案保持协调	• 网络安全法第二十五条
			• 等级保护6.2.5.12，7.2.5.13
		RS.CO-5：自愿信息共享与外部利益相关者实现更广泛的网络安全态势感知	• 网络安全法第三十九条（三）
			• 等级保护6.2.5.12，7.2.5.13
	分析（RS.AN）：进行分析，以确保有足够的响应并支持恢复活动。	NS.AN-1：检测系统的通知的调查	• 等级保护6.2.5.11，6.2.5.12，7.2.5.12，7.2.5.13
		RS.AN-2：事件的影响的了解	• 等级保护5.2.5.9，6.2.5.11，7.2.5.12
			• 个人信息安全规范2.7c
		RS.AN-3：取证的执行	• 等级保护5.2.5.9，6.2.5.11，7.2.5.12
		RS.AN-4：与应急方案相一致对事件进行分类	• 等级保护6.2.5.11，6.2.5.12，7.2.5.12，7.2.5.13
	缓解（RS.MI）：用以防止事件扩大、减轻其影响、并消除该事件的活动的执行。	RS.MI-1：事故遏制	• 网络安全法第二十五条
			• 等级保护6.2.5.11，7.2.5.12
			• 个人信息安全规范2.7c
			• 工业控制系统信息安全防护指南第七条（三）

（一）NIST控制框架与国内法律法规的对应关系（续）

功能	分类	子类	网络安全规范
R应急（续）	**缓解（RS.MI）：用以防止事件扩大、减轻其影响、并消除该事件的活动的执行。（续）**	RS.MI-2：事故缓解	• 网络安全法第二十五条
			• 等级保护6.2.5.11，7.2.5.12
			• 个人信息安全规范2.7c
			• 工业控制系统信息安全防护指南第七条（三）
		RS.MI-3：新确定的漏洞的缓解或记录为接受的风险	
	改进（RS.IM）：通过汲取当前和以前的检测/响应活动中的教训完善组织应对活动。	RS.IM-1：应急计划整合的经验教训	• 等级保护6.2.5.11，7.2.5.12
			• 中央企业商业秘密信息系统安全技术指引11.4.3（1）
		RS.IM-2：应对策略更新	• 等级保护6.2.5.11，7.2.5.12
			• 中央企业商业秘密信息系统安全技术指引11.1.3 中央企业商业秘密信息系统安全技术指引11.4.3（4）
R恢复	**恢复计划（RC.RP）：恢复过程和程序的执行和维护，以确保受影响的网络安全事件、系统或资产的及时恢复。**	RC.RP-1：事件期间或之后执行的恢复计划	• 网络安全法第三十九条（四）、网络安全法第五十四条（三）
			• 中央企业商业秘密信息系统安全技术指引11.4.2（1）（2）
	改进（RC.IM）：通过汲取在未来的活动的教训改善恢复规划和规程。	RC.IM-1：恢复计划结合吸取的经验教训	• 中央企业商业秘密信息系统安全技术指引11.4.3（4）
		RC.IM-2：恢复策略的更新	• 等级保护6.2.5.12，7.2.5.13
			• 中央企业商业秘密信息系统安全技术指引11.1.3 中央企业商业秘密信息系统安全技术指引11.4.2（4）
	通信（RC.CO）：恢复活动与内部和外部各方（如协调中心、互联网服务提供商、攻击系统、被害人、其他CSIRT的业主）和供应商的协调。	RC.CO-1：公共关系管理	• 网络安全法第二十八条、网络安全法第五十四条（三）、网络安全法第五十五条
			• 个人信息安全规范2.7c
			• 工业控制系统信息安全防护指南第七条（三）
		RC.CO-2：事件后声誉的修复	• 网络安全法第五十四条（三）
			• 工业控制系统信息安全防护指南第七条（三）
		RC.CO-3：恢复活动传达给内部利益相关者和执行管理团队	• 中央企业商业秘密信息系统安全技术指引11.4.2（5）

（二）NIST控制框架与国外及地区法律法规的对应关系

功能	分类	子类	网络安全规范
I识别	**资产管理（ID.AM）：识别能使组织达到商业目的的数据、人员、设备、系统和设施，并使其业务目标与企业风险战略保持一致。**	ID.AM-1：组织内的物理设备和系统的盘点	
		ID.AM-2：组织内的软件平台和应用的盘点	
		ID.AM-3：组织通信和数据流的映射	
		ID.AM-4：外部信息系统的编目	
		ID.AM-5：资源（例如，硬件、设备、数据和软件）基于其分类、临界性和商业价值优先次序的划分。	
		ID.AM-6：为全体员工和第三方利益相关者（如供应商、客户、合作伙伴）网络安全的角色和责任的建立。	• EU Directive on security of network and ISs Article 5 (1,6,7) • US Congress Cybersecurity Information Sharing Act Sec 303
	业务环境（ID.BE）：该组织优先考虑和易被接受的使命，目标，利益相关者和行动；并且这些信息被协助用于网络安全角色、责任和风险的管理决策。	ID.BE-1：该组织的在供应链中的作用是识别和沟通	
		ID.BE-2：组织重要基础设施和工业部门的地点的确定与通知	• NIPP 3 • US Congress Cybersecurity Information Sharing Act Sec 208
		ID.BE-3：组织使命、目标和活动的优先次序的建立和沟通	• EU Directive on security of network and ISs Article 7 (1,3) • US Government National Strategy to Secure Cyberspace – Critical priorities • NIPP 2
		ID.BE-4：关键业务提供的依赖关系和关键功能的建立	• Japan Congress Cyber Security Basic Act & Information Processing Promotion Act Article 13,24,25,26,27,28,29,30,31,33,34,35
		ID.BE-5：对于支持提供关键业务的韧性要求的建立	
	治理（ID.GV）：管理和监控组织的监管，法律，风险，环境和业务要求的政策，程序和流程的意识；以及网络安全风险管理的通报。	ID.GV-1：组织信息安全策略的建立	• Singapore Congress Personal Data Protection Act:12 • Processing Promotion Act Article 12 • Japan Congress Information Security Strategy for Protecting the Nation 2.1 • Japan Congress Information Security Strategy for Protecting the Nation 4.2

（二）NIST控制框架与国外及地区法律法规的对应关系（续）

功能	分类	子类	网络安全规范
I识别 （续）	**治理（ID.GV）：管理和监控组织的监管，法律，风险，环境和业务要求的政策，程序和流程的意识；以及网络安全风险管理的通报。** **（续）**	ID.GV-2：信息安全角色和职责的协调，内部角色和外部合作伙伴的一致	• GDPR Articles 26(1,2,3),28(1,2,3,4),29,31,36(1,2,3,4,5),37(1,2,3,4,5,6,7),38(1,2,3,4,5,6),39(1,2),50 • EU Directive on security of network and ISs Article 8(1,2,3,4,5,6,7),9(1,2,3,4,5),10(2,3),11(1,2,3,4,5),12(1,2,3,4,5) • 香港隐私保护条例 条:5,6,7,8,9,10,11,12,13 • Singapore Congress Personal Data Protection Act:5,6,7,8,9,10,29 • Japan Congress Cyber Security Basic Act & Information Processing Promotion Act Article 4,5,6,7,8,14,15,19,20,21,23 • US Government National Strategy to Secure Cyberspace –Priority 4 • US Congress Federal Information Security Management Act 3554 • US Congress Cybersecurity Information Sharing Act Sec 209
		ID.GV-3：关于网络安全的法律和监管要求，包括隐私和公民自由的义务的意识和管理	• GDPR Article 5(1,2),6(1,2,3,4),7(1,2,3,4),8(1,2),9(1),10,12(1),14(1,2,3,4,5),15(1,2),16,17(1,2,3),18(1,2,3),19,20(1,2,3,4),21(1,2,3,4,5,6),22(1,2,3,4),23(1,2),24(1,2,3),42(1,2) • 香港隐私保护条例条:51,51A,57,58,58A,59,59A,60,60A,60B,61,62,63,63A,63B,63C,63D,64,64A,64B,65,66A,66B,67,68,69,70 • SOX Sec 404 • Security of Canada Information Sharing Act:5,6,7,8,9,10 • Singapore Congress Personal Data Protection Act:11,13,14,15,16,17,33,34,35 • Japan Congress Cyber Security Basic Act & Information Processing Promotion Act Article 10,11,16,17,18 • US Congress Federal Information Security Management Act 3553,3555,3558 • US Congress Cybersecurity Information Sharing Act Sec 103,104,105,106,107,108,109,304,305
		ID.GV-4：应对网络安全风险的治理与风险的管理流程	• EU Directive on security of network and ISs Article 22(1,2),23(1,2) • 香港隐私保护条例：14,14A,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,43,45,46,47,48

（二）NIST控制框架与国外及地区法律法规的对应关系（续）

功能	分类	子类	网络安全规范
I识别（续）	**风险评估（ID.RA）：组织对组织业务（包括使命，功能，形象，声誉或）、企业资产和个人关于网络安全风险方面的意识。**	D.RA-1：资产漏洞的确定和记录	• NIPP 5
		ID.RA-2：从信息共享论坛和渠道关于威胁和漏洞信息的获得	
		ID.RA-3：内部和外部威胁的确定和记录	
		ID.RA-4：潜在的业务影响和可能性的确定	• EU Directive on security of network and ISs Article 6(1,2)
		ID.RA-5：威胁、脆弱性、可能性和影响来确定风险	
		ID.RA-6：风险响应识别并优先级区分	
	风险管理战略（ID.RM）：组织的优先事项、约束、风险承受力与设想的建立，并用于支持操作风险决策。	ID.RM-1：由组织利益攸关者进行风险管理流程的建立、 管理和商定	• US Government National Strategy to Secure Cyberspace –Priority 2 • US Congress Federal Information Security Management Act 3557
		ID.RM-2：组织风险承受能力的确定，并明确表示	
		ID.RM-3：通过对组织在重要基础设施中扮演的角色及行业特定风险分析展示的对风险承受能力的决心	• NIPP 3,4
P保护	**访问控制（PR.AC）：授权的用户、进程或设备、授权的活动和交易对于获得资产和相关的设施是有限制的。**	PR.AC-1：对经授权的设备和用户的身份的凭据管理	
		PR.AC-2：对资产的物理访问的管理和保护	
		PR.AC-3：远程访问管理	
		PR.AC-4：结合最小特权原则和职责分工管理访问权限	• Singapore Congress Personal Data Protection Act: 21,22
		PR.AC-5：网络完整性的保护，酌情结合网络隔离	

（二）NIST控制框架与国外及地区法律法规的对应关系（续）

功能	分类	子类	网络安全规范
P保护（续）	**意识和培训（PR.AT）：按照相关的政策、程序和协议，组织对工作人员和合作伙伴提供网络安全意识教育和使其得到充分的培训，以执行其信息安全相关的职务及职责。**	PR.AT-1：对全体员工的安全意识教育与培训	• Japan Congress - Cyber Security Basic Act & Information Processing Promotion Act Article 9,22 • US Government National Strategy to Secure Cyberspace –Priority 3
		PR.AT-2：特权用户了解角色和职责	
		PR.AT-3：第三方的利益相关者（如供应商，客户，合作伙伴）了解角色和职责	
		PR.AT-4：高级管理人员了解角色和职责	
		PR.AT-5：物理和信息安全人员了解角色和职责	
	数据安全（PR.DS）：信息和记录（数据）的管理与用以保护信息机密性、完整性和可用性的组织风险战略一致。	PR.DS-1：静态数据的保护	• GDPR Article 25(1,2),32(1,2,3,4) • Singapore Congress Personal Data Protection Act:23,24,25
		PR.DS-2：传输过程中数据的保护	• GDPR Article 25(1,2),32(1,2,3,4),44,45(1,2,3,4,5,6,7),46(1,2,3) • Singapore Congress Personal Data Protection Act:23,24
		PR.DS-3：资产在整个迁移、转让和处置中的正式管理	• Singapore Congress Personal Data Protection Act:26
		PR.DS-4：以确保有效性的足够的能力的维护	
		PR.DS-5：防止数据泄漏的保护功能的实现	
		PR.DS-6：用于验证软件、固件和信息完整性的完整性检查机制	
		PR.DS-7：开发和测试环境与生产环境互相独立	

（二）NIST控制框架与国外及地区法律法规的对应关系（续）

功能	分类	子类	网络安全规范
P保护（续）	**信息保护流程和程序（PR.IP）：安全策略（目的地址，范围，角色，职责，管理承诺和组织机构之间的协调）、流程和程序的维护，并用于管理信息系统和资产的保护。**	PR.IP-1：信息技术/工业控制系统的基本配置的创建和维护	
		PR.IP-2：管理系统的系统开发生命周期的实施	
		PR.IP-3：配置变更控制流程的到位	
		PR.IP-4：运行、维护、并定期测试的信息备份	
		PR.IP-5：关于满足组织资产的物理运行环境的政策和法规	
		PR.IP-6：根据策略销毁的数据	
		PR.IP-7：不断完善的保护程序	
		PR.IP-8：与相关各方共享的保护技术的有效性	
		PR.IP-9：响应计划（事件响应和业务连续性）和恢复计划（事故恢复和灾难恢复）的到位与管理	• US Congress Federal Information Security Management Act 3556 • US Congress Cybersecurity Information Sharing Act Sec 228
		PR.IP-10：响应和恢复计划的测试	
		PR.IP-11：在人力资源方面的做法（如撤销服务，人员筛选）的网络安全	
		PR.IP-12：漏洞管理计划的制定和实施	
	维护（PR.MA）：符合政策和程序的工业控制与信息系统组件的维护和维修的执行。	PR.MA-1：组织资产维护与维修的及时执行与记录，需使用已获批准和管控的工具	
		PR.MA-2：组织资产的远程维护被批准、记录与执行，并防止以未经授权的访问的方式进行	

（二）NIST控制框架与国外及地区法律法规的对应关系（续）

功能	分类	子类	网络安全规范
P保护（续）	**防护技术（PR.PT）：技术安全解决方案的管理，以确保系统和资产的安全性和弹性符合相关的政策、程序和协定。**	PR.PT-1：根据政策对审核/日志记录的确定、记载、实施、审查	• GDPR Article 30(1,2,3,4)
		PR.PT-2：根据限制使用政策对移动媒体的保护	
		PR.PT-3：结合功能最少的原则对系统和资产访问的控制	
		PR.PT-4：通信和控制网络的保护	
D检测	**异常和事件（DE.AE）：及时检测到异常活动和事件的潜在影响的理解。**	DE.AE-1：用户和系统的预期数据流和网络运营的基线的建立和管理	
		DE.AE-2：分析检测到的事件，以了解攻击目标和方法	
		DE.AE-3：聚合和关联来自多个源和传感器的事件数据	
		DU.AE-4：事件影响的确定	• US Congress Cybersecurity Information Sharing Act Sec 206
		DE.AE-5：事件警报阈值的建立	
	安全连续监测（DE.CM）：不定时监测信息系统和资产，确保网络安全的落实和保护措施的有效性。	DE.CM-1：监测网络，以发现潜在的网络安全事件	• US Congress Cybersecurity Information Sharing Act Sec 230
		DE.CM-2：监测物理环境，以发现潜在的网络安全事件	
		DE.CM-3：监视人员的活动，以发现潜在的网络安全事件	
		DE.CM-4：恶意代码的检测	
		DE.CM-5：未经授权的移动代码的检测	
		DE.CM-6：监测外部服务提供者的活动，以发现潜在的网络安全事件	
		DE.CM-7：对未经授权的人员、连接、设备和软件进行监控的执行	
		DE.CM-8：漏洞扫描的执行	

（二）NIST控制框架与国外及地区法律法规的对应关系（续）

功能	分类	子类	网络安全规范
D检测（续）	**检测过程（DE.DP）：维护和测试过程和程序的检测，以确保对异常事件及时和充分的认识。**	DE.DP-1：角色和责任检测的明确界定，以确保问责制	
		DE.DP-2：检测活动符合所有相应要求	• US Congress Cybersecurity Information Sharing Act Sec 205
		DE.DP-3：检测过程的测试	
		DE.DP-4：事件检测信息传达给相关方	
		DE.DP-5：检测过程的不断完善	• US Congress Cybersecurity Information Sharing Act Sec 204
R应急	**应急预案（RS.RP）：流程和程序应急的执行和维护，以确保网络安全检测事件的及时响应。**	RS.RP-1：事件期间或之后执行应急预案	• Japan Congress Information Security Strategy for Protecting the Nation 4.1 • US Government National Strategy to Secure Cyberspace –Priority 1
	沟通（RS.CO）：应急措施与内外部利益相关者（酌情包括来自执法机关的外部支持）保持协调。	RS.CO-1：需要应急时职员知道自己的角色和操作流程	• EU Directive on security of network and ISs Article 14,16-21
		RS.CO-2：事件报告与既定标准一致	
		RS.CO-3：信息共享符合应急预案	• GDPR Article 33(1,2,3,4,5),34(1,2,3,4)
		RS.CO-4：利益相关者与应急预案保持协调	
		RS.CO-5：自愿信息共享与外部利益相关者实现更广泛的网络安全态势感知	
	分析（RS.AN）：进行分析，以确保有足够的响应并支持恢复活动。	NS.AND-1：检测系统的通知的调查	
		RS.AND-2：事件的影响的了解	• GDPR Article 35(1,2,3,4,5,6,7,8,9,10,11)
		RS.AN-3：取证的执行	
		RS.AN-4：与应急方案相一致对事件进行分类	
	缓解（RS.MI）：用以防止事件扩大、减轻其影响、并消除该事件的活动的执行。	RS.MI-1：事故遏制	

（二）NIST控制框架与国外及地区法律法规的对应关系（续）

功能	分类	子类	网络安全规范
R应急（续）	**缓解（RS.MI）：用以防止事件扩大、减轻其影响、并消除该事件的活动的执行。（续）**	RS.MI-2：事故缓解	
		RS.MI-3：新确定的漏洞的缓解或记录为接受的风险	
	改进（RS.IM）：通过汲取当前和以前的检测/响应活动中的教训完善组织应对活动。	RS.IN-1：应急计划整合的经验教训	
		RS.IM-2：应对策略更新	
R恢复	**恢复计划（RC.RP）：恢复过程和程序的执行和维护，以确保受影响的网络安全事件、系统或资产的及时恢复。**	RC.RP-1：事件期间或之后执行的恢复计划	
	改进（RC.IM）：通过汲取在未来的活动的教训改善恢复规划和规程。	RC.IM-1：恢复计划结合吸取的经验教训	
		RC.IM-2：恢复策略的更新	
	通信（RC.CO）：恢复活动与内部和外部各方（如协调中心、互联网服务提供商、攻击系统、被害人、其他CSIRT的业主）和供应商的协调。	RC.CO-1：公共关系管理	
		RC.CO-2：事件后声誉的修复	
		RC.CO-3：恢复活动传达给内部利益相关者和执行管理团队	

（三）NIST控制框架与信息安全最佳实践的对应关系

NIST控制框架中IPDRR模型中各域与信息安全与IT风险控制最佳实践（例如：ISO27001、COBIT5等）。

功能	分类	子类	网络安全规范
I识别	**资产管理（ID.AM）：识别能使组织达到商业目的的数据、人员、设备、系统和设施，并使其业务目标与企业风险战略保持一致。**	ID.AM-1：组织内的物理设备和系统的盘点	• CCS CSC 1 • COBIT 5 BAI09.01，BAI09.02 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
			• CCS CSC 2 • COBIT 5 BAI09.01, BAI09.02, BAI09.05 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2：组织内的软件平台和应用的盘点	• CCS CSC 1 • COBIT 5 DSS05.02 • ISO/IEC 27001:2013 A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9,PL-8
		ID.AM-3：组织通信和数据流的映射	• COBIT 5 APO02.02 • ISO/IEC 27001:2013 A.11.2.6 • NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-4：外部信息系统的编目	• COBIT 5 APO03.03, APO03.04, BAI09.02 • ISO/IEC 27001:2013 A.8.2.1 • NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14
		ID.AM-5：资源（例如，硬件、设备、数据和软件）基于其分类、临界性和商业价值优先次序的划分。	• COBIT 5 APO01.02, DSS06.03 • ISO/IEC 27001:2013 A.6.1.1 • NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
。。	。。。	。。。	。。。

以上内容仅为示例，其他请参见：COBIT的CSF实施框架指南请参见：
http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/implementing-the-nist-cybersecurity-framework.aspx
中的Appendix A: Framework Core。

--- 结束 ---

致谢

ISACA 要特别感谢以下人员：

首席开发人员
陈伟，CISA，COBIT 5 Foundation，北京谷安天下科技有限公司
赵元勋，CCNP，CCSSP，PMP，普华永道，中国

开发人员
蔡俊磊，CISA，CRISC，CISM，CGEIT，上投摩根基金管理有限公司，中国
吴海川，CISA，CISM，埃森哲，中国
张辉，CISP，中国
孙锦泉，CISA，中国电信上海公司，中国
石宇，CISA，中国
段振华，PMP，PRINCE2，北京谷安天下科技有限公司，中国
邹国栋，CISA，CISM，CRISC，CGEIT，思科，中国

评审人员
Wu Hai Chuan，CISA，CISM，华为技术有限公司，中国
刘涤西，中国
顾伟，CISA，CRISC，CISM，CGEIT，CISSP，CCSP，GIAC MBA，(ISC)2 2017 APAC ISLA Honoree，阿斯利康，中国
冼嘉乐，CISA，CRISC，CISP，普华永道，中国香港
Darron Kin Kwok Sun，CISA，CRISC，信息技术部主管，香港房屋协会，中国香港
Kevin Yao，OSI (China) Co., Ltd.，中国
庄玉良，南京审计大学，中国

致谢
第3、5和6章中的一些内容参考北京谷安天下科技有限公司开发的知识体系和图表

本页为空白页