

NIST特别出版物800-12修订1

信息安全导论

迈克尔·尼尔斯
Kelley Dempsey Victoria
a Yan Pillitteri

该出版物可从<https://doi.org/10.6028/NIST.SP.800-12r1>免费获得

COMPUTER SECURITY



NIST特別出版物800-12

修订1

信息安全概论

迈克尔·尼尔斯
凯利·邓普西

Victoria Yan Pillitteri
计算机安全事业部信息技术实验室

该出版物可从<https://doi.org/10.6028/NIST.SP.800-12r1>免费获得

2017年6月



U.S. Department of Commerce Wilbur L.
Ross, Jr., Secretary

National Institute of Standards and Technology Kent Rochford, Acting NIST Director and Under Secretary of Commerce for
Standards and Technology

权威

本出版物由NIST根据2014年《联邦信息安全现代化法案》(FISMA), 44 U.S.C. § 3551 *et seq*规定的法定责任开发。公法(P.L.) 113-283。NIST负责制定信息安全标准和指南，包括联邦系统的最低要求，但未经适当的联邦官员对此类系统行使政策权力的明确批准，此类标准和指南不得适用于国家安全系统。本指南与管理与预算办公室(OMB)通告A-130的要求一致。

本出版物中的任何内容都不应与商务部长根据法定权力对联邦机构制定的强制性和约束性标准和指南相抵触。这些指导方针也不应被解释为改变或取代商务部长、行政管理和预算局局长或任何其他联邦官员的现有权力。本出版物可由非政府组织在自愿的基础上使用，在美国不受版权保护。然而，NIST会对署名表示赞赏。

美国国家标准与技术研究院特别出版物800-12修订版1
Natl. 站立。技术。Spec. Publ. 800-12 Rev. 1, 101页(2017年6月)
代码:nspue2
该出版物可从<https://doi.org/10.6028/NIST.SP.800-12r1>免费获得

为了充分描述实验过程或概念，可能会在本文档中识别某些商业实体、设备或材料。这样的标识并不意味着NIST的推荐或认可，也不意味着实体、材料或设备一定是最好的。

根据指定的法定职责，本出版物中可能会引用NIST目前正在开发的其他出版物。本出版物中的信息，包括概念和方法，甚至可以在此类配套出版物完成之前由联邦机构使用。因此，在每份出版物完成之前，现有的要求、指南和程序(如果存在)仍然有效。出于规划和过渡的目的，联邦机构可能希望密切关注NIST这些新出版物的发展。

鼓励各组织在公众评议期间审查所有出版物草案，并向NIST提供反馈。许多NIST网络安全出版物，除了上面提到的，都可以在<http://csrc.nist.gov/publications>上找到。

对本出版物的评论可提交至：

国家标准与技术研究院
分会场:信息技术实验室计算机安全研究室
盖瑟斯堡100 Bureau Drive (Mail Stop 8930), 马里兰州20899-8930
邮箱:sec-cert@nist.gov

所有评论均根据《信息自由法》(Freedom of Information Act, FOIA)进行发布。

计算机系统技术报告

国家标准与技术研究院(NIST)的信息技术实验室(ITL)通过为国家的测量和标准基础设施提供技术领导，促进了美国的经济和公共福利。ITL开发测试、测试方法、参考数据、概念验证实现和技术分析，以推进信息技术的开发和生产性使用。ITL的职责包括制定管理、行政、技术和物理标准和指导方针，以经济有效地保护联邦系统中除国家安全相关信息以外的其他信息的安全和隐私。特别出版物800系列报告了ITL在系统安全方面的研究、指导方针和扩展工作，以及它与工业、政府和学术组织的合作活动。

摘要

组织严重依赖于使用信息技术(IT)产品和服务来运行他们的日常活动。确保这些产品和服务的安全性对组织的成功至关重要。本刊物介绍了资讯保安原则，机构可借此了解其各自系统的资讯保安需要。

关键词

保证;计算机安全;信息安全;导论;风险管理;安全管控;安全要求

致谢

作者要感谢每一位花时间审查和评论本出版物草案的人，特别是美国国家标准与技术研究所(NIST)的Celia Paulsen、Ned Goren、Isabel Van Wyk和Rathini Vijayaverl。作者还要感谢原作者Barbara Guttman和Edward A. Roback，以及所有为本出版物的原始版本做出贡献的个人。

目录目录

1 简介	1
1.1 目的.....	1
1.2 受众群体	1
1.3 组织机构.....	1
1.4 重要术语	2
1.5 联邦信息安全计划法律基础	3
1.6 相关NIST出版物	4
2 信息安全要素	7
2.1 信息安全支持组织的使命.....	7
2.2 信息安全是健全管理的一个组成部分	8
2.3 资讯安全保护措施已落实到位 有风险	8
2.4 明确信息安全角色和职责.....	9
2.5 系统所有者的信息安全责任超越了自身 组织	9
2.6 信息安全需要综合综合的方法	9
2.6.1 安全控制的相互依赖性	10
2.6.2 其他相互依赖关系	10
2.7 定期评估和监测信息安全.....	10
2.8 信息安全受到社会和文化因素的制约.....	11
3 角色职责	13
3.1 风险执行职能(高级管理层)	13
3.2 首席执行官(CEO)	13
3.3 首席信息官(CIO)	14
3.4 信息所有者/管家	14
3.5 高级机构信息安全官(SAISO)	14
3.6 授权官员(AO)	15
3.7 授权官方指定代表	15
3.8 高级隐私机构官员(SAOP).....	15
3.9 公共控制提供商.....	15
3.10 系统所有者	16
3.11 SSO (System Security Officer)	16

3.12 信息安全架构师	16
3.13 系统安全工程师(SSE)	17
3.14 安全控制评估员	17
3.15 系统管理员	17
3.16 用户	17
3.17 配角	18
4 威胁和漏洞:简要概述	20
4.1 对抗性威胁来源和事件的例子	20
4.1.1 欺诈和盗窃	21
4.1.2 内部威胁	22
4.1.3 恶意黑客	22
4.1.4 恶意代码	23
4.2 非对抗性威胁源和事件示例	24
4.2.1 错误与遗漏	24
4.2.2 物理和基础设施支持的丧失	24
4.2.3 信息共享对个人隐私的影响	25
5 信息安全政策	26
5.1 标准、指南和程序	26
5.2 项目政策	27
5.2.1 计划政策的基本组成部分	27
5.3 具体问题政策	28
5.3.1 特定问题策略示例主题	28
5.3.2 特定问题策略的基本组成部分	29
5.4 系统特定策略	30
5.4.1 安全目标	31
5.4.2 操作安全规则	31
5.4.3 系统特定策略实现	32
5.5 相互依赖	32
5.6 成本考虑	33
6 信息安全风险管理	34
6.1 Categorize	36
6.2 选择	36

6.3 实现	37
6.4 评估	37
6.5 授权	37
6.6 监控	37
7 保证	38
7.1 授权	38
7.1.1 授权与保证	39
7.1.2 类似情况下产品运营授权	39
7.2 安全工程	39
7.2.1 规划与保障	39
7.2.2 设计与实现保证	39
7.3 运行保证	41
7.3.1 安全与隐私控制评估	42
7.3.2 审计方法和工具	42
7.3.3 监控方法和工具	44
7.4 相互依赖关系	46
7.5 成本考虑	46
8 系统支持和操作安全注意事项	47
8.1 用户支持	47
8.2 软件支持	48
8.3 配置管理	48
8.4 备份	49
8.5 Media Controls	49
8.6 文档	49
8.7 维护	50
8.8 相互依赖	50
8.9 成本考虑	51
9 Cryptography	52
9.1 密码学的使用	52
9.1.1 数据加密	52
9.1.2 完整性	53
9.1.3 电子签名	53

9.1.4 用户认证	54
9.2 实现问题	54
9.2.1 选择设计与实现标准	55
9.2.2 选择软件、硬件或固件实现 ..	55
9.2.3 管理密钥	55
9.2.4 加密模块安全	56
9.2.5 将密码学应用于网络	56
9.2.6 遵守导出规则	57
9.3 相互依赖	57
9.4 成本考虑	58
9.4.1 直接成本	58
9.4.2 间接成本	58
10 控制家庭	59
10.1 访问控制(AC)	59
10.2 意识与培训(AT)	59
10.3 审计与问责(AU)	60
10.4 CA (Assessment, Authorization, and Monitoring)	60
10.5 配置管理(CM)	61
10.6 应急规划(CP)	61
10.7 识别与认证(IA)	62
10.8 个人参与(IP)	63
10.9 事件响应(IR)	64
10.10 维护(MA)	64
10.11 媒体保护(MP)	65
10.12 隐私授权(PA)	65
10.13 物理与环境保护(PE)	66
10.14 规划(PL)	67
10.15 项目管理(PM)	67
10.16 人事安全(PS)	68
10.17 风险评估(RA)	68
10.18 系统与服务获取(SA)	69
10.19 系统与通信保护(SC)	69

10.20系统和信息完整性(SI)	70
-------------------------	----

附录列表

Appendix A— 参考文献	71
Appendix B— 词汇表	76
Appendix C— 缩略语	88

图表列表

图1 -风险管理框架(RMF)概述	36
-------------------------	----

1 介绍

1.1 目的

对于那些刚接触信息安全的人以及那些不熟悉NIST信息安全出版物和指南的人来说，本出版物是一个起点。本特别出版物的目的是通过介绍相关概念和安全控制族(如NIST SP 800-53中定义的)，提供信息安全原则的高级概述。联邦信息系统和组织的安全和隐私控制，组织可以利用这些控制来有效地保护他们的系统¹和信息。为了更好地理解后面描述的安全控制族的含义和意图，本出版物首先让读者熟悉各种信息安全原则。

在介绍了这些安全原则之后，该出版物提供了多个安全控制族的详细描述以及每个控制族的好处。重点不是向组织强加需求，而是探索将特定控制族应用于组织系统的可用技术，并解释采用所选控制的好处。

由于本出版物提供了信息安全的介绍，因此不包括有关如何实施安全控制或如何检查安全控制有效性的详细步骤。相反，可能提供有关特定主题的更详细信息的单独出版物将被注明作为参考。

1.2

本出版物的目标读者是那些不熟悉信息安全原则和原则的人，这些原则和原则需要以与风险相称的方式保护信息和系统。本出版物为任何负责或有兴趣了解如何保护系统的人提供了基本的概念和思想基础。

因此，对于任何寻求更好地理解信息安全基础知识或对该主题有高级见解的人来说，本出版物是一个很好的资源。本出版物中描述的技巧和技术可以应用于任何类型的组织中的任何类型的信息或系统。虽然联邦组织、学术界和私营部门在各自系统内处理、存储和传播信息的方式可能存在差异，但信息安全的基本原则适用于所有组织。

1.3 组织

本刊物组织架构如下：

- 第1章描述了目的、目标受众、重要术语、信息安全的法律基础，以及与信息安全和信息风险管理相关的NIST出版物列表。

¹ System is defined in SP 800-53 as any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions.

- 第2章列出了有关信息安全的八个主要要素。
- 第3章概述了几个角色、支持角色，以及这些角色在向组织提供信息安全方面的各自职责。
- 第4章介绍了威胁和漏洞，区分了两者的区别，并提供了不同威胁来源和事件的示例。
- 第5章讨论了信息安全策略以及程序策略、特定问题策略和特定系统策略之间的区别。
- 第6章考虑如何管理风险，并简要描述了NIST风险管理框架(RMF)的六个步骤。
- 第7章侧重于信息保障以及可以采取哪些措施来保护信息和系统。
- 第8章介绍系统支持和操作，它们共同起着运行系统的作用。
- 第9章提供了密码学的简要概述，以及几个NIST 800系列出版物，其中包含关于特定加密技术的额外更详细的信息。
- 第10章介绍了20个信息安全和隐私控制家族。
- 附录A提供了参考文献列表。
- 附录B提供了整个文档中使用的术语词汇表。
- 附录C提供了整个文档中使用的缩略语列表。

1.4 重要术语

“信息系统”一词由44 u.s.c.第3502节定义为“为收集、处理、维护、使用、共享、传播或处置信息而组织的一组离散的信息资源”。

在本出版物中，使用术语“系统”代替术语“信息系统”，以反映任何规模或复杂性的信息资源的更广泛的适用性，这些信息资源是明确为收集、处理、使用、共享、传播、维护或处置数据或信息而组织的。其他一些需要熟悉的关键术语有:²

- 信息-(1)事实或想法，可以表示(编码)为各种形式的数据;(2)可以在系统实体之间交流的任何媒介或形式的知识(例如，数据、指令)。
- 信息安全——保护信息和信息系统免受未经授权的访问、使用、披露、中断、修改或破坏，以确保机密性、完整性和可用性。
- 保密性-保留对信息访问和披露的授权限制;

² These terms and definitions were retrieved from CNSSI 4009, *Committee on National Security Systems (CNSS) Glossary*, dated April 6, 2015.

包括保护个人隐私和专有信息的手段。

- 完整性-防止不当的信息修改或破坏，并确保信息的不可否认性和真实性。
 - o 数据完整性-数据未以未经授权的方式被更改的属性。数据完整性包括存储、处理和传输过程中的数据。
 - o 系统完整性—系统在不受损害的情况下执行其预期功能时所具有的质量，不受未经授权的操作，无论是有意的还是意外的。

可用性-确保及时、可靠地获取和使用信息。

- 安全控制3—为保护系统及其信息的机密性、可用性和完整性而规定的管理、操作和技术控制(即保障措施或对策)。

1.5 联邦信息安全计划的法律基础

在联邦政府内部，许多法律法规要求联邦组织保护其系统、系统处理、存储或传输的信息以及相关的技术资源(例如，电信)。下面列出了这些法律法规的样本。

- 《[1987年计算机安全法](#)》要求各机构识别敏感系统，开展计算机安全培训，并制定[计算机安全计划](#)。[1987年计算机安全法](#)被[2002年联邦信息安全管理法\(FISMA\)](#)所取代，如下所述。
- 《[联邦信息资源管理条例](#)》(FIRMR)是联邦政府使用、管理和获取计算机资源的主要法规。该法根据[1996年《信息技术管理改革法》\(ITMRA\)](#)被废除，该法案被重新命名为《[克林格-科恩法案](#)》。
- 《[2002年电子政务法](#)》旨在通过在[管理和预算办公室\(OMB\)](#)内设立联邦首席信息官(CIO)，加强对电子政府服务和流程的管理和促进。并通过建立一个广泛的措施框架，要求使用基于互联网的信息技术来增强公民获得政府信息和服务的机会，并改进政府的运作方式。

³ In this document, the terms *security controls*, *safeguards*, *security protections*, and *security measures* have been used interchangeably.

- 《联邦信息安全管理法》(FISMA)作为《2002年电子政务法》的一部分颁布，旨在解决具体的信息安全需求，包括但不限于提供：为确保对支持联邦运作和资产的信息资源进行有效的信息安全控制提供了一个全面的框架；以及制定和维护保护联邦信息和系统所需的最低控制措施(如公法107-347第301条所述)。
- 2014年《联邦信息安全现代化法案》是对FISMA的一项修正案，该法案对联邦安全实践进行了几项修改，以实现联邦安全实践的现代化，并促进和加强持续监控的使用。
- OMB通告A-130，联邦信息资源管理，要求联邦机构建立包含特定元素的信息安全和隐私计划。
- 适用的OMB备忘录。

这不是与联邦系统相关的法律法规的全面列表。根据联邦机构存储、处理和传播的信息类型，对联邦机构有更具体的要求。此外，一些影响非政府组织的现行法律并未包括在此列表中。这些法律的例子包括：要求保护健康信息隐私和安全的《健康保险流通与责任法案》(HIPAA)；《萨班斯-奥克斯利法案》(Sarbanes-Oxley Act, SOX)要求保护公众免受金融系统中的会计错误和欺诈行为的影响。

联邦管理人员有责任熟悉并遵守适用的法律要求。然而，法律法规通常不会提供保护信息的详细说明。相反，它们规定了广泛而灵活的要求，例如限制个人数据仅供授权用户使用。本出版物为开发有效的、全面的信息安全方法以满足适用的法律或政策提供了指导。

1.6 相关NIST出版物

当涉及到信息安全和风险管理时，有一组特定的联邦信息处理标准(FIPS)和NIST特殊出版物(SP)适用。它们包括：

- FIPS 199 - 联邦信息和信息系统安全分类标准，列出了信息和系统分类的标准，这反过来又提供了一个共同的框架和理解，以促进有效管理和一致报告的方式表达安全。
- FIPS 200 - 联邦信息和信息系统的最低安全要求，规定了支持联邦政府执行机构的信息和系统的最低安全要求，以及基于风险的过程

用于选择必要的安全控制以满足最低安全要求。

- **SP 800-18** -制定系统安全计划指南，描述了制定系统安全计划的程序，提供了系统安全要求的概述，并描述了为满足这些要求而实施或计划的控制措施。
- **SP 800-30** -进行风险评估指南，为联邦系统和组织进行风险评估提供指导。
- **SP 800-34** -联邦信息系统应急计划指南，帮助组织理解信息系统应急计划(iscp)开发的目的、过程和格式，并提供实用的、现实世界的指导方针。
- **SP 800-37** -系统风险管理框架应用指南:安全生命周期方法提供了将风险管理框架应用于联邦系统的指导方针，包括进行安全分类、安全控制选择和实施、安全控制评估、系统授权和安全控制监控等活动。
- **SP 800-39** -管理信息安全风险:组织、使命和信息系统视图，为建立一个集成的、组织范围的方案提供指南，用于管理组织运营(如使命、职能、形象和声誉)、资产、个人、其他组织的信息安全风险。和国家由于联邦系统的运行和使用而产生的信息安全风险。
- **SP 800-53** -系统和组织的安全和隐私控制，为支持联邦政府执行机构的组织和系统选择和指定安全控制提供指导，以满足FIPS出版物200的要求。
- **SP 800-53A** -评估系统和组织中的安全和隐私控制:建立有效的评估计划，提供(i)建立有效的安全评估计划和隐私评估计划的指南;及(ii)用于评估支持联邦政府执行机构的系统和组织所采用的安全控制和隐私控制有效性的一套全面程序。
- **SP 800-60** -将信息和信息系统类型映射到安全类别指南，协助各机构始终如一地将安全影响级别映射到以下类型:(i)信息(例如，隐私、医疗、专有、金融、承包商敏感、商业秘密、调查);以及(ii)系统(例如，关键任务、任务支持、行政)。

- **SP 800-128** -信息系统的安全配置管理指南，为负责管理和管理联邦系统和相关操作环境安全的组织提供指南。
- **SP 800-137** -联邦信息系统和组织的信息安全持续监控(*ISCM*)，协助组织制定ISCM战略和实施ISCM计划，提供威胁和漏洞的意识，对组织资产的可见性;以及部署的安全控制措施的有效性。

2 信息安全要素

本出版物涉及信息安全的八个主要要素，以帮助读者更好地理解第10章中讨论的安全要求和控制是如何支持组织的整体运作的。这八个概念分别是：

1. 信息安全支持组织的使命。
2. 信息安全是健全管理的一个组成部分。⁴
3. 实施与风险相称的信息安全保护措施。
4. 明确信息安全角色和职责。
5. 系统所有者的信息安全责任超出了他们自己的组织。
6. 信息安全需要全面整合。
7. 定期评估和监测信息安全。
8. 信息安全受到社会和文化因素的制约。

2.1 信息安全支持组织的使命

在第一章中，信息安全被定义为保护信息和系统免受未经授权的访问、使用、披露、中断、修改或破坏，以提供机密性、完整性和可用性。仔细实施信息安全控制对于保护组织的信息资产以及其声誉、法律地位、人员和其他有形或无形资产至关重要。

组织无法选择和实施适当的安全规则和程序，可能会对组织的使命产生负面影响。然而，为保护重要资产而精心选择的安全规则和程序可以支持整个组织的使命。在今天恶意代码、系统破坏和内部威胁的环境中，公开的安全问题可能会产生可怕的后果，特别是对组织的盈利能力和声誉。当适当的安全保护措施到位时，私营和公共部门的组织可以提高利润和为客户提供服务。因此，信息安全是达到目的的一种手段，而不是目的本身。

了解组织的使命以及每个系统如何支持该使命是至关重要的。在定义了系统的角色之后，还可以定义该角色中隐含的安全需求。然后，就可以根据组织的使命明确地说明安全性。

系统的角色和功能可能不局限于单个组织。在组织间系统中，每个组织都能从保护系统中获益。例如，为了使电子商务取得成功，每个参与者都需要安全控制来

⁴ In the context of this publication, sound management refers to due diligence in taking all practical steps to ensure that information security management decisions are made in such a way that they not only protect the information stored, processed, and transmitted by an organization, but also the systems that fall under the purview of the organization.

保护他们的资源。买方系统上良好的安全性也使卖方受益;买方的系统不太可能被用于欺诈，变得不可用，或者以其他方式对卖方产生负面影响。(反之亦然。)

2.2 信息安全是健全管理的一个组成部分

考虑到安全控制的成本，管理人员最终负责确定特定系统和整个组织的可接受风险水平。由于信息安全风险不可能完全消除，因此目标是在保护信息或系统与利用可用资源之间找到最佳平衡。对于系统和相关流程来说，在考虑资源可用性的同时，具备保护信息、金融资产、实物资产和员工的能力是至关重要的。

当组织的信息和系统与外部系统相关联时，管理层的责任就会扩展到组织边界之外。这可能要求管理层(1)知道外部系统采用了什么一般级别或类型的安全，和/或(2)寻求确保外部系统为组织的信息和系统提供足够的安全。例如，云服务提供商(csp)和云供应链参与者可能承担存储、处理和传输组织信息的管理角色。然而，这并不能使组织⁵免于任何与安全相关的责任。组织有责任确保csp和云供应链参与者为存储、处理和传输的信息提供适当的安全级别。

2.3 实施信息保护，使其与风险相称

系统的风险永远不可能完全消除。因此，通过在可用性和安全保护的实施之间取得平衡来管理风险至关重要。风险管理的主要目标是实现与风险相称的安全保护。应用不必要的保护可能会浪费资源，使系统更难使用和维护。相反，不应用保护系统所需的保护可能会使系统及其信息在保密性、完整性和可用性方面容易受到破坏，所有这些都可能阻碍甚至停止组织的使命。

联邦组织使用影响等级(高、中、低)来识别和分类信息和/或系统的机密性、完整性或可用性丧失可能对组织运营产生的影响，并允许他们识别适当的保护措施。信息和系统的准确分类对于确定如何保护与风险相称的信息是不可或缺的。安全类别传达了机密性、完整性或可用性丧失可能对组织使命产生的影响。要确定系统的影响级别，组织可以参考FIPS 199、NIST SP 800-30和NIST SP 800-60中的指导。

⁵ An organization is an entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements).

系统影响级别的准确确定提供了从NIST SP 800-53中选择一组适当的安全控制所需的信息。选择过程包括评估实施和维护安全控制的成本以及应用这些控制所带来的预期安全效益(即风险降低)。

安全效益包括直接成本和间接成本。直接成本包括购买、安装和管理安全保护措施(如访问控制软件或灭火系统)。间接成本可能影响系统和业务绩效、员工士气或再培训需求。在某些情况下，间接成本可能超过控制的直接成本。组织管理人员负责权衡适当保护实施的成本与收益，并做出基于风险的决策。

2.4 明确信息安全角色和责任

系统所有者、公共控制提供者、授权官员、系统安全官员、用户和其他人的角色和职责是明确的，并形成文件。如果职责不明确，管理层可能会发现很难让人员对未来的后果负责。

记录信息安全责任并不取决于组织的规模。即使是小的组织也可以准备一份文件，陈述组织的方针，并确定一个系统或整个组织的信息安全责任。

角色和职责在本出版物的第3章中进行了简要讨论。有关关键信息安全参与者的详细信息，请参阅NIST SP 800-37的附录D。

2.5 系统所有者的信息安全责任超出了他们自己的组织

系统的用户并不总是位于他们使用或可以访问的系统的边界内。例如，当两个或多个系统之间存在互连时，参与组织可能会分担信息安全责任。在这种情况下，系统所有者有责任分享组织所使用的安全措施，以使用户相信系统是充分安全的，能够满足安全要求。除了共享与安全相关的信息外，事件响应团队还有责任及时响应安全事件，以防止对组织、人员和其他组织造成损害。

2.6 信息安全需要全面、综合的方法

提供有效的信息安全，需要综合考虑信息安全领域内外的各种领域。这种方法适用于整个系统生命周期。

例如，纵深防御是一种安全原则，通过实施多层安全对策，保护组织信息和系统免受威胁。纵深防御利用管理防御(例如，策略、程序)和安全技术(例如，入侵检测系统、防火墙、配置设置和防病毒软件)与物理安全防御(例如，大门、警卫)相结合，以最大限度地减少成功的可能性。

对系统的攻击。这些措施不仅有助于减少安全漏洞危及对系统资产的访问或对机密性、完整性或可用性产生有害影响的可能性，而且一旦发起攻击，还可以向组织提供近乎实时的通知。

2.6.1 安全控制的相互依赖关系

安全控制很少作为问题的独立解决方案来实施。当与另一种或一组控制措施配合使用时，它们通常会更有效。安全控制，如果选择得当，可以对系统的整体安全性产生协同效应。NIST SP 800-53中的每个安全控制都有一个相关的控制部分，列出了与该特定控制相补充的安全控制。如果用户不了解这些相互依赖关系，其结果可能对系统有害。

2.6.2 其他相互依赖关系

安全控制之间和之间的相互依赖关系并不是影响安全控制有效性的唯一因素。系统管理、法律约束、质量保证、隐私问题以及内部和管理控制也会影响所选控制的功能。系统管理人员必须能够认识到信息安全与物理和环境安全等其他安全学科之间的关系。在实施更全面的安全策略时，了解这些关系如何协同工作将被证明是有益的。NIST SP 800-160，*系统安全工程:可信赖安全系统工程中多学科方法的考虑*，提供了关于可信赖系统工程考虑的更详细的信息。

当系统连接到其他系统或与全球分布式供应链生态系统互连时，了解安全控制之间的关系尤为重要。供应链由公共和私营部门实体组成，并使用地理上不同的路线来提供高度精细、具有成本效益、可重复使用的信息和通信技术(ICT)解决方案。有关供应链风险管理的更多信息，请参见NIST SP 800-161，*联邦信息系统和组织的供应链风险管理实践*。

2.7 定期对信息安全进行评估和监控

信息安全不是一个静态的过程，需要持续的监控和管理，以保护信息的机密性、完整性和可用性，并确保快速识别新的漏洞和不断发展的威胁并做出相应的响应。在不断发展的劳动力和技术环境中，组织在可接受的风险水平下运行时提供及时准确的信息至关重要。

信息安全持续监控(ISCN)在NIST SP 800-137中定义为对信息安全、漏洞和威胁的持续意识的维护，以支持组织的风险管理决策。ISCN提供了对组织风险承受能力的清晰理解，以帮助官员以一致的方式确定优先事项和管理整个组织的风险。ISCN确保所选择的安全控制保持有效，并保持组织对威胁和漏洞的意识。

有关持续监测基础和持续监测过程的更详细信息，请参阅NIST [SP 800-137](#)。还可以利用NIST [SP 800-53A](#)来提供对评估程序的见解。

2.8 信息安全受到社会和文化因素的制约

社会因素影响个人如何理解和使用系统，从而影响系统和组织的信息安全。个人以不同的方式感知、推理和做出基于风险的决策。为了解决这个问题，组织使信息安全功能透明、易于使用和理解。此外，定期提供安全意识培训可以减轻风险感知的个体差异。与社会因素一样，在处理信息安全时，组织如何开展业务可以作为一个值得考虑的文化因素。一个组织自身的文化会影响其对信息安全的响应。仔细解释与业务实践相关的风险有助于提高所推荐的信息安全实践的透明度和接受度。

组织有责任在信息安全需求和可用性之间找到平衡。组织可以利用各种工具来满足其系统的安全需求，而不会给用户带来过度的负担。例如，考虑一个系统，它要求用户在一个会话期间多次输入用户名和密码来访问不同的应用程序。在这种情况下，组织可以根据风险与用户便利性的考虑，选择哪种类型的应用程序(如果有的话)将允许密码和密码哈希存储。

隐私曾经被认为与信息安全无关——这两个功能被讨论得好像它们不能在系统中共存一样。今天，隐私和信息安全之间的共生关系是必不可少的。没有信息安全的基本基础，组织就无法保护个人的隐私。然而，隐私不仅仅是安全，因为它还涉及到个人在整个数据生命周期中对其信息进行授权处理可能会遇到的问题。保护个人隐私是收集、使用、维护、共享和处理个人信息(PII)的组织的基本责任。有关更详细的隐私信息，请参阅[NISTIR 8062](#)，[联邦系统隐私工程和风险管理一个](#)和[NIST SP 800-122](#)，[保护个人信息\(P II\)机密性指南](#)。

总体而言，安全与社会规范之间的关系不一定是对立的。社会规范对信息安全既有正面影响，也有负面影响。例如，对信息安全的负面影响可以从用户写下密码并将其放在电脑附近的形式中看到。积极的影响可以通过更广泛地实施多因素身份验证来看到——为了让用户重置密码，需要多种形式的身份验证(例如，向用户发送文本消息，物理令牌)。安全性可以通过提供更准确和可靠的信息以及更大的系统可用性来增强数据和信息的访问和流动。安全机制还可以增强个人隐私(例如，加密)。一些安全机制可能会出现新的漏洞(例如，单点登录)。因此，重要的是要考虑如何以优化更广泛的社会目标的方式实现安全解决方案。

社会规范改变了，对系统的信息安全保护也必须改变。目前足够的安全控制可能无法跟上不断变化的计算环境。组织的文化和安全环境在员工的风险感知中也起着重要作用。安全标准的不充分或不存在可能导致组织安全态势的退化。提供更新和反复的培训，说明什么是组织系统的可接受使用，什么是不可接受的使用，有助于保障系统的整体安全性。

3 角色与职责

下一章概述了具体的组织角色及其各自的职责。明确定义的角色和职责通过指定谁负责执行某些任务，有助于组织及其员工以更有效的方式工作。在大型组织中，这将有助于确保没有任何任务被忽视。在规模较小、结构较松散的组织中，工作量可以分配得更均匀，因为员工可能需要承担多项任务。

下面提供的列表并不是一个组织中所有可能的角色的全面列表。每个组织可能会根据自己的使命或组织结构定义自己的特定角色或有不同的命名约定。但是，基本功能保持不变。有关分配给每个角色的职责的更详细描述，请参见NIST [SP 800-37中的附录D](#)。

3.1 风险执行功能(高级管理层)

风险执行功能是指组织内的个人或团体(如董事会成员、CEO、首席信息官)负责确保:(i)从组织范围的角度看待单个系统的风险相关考虑，考虑到组织在执行其核心任务和业务功能时的总体战略目标，以及(ii)系统相关安全风险的管理在整个组织内是一致的。反映组织的风险承受能力，并与其他类型的风险一起考虑，以确保任务/业务的成功。

职责包括但不限于:

- 定义一个整体的方法来解决整个组织的风险;
- 制定组织风险管理策略;
- 支持授权官员和组织内其他高级领导人之间的信息共享;以及
- 监督整个组织的风险管理相关活动。

3.2 首席执行官(CEO)

首席执行官是组织中负责提供与对组织运营资产、个人、其他组织的危害(即影响)的风险和程度相称的信息安全保护的最高级别高级官员或高管。和国家可能因未经授权的访问、使用、披露、中断、修改或销毁:(i)由组织或代表组织收集或维护的信息;以及(ii)由某一机构、某一机构的承包商或代表某一机构的另一组织使用或操作的系统。

职责包括但不限于:

- 确保信息安全管理流程与战略和运营规划流程的整合;
- 确保用于支持组织运营的信息和系统具有适当的信息安全保障措施;以及

- 确认受过培训的人员遵守相关的信息安全法规、政策、指令、说明、标准和指南。

3.3 首席信息(CIO)

首席信息官为组织官员，负责:(i)指定高级机构信息安全官;(ii)制定和维护安全政策、程序和控制技术，以满足所有适用要求;(iii)监督对信息安全负有重要责任的人员，并确保人员接受充分培训;(iv)协助高级组织官员履行其安全职责;(v)与其他高级官员协调，每年报告本组织信息安全计划的总体有效性，包括补救行动的进展情况。

职责包括但不限于:

- 分配资源专门用于保护支持组织使命和业务功能的系统;
- 确保系统受到批准的安全计划的保护，并被授权运行;以及
- 确保组织范围内的信息安全计划得到有效实施。

3.4 信息所有者/管理员

信息所有者/管理者是对特定信息具有法定、管理或操作权限的组织官员，负责建立管理信息生成、收集、处理、传播和处置的政策和程序。

职责包括但不限于:

- 制定适当使用和保护主体信息的规则;以及
- 向系统所有者提供有关充分保护主题信息所需的安全要求和安全控制的输入。

3.5 高级资讯保安主任(SAISO)

高级资讯保安主任是一名组织官员，负责:(i)执行FISMA规定的首席信息官安全职责;以及(ii)担任首席信息官与组织授权官员、系统所有者、通用控制提供商和系统安全官员之间的主要联络人。在一些组织中，这个角色可能也被称为首席信息安全官(CISO)。

职责包括但不限于:

- 管理和实施组织范围的信息安全计划;以及
- 在需要时担任授权官方指定代表或安全控制评估员的角色。

3.6 授权官员(AO)

授权官员是一名高级官员或行政人员，有权正式承担责任，以对组织业务和资产、个人和其他组织构成可接受的风险水平运行系统。

职责包括但不限于：

- 批准安全计划、协议或谅解备忘录、行动计划和里程碑，以及确定系统或操作环境的重大变更是否需要重新授权；以及
- 确保授权的官方指定代表执行与安全授权相关的所有活动和职能。

3.7 授权官员指定代表

授权官员指定代表是代表授权官员协调和执行与安全授权流程相关的所需日常活动的组织官员。指定代表履行AO的职能，但不能为系统承担风险。

职责包括但不限于：

- 执行指定的授权官员的职责；
- 就安全授权流程的规划和资源配置、安全计划的批准、行动计划和里程碑的批准和监督实施以及风险的评估和/或确定做出决策；及
- 准备最终授权包，获得授权官员在授权决策文件上的签名，并将授权包传递给相应的组织官员。

3.8 机构隐私高级官员(SAOP)

机构隐私高级官员是一名高级组织官员，负责确保机构实施信息隐私保护，包括机构完全遵守与信息隐私相关的联邦法律、法规和政策，如《隐私法》。

职责包括但不限于：

- 监督、协调和促进机构的隐私合规工作；
- 审查机构的信息隐私程序，以确保其全面和最新；以及
- 确保机构雇员和承包商接受有关信息隐私法律、法规、政策和管理机构处理个人信息程序的适当培训和教育计划。

3.9 公共控制提供者

公共控制提供者是负责公共控制(即安全性)的开发、实现、评估和监控的个人、团体或组织

系统继承的控件)。

职责包括但不限于:

- 在安全计划(或组织规定的等效文件)中形成组织确定的通用控制措施的文件;以及
- 确保由组织规定的具有适当独立性的合格评估人员对公共控制进行必要的评估。

3.10 系统所有者

系统所有者是负责采购、开发、集成、修改、操作、维护和处理系统的组织官员。

职责包括但不限于:

- 处理用户群体的操作利益(即，需要访问系统以满足任务、业务或操作需求的用户);
确保符合信息安全要求;以及
- 制定和维护系统安全计划，确保系统按照商定的安全控制部署和运行。

3.11 系统安全官(SSO)

系统安全官负责确保系统维持适当的运作保安状态，并因此与系统拥有人密切合作。

职责包括但不限于:

- 监督系统的日常安全操作;以及
- 协助制定安全政策和程序，并确保这些政策和程序得到遵守。

3.12 信息安全架构师

信息安全架构师是负责确保在企业架构的所有方面(包括参考模型、分段和解决方案模型)充分处理保护组织核心任务和业务流程所必需的信息安全需求的个人、团体或组织。以及支持这些任务和业务过程的最终系统。

职责包括但不限于:

- 作为企业架构师和信息安全工程师之间的联络人;以及
- 与系统所有者、公共控制提供者和系统安全官员协调，将安全控制分配为系统特定的、混合的或公共的控制。

3.13 系统安全工程师(SSE)

系统安全工程师是负责进行系统安全工程活动的个人、团体或组织。

职责包括但不限于:

- 设计和开发组织系统或升级遗留系统;以及
- 与信息安全架构师、高级机构信息安全官员、系统所有者、公共控制提供商和系统安全官员协调安全相关活动。

3.14 安全控制评估员

安全控制评估员是一个个人、团体或组织，负责对系统内使用或继承的管理、操作和技术安全控制和控制增强进行全面评估，以确定控制的总体有效性(即:控制被正确实施的程度，按预期运行的程度，以及在满足系统安全需求方面产生预期结果的程度)。

职责包括但不限于:

- 提供评估，以识别系统及其运行环境中的弱点或缺陷;
- 建议纠正措施，以解决已识别的漏洞;以及
- 准备包含评估结果和发现的安全评估报告。

3.15 系统管理员

系统管理员是负责设置和维护系统或系统的特定组件的个人、团体或组织。

职责包括但不限于:

- 安装、配置和更新硬件和软件;
- 建立和管理用户账号;
- 监督备份和恢复任务;以及
- 实施技术安全控制。

3.16 用户

用户是为了执行指定的职责而被授予访问组织信息的个人、团体或组织。

职责包括但不限于:

- 坚持管理可接受的组织系统使用的政策;
 - 仅为规定的目地使用组织提供的IT资源;以及
- 报告异常或可疑的系统行为。

3.17 配角

- 审计员。审核员负责检查系统，以确定:(i)系统是否符合规定的安全要求和组织政策;以及(ii)安全控制是否适当。非正式审核可以由被审核系统的运营者或公正的第三方审核员进行。
- 实物安全人员。物理安全办公室负责制定和实施适当的物理安全控制，通常与信息安全管理人、项目和职能经理以及其他人员协商。物理安全涉及中央系统安装、备份设施和办公环境。在政府中，这个办公室通常负责处理人员的背景调查和安全许可。
- 灾难恢复/应急计划人员。一些组织有单独的灾难恢复/应急计划人员。在这种情况下，该人员通常负责整个组织的应急计划，并与程序和职能经理/应用程序所有者、信息安全人员和其他人合作，根据需要获得额外的应急计划支持。
- 质量保证人员。许多组织已经建立了质量保证程序来改进他们提供给顾客的产品和服务。质量保证人员应具备信息安全的工作知识，以及如何利用信息安全来提高程序的质量(例如，确保基于计算机的信息的完整性、服务的可用性和客户信息的保密性)。
- 采购办公室人员。采购(或采购)办公室负责确保组织采购已由适当的官员进行审查。虽然采购办公室的工作人员缺乏保证货物和服务满足信息安全期望的技术专长，但他们仍然应该了解信息安全标准，并应将潜在的信息安全问题提请请求此类技术的人注意。
- 培训办公室工作人员。组织确定培训用户、操作员和信息安全管理的主要责任是由培训办公室还是由信息安全项目办公室承担。在任何一种情况下，这两个组织都应共同努力，制定有效的培训计划。
- 人力资源。人力资源办公室通常是经理们在决定是否需要对某一特定职位进行安全背景调查时需要协助的第一个联络点。人力资源办公室和安全办公室通常在涉及背景调查的问题上密切合作。当员工离开公司时，人力资源办公室也可能负责与安全相关的离职手续。
- 风险管理/计划人员。一些组织雇佣专职人员专门分析组织可能面临的各种风险。虽然这个办公室通常关注组织的风险问题，但它也应该考虑信息

安全相关风险。特定系统的风险分析通常不由本办公室执行。

- 工厂物理人员。该办公室负责确保提供必要的服务，以确保组织系统的安全运行(例如，电力和环境控制)。该办公室通常配备独立的医疗、消防、危险废物或生命安全人员。
- 隐私办公室工作人员。该办公室负责维护一个全面的隐私计划，以确保遵守适用的隐私要求，制定和评估隐私政策，并管理隐私风险。本办公室包括一名负责隐私的高级授权官员、隐私合规和风险评估专家、法律专家和其他专注于管理隐私风险的专业人员，特别是与本出版物相关的信息安全措施可能产生的风险。

4 威胁和漏洞：简要概述

漏洞是系统、系统安全过程、内部控制或实现中的弱点，可能被威胁源利用。⁶漏洞使系统容易受到大量活动的影响，这些活动可能导致对个人、团体或组织造成重大的、有时是不可逆转的损失。这些损失的范围可以从笔记本电脑或移动设备上的单个文件损坏到运营中心的整个数据库受到损害。有了正确的工具和知识，攻击者就可以利用系统漏洞并访问存储在系统上的信息。对受损系统造成的损害可能因威胁来源而异。

威胁源可以是对抗性的，也可以是非对抗性的。对抗性威胁来源是寻求利用组织对网络资源依赖的个人、团体、组织或实体。即使是员工、特权用户和受信任的用户也会欺骗组织系统。非对抗性威胁来源是指自然灾害或个人在履行日常职责过程中采取的错误行为。

如果系统存在脆弱性，则威胁源可能导致威胁事件。威胁事件是指可能导致不良后果或影响的事件或情况。导致威胁事件的威胁源的一个例子是黑客在组织系统上安装击键监视器。威胁事件对系统造成的损害差别很大。有些威胁会影响系统中存储信息的机密性和完整性，而其他威胁只会影响系统的可用性。有关威胁来源和威胁事件的更多信息，请参阅NIST SP 800-30。

本章对当今系统运行的环境进行了广泛的概述，对于寻求更好地了解特定威胁环境的组织可能是有价值的。这里提供的列表并不是一个包罗万象的列表。这里提供的信息范围可能过于宽泛，针对特定系统的威胁可能与本章讨论的内容大不相同。

为了保护系统免受风险并实施最具成本效益的安全措施，系统所有者、管理人员和用户需要知道和理解系统的漏洞，以及可能利用漏洞的威胁来源和事件。在确定对已发现的漏洞的适当响应时，应注意在存在很少威胁或没有威胁的情况下尽量减少对漏洞的资源支出。有关威胁、漏洞、保障措施选择和风险响应如何相关的更详细信息，请参见第6章“信息安全风险管理”。

4.1 对抗性威胁来源和事件示例

上一节定义了威胁源和威胁事件。本节分别提供了几个示例，并附有说明。

⁶ Threat Source –The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability.

4.1.1 欺诈与盗窃

通过“自动化”传统的欺诈方法或利用新方法，系统可以被用于欺诈和盗窃。系统欺诈和盗窃可以由内部人员(即授权用户)和外部人员实施。获得授权的系统管理员和能够访问和熟悉系统的用户(例如，系统控制的资源、缺陷)往往是造成欺诈的原因。考虑到组织的前雇员对组织运作的了解，特别是在不及时终止其访问权的情况下，他们也会构成威胁。

经济利益是欺诈和盗窃背后的主要动机之一，但金融系统并不是唯一面临风险的系统。个人可以使用几种技术来收集他们本来无法获得的信息。其中一些技术包括：

- 社交媒体。无处不在的社交媒体(如Facebook、Twitter、LinkedIn)使网络犯罪分子能够利用该平台进行有针对性的攻击。网络犯罪分子利用容易制作、伪造和未经验证的社交媒体账户，可以冒充同事、客户服务代表或其他可信任的个人，以发送恶意代码的链接，窃取个人或敏感的组织信息。社交媒体加剧了持续存在的欺诈问题，组织在实施系统时应将其视为一个严重问题。社交媒体账户提供了一种收集目标个人的联系信息、兴趣和个人关系的手段，这些信息反过来又可以用来进行社会工程攻击。
- 社会工程。社会工程，在信息安全的背景下，是一种严重依赖人际互动来影响个人违反安全协议并鼓励个人泄露机密信息的技术。这些类型的攻击通常是通过电话或网络进行的。通过电话实施的攻击是最基本的社会工程攻击。例如，攻击者可能会误导一家公司，使其相信攻击者是该公司的现有客户，并让该公司泄露该客户的信息。在网上，这种技术被称为网络钓鱼——一种基于电子邮件的攻击，旨在欺骗个人进行有利于攻击者的行为(例如，点击链接或泄露个人信息)。社会工程在线攻击也可以通过使用包含恶意代码的附件来完成，这些附件以个人的地址簿为目标。获得的信息使攻击者可以向受害者地址簿中的所有联系人发送恶意代码，传播初始攻击的损害。
- 高级持续威胁(APT)。高级持续性威胁是一种试图获得特定数据和信息访问权限的长期入侵。APT攻击不是试图造成破坏，而是旨在从网络或目标中获取信息。一些APT攻击可能非常复杂，以至于要想不被网络中的入侵检测系统(ids)发现，它们需要管理员全天候重写代码。一旦收集到足够的网络信息，攻击者就可以创建一个后门，这是绕过系统安全机制的一种方式，并获得对网络的未被发现的访问权限。然后，攻击者利用外部命令和控制系统对系统进行持续监控，以提取信息。

4.1.2 Insider Threat

考虑到员工对雇主的系统和应用程序的熟悉程度，以及哪些行为可能造成最大的损害、恶作剧或混乱，他们可能代表着对组织的内部威胁。员工的破坏行为——通常是由知情或被解雇的威胁所煽动的——对组织及其系统来说是一个关键问题。为了减轻员工蓄意破坏所造成的潜在损害，被解雇的员工应立即禁止访问IT基础设施，并应将其拒之门外。

与系统相关的员工破坏行为的例子包括但不限于：

- 破坏硬件或设施；
- 植入恶意代码，破坏程序或数据；
- 错误输入数据、持有数据或删除数据；
- 系统崩溃；以及
- 更改管理密码以防止系统访问。

4.1.3 恶意黑客

恶意黑客是一个术语，用来描述那些利用对系统、网络和编程的理解来非法访问系统、造成破坏或窃取信息的个人或团体。了解驱动恶意黑客的动机可以帮助组织实施适当的安全控制，以防止系统破坏的可能性。恶意黑客是对抗性威胁的一个广泛类别，根据恶意黑客的具体行为或意图，可以细分为更小的类别。根据NIST SP 800-82《工业控制系统(ICS)安全指南》改编的一些子类别包括：

- 攻击者。攻击者闯入网络是为了刺激和挑战，或者是为了在攻击者社区中炫耀。虽然远程黑客攻击曾经需要相当的技能或计算机知识，但攻击者现在可以从互联网上下载攻击脚本和协议，并对受害者网站发动攻击。这些攻击工具变得更加复杂，也更容易使用。在某些情况下，攻击者并不具备威胁关键政府网络等困难目标的必要专业知识。尽管如此，全球范围内的攻击者构成了相对较高的威胁，即孤立的或短暂的中断，可能对企业或基础设施造成严重损害。
- 僵尸网络运营商。机器人网络运营商控制多个系统来协调攻击并分发网络钓鱼方案、垃圾邮件和恶意代码。被破坏的系统和网络的服务可以在网上的地下市场找到(例如，购买拒绝服务攻击，使用服务器中继垃圾邮件或网络钓鱼攻击)。
- 犯罪集团。犯罪集团寻求攻击系统以获取金钱利益。具体来说，有组织的犯罪集团使用垃圾邮件、网络钓鱼和间谍软件/恶意代码来进行身份盗窃和在线欺诈。国际商业间谍和有组织犯罪组织也基于其进行工业间谍活动、大规模货币盗窃和招募新攻击者的能力，对国家构成威胁。一些犯罪集团可能会试图通过威胁网络来勒索组织的钱财

攻击或通过加密和破坏其系统以获取赎金。勒索或赎金攻击已经扰乱了许多企业，并花费了大量资源和计划来缓解。由于没有有效的备份计划和恢复程序，许多企业不得不支付昂贵的赎金来恢复其加密系统。

- 外国情报局(Foreign Intelligence Services)。外国情报机构使用网络工具作为信息收集和间谍活动的一部分。此外，一些国家正在积极努力发展信息战理论、项目和能力。这种能力使单个实体能够通过破坏支持军事力量的供应、通信和经济基础设施来产生重大而严重的影响，这些影响可能会影响美国公民的日常生活。在某些情况下，可能存在外国政府情报机构构成的威胁。除了可能的经济间谍活动外，外国情报机构还可能以非机密系统为目标，以推进其情报任务。一些可能引起他们兴趣的非机密信息包括高级官员的旅行计划、民防和应急准备、制造技术、卫星数据、人事和工资数据以及执法、调查和安全文件。
- 钓鱼者。钓鱼者是执行网络钓鱼计划以窃取身份或信息以获取金钱利益的个人或小团体。钓鱼者也可能使用垃圾邮件和间谍软件/恶意代码来实现他们的目标。
- 垃圾邮件发送者。垃圾邮件发送者是通过发送带有隐藏或虚假信息的未经请求的电子邮件来销售产品、实施网络钓鱼计划、分发间谍软件/恶意代码或攻击组织(例如DoS)的个人或组织。
- 间谍软件/恶意代码作者。通过生产和分发间谍软件和恶意代码对用户进行恶意攻击的个人或组织。破坏文件和硬盘驱动器的破坏性计算机病毒和蠕虫包括Melissa Macro病毒、explorer.zip蠕虫、CIH(切尔诺贝利)病毒、Nimda、Code Red、Slammer和Blaster。
- 恐怖分子。恐怖分子试图破坏、瘫痪或利用关键基础设施，以威胁国家安全，造成大规模伤亡，削弱美国经济，损害公众士气和信心。恐怖分子可能使用网络钓鱼计划或间谍软件/恶意代码来获取资金或收集敏感信息。他们也可能攻击一个目标，以转移对其他目标的注意力或资源。
- 工业间谍。工业间谍活动旨在通过秘密手段获取知识产权和技术诀窍。

4.1.4 恶意代码

恶意代码指的是病毒、特洛伊木马、蠕虫、逻辑炸弹，以及任何其他以攻击平台为目的而创建的软件。

- 病毒。通过将自身的副本附加到现有的可执行文件上进行复制的代码段。当用户执行新的主机程序时，新的病毒副本就会被执行。病毒可能包含一个额外的“有效载荷”，当满足特定条件时触发。

- 特洛伊木马。执行预期任务的程序，但也包含意想不到的和不需要的功能。例如，考虑一个用于多用户系统的编辑程序。这个程序可以被修改为每次用户执行一个有用的功能(例如，编辑)时随机和意外地删除用户的文件。
- 蠕虫。一种自我复制的程序，它是自包含的，不需要主机程序或用户干预。蠕虫通常使用网络服务传播到其他主机系统。
- 逻辑炸弹。这种类型的恶意代码是一组秘密地、故意地插入程序或软件系统的指令，目的是在预先设定的时间和日期或满足特定条件时执行恶意功能。
- 勒索软件。是一种恶意代码，通过锁定整个屏幕或锁定或加密特定文件来阻止或限制对系统的访问，直到支付赎金。勒索软件攻击有两种不同的类型——加密器和锁锁器。加密器阻止(加密)系统文件，并要求支付解锁(或解密)这些文件的费用。加密器或加密勒索软件是最常见和最令人担忧的(例如，WannaCry)。储物柜的设计目的是将用户锁定在操作系统之外。用户仍然可以访问设备和其他文件，但为了解锁受感染的计算机，用户被要求支付赎金。更糟糕的是，即使用户支付了赎金，也不能保证攻击者真的会提供解密密钥或解锁受感染的系统。

4.2 非对抗性威胁来源和事件示例

4.2.1 错误与遗漏

错误和遗漏可能是由每天处理数百笔交易的系统操作员或在组织系统上创建和编辑数据的用户无意中造成的。这些错误和遗漏会降低数据和系统的完整性。软件应用程序，无论其复杂程度如何，都不可能检测到所有类型的输入错误和遗漏。因此，组织有责任建立健全的意识和培训计划，以减少错误和遗漏的数量和严重程度。

用户、系统操作员或程序员的错误可能发生在系统的整个生命周期中，并可能直接或间接地导致安全问题。在某些情况下，错误是一种威胁，例如导致系统崩溃的数据输入错误或编程错误。在其他情况下，错误会导致漏洞。编程和开发错误，通常被称为“bug”，可能是良性的，也可能是灾难性的。

4.2.2 物理和基础设施支持的丧失

支持性基础设施的损失包括电力故障(例如，停电、峰值、限电)、通信中断、水中断和泄漏、下水道故障、交通服务中断、火灾、洪水、内乱和罢工。支持性基础设施的损失通常会导致系统以意想不到的方式停机。例如，在冬季风暴期间，员工可能无法上班，尽管工作现场的系统可能会正常运行。更多信息可以在第10.11节，物理和环境保护中找到。

4.2.3 信息共享对个人隐私的影响

政府和私人组织积累了大量的个人身份信息，这为个人创造了无数的机会，使其作为安全漏洞的副产品或意外后果而经历隐私问题。例如，将信息迁移到云服务提供商已经成为许多个人和组织使用的可行选择。从云端访问数据的便利性使其成为长期存储的更具吸引力的解决方案。所有被写入、上传或发布的内容都存储在个人无法控制的云系统中。然而，云服务用户不知道的是，个人信息可以被一个拥有合适工具和技术技能的陌生人访问。

个人通过社交媒体自愿分享PII也造成了新的威胁，恶意黑客可以利用这些信息进行社会工程或绕过常见的身份验证措施。将所有这些信息和技术联系在一起，恶意黑客就有能力使用他人的信息创建账户或获得网络访问权限。

组织可能会共享包括PII在内的网络威胁信息。这些披露可能导致对此类信息的意外使用，包括监视或其他执法行动。

5 信息安全政策

在讨论信息安全时，策略一词有多个定义。NIST SP 800-95《安全Web服务指南》将策略定义为“指定实体的正确或预期行为的声明、规则或断言”。例如，授权策略可能为软件组件指定正确的访问控制规则。术语策略还可以指系统的特定安全规则，甚至是指定组织的电子邮件隐私策略或远程访问安全策略的特定管理决策。

信息安全策略被定义为指令、法规、规则和实践的集合，规定了组织如何管理、保护和分发信息。在做出这些决策时，管理人员面临着关于资源分配、竞争目标和组织战略的困难决策，所有这些都与保护技术和信息资源以及指导员工行为有关。各级管理者所做的选择可能会影响政策，政策的适用范围会根据管理者的权限范围而有所不同。

关于信息安全问题的管理决策差别很大。为了区分各种策略，本章将其分为三种基本类型：程序策略、特定问题策略和特定系统策略。

策略控制由NIST SP 800-53中每个安全控制系列的“-1”控制来解决。“-1”控制为有效实施选定的安全控制和控制增强建立了策略和程序。

5.1 标准、指导方针和程序

因为政策是在广泛的层面上编写的，所以组织也会制定标准、指导方针和程序，为用户、经理、系统管理员和其他人提供实施政策和实现组织目标的更清晰的方法。标准和指南规定了用于保护系统的技术和方法。程序是完成与安全有关的任务所要遵循的更详细的步骤。标准、指导方针和程序可以通过手册、规章或手册在整个组织内颁布。

- 组织标准(不要与美国国家标准、FIPS、联邦标准或其他国家或国际标准混淆)规定了对特定技术、参数或程序的统一使用，当这种统一使用将使组织受益时。组织范围内识别徽章的标准化是一个典型的例子，它提供了员工流动的便利性和进出系统的自动化。标准在组织中通常是强制性的。
- 指导方针帮助用户、系统人员和其他人有效地保护他们的系统。然而，指南的本质立即认识到系统差异很大，标准的强制实施并不总是可实现的、适当的或具有成本效益的。例如，组织指南可用于帮助制定系统特定的标准程序。指导方针通常用于帮助确保特定的安全措施不会被忽视，尽管它们可以以多种方式正确地实现。

- 程序描述了如何实施适用的安全策略、标准和指导方针。它们是用户、系统操作人员或其他人为完成特定任务(例如，准备新用户帐户和分配适当的特权)所遵循的详细步骤。
- 一些组织发布总体信息安全手册、规章、手册或类似的文件。这些文件可能混合了政策、指导方针、标准和程序，因为它们是紧密相连的。虽然手册和法规可以作为重要的工具，但如果它们能明确区分政策及其实施，往往是有用的。这可以通过提供实现政策目标的替代执行方法，帮助提高灵活性和成本效益。

5.2 项目政策

项目策略用于创建组织的信息安全计划。程序策略为安全设定战略方向，并为其在组织内的实施分配资源。管理官员(通常是首席信息安全官)发布计划政策，以建立或重组组织的信息安全计划。这一高级政策定义了计划的目的及其在组织内的范围，解决了合规问题，并为信息安全组织分配了直接实施计划以及其他相关责任的责任。

5.2.1 项目政策的基本组成部分

项目政策涉及以下内容：

- 目的。项目政策通常包括描述项目目的和目标的声明。与安全相关的需求，如完整性、可用性和机密性，可以构成在策略中建立的组织目标的基础。例如，在负责维护大型关键任务数据库的组织中，可能特别强调减少错误、数据丢失、数据损坏和恢复。然而，在负责维护机密个人数据的组织中，目标可能强调加强保护，防止未经授权的泄露。
- 范围。项目政策明确信息安全项目所保护的资源(如设施、硬件和软件、信息和人员)。在许多情况下，计划将包括所有系统和组织人员，而在其他情况下，组织的信息安全计划在范围上更有限可能是合适的。例如，旨在保护存储在分类或高影响系统上的信息的政策将比旨在保护被认为是低影响的系统的政策严格得多。
- 责任。一旦建立了信息安全项目，其管理通常被分配给新成立的或现有的办公室。整个组织的官员和办公室的职责也需要得到解决。例如，政策声明的这一部分将区分信息服务提供者和使用所提供的应用程序的管理人员的责任

services。该政策还将为主要系统设立业务安全办公室，特别是那些高风险或对组织业务最关键的系统。它还可以作为建立员工问责制的基础。角色和责任在本出版物的第3章中讨论。

- 合规。项目政策通常解决两个合规性问题：

1. 总体合规性，以确保满足建立程序的要求，并在其中分配给组织各组成部分的责任。通常，一个监督实体(如监察长)被指派监督合规性的责任，包括组织如何很好地实施管理部门对规划的优先事项。
2. 使用规定的处罚和纪律处分。由于安全政策是一份高层文件，所以对各种违规行为的具体处罚通常不在这里详细说明。相反，该策略可能授权创建包含违规行为和具体纪律处分的合规结构。

制定合规政策的一个重要方面是要记住，员工违反政策可能是无意的。例如，不符合通常是缺乏知识或培训的结果。在处理涉及个人处罚和纪律处分的问题时，从适当的法律顾问那里获得指导是至关重要的。该政策不需要重申法律已经规定的处罚，尽管如果该政策也将用作意识或培训文件，则可以列出这些处罚。

5.3 具体问题政策

基于信息安全政策的指导，制定特定问题的政策，以解决当前与组织相关和关注的领域。其目的是为组织内的员工提供有关正确使用系统的具体指导和说明。针对特定问题的政策适用于组织使用的每一项技术，并以用户清楚的方式编写。与程序策略不同，由于组织中频繁的技术变更，特定问题策略必须定期进行审查。

5.3.1 特定问题政策的示例主题

针对特定问题的政策可能适用于许多领域。新技术和新威胁的发现往往需要制定针对特定问题的政策。具体问题策略的例子包括：

- 互联网接入。接入互联网带来了很多好处，也带来了很多问题。互联网接入政策可能解决的一些问题包括确定谁将有权访问，什么类型的系统可以连接到网络，什么类型的信息可以通过网络传输，连接互联网的系统的用户认证要求，以及防火墙的使用。

- **电子邮件隐私。**本政策将阐明收集和存储的信息以及使用信息的方式。管理层可能希望监控员工，以确保他们仅将组织系统用于商业目的，或确定员工是否在传播病毒、发送冒犯性内容或泄露私人商业信息。关于电子邮件，用户可能被赋予一定程度的隐私，本政策说明了预期的隐私水平以及电子邮件可能被阅读的情况。
- **自带设备(BYOD)。**允许个人在工作场所使用个人设备。允许BYOD可以提高生产力并降低组织的成本。然而，在组织网络中引入不同的操作系统和用户配置可能是具有挑战性的，不仅对组织信息的安全性，而且对员工的隐私也是如此。一个全面的BYOD政策对设备和用户有特定的考虑，以及使用个人设备访问组织资源必须遵守的行为规则。
- **社交媒体。**即使组织没有社交媒体，他们的用户也有机会。制定社交媒体政策对于保护组织及其员工至关重要。社交媒体政策为用户提供了指导方针，描述了使用不同社交媒体平台时的预期行为。根据组织的不同，政策可以是严格的-不允许在组织提供的资源上使用社交媒体-或者是宽松的政策，允许在组织指定的限制内使用社交媒体。

其他可列入特定问题政策的主题包括但不限于:风险管理方法、机密/专有信息的保护、未经授权的软件、未经授权的设备使用、违反政策、使用外部存储、隐私权和物理紧急情况。

5.3.2 特定问题政策的基本组成部分

针对特定问题的策略可以分解为以下组件:

- **问题声明。**为了制定关于某个问题的政策，信息所有者/管理员首先用相关的术语、区别和条件来定义该问题。指定政策的目标或理由以促进遵守通常是有用的。例如，一个组织可能想要制定一个关于使用“非官方软件”的特定问题的政策，这可能被定义为任何未被组织批准、购买、筛选、管理或拥有的软件。此外，对于某些软件，可能需要包括适用的区别和条件，例如员工私人拥有但批准在工作中使用的软件，或根据组织的合同由其他业务拥有和使用的软件。

- 本组织立场声明。一旦问题被陈述，相关条款和条件被详细说明，这一节用于清楚地陈述组织对该问题的立场(即管理层的决定)。根据前面的例子，这将意味着说明是否在所有或某些情况下禁止使用定义的非官方软件，是否有进一步的批准和使用指导方针，或者是否可以逐案授予例外，由谁授予，以什么为基础。
- 适用性。针对特定问题的政策还需要包括适用性声明。这意味着要明确政策适用的地点、方式、时间、对象和内容。例如，关于非官方软件的假设政策可能只适用于组织自己的现场资源和员工，而不适用于在其他地点设有办公室的承包商。此外，该政策的适用性可能需要澄清，因为它适用于在不同地点之间旅行、在家工作或需要在多个地点运输和使用磁盘的员工。
- 角色和职责。角色和职责的分配通常也包含在特定问题的政策中。例如，如果政策允许员工在工作中使用私人拥有的非官方软件，并获得适当的批准，那么就需要说明授予这种许可的审批机构。(政策将规定，根据职位，谁拥有这种权力。)同样，需要澄清谁将负责确保只在组织系统资源上使用经批准的软件，并在可能的情况下监督有关非官方软件的用户。
- 遵从性。对于某些类型的政策，更详细地描述不可接受的违规行为和此类行为的后果可能是合适的。处罚可以明确说明，并与组织的人事政策和做法保持一致。在使用时，可以与适当的官员、办公室甚至员工谈判单位协调。也可能需要在组织中指定一个特定的办公室来监督遵守情况。
- 联系点和补充信息。对于任何特定问题的政策，指出在组织中可以联系的适当人员，以获得进一步的信息、指导和遵守。由于职位的变动往往不如占据职位的个人频繁，因此具体职位作为联系点可能是可取的。例如，对于某些问题，联络人可能是部门经理;对于其他问题，可能是设施经理、技术支持人员、系统管理员或安全程序代表。再次使用上面的例子，员工需要知道问题和程序信息的联系人是他们的直接上级、系统管理员还是信息安全官员。

5.4 系统特定策略

计划和特定问题的政策是广泛的、高层次的政策，旨在涵盖整个政策

在这种组织中，特定于系统的策略提供了在特定系统上允许哪些操作的信息和指导。这些策略与特定问题策略相似，因为它们与整个组织的特定技术相关。然而，特定于系统的策略向负责实现所需安全控制的人员规定了适当的安全配置，以满足组织的信息安全需求。

为了开发一套有凝聚力和全面的安全策略，官员们可以使用从安全目标中派生出安全规则的管理过程。考虑系统安全策略的两级模型是有帮助的：安全目标和操作安全规则。然而，紧密相连且往往难以区分的是策略在技术上的实施。与特定于问题的策略类似，建议根据组织规定的时间周期的要求审查特定于系统的策略，以确保符合最新的安全程序。

5.4.1 安全目标

管理过程的第一步是为特定系统定义与风险相称的安全目标。尽管这一过程可能从分析完整性、机密性和可用性的需要开始，但它可能不会止步于此。安全目标需要是具体的、具体的、定义明确的，并以一种明确可实现的目标的方式加以表述。利益相关者在制定全面而实用的政策方面发挥着重要作用。因此，必须记住，政策不仅仅是由管理人员制定的。

5.4.2 操作安全规则

在管理层确定了安全目标之后，可以识别和记录管理和操作系统的规则。例如，规则可以定义授权的修改-指定允许个人在特定条件下对特定类别和信息记录采取某些行动。操作安全所需的具体程度因系统而异。规则越详细，管理员就越容易确定何时发生了违规行为。详细的描述还可以简化自动执行策略的过程。

除了决定详细程度之外，管理层还决定了记录特定于系统的策略的正式程度。同样，文档越正式，就越容易执行和遵循该策略。例如，一个有用的做法是起草一个系统访问权限的声明以及安全责任的分配。系统使用的规则和不遵守的后果也应该被处理。记录访问控制策略可以使更容易遵循和执行。

信息安全其他领域的政策决策，如本出版物中描述的，通常记录在风险分析、认证声明或程序手册中。然而，任何有争议的、非典型的或不常见的政策也需要正式的声明。非典型政策可能包括系统政策与组织政策或组织内正常实践不同的领域。典型政策的文档包含一份声明，解释偏离组织标准政策的原因。

5.4.3 系统特定政策实施

技术在执行系统特定策略方面发挥着重要作用，但它并不仅仅负责满足组织的安全需求。当使用技术来执行策略时，重要的是要考虑手动方法。例如，可以使用基于系统的技术控制来限制机密报告的打印到特定的打印机。然而，相应的物理安全措施也必须到位，以限制对打印机输出的访问，否则预期的安全目标将无法实现。

经常用于实现系统安全策略的技术方法可能包括使用逻辑访问控制。访问控制的一些例子将是：职责分离，这是一种控制，旨在解决滥用授权特权的可能性，并有助于在没有共谋的情况下降低恶意活动的风险；以及最小权限(least privilege)，它只允许代表用户行事的用户或流程进行授权访问，这是根据组织使命和业务功能完成分配任务所必需的。然而，还有其他自动执行或支持安全策略的方法，这些方法通常是对逻辑访问控制的补充。例如，入侵检测软件可以提醒系统管理员注意可疑活动，甚至采取措施阻止此类活动。

基于技术的系统安全策略实施既有优点也有缺点。一个系统，经过适当的设计、编程、安装、配置和维护，可以始终如一地在系统内执行策略，尽管没有一个系统可以强迫用户遵循所有的程序。管理控制在政策执行中也起着重要的作用，因此忽视它们对组织是有害的。此外，偏离政策有时可能是必要和适当的；这样的偏离，在一些技术控制下，可能很难轻易实现。如果安全策略的实现过于严格，这种情况就会频繁发生，当系统分析人员无法预测突发事件并为此做好准备时，就会出现这种情况。

5.5 相互依赖

政策与本出版物中涉及的许多主题相关：

- 项目管理。方针用于建立组织的信息安全计划，因此与计划的管理和行政密切相关。在本出版物所涵盖的任何领域都可以建立特定于程序和系统的策略。例如，一个组织可能希望对其所有系统的应急计划有一个一致的方法，并将发布适当的计划政策来做到这一点。另一方面，它可能决定其系统彼此之间足够独立，以便系统所有者可以单独处理事件。
- 访问控制。系统特定的策略通常使用访问控制来实现。例如，可能是一个策略决定，在一个组织中只有两个人被授权运行支票打印程序。系统使用访问控制来实现或强制执行此策略。
- 链接到更广泛的组织策略。了解信息安全策略通常是其他组织策略的延伸是很重要的。支持和

信息安全和其他组织政策之间的协调应该是相互的，以尽量减少混淆。例如，一个组织的电子邮件政策可能与其更广泛的隐私政策相关。

5.6 成本考虑

与制定和实施信息安全策略相关的一些潜在成本。最重要的成本是实施策略并处理其对组织、资源和人员的后续影响。通过政策来完成信息安全计划的建立，其成本可能不会是微不足道的。

其他成本可能是在政策制定过程中产生的成本。许多行政和管理活动可能需要起草、审查、协调、澄清、传播和宣传政策。在许多组织中，政策的成功实施可能需要额外的人员配备和培训。一般来说，组织制定和实施信息安全策略的成本将取决于变更的范围有多广，以便管理层决定已达到可接受的风险水平。

保护信息和系统的成本是不可避免的。目标是通过在满足组织安全目标所需的保护与此类保护的成本之间取得平衡，确保安全保护与风险相称。

6 信息安全管理

风险是衡量实体受到潜在环境或事件威胁程度的尺度，通常是以以下函数:(i)如果环境或事件发生将产生的不利影响;以及(ii)发生的可能性。个人每天都在管理风险，尽管他们可能没有意识到这一点。像系好汽车安全带、预报下雨时带着雨伞、写下要做的事情清单而不是依靠记忆这样的日常行为，都属于风险管理的范畴。个人认识到对他们最大利益的各种威胁，并采取预防措施来防范这些威胁或将其影响降到最低。

政府和工业界都在例行地管理着无数的风险。例如，为了使投资回报最大化，企业经常必须在积极而高风险的增长投资计划和缓慢而安全的增长投资计划之间做出选择。这些决策需要分析相对于潜在收益的风险，考虑备选方案，最后，执行管理层确定的最佳行动方案。

就信息安全而言，风险管理是将系统运行对组织运营(如使命、功能、形象和声誉)、组织资产、个人、其他组织和国家造成的风险最小化的过程。NIST SP 800-39确定了风险管理的四个不同步骤。风险管理要求组织(i)构建风险，(ii)评估风险，(iii)应对风险，(iv)监控风险。

(i)风险框架-描述组织如何为做出基于风险的决策的环境建立风险背景。风险框架组件的目的是产生一种风险管理策略，解决组织打算如何评估、应对和监控风险的问题，同时使组织在做出投资和运营决策时经常使用的风险感知变得明确和透明。

(ii)评估风险-描述组织如何在组织风险框架的背景下分析风险。风险评估部分的目的是识别:(i)对组织运营和资产、个人、其他组织和国家的威胁;(ii)组织的内部和外部脆弱性;(iii)鉴于利用漏洞的潜在威胁可能对组织造成的伤害(即后果/影响);以及(iv)伤害发生的可能性。

(iii)对风险做出反应——说明一旦风险根据风险评估的结果确定，组织如何对风险做出反应。风险应对部分的目的是根据组织风险框架，通过以下方式提供一致的全组织范围的风险应对:(i)制定应对风险的替代行动方案;(ii)评价可选的行动方案;(iii)确定与组织风险承受能力相一致的适当行动方案;(iv)根据选定的行动方案实施风险应对措施。

- (iv) 监控风险——解决组织如何随时间监控风险。风险监控组件的目的是:(i)验证计划的风险应对措施是否得到实施，以及源自/可追溯至组织任务/业务职能、联邦立法、指令、法规、政策、标准和指南的信息安全要求是否得到满足;(ii)确定实施后风险应对措施的持续有效性;(iii)识别对组织系统和系统运行环境产生风险影响的变化。

为了帮助组织在系统级别管理信息安全风险，NIST开发了风险管理框架(RMF)。RMF通过实施稳健的连续监测过程，促进了近实时风险管理持续系统授权的概念。RMF还为高级领导提供必要的信息，以制定具有成本效益的、基于风险的决策，这些决策与支持其核心任务和业务功能的组织系统有关，并将信息安全集成到企业架构和系统开发生命周期(SDLC)中。参见NIST SP 800-160。

构成RMF的六个步骤包括：

1. 系统分类;
 2. 安全控制选择;
 3. 安全控制实施;
 4. 安全控制评估;
 5. 系统授权;及
 6. 安全控制监控
-



图1 -风险管理框架(RMF)概述

6.1 Categorize

RMF的第一步侧重于系统的分类。在这里，组织根据影响分析对系统和由该系统处理、存储和传输的信息进行分类。非国家安全系统的安全分类指南可在FIPS 199和NIST SP 800-60.⁷中找到

6.2 选择

RMF过程的第二步包括基于安全分类为系统选择一组初始的基线安全控制，以及根据组织对风险和局部的评估根据需要裁剪和补充安全控制基线

⁷ The National Archives and Records Administration (NARA) has developed a Controlled Unclassified Information (CUI) Registry. The CUI Registry is an online repository for information, guidance, policy, and requirements on handling CUI, including issuances by the CUI Executive Agent. The registry is available at <https://www.archives.gov/cui/registry/category-list>.

条件。安全控制选择指南在NIST SP 800-53和FIPS 200中提供。

6.3 实现

在第三步中，组织负责实现安全控制，并描述如何在系统及其操作环境中使用这些控制。许多NIST出版物提供了有关安全控制实现的信息，并可在计算机安全资源中心网站上参考。

6.4 评估

第四步确保组织使用适当的评估程序评估安全控制，并确定控制正确实施的程度，按预期运行的程度，以及在满足系统安全要求方面产生预期结果的程度。NIST SP 800-53A为评估方法和程序的发展提供了指南，以确定联邦系统的安全控制有效性，并在安全评估报告中报告评估结果。

6.5 授权

第五步，高级管理人员根据完整彻底的安全控制评估结果，正式授权系统运行或继续运行。该决策是基于对系统运行对组织业务和资产、个人、其他组织和国家产生的风险的确定，以及该风险是可接受的决定。

6.6 监控

RMF的第六步是持续监控系统中的安全控制，以确保当系统和系统运行的环境发生变化时，它们随着时间的推移而有效。组织在持续的基础上监视系统中的安全控制，包括评估控制有效性，记录系统或其运行环境的变化，对相关变化进行安全影响分析，并向指定的组织官员报告系统的安全状态。关于连续监测的具体指导可在NIST SP 800-137中找到。

7 保证

信息保障是指通过确保信息和系统的可用性、完整性、身份验证、机密性和不可否认性，人们对安全措施保护和防御信息和系统的信心程度。这些措施包括通过结合保护、检测和反应能力来提供系统的恢复。

然而，保证并不是绝对保证这些措施将按预期工作。理解这种区别是至关重要的，因为量化系统的安全性可能是令人生畏的。然而，这是个人期望和获得的东西，通常没有意识到这一点。例如，个人可能经常从同事那里收到产品推荐，但可能不认为这种推荐提供了保证。

本章讨论了保证的规划，并提出了两类保证方法和工具：保证的设计和后续实施以及操作保证(进一步分类为审计和监控)。由于存在显著的重叠，这两类之间的划分有时可能是模糊的。虽然配置管理或审计等问题是在操作保证下讨论的，但它们在系统开发过程中也可能是至关重要的。讨论倾向于更多地关注设计和实现保证期间的技术问题，并且是在操作保证下的管理、操作和技术问题的混合。

7.1 授权

授权是授权系统操作的官方管理决策。授权官员(组织高级管理人员)在实施一套商定的安全和隐私控制措施的基础上，明确接受操作该系统对组织运营(如使命、职能、形象、声誉)、组织资产、个人、其他组织和国家的风险。授权官员和SAOP之间需要一种协作关系。OMB A-130让SAOPs在授权前审查和批准隐私计划，并审查带有PII的系统的授权包。因此，在做出风险确定和接受决策之前，授权官员与SAOP进行沟通，以在做出最终授权决策之前解决任何与隐私相关的问题。授权过程要求管理人员和技术人员共同努力，在安全需求、技术和操作约束、其他系统质量属性(如隐私)的要求以及任务或业务需求的情况下，找到实用的、具有成本效益的解决方案。

为了促进健全的基于风险的决策，决策是基于有关技术和非技术保障措施的实施和有效性的可靠和最新信息。这些措施包括：

- 技术特性(它们是否按预期运行?);
- 操作政策和实践(系统是否按照规定的政策和实践进行操作?);
- 整体安全性(是否存在安全措施无法解决的威胁?);以及

· 剩余风险(剩余风险⁸是否处于可接受的水平?)
授权官员负责在系统被允许运行之前对其进行授权，并制定如何持续监控该系统的计划。

7.1.1 授权与保证

在决定授权系统运行时，保证是一个不可或缺的因素。保证涉及技术措施和程序是否按照一套安全要求和规范以及一般质量原则运行。

授权官员对一个系统需要多少和什么类型的保证做出最终决定。为了做出合理的决策，授权官员会考虑[系统分类/影响水平](#)，并审查风险评估的结果。授权官员分析保证成本、控制成本和组织风险的利弊。当授权流程完成后，接受系统中的剩余风险是授权官员的责任。

7.1.2 产品在类似情况下运行的授权

另一个产品或系统在类似情况下运行的授权可以用来提供一些保证(例如，互惠)。然而，重要的是要认识到授权是特定于环境和系统的。由于授权平衡了风险和优势，同一产品可能在一种环境下被适当授权，而在另一种环境下却不被适当授权，即使是由同一授权官员授权。例如，授权官员可能批准将云存储用于研究数据，但不批准将云存储用于同一系统权限下的人力资源数据。

7.2 安全工程

当今系统的规模和复杂性使得构建一个值得信赖的系统成为当务之急。系统安全工程为在当今复杂的计算环境中构建可靠的系统提供了一种基本的方法。有关安全工程的更多信息，请参考[NIST SP 800-160](#)。

7.2.1 规划与保证

对于新系统或系统升级，保证要求在系统生命周期的规划阶段开始。将保证作为系统要求的一部分进行规划也是切实可行的，并有助于授权官员在构建系统或购买为旧系统提供保证所需的组件/设备时做出具有成本效益的决策。

7.2.2 设计和实施保证

设计和实现保证涉及系统的设计以及系统、应用程序或组件的功能是否满足安全要求和规范。设计和实现保证检查系统的设计、开发和安装，通常与系统的开发/获取和实现阶段有关

⁸ Residual Risk is the portion of risk remaining after security measures have been applied.

系统生命周期。但是，随着系统的修改，也可以考虑整个生命周期。

7.2.2.1 使用高级或可信的开发

在商用现货(COTS)产品和定制系统的开发中，使用先进或可信的系统架构、开发方法或软件工程技术可以提供保证。示例包括安全设计和开发评审、形式化建模、数学证明、ISO 9000质量技术、ISO 15288(系统安全工程标准)，或安全体系结构概念的使用，例如可信计算基础(TCB)。

由于信息技术产品的安全保证不能得到完全保证，因此有一些公认的评估过程可用来建立一定程度的信心，以确定这些IT产品的安全功能和应用于这些IT产品的保证措施符合某些要求。通用标准(CC)允许独立评估之间的结果具有可比性。CC可作为具有安全功能的IT产品的开发、评估和采购指南。有关CC的更多信息，请参见<http://www.commoncriteriaportal.org> 或 <https://buildsecurityin.us-cert.gov/articles/best-practices/requirements-engineering/the-common-criteria>。

7.2.2.2 可靠架构的使用

一些系统架构本质上更可靠，例如使用容错、冗余、阴影或冗余独立磁盘阵列(RAID)功能的系统。这些例子主要与系统可用性有关。

7.2.2.3 使用可靠的安全性

可靠安全的一个因素是易于安全使用的概念，它假定一个更容易保护的系统实际上更有可能是安全的。当初始系统默认为“最安全”选项时，安全功能可能更有可能被利用。此外，如果系统不使用尚未在“真实”世界中测试的新技术(通常称为“前沿”技术)，则系统的安全性可能被认为更可靠。相反，使用旧的、经过良好测试的软件的系统可能不太可能包含错误。

7.2.2.4 评估

产品评估通常包括测试。评估可以由许多类型的组织进行，包括：国内外政府机构；贸易和专业组织等独立组织；其他供应商或商业团体；或个人用户或用户联盟。贸易文献中的产品评论是一种评估形式，就像针对特定标准进行的更正式的评论一样。使用评估时需要考虑的重要因素是评估小组的独立程度，评估标准是否反映了所需的安全特性，测试的严谨性，测试环境，评估的年龄，评估组织的能力，以及评估组对评估所施加的限制(例如，对威胁或操作环境的假设)。

7.2.2.5 保证文档

描述安全需求以及如何满足这些需求的能力可以反映系统或产品设计师对适用的安全问题的理解程度。如果没有对需求的全面理解，设计人员就不太可能满足这些需求。

保证文档可以解决系统或特定组件的安全性问题。系统级文档描述了系统的安全需求以及它们是如何实现的，包括应用程序、操作系统或网络之间的相互关系。系统级文档不仅仅涉及操作系统、安全系统和应用程序；它描述了在特定环境中集成和实现的系统。组件文档通常是现成的产品，而系统设计者或实现者通常会开发系统文档。

7.2.2.6 保证、完整性声明和责任

保证是保证的另一个来源。制造商、生产者、系统开发商或集成商愿意在一定的时间框架内或在下一个版本发布之前纠正错误，给系统经理一种对产品的承诺感，也说明了产品的质量。完整性声明是对产品的正式声明或认证。它可以通过承诺(a)修复项目(即保证)或(b)支付损失(即责任)来增强，如果产品不符合完整性声明。

7.2.2.7 制造商发布的声明

制造商或开发人员发布的声明或正式声明提供了基于声誉的有限数量的保证。当存在合同时，考虑到对制造商施加的法律责任，仅凭声誉是不够的。

7.2.2.8 分销保证

通常重要的是要知道软件是未经修改的，特别是如果它是以电子方式分发的。在这种情况下，校验位或数字签名可以高度保证代码没有被修改过。防病毒软件可用于检查来自可靠性未知来源的软件(例如，互联网论坛)。

7.3 操作保证

设计和实现保证解决了系统内建安全特性的质量问题。操作保证涉及系统的技术特征是否被绕过或存在漏洞，以及是否遵循了所需的程序。它不涉及系统安全需求的变化，这些变化可能是由系统及其操作或威胁环境的变化引起的。(这些变化在第10.15节中得到解决)。

在系统生命周期的操作阶段，安全性趋于降低。系统用户和操作人员会发现有意或无意地绕过或破坏安全性的新方法，特别是如果他们认为绕过安全性可以提高功能，或者不会对它们或他们的系统产生任何影响。严格遵守程序的情况很少见。政策变得过时，系统管理中的错误经常发生。

Organizations use three basic methods to maintain operational assurance:

- 系统评估。评估安全性的事件或连续过程。评估的范围可以有很大的不同:它可以为了授权的目的检查整个系统,也可以调查单个异常事件;
- 系统审核。对记录和活动的独立审查和检查,以评估系统控制的充分性,并确保符合既定的政策和操作程序;以及
- 系统监控。维持对信息安全、漏洞和威胁的持续意识,以支持组织风险管理决策的过程。

一般来说,一项活动越“实时”,就越属于监控的范畴。这种区分可能会造成一些不必要的语言上的细微差别,特别是在系统生成的审计跟踪方面。每天或每周审查未经授权的访问尝试的审计跟踪通常被认为是监控,而对几个月的跟踪价值的历史审查(例如,跟踪特定用户的操作)通常被认为是审计。不过,总的来说,与实际维护运营保证的实际工作相比,应用于保证相关活动的特定术语要重要得多。

7.3.1 安全和隐私控制评估

评估可以解决系统在构建、实现或运行时的质量问题。评估可以在整个开发周期、系统安装之后以及整个操作阶段进行。评估方法包括面谈、考试和测试。一些常见的测试技术以功能测试(看看给定的功能是否按照其需求工作)或渗透测试(看看是否可以绕过安全性)为特征。这些技术可以尝试几个测试用例,也可以使用度量、自动化工具或多个详细的测试用例进行深入研究。评估指导请参见NIST [SP 800-53A](#)。

7.3.2 审核方法和工具

为支持运行保证而进行的审计检查系统是否符合规定或暗示的安全要求以及系统和组织政策。一些审计还检查安全要求是否适当,尽管这超出了运行保证的范围。(见第10.15节。)不太正式的审计通常被称为安全审查。

审计可以是自我管理的,也可以是独立的,这意味着它们可以在内部或外部进行管理。这两种类型都可以提供关于技术、程序、管理或其他安全方面的优秀信息。自我审计和独立审计的本质区别在于客观性。由系统管理人员进行的审查——通常称为自我审计/评估——存在内在的利益冲突。系统管理人员可能没有什么动机去报告系统设计不良或操作疏忽。另一方面,他们的动机可能是提高系统安全性的强烈愿望。此外,他们对系统很了解,可能能够发现隐藏的问题。

相比之下,独立审计员在系统中没有专业利益。进行独立审计的人在组织上是独立的,不受可能损害其独立性的个人或外部约束。独立审计可以由专业审计人员按照公认的审计准则进行。

有许多方法和工具可用于审计，这里介绍其中的一些。

7.3.2.1 自动化工具

即使对于小型多用户系统，手动审查安全特性也可能需要大量资源。自动化工具使得审查大型系统的各种安全漏洞成为可能。

自动化工具有两种类型：(1)主动工具，通过尝试利用漏洞来发现漏洞；(2)被动测试，它只检查系统，从系统的状态推断问题的存在。

自动化工具可用于帮助发现各种威胁和漏洞，例如访问控制或访问控制配置不当、弱密码、缺乏系统软件完整性，或未应用所有相关软件更新和补丁。这些工具通常在发现漏洞方面非常成功，有时也会被黑客用来入侵系统。利用这些工具给系统管理员带来了优势。许多工具使用起来很简单。然而，有些程序（例如，大型主机系统的访问控制审计工具）需要专门的技能来使用和解释。

7.3.2.2 内部控制审计

审计师可以审查现有的控制措施，并确定它们是否有效。审核员通常会分析系统控制和非系统控制。所使用的技术包括对数据和控制本身的查询、观察和测试。审计还可以发现非法行为、错误、违规或不遵守法律法规的情况。可以使用下面讨论的系统安全计划和渗透测试。

7.3.2.3 使用系统安全计划(SSP)

系统安全计划提供了对系统进行审计的实现细节。该计划在第10.12节中讨论，概述了系统的主要安全考虑因素，包括管理、操作和技术问题。使用系统安全计划的一个优点是，它反映了系统的独特安全环境，而不是一个通用的控制列表。可以开发安全控制集，包括国家或组织的安全政策和实践（通常称为基线）。SSP也用于历史目的，并且在存在系统互连的情况下，可能需要与其他组织共享。

基线是系统安全控制选择过程的起点。使用FIPS 200中定义的高水位标记⁹，确定了对应于低影响、中等影响和高影响系统的三个安全控制基线，为每个影响级别提供一组初始安全控制。一旦选择了安全控制基线，组织就可以使用NIST SP 800-53中的裁剪指导来从基线中删除控制

⁹ High Water Mark—For a system, the potential impact values assigned to the respective security objectives (confidentiality, integrity, availability) shall be the highest values from among those security categories that have been determined for each type of information resident on the system (retrieved from FIPS 199).

(并附有基于风险的理由)或添加补偿或补充控制以加强特定系统的安全态势。

需要注意确保对基线的偏离是基于对相关风险的评估，因为变更可能适合系统的特定环境或技术限制。

7.3.2.4 渗透测试

渗透测试可以使用许多方法来尝试系统入侵。除了使用如上所述的主动自动化工具外，渗透测试还可以“手动”完成。最有用的渗透测试类型包括使用可能被用来对付系统的方法。对于互联网上的主机，这当然包括自动化工具。对于许多系统来说，松散的程序或缺乏对应用程序的内部控制是渗透测试可以针对的常见漏洞。另一种方法是社会工程，即欺骗用户或管理员泄露系统信息，包括密码。

7.3.3 监控方法和工具

安全监视是一项持续进行的活动，旨在找出漏洞和安全问题。许多方法类似于用于审计的方法，但更经常地进行，或者对于一些自动化工具来说，是实时进行的。

7.3.3.1 系统日志的审查

定期检查或使用自动化工具分析系统生成的日志可以检测安全问题，包括试图超越访问权限或在异常时间获得系统访问权限(参见第10.15节)。

7.3.3.2 自动化工具

有几种类型的自动化工具监视系统的安全问题。下面是一些例子：

- 恶意代码扫描器是检查恶意代码感染的常用手段。这些程序测试可执行程序文件中是否存在恶意代码；
- 校验和函数生成一个数学值，用于根据文件的内容检测数据的变化。当对文件的完整性进行验证时，会在当前文件上生成校验和，并与之前生成的值进行比较。如果两个值相等，则验证该文件的完整性。在程序上运行校验和可以检测到恶意代码、对文件的意外更改以及对文件的其他更改。然而，它们可能会被系统入侵者隐蔽地替换掉。数字签名不仅可以防止对文件的意外更改，而且远远优于校验和，也可以用来验证文件的完整性；
- 密码强度检查器根据字典(要么是“常规”字典，要么是带有易于猜测密码的专门字典，或者两者兼而有之)测试密码，还检查密码是否为用户ID的常见排列。特殊字典的例子

参赛作品可以是地区运动队和球星的名字。常见的排列方式可以是用户ID的倒写，也可以是在常用密码后加上数字或特殊字符；

- 完整性验证程序可以被应用程序用来寻找数据篡改、错误和遗漏的证据。技术包括数据输入和处理过程中的一致性和合理性检查和验证。这些技术可以根据期望值或值范围检查数据元素(作为输入或作为处理);分析事务以确定正确的流程、顺序和授权;或者检查数据元素，寻找预期的关系。完整性验证程序包括一套关键的过程，旨在确保个人的不当行为，无论是偶然的还是故意的，都会被发现。许多完整性验证程序依赖于记录个人用户活动；
- 基于主机的入侵检测系统分析系统审计跟踪，寻找可能代表未授权活动的活动，特别是登录、连接、操作系统调用和各种命令参数。入侵检测将在10.1节和10.3节中介绍；以及
- 系统性能监控实时分析系统性能日志，寻找可用性问题，包括主动攻击、系统和网络减速以及崩溃。

7.3.3.3 配置管理

配置管理提供保证，运行中的系统已根据组织的需要和标准进行了配置，要进行的任何更改都经过了安全影响的审查，并且这些更改在实施之前已得到管理层的批准。配置管理可用于帮助确保变更发生在可识别和受控的环境中，并且这些变更不会无意中损害系统的任何属性，包括其安全性。一些组织，特别是那些拥有非常大的系统的组织(例如，联邦政府)，使用配置控制委员会进行配置管理。当这样的委员会存在时，信息安全专家的参与是至关重要的。

系统的变化可能会对安全产生影响。此类更改可能会引入或减轻漏洞，并可能需要更新应急计划、风险分析或授权。有关配置管理的更多详细信息，请参见第10.5节。

7.3.3.4 贸易文献/出版物/电子新闻

除了监测系统外，监测外部信息来源也很有用。诸如印刷和电子的贸易文献等来源都有有关安全漏洞、补丁和其他影响安全的领域的信息。事件响应小组论坛(FIRST)有一个电子邮件列表，用于接收有关威胁、漏洞和补丁的信息。国家漏洞数据库(NVD)是使用安全内容自动化表示的基于标准的漏洞管理数据的存储库

协议(SCAP)。这些数据可以实现漏洞管理、安全度量和遵从性的自动化。NVD包括安全检查表、与安全相关的软件缺陷、错误配置、产品名称和影响度量的数据库。美国计算机应急准备小组(US-CERT)是国土安全部的一个组成部分，负责响应重大事件，分析威胁，并与全球可信赖的合作伙伴交换关键网络安全信息。此外，信息共享和分析中心(ISACs)沟通有关物理、网络威胁和缓解的关键部门特定信息，以保持全部门的态势感知。

7.4 相互依赖关系

保证是本出版物中讨论的每个控制和保障的问题。这里需要再次强调的重要一点是，保证不仅适用于技术控制，也适用于操作控制。虽然这一章的重点是系统保证，但保证管理控制正常工作也很重要。用户id和访问权限是否保持最新?应急计划是否经过测试?审计线索能不能被篡改?安全程序是否有效?政策是否被理解和遵守?正如本章引言中所指出的，对保障的需求比个人通常意识到的要广泛得多。

保证与系统生命周期中的安全规划密切相关。系统可以设计成便于针对指定的安全要求进行各种测试。通过在过程的早期规划这种测试，可以降低成本。如果没有适当的计划，就无法获得某些类型的保证。

7.5 成本考虑

有许多方法可以确保安全功能按预期工作。由于保证方法往往是定性的而不是定量的，因此需要对它们进行评估。保证也可能是相当昂贵的，特别是如果进行了广泛的测试。评估收到的保证的数量以做出最佳价值决策的成本是很有用的。一般来说，人员成本会推高保证成本。自动化工具通常仅限于解决特定问题，但它们往往成本较低。

8 系统支持与操作安全注意事项

系统支持和操作是指系统运行所涉及的所有方面。这包括系统管理和系统外部支持其运行的任务(例如，维护文档)。它不包括系统规划或设计。支持和操作任何系统——从三人局域网到服务数千用户的全球应用程序——对维护系统的安全性至关重要。支持和操作是使系统正常运行的日常活动。这些包括修复软件或硬件问题，安装和维护软件，以及帮助用户解决问题。

未能将安全视为系统支持和操作的一部分，可能对组织有害。信息安全系统文献包括组织如何通过糟糕的文档、旧的用户帐户、冲突的软件或对维护帐户的不良控制来破坏其通常昂贵的安全措施的例子。一个组织的政策和程序常常不能解决这些重要的问题。一些主要的类别包括：

- 用户支持；
- 软件支持；
- 配置管理；
- 备份；
- 媒体控制；
- 文档；以及
- 维护

尽管系统支持和操作的目标与信息安全密切相关，但两者之间存在区别。系统支持和运行的主要目标是系统的持续和正确运行，而系统的信息安全目标包括保密性、可用性和完整性。

本章讨论与安全直接相关的支持和操作活动。本出版物中讨论的每个控制都以这样或那样的方式依赖于系统支持和操作。然而，本章着重于其他章节未涉及的领域。例如，操作人员通常在系统上创建用户帐号。本节内容将在10.7中介绍。同样，支持和运营人员对安全意识和培训计划的投入也在10.2节中介绍。

8.1 用户支持

在许多组织中，用户支持是通过服务台进行的。服务台可以支持整个组织、子单位、特定系统或这些的组合。对于较小的系统，系统管理员通常提供直接的用户支持。经验丰富的用户在大多数系统上提供非正式的用户支持。用户支持与组织处理事件响应的能力密切相关，这并不罕见。

对于用户支持人员来说，一个重要的安全考虑是能够识别哪些问题(由用户提请他们注意)与安全相关。例如，用户无法登录一个系统，可能是由于失败太多导致他们的帐户被禁用。

访问尝试。这可能表明存在恶意用户试图猜测用户的密码。

一般来说，系统支持和操作人员需要能够识别安全问题，做出相应的反应，并通知适当的个人。可能存在的安全问题范围很广；其中一些将是自定义应用程序的内部问题，而另一些则适用于现成的产品。此外，问题可能是基于软件或硬件的。

系统支持和操作人员的反应能力越强、知识越丰富，非正式提供的用户支持就越少。其他用户提供的支持可能是有价值的，但他们可能不了解整个组织的所有问题，也不知道这些问题是如何相互关联的。

8.2 软件支持

无论系统的大小和复杂程度如何，软件都是组织系统运行的核心。因此，确保软件正常运行并防止腐败是至关重要的。软件支持的要素有很多。

第一个要素是控制在系统上使用什么软件。如果用户或系统人员可以在系统上安装和执行任何软件，那么系统就更容易受到病毒、意外的软件交互以及可能破坏或绕过安全控制的软件的攻击。控制软件的一种方法是在软件安装之前对其进行检查或测试（例如，确定与自定义应用程序的兼容性，识别其他不可预见的交互）。这可以应用于新的软件包、升级、现成的产品，或者被认为合适的定制软件。除了控制新软件的安装和执行外，组织还监督功能强大的系统实用程序的配置和使用。系统实用程序会损害操作系统的完整性和逻辑访问控制。

软件支持的第二个要素是确保软件在未经适当授权的情况下不会被修改。这涉及到对软件和备份副本的保护，可以通过逻辑和物理访问控制的结合来实现。

许多组织还包括一个程序，以确保软件按要求获得适当的许可。例如，一个组织可能会审核其系统是否存在非法拷贝的版权软件。这个问题主要与用户系统（或设备）有关，但也可以适用于任何类型的系统。

8.3 配置管理

与软件支持密切相关的是配置管理——跟踪和批准系统变更的过程。配置管理可以是正式的，也可以是非正式的，通常涉及硬件、软件、网络和其他更改。配置管理的主要安全目标是确保对系统的更改不会无意或不知不觉地降低安全性。可以使用软件支持下讨论的一些方法（例如，例如检查和测试软件更改）。第7章讨论了其他方法。

注意，安全性的目标是知道发生了什么变化，而不是防止安全性被改变。可能在某些情况下，由于需要完成任务，降低安全性被认为是一种可接受的风险。在这种情况下，安全措施的减少是由授权官员在考虑了所有适当因素后作出的决定。此外，将持续监测由此导致的风险增加情况。

配置管理的第二个安全目标是确保对系统的更改反映在其他文档中，例如应急计划。如果变更量是重大的，可能需要重新分析系统的部分或全部安全性。这将在第10.15节中讨论。

8.4 备份

支持和操作人员，有时用户备份软件和数据。这一功能对应急计划至关重要。备份的频率取决于数据变化的频率和这些变化的重要性。咨询系统管理员，确定什么样的备份计划是合适的。此外，测试备份副本是否实际可用也很重要。最后，安全存储备份(下面讨论)。

8.5 媒体控制

媒体控制包括为数字和非数字媒体提供物质和环境保护以及问责制的各种措施。数字媒体的例子包括软盘、磁带、外部/可移动硬盘驱动器、闪存驱动器、光盘和数字视频磁盘。非数字媒体的例子包括纸张和缩微胶卷。从安全的角度来看，媒体控制的目的是防止在系统外存储或传播信息(包括数据或软件)时失去机密性、完整性和可用性。这可以包括信息输入系统前和输出系统后的存储。

媒体控制的程度取决于许多因素，包括数据的类型、媒体的数量和用户环境的性质。物理和环境保护是用来防止未经授权的个人访问媒体，并防止诸如热、冷或有害磁场等因素。必要时，记录个人介质(如磁带盒)的使用可提供详细的责任制，以便组织可以要求授权的个人对其行为负责。有关媒体保护的更多信息，请参见第10.10节。

8.6 文档

系统支持和操作的所有方面的文档对于确保连续性和一致性非常重要。充分详细地形式化操作实践和程序有助于消除安全漏洞和疏忽，为新人员提供足够详细的指导，并提供质量保证功能，以帮助确保正确有效地执行操作。

系统的具体安全实施细节也要记录下来。这包括许多类型的文档，如安全计划、应急计划、风险分析、安全策略和过程。许多此类信息，特别是风险和威胁分析，必须加以保护，防止未经授权的泄露。安全文档也需要是最新的和可访问的。可访问性需要考虑特殊因素，例如在灾难期间找到应急计划的需要。

可能需要设计一些安全文档来满足不同系统角色的需求。出于这个原因，许多组织将文档分为策略和过程。可能会编写安全程序手册，告知系统用户如何完成他们的工作。

安全。对于系统操作和支持人员，安全程序手册可以相当详细地处理各种各样的技术和操作问题。

8.7 维护

系统维护需要对系统进行物理或逻辑访问。支持和操作人员、硬件或软件供应商或第三方服务提供商可能维护系统。维护可以在现场进行，也可以通过通信连接远程进行。也可能需要将设备移到维修点进行维护。如果通常没有系统访问权限的人执行维护，那么就引入了安全漏洞。

在某些情况下，可能需要采取额外的预防措施(例如，对服务人员进行背景调查)，以防止诸如“窥探”物理区域之类的一些问题。然而，一旦有人进入系统，监管人员就很难防止通过维护过程造成的损害。

很多系统都提供维护账号。这些特殊的登录账号通常在出厂时就预先配置好了，有预先设定好的、众所周知的密码。更改这些密码或以其他方式限制对这些账户的访问至关重要。制定程序，确保只有授权的维护人员才能访问预配置的帐户。如果需要远程使用该帐号，则可以通过回调确认的方式对维护提供商进行认证。这有助于确保远程诊断活动实际上来自供应商现场的既定电话号码。其他有用的技术包括诊断通信的加密和解密、强识别和认证技术(如令牌)以及远程断开连接验证。

较大系统的制造商和第三方提供商可能会提供更多的诊断和支持服务，较大的系统可能有诊断端口。确保这些端口仅供授权人员使用，不能被恶意用户访问，并且仅在需要时激活是至关重要的。

8.8 相互依赖关系

在本出版物中讨论的大多数控件中都有支持和操作组件，例如：

- **人员。**大多数支持和操作人员都有访问系统的特殊权限。一些组织对这些职位的个人进行背景调查。(见第10.13节);
- **事件处理。**支持和操作可能包括组织的事件处理人员。即使他们是独立的组织，他们也需要一起工作来识别和响应事件。(见第10.8节);
- **应急计划。**支持和运营通常为应急计划提供技术投入，并开展创建备份，更新文件和演练应急反应的活动。(见10.6节);

- 安全意识、培训和教育。支持和操作人员接受过安全程序培训，并意识到安全的重要性。此外，他们还提供必要的技术专长，教导用户如何保护他们的系统。(见10.2节);
- 物理和环境。支持和操作人员经常控制系统周围的直接物理区域。(见第10.11节);
- 技术控制。技术控制由支持和操作人员安装、维护和使用。他们创建用户帐户，将用户添加到访问控制列表中，审查异常活动的审计日志，控制电信链路上的批量加密，并执行有效使用技术控制所需的无数操作任务。此外，支持和操作人员根据他们对系统能力和操作约束的了解，为选择控制提供所需的输入。(见第10章);及
- 保证。支持和操作人员通过使用保证方法来评估或测试更改及其对系统的影响，确保系统的更改不会引入安全漏洞。操作保证通常由支持和操作人员执行。(见第7章)。

8.9 成本考虑

确保日常支持和操作中充分安全的成本在很大程度上取决于操作环境的规模和特征以及正在执行的处理的性质。可能没有必要雇用额外的支持和操作安全专家。如果有足够的支持人员，重要的是要对他们进行分配工作的安全方面的培训。初始和持续的培训是成功地将安全措施纳入支持和业务活动的成本。

另一个成本是与创建和更新文件相关的成本，以确保安全问题在支持和运营政策、程序和职责中得到适当反映。

9 Cryptography

密码学是基于数据变换的数学分支。它是保护信息的重要工具，在信息安全的许多方面都有应用。例如，密码学可以帮助提供数据的保密性和完整性。这些安全目标可以通过使用各种加密算法(如电子签名、高级用户认证)来实现。尽管现代密码学依赖于高等数学，但用户可以在不了解其数学基础的情况下获得其好处。

NIST发布了一系列特殊出版物(SPs)和联邦信息处理标准(FIPS)，适用于联邦政府内部使用密码学。这些SPs和FIPS的列表可以在NIST SP 800-175B附录A中找到，使用加密标准指南:加密机制。公法、总统行政命令和指令，以及总统行政办公室组织的其他指导，推动了NIST编写的SPs和FIPS。NIST SP 800-175A《使用加密标准指南:指令、授权和政策》中介绍了专门针对密码学的立法授权、政策和指令。

仅靠密码学并不能满足任何组织的信息保障需求。相反，当与其他安全措施相结合时，密码学是满足广泛的信息安全需求和要求的有用工具。本章描述了基本加密技术的基本方面，以及应用加密技术提高安全性的一些具体方法。本章还探讨了将密码学纳入系统时需要考虑的一些重要问题。

9.1 密码学的使用

密码学用于保护系统边界内外的数据。系统内的数据可以通过逻辑和物理访问控制(可能辅以密码学)得到充分的保护。然而，在系统之外，加密有时是保护数据的唯一方法。例如，当数据在跨通信线路传输或驻留在另一个系统中时，无法通过发起者的逻辑或物理访问控制来保护数据。密码学提供了一种解决方案，即使在数据不再受始发方控制的情况下也能保护数据。

9.1.1 数据加密

获得经济有效的数据机密性的最佳方法之一是使用加密。加密将可理解的数据(称为明文)转换为不可理解的形式(称为密文)。这通过解密的过程被逆转。保护电子数据的一种方法是使用高级加密标准(AES)。AES算法是一种加密算法，可用于对信息进行加密和解密。一旦数据被加密，就不需要对密文进行防止泄露的保护。但是，如果修改了密文，就不能正确解密。对AES的更全面的解释可以在FIPS 197，高级加密标准(AES)中找到。

秘密加密和公钥加密都可以用于数据加密，尽管并非所有公钥算法都提供数据加密。要使用密钥算法，需要使用特定的密钥对数据进行加密。解密数据时必须使用相同的密钥。当使用公钥加密进行加密时，任何一方都可以使用其他任何一方的公钥进行加密^a

message。然而，只有拥有相应私钥的一方才能解密，从而读取消息。选择一种加密形式而不是另一种加密形式有几个原因。例如，一个组织可能决定使用公钥加密，因为它更安全，更方便使用，因为私钥不必传输给任何人。为了使密钥加密发挥作用，密钥必须传输，因为加密和解密该特定数据使用的是相同的密钥。关于公钥基础设施(PKI)的更详细指导，请参见NIST SP 800-32，公钥技术和联邦PKI基础设施介绍，NIST SP 800-57第3部分，密钥管理建议:第3部分-特定应用密钥管理指南，以及NIST SP 800-152，美国联邦密码密钥管理系统(CKMS)概要。

9.1.2 完整性

完整性是一种属性，即数据自创建、传输或存储以来没有以未经授权的方式被改变。在系统中，人类并不总是能够通过扫描信息来确定数据是否被擦除、添加或修改。即使扫描是可能的，个人也可能无法知道正确的数据应该是什么。例如，“做”可能被改成“不做”，或者1000美元可能被改成10000美元。因此，希望有一种自动化的办法来检测有意和无意的数据修改。

虽然错误检测码(例如，奇偶校验位)早已在通信协议中使用，为了检测无意的修改，攻击者拦截和修改消息也可以替换消息的错误检测码。密码学可以有效地检测有意和无意的修改。

9.1.3 电子签名

今天的系统以电子形式存储和处理文件。电子形式的文件允许快速处理和传输，并提高整体效率。传统上，对纸质文件的批准是通过书面签名来表示的。因此，需要的是与书面签名等同的电子签名，它可以被认为与书面签名具有相同的法律地位。除了上面讨论的完整性保护之外，密码学还可以提供一种将文档与特定的人联系起来的手段，就像书面签名一样。电子签名可以使用密钥或公钥加密。不过，公钥方法通常更容易使用。

简单地拍摄书面签名的数字照片并不能提供足够的安全性。这样的数字化书面签名很容易从一个电子文件复制到另一个电子文件，而且没有办法确定它是否合法。另一方面，电子签名可以对一条信息进行唯一的验证，而且只能对那条信息进行验证。例如，加密散列函数¹⁰(如SHA-3)可用于提高数字签名的安全性和效率，从而确保原始消息不会被更改为具有相同散列值的不同消息，因此不会被更改为相同的签名。要了解更多关于

¹⁰ A cryptographic hash function is a hash function that is designed to provide special properties including collision resistance, and preimage resistance, that are important for many applications in information security.

加密哈希函数,特别是SHA-3,请参见FIPS 202, SHA-3标准:基于排列的哈希和可扩展输出函数。

9.1.3.1 秘钥电子签名

电子签名可以使用密钥消息验证码(mac)来实现。例如,如果双方共享一个密钥,并且其中一方接收到的数据具有使用共享密钥正确验证的MAC,则该方可以假设另一方对数据进行了签名。这也假定双方相互信任。通过使用MAC,可以获得数据完整性和一种电子签名形式。使用额外的控制,如密钥公证¹¹和密钥属性¹²,即使双方互不信任,也可以提供电子签名。

9.1.3.2 公钥电子签名

另一种类型的电子签名为数字签名,使用公钥加密实现。通过将发送者的私钥应用于数据,对数据进行电子签名。(这样做的精确数学过程对于本讨论并不重要。)为了提高处理速度,私钥应用于数据的较短形式,称为“哈希”或“消息摘要”,而不是应用于整个数据集。生成的数字签名可以随数据一起存储或传输。签名可以由任何一方使用签名者的公钥进行验证。这个功能非常有用,例如,在分发经过签名的无病毒软件副本时。任何接收方都可以验证该程序是否没有病毒。如果签名验证正确,那么验证者就有信心在签名后数据没有被修改,并且公钥的所有者就是签名者。

NIST已经在FIPS 186-4(数字签名标准)和FIPS 180-4(安全哈希标准)中发布了供联邦政府使用的数字签名和安全哈希标准。

9.1.4 用户身份验证

身份验证是向接收实体提供信息源保证的过程。密码学可以提高用户身份验证技术的安全性。如10.7节所述,密码学是几种高级身份验证方法的基础。代替在开放网络上通信密码,身份验证可以通过展示对加密密钥的了解来执行。使用这些方法,就可以使用一次性密码,这种密码不容易被窃听。用户认证可以使用秘密或公钥加密。

9.2 实现问题

本节探讨了在系统中使用(例如,设计,实现,集成)密码学时需要考虑的几个重要问题。NIST已经开发了几个FIPS和SP

¹¹ Key Notarization –is a method, in conjunction with cryptographic facilities (called Key Notarization Facilities), that applies additional security to keys by identifying the sender and recipient, thus, providing assurance on the authenticity of the exchanged keys.

¹² Key Attributes –is a distinct identifier of an entity.

适用于在联邦信息和联邦系统中实现密码学。这些FIPS和SP的列表位于NIST SP 800-175B的附录A中。

9.2.1 选择设计和实施标准

NIST和其他组织已经为设计、实现和使用密码学以及将其集成到自动化系统中开发了许多标准。通过使用这些标准，组织可以降低成本并保护他们在技术上的投资。标准提供的解决方案已被广泛的社区所接受，并经过相关领域专家的审查。标准有助于确保不同供应商设备之间的互操作性，从而允许组织从各种产品中进行选择，以找到具有成本效益的解决方案。

系统的管理人员和用户根据成本效益分析、标准接受的趋势和互操作性要求选择适当的加密标准。此外，每个标准都要仔细分析，以确定它是否适用于组织和期望的应用。

9.2.2 在软件、硬件或固件实现之间做出决定

在安全性、成本、简单性、效率和易实现性之间进行权衡，需要获得符合标准的各种安全产品的管理人员进行研究。密码学可以在软件、硬件或固件中实现。每一种都有其相关的成本和收益。

一般来说，软件比硬件更便宜，速度也更慢，尽管对于大型应用程序来说，硬件可能更便宜。此外，软件可能不那么安全，因为它比同等的硬件产品更容易被修改或绕过。硬件的防篡改能力通常被认为更可靠。

在许多情况下，密码学是在硬件设备(如电子芯片、rom保护的处理器)中实现的，但由软件控制。这种软件需要完整性保护，以确保硬件设备提供正确的信息(例如，控件、数据)而不被绕过。因此，即使在硬件中实现了基本的加密，通常也会提供混合解决方案。有效的安全性需要对整个混合解决方案进行正确的管理。

固件几乎可以在今天使用的每一项技术中找到，包括手机、智能电视，甚至USB键盘。因此，确保固件实现的安全至关重要。保护系统的一种方法是购买具有内置保护功能的硬件，以防止恶意固件修改。有关固件加固的更多信息，请参阅NIST SP 800-147, BIOS保护指南和NIST SP 800-155(草案)，BIOS完整性测量指南。

9.2.3 管理密钥

受密码学保护的信息的安全性直接取决于对密钥的保护。所有密钥都需要防止修改，密钥和私钥需要防止未经授权的泄露。密钥管理涉及在密钥的整个生命周期中使用的手动和自动的程序和协议。这包括加密密钥的生成、分发、存储、输入、使用、销毁和存档。

在一个小的用户社区中，公钥和它们的“所有者”可以被简单地强绑定

交换公钥(例如，将其放在CD-ROM或其他媒体上)。然而，进行更大规模的电子商务——可能涉及地理上和组织上分布的用户——需要一种以电子方式获取公钥的手段，对公钥的完整性和对个人的约束力有高度的信心。对密钥及其所有者之间绑定的支持通常被称为公钥基础设施。

用户还需要能够进入密钥持有者的社区，生成密钥(或让人代其生成密钥)，传播公钥，撤销密钥(例如，在私钥泄露的情况下)，以及更改密钥。此外，可能需要合并时间/日期戳，并存档密钥以验证旧签名。

有关密钥管理的更多信息，请参阅*NIST SP 800-57第1部分,密钥管理建议,第1部分:一般,NIST SP 800-57第2部分,密钥管理建议,第2部分:密钥管理组织的最佳实践,以及NIST SP 800-57第3部分*。

9.2.4 加密模块安全

密码学通常在软件、固件、硬件或其组合的模块中实现。该模块包含加密算法、某些控制参数以及算法所使用的密钥的临时存储设施。密码学的正常运行需要安全的设计、实现和使用密码学模块。这包括保护模块不被篡改。

由于许多原因，符合标准可能很重要，包括互操作性或提供的安全性强度。NIST建立了加密模块验证程序(CMVP)，根据FIPS 140-2《加密模块安全要求》对加密模块进行验证。CMVP的目标是促进使用经过验证的加密模块，并为联邦机构提供在采购包含经过验证的加密模块的设备时使用的安全度量。通过NIST验证的模块列表可在计算机安全资源中心(CSRC)网站上获得。

FIPS 140-2规定了在保护敏感但非机密信息的安全系统中使用的加密模块将满足的安全要求。该标准为加密模块定义了四个安全级别，每一个级别都比前一个级别提供了显著的安全性提高。这四个级别允许提供适合不同程度的数据敏感性和不同应用环境的经济高效的解决方案。用户可以为任何给定的应用或系统选择最佳模块，避免不必要的安全功能成本。

9.2.5 将密码学应用于网络

在网络应用程序中使用密码学通常需要特别考虑。在这些应用中，加密模块的适用性可能取决于其处理本地附加通信设备或网络协议和软件施加的特殊要求的能力。

加密的信息、mac或数字签名可能需要透明的通信协议或设备，以避免被通信设备或软件误解为控制信息。可能需要对加密信息、MAC或数字签名进行格式化，以确保其不会混淆通信设备或软件。密码学必须满足通信所施加的要求

设备，不干扰网络的正常、高效运行。

数据在网络上使用链路加密或端到端加密进行加密。一般来说，链路加密是由服务提供商执行的，比如数据通信提供商。链路加密对通信路径(如卫星链路、电话线路、T3线路)上的所有数据进行加密。由于链路加密也会对路由数据进行加密，因此通信节点需要对数据进行解密才能继续路由。在端到端加密中，数据在通过网络时被加密，但路由信息仍然是可见的。端到端加密通常由最终用户组织执行。端到端加密的一些现代用法的例子包括相当好的隐私(PGP)和用于电子邮件的安全/多用途互联网邮件扩展(S/MIME)。将这两种类型的加密结合起来是可能的。

9.2.6 遵守出口规则

美国政府控制着加密实现的出口。管理出口的规则可能相当复杂，因为它们考虑了多种因素。此外，密码学是一个快速发展的领域，规则可能会不时发生变化。向适当的法律顾问解决有关加密实现出口的问题。

9.3 相互依赖关系

密码学和本出版物中强调的其他安全控制之间存在许多相互依赖关系。密码学既依赖于其他安全保障措施，又有助于提供这些措施。例如：

- 物理安全。需要对加密模块进行物理保护，以防止或至少检测到对加密系统及其密钥的物理替换或修改。在许多环境中(例如，开放式办公室、笔记本电脑)，加密模块本身必须提供所需的物理安全级别。在其他环境中(例如，封闭的通信设施，钢壳的发钞终端)，加密模块可以安全地使用在安全设施内。
- 用户认证。密码学既可用于保护存储在系统中的密码，也可用于保护系统间通信的密码。此外，基于密码学的身份验证技术可以与基于密码的技术结合使用或代替基于密码的技术来提供更强的用户身份验证。
- 逻辑访问控制。在许多情况下，加密软件可能会嵌入到主机系统中，并且可能无法为主机系统提供广泛的物理保护。在这些情况下，逻辑访问控制可以提供一种手段，将加密软件与主机系统的其他部分隔离开来，保护加密软件不被篡改，并保护密钥不被替换或泄露。这种控制的使用提供了相当于物理保护的功能。
- 审计跟踪。密码学可能在审计跟踪中发挥有用的作用，审计跟踪用于帮助支持电子签名。审计记录可以实现电子签名

完整性和密码学可能需要保护存储在系统上的审计记录不被披露或修改。

- 保证。确保加密模块正确安全地实现对于有效使用加密至关重要。NIST维护了它的几个密码学标准的验证程序(参见第9.2.4节)。供应商可以通过一组严格的测试来验证他们的产品是否符合标准。这样的测试增加了对模块符合规定标准的保证，系统设计师、集成商和用户可以更有信心地认为经过验证的产品符合公认的标准。

对密码系统进行监控和定期审计，以确保它们仍然满足其安全目标。审查与密码系统正确操作有关的所有参数;定期对系统本身的运行情况进行测试;并对结果进行审计。某些信息，如公钥系统中的密钥或私钥，不受审计。然而，非秘钥或非私钥可以在模拟审计过程中使用。

9.4 成本考虑

使用加密技术来保护信息既有直接成本，也有间接成本，这部分取决于产品的可用性。在集成电路、附加板或适配器以及独立单元中实现加密的产品种类繁多。

9.4.1 直接成本

密码学的直接成本包括:

- 获取或实现加密模块并将其集成到系统中。介质(即硬件、软件、固件或其组合)和安全级别、逻辑和物理配置、特殊处理要求等各种其他问题将对成本产生影响;以及
- 管理密码学和密码学密钥的生成、分发、归档和处置，以及保护密钥的安全措施。

9.4.2 间接成本

密码学的间接成本包括:

- 系统或网络性能下降，这是由于对存储或通信数据应用加密保护的额外开销造成的;以及
- 由于更严格的安全执行，用户与系统交互方式发生了变化。然而，密码学可以对用户几乎透明，这样影响就最小了。

10控制家族

为了确保保密性、完整性和可用性的保护，FIPS 200规定了多个安全相关领域的最低安全要求。下面介绍的领域代表了一个广泛的、平衡的信息安全计划，涉及保护联邦信息和系统的管理、操作和技术方面。

本节的目的是提供每个安全控制族的简要描述。每个家族都有一个控件列表，用于解决特定的安全目标。要查看完整的安全控制目录和所有控制的描述，请参阅NIST SP 800-53。

10.1访问控制(AC)

在不同的系统中，使用各种系统资源的要求和禁止使用的要求有很大的不同。例如，有些信息必须对所有用户开放，有些信息可能由几个组或部门使用，而有些信息可能仅由少数个人使用。虽然用户必须能够访问执行其工作所需的特定信息，但可能需要拒绝访问与工作无关的信息。控制允许的访问类型也可能很重要(例如，普通用户执行但不能更改系统程序的能力)。这些类型的访问限制强制执行策略，并有助于确保不采取未经授权的操作。

访问是使用任何系统资源的能力。访问控制是授予或拒绝以下特定请求的过程:1)获取和使用信息及相关信息处理服务;以及2)进入特定的物理设施(例如，联邦大楼、军事机构、边境口岸入口)。基于系统的访问控制被称为逻辑访问控制。逻辑访问控制不仅可以规定谁或什么(在进程的情况下)可以访问特定的系统资源，还可以规定允许访问的类型。这些控制可以内置于操作系统中，也可以合并到应用程序或主要工具中(例如，数据库管理系统、通信系统)，或者通过附加的安全包来实现。逻辑访问控制可以在被保护的系统内部或在外部设备中实现。

访问控制安全控制的例子包括:帐户管理、职责分离、最小特权、会话锁定、信息流强制和会话终止。

组织限制:(i)对授权用户的系统访问;(ii)代表授权用户行事的流程;(iii)设备，包括其他系统;以及(iv)授权用户被允许行使的交易类型和功能。

10.2意识和培训(AT)

通常，用户社区被认为是保护系统的最薄弱环节。这是由于用户没有意识到他们的行为可能会如何影响系统的安全性。让系统用户意识到他们的安全责任并教他们正确的做法有助于改变他们的行为。它还支持个人问责制，这是提高信息安全的最重要途径之一。在不知道必要的安全措施或如何使用这些措施的情况下，用户无法真正对自己的行为负责。《计算机安全法》强调了这种培训的重要性，该法案要求对参与联邦系统管理、使用和操作的人员进行培训。

信息安全意识、培训和教育的目的是通过以下方式增强安全性:(i)提高需要保护系统资源的意识;(ii)发展技能和知识，使系统用户能够更安全地执行其工作;(iii)根据需要建立深入的知识，为组织和系统设计、实施或操作安全程序。组织有责任确保管理者和用户意识到与其活动相关的安全风险，并确保组织人员接受了充分的培训，以履行其与信息安全相关的职责。

意识和培训安全控制的例子包括:安全意识培训、基于角色的安全培训和安全培训记录。

组织:(i)确保组织系统的管理人员和用户了解与其活动相关的安全风险，以及与组织系统安全相关的适用法律、行政命令、指令、政策、标准、指示、法规或程序;以及(ii)确保组织人员得到充分培训，以履行其指定的信息安全相关职责。

10.3 审计和问责制(AU)

审计是对记录和活动的独立审查和检查，以评估系统控制的充分性，并确保遵守既定的政策和操作程序。审计跟踪是访问过系统的个人的记录，以及用户在特定时期内所执行的操作。审计跟踪通过系统和应用程序过程以及系统和应用程序的用户活动维护系统活动的记录。与适当的工具和程序相结合，审计跟踪可以帮助检测应用程序中的安全违规、性能问题和缺陷。

审计跟踪可以作为对常规系统操作的支持，也可以作为一种保险单，或者两者兼而有之。作为保险，审计跟踪被维护，但不使用，除非需要(例如，在系统中断后)。作为对运营的支持，审计跟踪用于帮助系统管理员确保系统或资源没有受到黑客、内部人员或技术问题的损害。

审计和问责制控制的例子包括:审计事件、时间戳、不可否认性、审计信息保护、审计记录保留和会话审计。

组织:(i)创建、保护和保留系统审计记录，使其达到监控、分析、调查和报告非法、未经授权或不适当的系统活动所需的程度;以及(ii)确保单个系统用户的行为可以被唯一地追踪到这些用户，以便他们可以被追究责任。

10.4 评估、授权和监督(CA)

安全控制评估是对系统的管理、操作和技术安全控制进行测试和/或评估，以确定控制正确实施的程度，按预期运行的程度，以及在满足系统安全要求方面产生预期结果的程度。评估还有助于确定所实施的控制对于其预期服务的功能来说是否是最有效和最具成本效益的解决方案。安全控制的评估是在持续的基础上进行的，以支持对组织当前安全状况的近乎实时的分析。

在完成完整彻底的安全控制评估后，授权官员做出

授权系统运行(对于新系统)或继续运行的决定。

安全评估和授权控制的示例包括:安全评估、系统互连、行动计划和里程碑以及持续监控。

组织:(i)定期评估组织系统中的安全控制,以确定这些控制在其应用中是否有效;(ii)制定和实施旨在纠正组织系统中的缺陷和减少或消除漏洞的行动计划;(iii)授权组织系统和任何相关系统连接的运行;(iv)持续监控安全控制,以确保控制的持续有效性。

10.5配置管理(CM)

配置管理是集中于建立和维护信息技术产品和系统的完整性的一系列活动的集合,通过控制在整个SDLC中初始化、变更和监视这些产品和系统的配置的过程。配置管理包括确定和记录系统的适当的特定设置,进行安全影响分析,并通过变更控制委员会管理变更。它允许对整个系统进行审查,以帮助确保对一个系统所做的更改不会对另一个系统产生不利影响。有关配置管理的详细信息,请参阅NIST SP 800-128。

常见的安全配置(也称为安全配置清单)提供了公认的、标准化的、已建立的基准,规定了信息技术平台和产品的安全配置设置。一旦实施,检查清单可用于从安全角度验证对系统的更改是否已经进行了审查。常见的审计检查系统的配置,看看是否发生了尚未分析的重大变化(如连接到互联网)。作为国家漏洞数据库(NVD)的一部分维护的NIST检查表存储库提供了多个检查表,可用于检查系统安全计划中指定的安全配置是否符合要求。这些清单可以在<https://web.nvd.nist.gov/view/ncp/repository>上访问。

配置管理控制的例子包括:基线配置、配置变更控制、安全影响分析、最小功能和软件使用限制。

组织:(i)建立和维护组织系统的基线配置和清单,包括硬件、软件、固件和各自SDLC中的文件;以及(ii)建立和实施组织系统中使用的信息技术产品的安全配置设置。

10.6应急计划(CP)

信息安全突发事件是指有可能破坏系统运行,从而破坏关键任务和业务功能的事件。此类事件可能是停电、硬件故障、火灾或风暴。特别具有破坏性的事件通常被称为“灾难”。为了避免潜在的突发事件和灾难或尽量减少它们造成的损害,组织可以采取早期措施来控制事件的结果。一般来说,这种活动被称为应急计划。

应急计划是一种管理政策和程序,用于指导组织的反应

对任务能力的感知损失。风险管理人员使用系统应急计划(SCP)来确定发生了什么、为什么发生以及应该做什么。对于重大中断，SCP可以指向运营连续性计划(COOP)或灾难恢复计划(DRP)。应急计划涉及的不仅仅是灾难摧毁数据中心后的异地迁移计划。它还涉及如何在发生大大小小的中断时保持组织的关键功能的运行。这种关于应急计划的更广泛的观点是基于整个组织中系统支持的分布。有关应急计划的更多信息，请参阅NIST SP 800-34。

应急计划控制的示例包括：应急计划、应急培训、应急计划测试、系统备份以及系统恢复和重构。

组织：(i)建立、维护并有效实施应急响应计划，(ii)备份操作，以及(iii)监督组织系统的灾后恢复，以确保紧急情况下关键信息资源的可用性和操作的连续性。

10.7 身份识别和认证(IA)

对于大多数系统来说，识别和认证通常是第一道防线。识别是验证用户、进程或设备身份的手段，通常作为授予对系统中资源的访问权限的先决条件。识别和认证是一种防止未经授权的个人或进程进入系统的技术措施。

身份识别和身份验证是信息安全的关键组成部分，因为它是大多数类型的访问控制和建立用户责任的基础。访问控制通常要求系统能够识别和区分不同的用户。例如，访问控制通常基于最小权限，即只授予用户履行职责所需的访问权限。用户问责制要求将系统上的活动与特定的个人联系起来，因此要求系统识别用户。

系统根据系统接收到的认证数据来识别个人。身份验证提出了几个挑战：收集身份验证数据，安全地传输数据，以及知道最初经过身份验证的个人是否仍然是使用该系统的个人。例如，用户可能在仍然登录的情况下离开终端，而另一个人可能开始使用该终端。

验证用户身份的方法有四种，可以单独使用，也可以组合使用。用户身份可以通过以下方式进行认证：

- 个人知道的东西——例如；密码或个人识别号码(PIN)；
- 个人拥有的东西(令牌)——例如；ATM卡或智能卡；
- 个人的身份(静态生物识别)——例如；指纹、视网膜、面部；以及
- 个人行为(动态生物识别)——例如；语音模式，笔迹，打字节奏

虽然这些方法中的任何一种似乎都可以提供强大的身份验证，但每种方法都有相关的问题。如果一个人想在系统上冒充其他人，他们可以猜测或学习另一个用户的密码或窃取或制造令牌。每一个

对于合法用户和系统管理员来说，该方法也有缺点：用户忘记密码并可能丢失令牌，跟踪标识和授权数据以及令牌的管理开销可能很大。生物识别系统也存在重大的技术、用户接受度和成本问题。

识别和认证控制的例子包括：设备识别和认证、标识符管理、认证者管理、认证者反馈和重新认证。

组织：(i)识别系统用户、代表用户的过程或设备；(ii)认证或验证这些用户、过程或设备的身份，作为允许访问组织系统的先决条件。

10.8 个人参与(IP)

与信息正在被系统处理的个人进行接触，是隐私保护和可信系统开发的重要方面。系统功能可以对人们的生活质量和他们成为自主个体的能力产生重大影响。有效的参与有助于减轻这些风险，防止一系列问题的发生。例如，个人可能会感到被系统监视，这可能会对日常行为产生寒蝉效应，或导致他们以意想不到的方式改变与系统的互动。他们可能会觉得信息被挪用了一—或被用于利润或组织利益，而没有得到他们的许可或获得足够的经济利益。排除对信息的获取可能会影响数据质量，从而可能导致对用户不利的决策，包括对获取产品或服务的不适当限制或其他类型的歧视。

个人参与控件处理用户与系统的交互，使他们能够对系统如何处理有关他们的信息作出可靠的假设。此外，这些控制创建了接触点，以便用户可以更好地参与系统和管理他们的信息。有能力参与有关其信息处理的决策的用户可能更有可能对系统产生信任，并以建设性的方式与系统互动。此外，使用户能够纠正不准确的信息可以改善系统功能，并保护这些用户免受基于不准确信息处理的系统操作所产生的问题。

通过个人参与控制，组织可以随时通知个人其PII的处理情况。在适当的情况下，这些控制还通过信息访问和同意选项，使个人积极参与有关其PII的决策过程，并为他们提供通过适当的补救机制纠正或修改其PII的能力。

个人参与控制的例子包括：同意、补救、隐私通知、联邦机构隐私法声明和个人访问。

组织：(i)请求同意处理PII；(ii)提供查阅PII的机会，并为个人提供修正或更正PII的机会；以及(iii)就PII的处理向个人发出通知。

10.9事件响应(IR)

系统会受到各种威胁事件的影响，从损坏的数据文件到病毒再到自然灾害。对于某些威胁事件的脆弱性，可以通过拥有相关的标准操作程序来减轻，这些程序在发生事件时可以遵循。例如，经常发生的错误删除文件之类的事情，通常可以通过从备份文件中恢复来修复。更严重的威胁事件，如自然灾害造成的中断，通常会在组织的应急计划中解决。

威胁事件也可能由病毒、其他恶意代码或系统入侵者(内部人员或外部人员)引起。它们可以更普遍地指那些在没有技术专家响应的情况下可能导致严重损害的事件。需要立即进行技术响应的威胁事件的一个例子是，组织遭受了拒绝服务攻击。这种攻击需要事件响应团队迅速采取行动，以减少攻击对组织的影响。威胁事件的定义有些灵活，可能因组织和计算环境而异。

虽然黑客和恶意代码对系统和网络构成的威胁是众所周知的，但这种有害事件的发生仍然是不可预测的。大型网络(如互联网)上的安全事件，如入侵和服务中断，已经损害了各种组织的计算能力。当最初遇到此类事件时，大多数组织以一种临时的方式作出反应。然而，类似事件的反复发生可以使开发快速发现和响应此类事件的标准能力具有成本效益。这一点尤其正确，因为如果不加以控制，事件往往会“蔓延”，从而使损害升级并严重损害组织。

事件处理与应急计划密切相关。事件处理能力可以被视为应急计划的一个组成部分，因为它允许对正常处理中的中断快速有效地作出反应的能力。一般来说，应急计划处理有可能中断系统运行的事件。事件处理可以被认为是应急计划的一部分，专门用于响应恶意技术威胁。有关事件响应的更多信息，请参阅NIST SP 800-61，计算机安全事件处理指南。

事件响应控制的示例包括:事件响应培训、事件响应测试、事件处理、事件监控和事件报告。

组织:(i)为组织系统建立可操作的事件处理能力，包括充分的准备、检测、分析、遏制、恢复和用户响应活动;以及(ii)跟踪、记录并向适当的组织官员和/或当局报告事件。

10.10维护(MA)

为了保持系统处于良好的工作状态，并将硬件和软件故障的风险降至最低，组织建立维护组织系统的程序是至关重要的。一个组织有许多不同的方法来满足这些维护需求。

系统的受控维护是指按照制造商的规格安排和执行的维护。在系统之外进行的维护

预定周期，称为纠正性维护，发生在系统发生故障或产生必须纠正的错误条件以使系统恢复到运行条件时。维护可以在本地或非本地进行。非本地维护是由通过内部或外部网络(例如Internet)通信的个人执行的任何维护或诊断。

维护控制的例子包括:受控维护、维护工具、非本地维护、维护人员和及时维护。

组织:(i)对组织系统进行定期和及时的维护;以及(ii)对用于进行系统维护的工具、技术、机制和人员提供有效控制。

10.11媒体保护(MP)

媒体保护是一种解决系统媒体防御的控制，可以将其描述为数字媒体和非数字媒体。数字媒体的例子包括:软盘、磁带、外部/可移动硬盘驱动器、闪存驱动器、光盘和数字视频磁盘。非数字媒体的例子包括纸张或缩微胶卷。

媒体保护可以限制访问并使媒体仅供授权人员使用，对敏感信息应用安全标签，并提供关于如何从媒体中删除信息以使信息无法检索或重建的说明。媒体保护还包括物理控制系统媒体和确保问责制，以及限制能够存储和携带信息进入或离开限制区域的移动设备。

媒体保护控制的例子包括:媒体访问、媒体标记、媒体存储、媒体运输和媒体消毒。

组织:(i)保护系统媒体，包括纸质和数字媒体;(ii)限制授权用户访问系统媒体上的信息;以及(iii)在处置或释放以供再利用之前对系统介质进行消毒或销毁。

10.12隐私授权(PA)

为了更好地保护个人隐私并限制因系统处理其信息而产生的问题，组织应该对个人可识别信息(PII)的收集、使用、维护和共享有一个明确的理由。过于宽泛的信息收集和维护可能会产生潜在的安全漏洞，或允许内部滥用或跨越隐私边界的扩展使用。个人可能会因其信息的泄露而蒙受耻辱，或遭受身份盗窃。与之共享信息的第三方可能会无视收集信息的目的或背景，并以与个人隐私利益相矛盾的方式使用该信息。因此，个人可能会对这些系统失去信任，这可能导致放弃或威胁采用新技术，即使是那些旨在改善公共服务获取的技术。

组织可能必须遵守外部法律或法规，以及与PII处理相关的内部政策。隐私授权控制可帮助组织确保仅以其有权和明确目的的方式处理PII。这种保证有助于组织对遵循相关的隐私授权负责

政策，并最大限度地减少潜在的违规成本和声誉损害。记录这些信息还有助于个人理解系统对其PII的处理。

隐私授权控制的示例包括：收集权限、目的规范和与外部方的信息共享。

组织：(i)确定授权收集、使用、维护和共享特定个人信息(PII)的法律依据；(ii)在其通知中指明收集PII的目的；以及(iii)管理与外部方的PII共享。

10.13物理与环境保护(PE)

物理和环境安全是指为保护系统、建筑物和相关配套基础设施免受与其物理环境相关的威胁而采取的措施。物理和环境控制涵盖三个广泛的领域：

1. 物理设施通常是容纳系统和网络组件的建筑物、其他结构或车辆。根据其操作位置，系统可以分为静态、移动或便携式。静态系统安装在固定位置的结构中。移动系统安装在执行结构功能的车辆中，但不安装在固定位置。便携式系统可以在各种各样的地点操作，包括建筑物、车辆或露天场所。这些结构和车辆的物理特性决定了诸如火灾、屋顶泄漏或未经授权访问等物理威胁的级别。
2. 设施的一般地理运行位置决定了自然威胁的特征，包括地震和洪水；人为威胁，如入室盗窃、内乱或截获传输和发射；以及破坏附近活动，包括有毒化学品泄漏、爆炸、火灾和发射器(如雷达)的电磁干扰。
3. 配套设施是指维持系统运行的服务(包括技术和人力)。系统的运行通常依赖于电力、供暖和空调、电信等配套设施。这些设施的故障或不合格的性能可能会中断系统的运行，并对系统硬件或存储的数据造成物理损坏。

物理和环境控制的例子包括：物理访问授权、物理访问控制、监控物理访问、紧急关闭、应急电源、应急照明、备用工作地点、信息泄漏、资产监控和跟踪。

组织：(i)将物理访问系统、设备和相应操作环境的权限限制为授权个人；(ii)保护系统的物理设备和支持基础设施；(iii)为系统提供配套设施；(iv)保护系统免受环境危害；(v)在包含系统的设施中提供适当的环境控制。

10.14规划(PL)

系统在组织中扮演着越来越重要的战略角色。它们协助组织进行日常活动并支持决策制定。通过适当的规划，系统可以提供与系统运行相关的风险相称的安全级别，提高生产力和性能，并启用新的管理和组织方式。系统规划对于组织信息安全目标的制定和实施至关重要。

制定系统安全计划(ssp)¹³是为了提供系统安全需求的概述，以及安全控制和控制增强如何满足这些安全需求。仅有安全控制措施并不能保证对系统的全面保护。组织还需要制定、记录和传播这些控制是如何实现的，描述用户责任的规则，以及组织如何从信息安全的角度操作系统。

规划控制的例子包括：系统安全计划、行为规则、操作的安全概念、信息安全架构和集中管理。

组织：制定、记录、定期更新和实施组织系统的安全计划，这些计划描述了为系统所实施的或计划的安全控制，以及访问系统的个人的行为规则。

10.15程序管理(PM)

系统及其处理的信息对于许多组织执行其任务和业务功能的能力至关重要。管理人员将系统安全视为管理问题，并寻求保护组织的信息技术资源，就像保护任何其他有价值的资产一样，这是有道理的。要有效地做到这一点，需要开发一种全面的管理方法。

分布在整个组织中的许多安全计划都有执行各种功能的不同元素。虽然这种方法有好处，但许多组织中系统安全功能的分布是随意的，通常基于历史(即，当需要出现时，组织中谁可以做什么)。理想情况下，系统安全功能的分布是经过计划和集成的管理哲学的结果。

在多个层次上管理系统安全有其好处。每个级别都以不同类型的专业知识、权限和资源为整个系统安全计划做出贡献。一般来说，级别较高的官员(例如，上述机构中总部、单位级别的官员)对整个组织有更好的了解，并且拥有更多的权力。另一方面，较低级别的官员(例如，系统设施和应用级别的官员)更熟悉系统和用户的具体技术和程序要求和问题。系统安全程序管理的层次是互补的；每一层都可以帮助另一层更有效。

程序管理控制的例子包括：信息安全程序计划、信息安全资源、行动计划和里程碑过程、系统清单。

¹³ For more information on developing a System Security Plan, see NIST SP 800-18.

企业架构、风险管理策略、内部威胁程序、威胁感知程序。

10.16人员安全(PS)

用户在保护系统方面起着至关重要的作用，因为信息安全中的许多重要问题涉及用户、设计人员、实现者和管理人员。这些个人如何与系统交互以及他们完成工作所需的访问级别也会影响系统的安全状态。如果不妥善解决这些人员安全方面的问题，几乎没有一个系统能够得到安全保障。

人员安全旨在最大限度地减少员工(永久、临时或承包商)通过恶意使用或利用其对组织资源的合法访问而对组织资产构成的风险。员工的行为可能会对组织的地位和声誉造成不利影响。员工可能会接触到极其敏感、机密或专有的信息，这些信息的泄露可能会破坏一个组织的声誉或使其在经济上陷入瘫痪。因此，组织在招聘和雇用新员工时，以及员工调动或被解雇时，都必须保持警惕。组织资产的敏感性和价值需要深入的人员安全措施。

人员控制的例子包括：人员筛选、人员终止、人员调动、访问协议和人员制裁。

组织：(i)确保在组织(包括第三方服务提供商)内担任责任职位的个人是值得信赖的，并符合这些职位的既定安全标准；(ii)确保组织信息和系统在解雇和调动等人事行动期间和之后得到保护；(iii)对未遵守组织安全政策和程序的人员采取正式制裁。

10.17风险评估(RA)

组织依赖于信息技术和相关系统来成功地执行其任务。虽然各种组织和行业中使用的越来越多的信息技术产品可能是有益的，但在某些情况下，它们也可能引入严重的威胁，通过利用已知和未知的漏洞，对组织的系统产生不利影响。利用组织系统中的漏洞可能会危及这些系统正在处理、存储或传输的信息的机密性、完整性或可用性。

执行风险评估是NIST SP 800-39中描述的风险管理的四个组成部分之一。风险评估识别并确定系统运行可能对组织运营、资产、个人、其他组织和国家造成的风险的优先级。风险评估可以在风险管理层级的所有三个层次进行，通过识别以下内容为决策者提供信息并支持风险应对：(i)对组织的相关威胁或通过组织直接针对其他组织的威胁；(ii)组织内部和外部的脆弱性；(iii)考虑到利用漏洞的潜在威胁，可能对组织造成的影响(即伤害)；以及(iv)伤害发生的可能性。有关风险评估的更多信息，请参阅NIST SP 800-30。

风险评估控制的示例包括:安全分类、风险评估、漏洞扫描、技术监控对策调查。

组织:定期评估组织运行(如使命、职能、形象、声誉)、组织资产和个人所面临的风险，这些风险可能来自组织系统的运行以及组织信息的相关处理、存储或传输。

10.18系统和服务采购(SA)

与信息处理系统的其他方面一样，如果在系统的整个生命周期(从最初的计划到设计、实施、操作和处置)中进行规划和管理，安全性是最有效和最高效的。许多与安全相关的事件和分析发生在系统的生命周期中，从组织获得必要的工具和服务开始。将安全需求有效地集成到企业架构中还有助于确保重要的安全考虑因素在SDLC的早期得到处理，并且这些考虑因素与组织任务/业务流程直接相关。

ssp可以在系统生命周期的任何时间点进行开发。然而，为了最大限度地降低成本并防止正在进行的操作中断，建议的方法是在系统生命周期开始时纳入该计划。向系统中添加安全特性比从一开始就包含它们的成本要高得多。重要的是要确保安全需求与计算环境、技术和人员的变化保持同步。

系统和服务获取控制的例子包括:资源分配、获取过程、系统文档、供应链保护、可信度、关键性分析、开发人员提供的培训、组件真实性和开发人员筛选。

组织:(i)分配足够的资源以充分保护组织系统;(ii)采用纳入信息安全考虑的SDLC流程;(iii)采用软件使用和安装限制;以及(iv)确保第三方提供商采用适当的安全措施来保护组织外包的信息、应用程序和/或服务。

10.19系统和通信保护(SC)

系统和通信保护控制为系统提供了一系列保护措施。该系列中的一些控制解决了静态和传输中信息的保密性和完整性问题。这些控制可以通过物理或逻辑手段来提供保密性和完整性的保护。例如，组织可以通过将某些功能隔离到单独的服务器来提供物理保护，每个服务器都有自己的一组IP地址。

组织可以通过分离用户功能和系统管理功能来更好地保护他们的信息。提供这种类型的保护可以防止在非特权用户的界面上呈现与系统管理相关的功能。系统和通信保护还建立了边界，限制对系统内可公开访问的信息的访问。使用边界保护，组织可以监视和控制外部边界以及系统内关键内部边界的通信。

系统和通信保护控制的示例包括:应用分区、拒绝服务保护、边界保护、可信路径、移动代码、会话真实性、瘦节点、蜜罐、传输机密性和完整性、操作安全、静态和传输信息保护以及使用限制。

组织:(i)在系统的外部边界和关键内部边界对组织通信(即组织系统传输或接收的信息)进行监视、控制和保护;以及(ii)采用促进组织系统内有效信息安全的架构设计、软件开发技术和系统工程原则。

10.20 系统和信息完整性(SI)

完整性被定义为防止不正当的信息修改或破坏,包括确保信息的不可否认性和真实性。它是数据只能被授权人员访问或修改的断言。系统和信息完整性保证被访问的信息没有被系统中的错误干扰或损坏。

系统和信息完整性控制的例子包括:缺陷修复、恶意代码保护、安全功能验证、信息输入验证、错误处理、非持久性和内存保护。

组织:(i)及时识别、报告和纠正信息和系统缺陷;(ii)在组织系统内的适当位置提供针对恶意代码的保护;以及(iii)监控系统安全警报和建议,并作出适当回应。

Appendix A—References

- [CSA of Computer Security Act of 1987, Public Law 100-235, 101 Stat 1724
1987] <https://www.gpo.gov/fdsys/pkg/STATUTE-101/pdf/STATUTE-101-Pg1724.pdf>
- [E-Gov Act] E-Government Act of 2002, Public Law 107-347, 116 Stat 2899. <http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf>
- [Clinger-Cohen Act, Public Law 107-217, 116 Stat 1234.
Cohen Act] <https://www.gsa.gov/graphics/staffoffices/Clinger.htm>
- [FISMA₂₀₀₂] Federal Information Security Management Act of 2002, Pub. L. 107-347
(Title III), 116 Stat. 2946. <https://www.gpo.gov/fdsys/pkg/CHRG-107hhrg86343/pdf/CHRG-107hhrg86343.pdf>
- [FISMA₂₀₁₄] Federal Information Security Modernization Act of 2014, Pub. L. 113-283,
128 Stat. 3073. <http://www.gpo.gov/fdsys/pkg/PLAW-113publ283.pdf>
- [OMB Office of Management and Budget (OMB), *Managing Information as a Circular
A- Strategic Resource*, OMB Memorandum Circular A-130, Revised July 28,
130] 2016. <https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf>
- [FIPS140-2] U.S. Department of Commerce. *Security Requirements for Cryptographic
Modules*, Federal Information Processing Standards (FIPS) Publication 140-2, May
25, 2001 (with Change Notices through December 3, 2002), 69pp. <https://doi.org/10.6028/NIST.FIPS.140-2>
- [FIPS180-4] U. S. Department of Commerce. *Secure Hash Standard (SHS)*, Federal
Information Processing Standards (FIPS) Publication 180-4, August 2015, 36pp.
<https://doi.org/10.6028/NIST.FIPS.180-4>
- [FIPS186-4] U.S. Department of Commerce. *Digital Signature Standard (DSS)*, Federal
Information Processing Standards (FIPS) Publication 186-4, July 2013, 130pp.
<https://doi.org/10.6028/NIST.FIPS.186-4>
- [FIPS 197] U.S. Department of Commerce. *Advanced Encryption Standard*, Federal
Information Processing Standards (FIPS) Publication 197, November 2001, 51pp.
<https://doi.org/10.6028/NIST.FIPS.197>
- [FIPS199] U. S. Department of Commerce. *Standards for Security Categorization of
Federal Information and Information Systems*, Federal Information
Processing Standards (FIPS) Publication 199, February 2004, 13pp.

<https://doi.org/10.6028/NIST.FIPS.199>

[FIPS200] U.S. Department of Commerce. *Minimum Security Requirements for Federal Information and Information Systems*, Federal Information Processing Standards (FIPS) Publication 200, March 2006, 17pp. <https://doi.org/10.6028/NIST.FIPS.200>

[FIPS 202] U.S. Department of Commerce. *SHA-3: Permutation-Based Hash and Extendable-Output Functions*, Federal Information Processing Standards (FIPS) Publication 202, August 2015, 37pp. <https://doi.org/10.6028/NIST.FIPS.202>

[NISTIR Kissel, R., *Glossary of Key Information Security Terms*, NISTIR 7298

7298] Revision 2, National Institute of Standards and Technology, Gaithersburg, Maryland, May 2013, 222pp. <https://doi.org/10.6028/NIST.IR.7298r2>[NISTIR Brooks, S., Garcia, M., Lefkovitz, N., Lightman, S., Nadeau, E., An

8062] *Introduction to Privacy Engineering and Risk Management in Federal Systems*, NISTIR 8062, National Institute of Standards and Technology, Gaithersburg, Maryland, January 2017, 49pp. <https://doi.org/10.6028/NIST.IR.8062>

[SP800-18] NIST Special Publication (SP) 800-18 Revision 1, *Guide for Developing Security Plans for Systems*, National Institute of Standards and Technology, Gaithersburg, Maryland, February 2006, 48pp. <https://doi.org/10.6028/NIST.SP.800-18r1>

[SP800-30] NIST Special Publication (SP) 800-30 Revision 1, *Guide for Conducting Risk Assessments*, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2012, 95pp. <https://doi.org/10.6028/NIST.SP.800-30r1>

[SP800-32] NIST Special Publication (SP) 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, National Institute of Standards and Technology, Gaithersburg, Maryland, February 2001, 54pp. <https://doi.org/10.6028/NIST.SP.800-32>

[SP800-34] NIST Special Publication (SP) 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems*, National Institute of Standards and Technology, Gaithersburg, Maryland, May 2010 (updated November 2010), 149pp. <https://doi.org/10.6028/NIST.SP.800-34r1>

[SP800-37] NIST Special Publication (SP) 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Systems: A Security Life Cycle Approach*, National Institute of Standards and Technology, Gaithersburg, Maryland, February 2010 (updated June 2014), 102pp. <https://doi.org/10.6028/NIST.SP.800-37r1>

[SP800-39] NIST Special Publication (SP) 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, National Institute of Standards and Technology, Gaithersburg, Maryland, March 2011, 88pp. <https://doi.org/10.6028/NIST.SP.800-39>

[SP800-53] NIST Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Systems and Organizations*, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2013 (updated January 2015), 462pp.

<https://doi.org/10.6028/NIST.SP.800-53r4>

[SP800-53A] NIST Special Publication (SP) 800-53A Revision 4, *Assessing Security and Privacy Controls in Systems and Organizations*, National Institute of Standards and Technology, Gaithersburg, Maryland, December 2014, 487pp. <https://doi.org/10.6028/NIST.SP.800-53Ar4>

[SP800-57] NIST Special Publication (SP) 800-57 part 1 Revision 4, *Recommendation*

part 1] *for Key Management, Part 1: General*, National Institute of Standards and Technology, Gaithersburg, Maryland, January 2016, 160pp. <https://doi.org/10.6028/NIST.SP.800-57pt1r4>

[SP800-57] NIST Special Publication (SP) 800-57 part 2, *Recommendation for Key*

part 2] *Management, Part 2: Best Practices for Key Management Organizations*, National Institute of Standards and Technology, Gaithersburg, Maryland, August 2005, 79pp.

<https://doi.org/10.6028/NIST.SP.800-57p2>

[SP800-57] NIST Special Publication (SP) 800-57 part 3 Revision 1, *Recommendation*

part 3] *for Key Management, Part 3: Application-Specific Key Management Guidance*, National Institute of Standards and Technology, Gaithersburg, Maryland, January 2015, 102pp.

<https://doi.org/10.6028/NIST.SP.800-57Pt3r1>

[SP800-60] NIST Special Publication (SP) 800-60 volume 1 Revision 1, *Guide for Mapping Types of Information Systems to Security Categories*, National Institute of Standards and Technology, Gaithersburg, Maryland, August 2008, 53pp. <https://doi.org/10.6028/NIST.SP.800-60v1r1>

[SP800-61] NIST Special Publication (SP) 800-61 Revision 2, *Computer Security Incident Handling Guide*, National Institute of Standards and Technology, Gaithersburg, Maryland, August 2012, 79pp. <https://doi.org/10.6028/NIST.SP.800-61r2>

[SP800-82] NIST Special Publication (SP) 800-82 Revision 2, *Guide to Industrial Control Systems (ICS) Security*, National Institute of Standards and Technology, Gaithersburg, Maryland, May 2015, 247pp. <https://doi.org/10.6028/NIST.SP.800-82r2>

[SP800-95] NIST Special Publication (SP) 800-95, *Guide to Secure Web Services*, National Institute of Standards and Technology, Gaithersburg, Maryland, August 2007, 128pp.

<https://doi.org/10.6028/NIST.SP.800-95>

[SP800-122] NIST Special Publication (SP) 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2010, 59pp.

<https://doi.org/10.6028/NIST.SP.800-122>

[SP800-128] NIST Special Publication (SP) 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, National Institute of Standards and Technology, Gaithersburg, Maryland, August 2011, 88pp. <https://doi.org/10.6028/NIST.SP.800-128>

[SP800-137] NIST Special Publication (SP) 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2011, 80pp. <https://doi.org/10.6028/NIST.SP.800-137>

[SP800-147] NIST Special Publication (SP) 800-147, *BIOS Protection Guidelines*, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2011, 26pp. <https://doi.org/10.6028/NIST.SP.800-147>

[SP800-152] NIST Special Publication (SP) 800-152, *A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS)*, National Institute of Standards and Technology, Gaithersburg, Maryland, October 2015, 147pp. <https://doi.org/10.6028/NIST.SP.800-152>

[SP800-155] NIST Special Publication (SP) 800-155 (DRAFT), *BIOS Integrity Measurement Guidelines*, National Institute of Standards and Technology, Gaithersburg, Maryland, December 2011, 47pp. http://csrc.nist.gov/publications/drafts/800-155/draft-SP800-155_Dec2011.pdf

[SP800-160] NIST Special Publication (SP) 800-160, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, National Institute of Standards and Technology, Gaithersburg, Maryland, May 2016, 307pp. <https://doi.org/10.6028/NIST.SP.800-160>

[SP800-161] NIST Special Publication (SP) 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2015, 282pp.

<https://doi.org/10.6028/NIST.SP.800-161>

[SP800-162] NIST Special Publication (SP) 800-162, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*, National Institute of Standards and Technology, Gaithersburg, Maryland, January 2014, 46pp. <https://doi.org/10.6028/NIST.SP.800-162>

[SP800- NIST Special Publication (SP) 800-175A, *Guideline for Using 175A] Cryptographic Standards in the Federal Government: Directives, Mandates and Policies*, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2016, 44pp. <https://doi.org/10.6028/NIST.SP.800-175A>

[SP800-175B] NIST Special Publication (SP) 800-175B, *Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms*, National Institute of Standards and Technology, Gaithersburg, Maryland, March 2016, 81pp. <https://doi.org/10.6028/NIST.SP.800-175B>

Appendix B—词汇表**访问控制**

允许或拒绝特定请求的过程:1)获取和使用信息及相关信息处理服务;以及2)进入特定的物理设施(例如, 联邦大楼、军事机构、边境口岸入口)。

来源:fips 201-2**问责制**

安全目标, 它产生了对实体的行为进行唯一跟踪的需求。这支持不可否认、威慑、故障隔离、入侵检测和预防, 以及事后恢复和法律行动。

来源:SP 800-27 Rev. A**保证**

确信其他四个安全目标(完整性、可用性、保密性和可问责性)已被特定实现充分满足的理由。“充分满足”包括(1)正确执行的功能, (2)对(用户或软件)无意错误的充分保护, 以及(3)对故意渗透或旁路的充分抵抗。

来源:SP 800-27 Rev. A**攻击**

任何一种试图收集、破坏、拒绝、降级或破坏信息系统资源或信息本身的恶意活动。

来源:cnsi-4009**审核**

独立审查和检查记录和活动, 以评估系统控制的充分性, 以确保符合既定的政策和操作程序。

SOURCE:cnsi -4009**认证信息**

验证用户、进程或设备的身份, 通常作为允许访问系统中资源的先决条件。

SOURCE:fips 200**授权**

由高级官员作出的正式管理决策, 授权某一系统的运行或指定组织系统继承的共同控制, 并明确接受组织运行(包括使命、职能、形象和声誉)、组织资产、个人、其他组织、以及基于实施一套商定的安全和隐私控制措施的国家。也被称为运营授权。

**授权官(AO)
后门****SOURCE:管理和预算局通告A-130, 改编**

高级(联邦)官员或行政人员, 有权正式承担对组织运营(包括使命、职能、形象或声誉)、组织资产、个人、其他组织和国家在可接受的风险水平上运营系统的责任。

来源:SP 800-37 Rev 1**生物识别技术**

一种未被记录的进入计算机系统的方式。后门是一种潜在的安全风险。

来源:NIST SP 800-82 Rev 2

一种可测量的身体特征或个人行为特征, 用于识别申请人的身份, 或验证申请人声称的身份。面部图像、指纹和虹膜扫描样本都是生物识别技术的例子。

比特**来源:fips 201****挑战-响应协议**

值为0或1的二进制数。

来源:fips 180-4

一种认证协议, 验证者向请求者发送一个质询(通常是一个随机值或nonce), 请求者将该质询与一个秘密(通常通过将质询和共享秘密散列在一起, 或通过对质询应用私钥操作)组合在一起, 以生成发送给验证者的响应。验证者可以独立地验证索赔人生成的响应(例如通过重新计算挑战和共享秘密的哈希值并与响应进行比较, 或对响应执行公钥操作), 并确定索赔人拥有并控制该秘密。

校验和**来源:sp 800-63-2**

(A)由依赖于数据对象内容的函数计算的值, (b)与对象一起存储或传输的值, 用于检测数据的变化

密文**来源:IETF RFC 4949 Ver. 2**

加密形式的数据。

**拒绝服务
数字签名**

来源:SP 800-57 Part 1 Rev. 4

防止授权访问资源或延迟时间关键操作。(时间关键可能是毫秒，也可能是小时，这取决于所提供的服务)。

加密

来源:cnssi-4009

对数据进行加密转换的结果，如果实现得当，可以提供以下服务:1;来源认证，2;数据完整性，以及3。签名者不可否认性。

端到端加密

来源:fips 140-2

对数据进行加密变换以产生密文。

防火墙

根据本地安全策略限制网络间访问的网关。

来源:sp 800-32

网关

一种中间系统(接口、中继)，它连接到两个(或多个)具有相似功能但实现方式不同的计算机网络，使网络之间能够进行单向或双向通信。

来源:IETF RFC 4949 Ver. 2

黑客

试图或获得访问信息系统的未经授权的用户。

来源:cnssi-4009

I事件

实际或潜在危害信息系统或系统处理、存储或传输的信息的保密性、完整性或可用性的事件，或构成违反或即将威胁违反安全政策、安全程序或可接受使用政策的事件。

来源:fips 200

信息

1. 事实和想法，可以被表示(编码)为各种形式的数据。

2. 知识——例如,数据、指令——可以在系统实体之间交流的任何媒介或形式。

来源:IETF RFC 4949 Ver. 2

**I信息保障
I信息安全**

通过确保信息和信息系统的可用性、完整性、身份验证、机密性和不可抵赖性来保护和防御信息和信息系统的措施。这些措施包括通过整合保护、检测和反应能力来提供信息系统的恢复。

注:DoDI 8500.01已从术语“信息保障(IA)”过渡为术语“网络安全”。这可能会影响到IA相关的术语。

I信息安全政策

来源:cnssi-4009

保护信息和信息系统免受未经授权的访问、使用、披露、中断、修改或破坏,以提供机密性、完整性和可用性。

I信息安全风险

资料来源:《美国法典》第44编第3542节

规定组织如何管理、保护和分发信息的指令、法规、规则和实践的总和。

I信息系统

来源:cnssi-4009

对组织运营(包括使命、职能、形象、声誉)、组织资产、个人、其他组织和国家因信息和/或系统可能遭到未经授权的访问、使用、披露、破坏、修改或破坏而造成的风险。

资料来源:SP 800-30 Rev 1

为收集、处理、维护、使用、共享、传播或处置信息而组织起来的一组离散的信息资源。[注:信息系统还包括专门的系统,如工业/过程控制系统、电话交换和专用交换机(PBX)系统以及环境控制系统。]

资料来源:44 u.s.c., Sec. 3502

I信息技术	(A)就执行机构而言，是指用于执行机构自动获取、存储、分析、评估、操作、管理、移动、控制、显示、切换、交换、传输或接收数据或信息的任何设备或互联系统或设备子系统;如果该设备由执行机构直接使用，或由承包商根据与执行机构签订的要求使用该设备的合同使用- (i);或(ii)该设备在执行服务或提供产品方面的重要程度;(B)包括计算机、辅助设备(包括成像外围设备、输入、输出和安全和监视所需的存储设备)、设计由计算机中央处理单元控制的外围设备、软件、固件和类似程序、服务(包括支持服务);及相关资源;但(C)不包括联邦承包商附带获得的任何设备。
I诚信	
入侵检测系统(IDS)	

关键字 资料来源:《美国法典》第40卷第11101节

防范不当的信息修改或破坏，并包括确保信息的不可否认性和真实性。

来源:《美国法典》第44编第3542节

使入侵检测过程自动化的软件。

来源:sp 800-94

密钥管理 与决定其操作的加密算法一起使用的参数。

适用于本标准的示例包括:

1. 从数据中计算出数字签名，并且
2. 对数字签名的验证。

来源:fips 186-4

在密钥的整个生命周期中，涉及处理加密密钥和其他相关安全参数(如初始化向量)的活动，包括密钥的生成、存储、建立、输入和输出、使用和销毁。

来源:SP 800-57 Part 1 Rev 4

**按键监控
最小权限**

在交互会话期间，用来查看或记录计算机用户输入的按键和计算机的响应的过程。击键监控通常被认为是审计跟踪的一种特殊情况。

安全体系结构的设计原则，应使每个实体被授予执行其功能所需的最小系统资源和授权。

链路加密**来源:cnsi -4009**

通信系统节点之间的信息加密。

逻辑炸弹**来源:cnssi-4009**

故意插入到软件系统中的一段代码，在满足指定条件时将触发恶意功能。

恶意代码**来源:cnssi-4009**

用于执行将对系统的机密性、完整性或可用性产生不利影响的未经授权进程的软件或固件。感染主机的病毒、蠕虫、特洛伊木马或其他基于代码的实体。间谍软件和某些形式的广告软件也是恶意代码的例子。

恶意软件**来源:sp 800-53**

参见恶意代码。

密码**来源:sp 800-53**

用于验证身份或验证访问授权的一串字符(字母、数字和其他符号)。

来源:fips 140-2**渗透测试**

一种测试方法，评估人员通常在特定的约束下工作，试图绕过或破坏系统的安全特性。

网络钓鱼**来源:sp 800-53**

一种试图通过电子邮件或网站上的欺诈性请求获取敏感数据(如银行账号)的技术，在这种技术中，犯罪者伪装成合法用户

**私钥
特权**

商业或信誉良好的人。

来源:IETF RFC 4949 Ver 2

一种加密密钥，与公钥加密算法一起使用，它与一个实体唯一地关联，并且不公开。

来源:fips 140-2**公钥**

授予个人、程序或过程的权利

来源:cnssi-4009

与公钥加密算法一起使用的加密密钥，该密钥与一个实体唯一关联，并且可以公开。

公钥加密**来源:fips 140-2**

使用公私密钥对进行加密和/或数字签名的加密系统。

来源:cnssi-4009**公钥基础设施(PKI)**

为颁发、维护和撤销公钥证书而建立的框架。

来源:fips 186-4**互惠**

参与企业之间相互同意接受彼此的安全评估，以便重用信息系统资源和/或接受彼此评估的安全态势，以便共享信息。

资料来源:nist sp 800-37**风险**

衡量一个实体受到潜在环境或事件威胁的程度，通常是以下因素的函数:(i)如果环境或事件发生将产生的不利影响;以及(ii)发生的可能性。[注:与系统相关的安全风险是指因信息或系统的保密性、完整性或可用性丧失而产生的风险，并反映了对组织运营(包括使命、职能、形象或声誉)、组织资产、个人、其他组织和国家的潜在不利影响。对国家的不利影响包括，例如，对支持关键基础设施应用或至关重要的系统的危害

由国土安全部定义的政府运作连续性。]

来源:sp 800-37

识别系统运行所产生的对组织运营(包括使命、职能、形象、声誉)、组织资产、个人、其他组织和国家的风险的过程。风险管理的一部分，包括威胁和脆弱性分析，并考虑由计划或到位的安全控制提供的缓解措施。与风险分析同义。

风险评估 风险管理

来源:sp 800-39

管理组织运营(包括使命、职能、形象、声誉)、组织资产、个人、其他组织和国家面临的信息安全风险的计划和支持过程，包括:(i)建立风险相关活动的环境;(ii)评估风险;(iii)一旦确定，对风险作出反应;(iv)随时间监测风险。

风险管理框架 (RMF)

来源:sp 800-39

用于监督和管理企业风险的结构化方法。

来源:cnssi-4009

角色

在一个系统中，人员或其他系统实体可能被分配到的工作职能或雇佣职位。

来源:IETF RFC 4949 Ver 2

防护措施

为满足系统规定的安全要求(即保密性、完整性和可用性)而规定的保护措施。保障措施可能包括安全特征、管理约束、人员安全以及物理结构、区域和设备的安全。与安全控制和对策同义。

来源:fips 200

秘钥

与密钥加密算法一起使用的加密密钥，它与一个或多个实体唯一地关联，不应公开。

**安全
安全控制评估****来源:fips 140-2**

由于建立和维护保护措施而产生的一种状态，这种保护措施使企业能够在其使用信息系统的威胁带来风险的情况下执行其任务或关键功能。保护措施可能包括威慑、避免、预防、检测、恢复和纠正的组合，这些措施应构成企业风险管理方法的一部分。

安全控制**来源:cnssi-4009**

对系统中的管理、运行和技术安全控制进行测试和/或评估，以确定控制措施正确实施的程度，按预期运行，并在满足系统安全要求方面产生预期结果。

安全工程**来源:sp 800-37**

为保护系统及其信息的机密性、完整性和可用性而规定的管理、操作和技术控制(即保障措施或对策)。

来源:fips 199

一种跨学科的方法和手段，使安全系统得以实现。它侧重于在系统开发生命周期的早期定义客户需求、安全保护需求和所需的功能，记录需求，然后在考虑完整问题的同时进行设计、综合和系统验证。

安全标签**来源:cnsi -4009**

用于将一组安全属性与特定信息对象相关联的方法，作为该对象的数据结构的一部分。

灵敏度**来源:sp 800-53**

衡量信息所有者赋予信息的重要性，以表明信息是否需要保护。

来源:sp800 -60

署名 垃圾邮件	与攻击相关的可识别的、可区分的模式，例如病毒中的二进制字符串或用于获得对系统的未经授权访问的一组特定击键。 来源:sp 800-61 电子垃圾邮件或滥用电子讯息系统滥发未经请求的大量讯息。
间谍软件	来源:cnssi-4009
系统	在个人或组织不知情的情况下，秘密或秘密地安装到系统中以收集个人或组织信息的软件;恶意代码的一种。 来源:sp 800-53 通过相互作用或相互依赖而统一和规范的任何有组织的资源和程序的集合，以完成一套特定的功能。 注:系统还包括专门的系统，如工业/过程控制系统、电话交换和专用交换机(PBX)系统以及环境控制系统。
系统完整性	资料来源:sp 800-53 当系统以不受损害的方式执行其预期功能时所具有的质量，不受未经授权的系统操纵，无论是有意的还是偶然的。
系统安全规划	来源:sp 800-27 提供系统安全需求概述并描述为满足这些需求而实施或计划实施的安全控制的正式文件。
剪裁	来源:sp 800-18 基于以下因素修改安全控制基线的过程:(i)应用范围界定指南;(ii)必要时补偿安全控制的规范;(iii)通过明确的赋值和选择语句对安全控制中组织定义的参数进行规范。
威胁	来源:sp 800-37 任何可能对组织运作(包括使命、职能、形象或其他)产生不利影响的情况或事件

声誉)、组织资产、个人、其他组织或国家通过未经授权的访问、破坏、披露、修改信息和/或拒绝服务通过系统。

资料来源:sp800 -30

有可能造成不良后果或影响的事件或情况。

威胁事件**Token****来源:nist sp 800-30**

索赔人拥有和控制的东西(通常是密钥或密码), 用于验证索赔人的身份。

特洛伊木马**来源:sp 800-63-2**

一种计算机程序, 表面上具有有用的功能, 但同时也具有隐藏的、潜在的恶意功能, 可以规避安全机制, 有时会利用调用该程序的系统实体的合法授权。

可信计算基地**来源:cnssi-4009**

计算机系统内保护机制的总和, 包括硬件、固件和软件, 负责执行安全策略的组合。

来源:cnssi-4009**可信系统**

计算机硬件、软件和程序

1)合理安全, 不受入侵和误用;

2)提供合理水平的可用性、可靠性和正确操作;

3)合理地适合于执行其预期功能;以及

4)遵守普遍接受的安全程序。

来源:sp 800-32**V确认**

确认(通过提供强有力的、合理的、客观的证据)特定预期用途或应用的要求已经满足(例如, 已经提供了可信赖的凭证, 或者数据或信息已经按照一套定义的规则格式化;或者一个特定的过程已经证明, 被考虑的实体在所有方面都符合其定义的属性

或者需求)。

来源:cnssi-4009

V病毒

一种计算机程序，可以在未经用户许可或不知情的情况下自我复制并感染计算机。病毒可能破坏或删除计算机上的数据，利用电子邮件程序将自己传播到其他计算机，甚至清除硬盘上的所有内容。参见恶意代码。

来源:CNSSI-4009

V漏洞

信息系统、系统安全程序、内部控制或实施中可能被威胁来源利用的弱点。

资料来源:NIST SP 800-30 Rev 1

蠕虫

一种自我复制、自我传播、自我包含的程序，利用网络机制进行自我传播。参见恶意代码。

来源:cnssi-4009

Appendix C—缩略语

本文中使用的精选缩略语定义如下。

ac	访问控制
爱斯	高级加密标准
AO授权官方	
apt	高级持续威胁
高级持续威胁	意识和培训
非盟审计和问责制	
自带设备	
ca	安全评估与授权
CAP跨机构优先	
CC共同标准	
CEO首席执行官	
cio	首席信息官
ciso	首席信息安全官
CKMS加密密钥管理系统	
CM配置管理	
CMVP加密模块验证程序	
CNSSI国家安全系统指令委员会	
coop	运营计划的连续性
COTS商用现货	
CP应急计划	
CSP云服务提供商	
证监会计算机安全资源中心	
崔	受控非机密信息

DHS美国国土安全部

DRP灾难恢复计划

FIPS联邦信息处理标准FIRMR联邦资源管理条例第一届事件响应
小组论坛FISMA2002联邦信息安全管理法FISMA₂₀₁₄联邦信息安全
现代化法案FOIA信息自由法案

HTTP超文本传输协议

IA识别与认证

ICS工业控制系统

ICT信息与通信技术IDS入侵检测系统

IP个人隐私

IR事件回应

IRM信息资源管理ISAC信息共享与分析中心ISCM信息安全持续
监测ISO国际IT信息技术标准化组织

ITL信息技术实验室

MA维修

MAC消息认证码

MP媒体保护

NARA国家档案记录管理局

nist	国家标准与技术研究所
NVD	国家漏洞数据库
omb	管理和预算办公室
P.L.公法	
PA个人授权	
PBX专用分支交换机	
PE物理与环保	
PGP相当好的隐私性	
PII个人信息	
PIN个人识别号码	
PKI公钥基础设施	
PL规划	
PM项目管理	
PS人事安全	
RA风险评估	
RAID独立磁盘冗余阵列	
RMF风险管理框架	
s / mime	安全/多用途内部邮件扩展
SA系统和服务收购	
SAISO高级机构信息安全官	
SAOP高级机构隐私官	
SC系统和通信保护	
SCP系统应急预案	
SI系统与信息保护	
SP特刊	

SSE	System Security Engineer
SSO	System Security Officer
SSP	System Security Plan
TCB	Trusted Computing Base