D1：安全和风险管理

单元一：信息安全管理基础

1.1　理解和应用机密性、完整性和可用性的概念

A、信息安全的定义

业务视角：采取措施保护信息资产，使之不因偶然或者恶意侵犯而遭受破坏、更改及泄露，保证信息系统能够连续、可靠、正常地运行，使安全事件对业务造成的影响减到最小，确保组织业务运行的连续性。

安全视角：安全的核心目标是为关键资产提供可用性、完整性和机密性（CIA 三元组）保护。

B、信息安全的核心原则

信息安全的核心原则是为重要业务信息系统提供机密性、完整性和可用性（CIA 三元组）的保护。其中：

- 机密性（Confidentiality）：确保信息在存储、使用、传输过程中不会泄漏给非授权用户或实体。
- 完整性（Integrity）：确保信息在存储、使用、传输过程中不会被非授权篡改，防止授权用户或实体不恰当地修改信息，保持信息内部和外部的一致性。
- 可用性（Availability）：确保授权用户或实体对信息及资源的正常使用不会被异常拒绝，允许其可靠而及时地访问信息及资源。

所有的安全机制、控制和防护措施都是为了支撑这些原则中的一个或者多个，并且根据业务中动态变化的风险，来平衡一个或者多个 CIA 原则。这三个元组的对立面通常称为 DAD，即：泄漏、篡改、破坏。

C、除了 CIA 还有其它什么相关安全概念？

帕克里安（Parkerian Hexad）六元组架构，除了 CIA 三元组外还包括了：

- 真实性（Authenticity）：指信息确实来自其所有者，能够对伪造的信息进行鉴别。
- 实用性（Utility）：信息能够被用于特定的目的。

- 拥有或控制（Possession or control）：财务上能否确认一项资产，很重要的一个判断标准是看该项资源是否为本单位所拥有或能够控制。

除了帕克里安六元组架构之外，还可能会经常涉及一些其它基本安全概念。这些概念包括两个方面的：描述安全问题方面的概念和描述安全控制方面的概念。

其中描述安全问题方面的概念：

- 脆弱性（vulnerability）：指系统中允许威胁来破坏其安全性的缺陷。
- 威胁（threat）：指利用脆弱性而带来的任何潜在危害。
- 风险（risk）：指威胁利用信息系统的脆弱性的可能性以及带来的相应业务影响。
- 暴露（exposure）：指造成损失的实例。

其中描述安全控制方面的概念：

- 按类型分：行政类控制（administrative control）、技术类控制（technical control）、物理类控制（physical control）。
- 按功能分：预防性控制（Preventive）、检测性控制（Detective）、纠正性控制（Corrective）、威慑性控制（Deterrent）、恢复性控制（Recovery）、补偿性控制（Compensating）、指引性控制（Directive）

1.2 评估和应用安全治理原则

A、信息安全治理的定义

信息安全治理是一套信息安全解决方案和相互紧密联系的管理方法。信息安全治理提供了一个框架：定义目标、协调、实施和监督涉及所有安全相关方面。信息安全治理不仅仅是技术，同时信息安全治理经常放在一个层次较高的层面，保障业务的持续运行和向更好的方向发展。

B、信息安全治理的重要性

信息安全治理要把安全能力与业务战略、任务、使命和目标联系在一起，并支撑着组织的业务架构和目标。为了达到这样的目的：

- 作为管理层对于信息安全治理要关注以下内容：设定策略和战略的方向，提供安全活动资源，指派管理责任，设定安全计划的优先级，支持必须变更，定义与风险评估相关文化，从内外部审计获取保障以及坚持安全投资被度量和听取项目有效性的汇报。
- 作为安全专家对于信息安全治理要关注以下内容：要认识组织的愿景、任务和目标，掌握组织在其生命周期中的安全问题，理解组织中与安全相关的角色和责任，理解和保障信息安全策略的实施，理解和保证企业符合法律、法规和道德的

要求。以此同时，安全专家需要和管理层建立联系，以确保这些目标的实现。

C、通过制定和实施信息安全计划达到安全目标

安全计划能确保安全策略的适当创建、实现和实施。安全计划将安全功能与组织的战略、目标、任务和愿景相结合，这包括根据商业论证、预算限制或稀缺资源设计和实现安全性。

安全计划由多个实体有机构成的框架，包括：管理、技术和物理类的保护机制，程序、业务过程和人。这些实体有些是模块，如果一个缺失或不完整，那么整个架构就会搜到影响；有些实体是过程，把相关安全机制能够有效的连接起来，并通过一定的顺序为企业信息系统提供保护级别。解决安全计划编制的最有效方法是采用自上而下的方式，安全规划必须得到高级管理者的支持和批准。

安全计划主要包括四个阶段：计划和组织、实施、运营和维护、监测和评估。其中：

- 计划和组织阶段包括：建立管理承诺、建立监督指导委员会、评估业务驱动、开发组织的威胁配置文件、进行风险评估、开发安全框架、确定每个架构层面的解决方案、获得管理层的批准和支持；
- 实施阶段包括：分配角色和职责、开发和实现安全策略、实现安全架构、开发审计和监控解决方案、建立服务水平（SLA）和度量指标；
- 运营和维护阶段：遵守流程以确保架构中每个机制都满足基线要求，进行内部和外部审计，执行相关架构中要求的任务，管理服务水平协议（SLA）；
- 监测与评估阶段：审查和分析日志、评估架构目标和 SLA 的完成情况、形成结果报告、开会评审、制定开进计划并融入计划和组织阶段。

这里有不少的行业标准和经验值得我们借鉴，包括：

- 企业框架，如：Zachman、TOGAF 和 SABSA
  - Zachman 框架：是一个二维模型，“它使用了 6 个基本的疑问词（什么、如何、哪里、谁、何时、为何）和不同的视知观点（计划人员、所有者、设计人员、建设人员、实施人员和工作人员）二维交叉，”它给出了企业的一个整体性理解。
  - TOGAF（开放群组架构框架，The Open Group Architecture Framework，TOGAF）：是由美国国防部开发并提供了设计、实施和治理企业信息架构的方法。架构允许技术架构设计师从企业的不同视角（业务、数据、应用程序和技术）去理解企业，以确保开发出环境及组件所必需的技术，最终实现业务需求。
  - SABSA（舍伍德的商业应用安全架构，Sherwood Applied Business Security Architecture）：是一个分层模型，它在第一层从安全的角度定义了业务需求。
- 安全控制框架，如：COSO、COBIT

- ◆ COSO（反欺诈财务报告全国委员会发起组织委员会）：是由 COSO 于 1985 年开发的，旨在用来处理财务欺诈活动并汇报。COBIT 派生于 COSO 内部控制整合框架。
- ◆ COBIT （信息及相关技术的控制目标）：是一组由国际信息系统审计与控制协会（ISACA）和 IT 治理协会（ITGI）制定的一个治理与管理的框架。COBIT 规定了安全控制的目标和要求，鼓励将 IT 的理想安全目标映射到商业目标中。COBIT 5 的基础是企业 IT 治理和管理的 5 条关键原则：原则 1 ：满足利益相关者的需求；原则 2：对企业做到端到端的覆盖：原则 3：使用单一的集成框架；原则 4：使用整合处理法：原则 5：把治理从管理中分离出来。COBIT 不仅可用于计划组织的盯安全， 也可以作为组织审计师的指导方针。

■ 安全管理架构，如 ISO/IEC 27000 系列
- ◆ ISO/IEC 27000 系列 ISO 和 IEC 联合开发的关于如何开发和维护信息安全管理体系（ISMS）的国际标准，主要包括：
  - ● ISO/IEC 27000：概述和词汇
  - ● ISO/IEC 27001：ISMS 要求
  - ● ISO/IEC 27002：信息安全管理实践措施
  - ● ISO/IEC 27003：信息安全管理体系实施指南
  - ● ISO/IEC 27004：信息安全管理衡量指南与指标框架
  - ● ISO/IEC 27005：信息安全风险管理指南

■ 过程管理开发，如 ITIL 和 CMMI
- ◆ ITIL：用于 IT 服务管理的过程。
- ◆ CMMI（能力成熟度模型集成）：用来作为确定组织流程成熟度的一种方式。

D、组织中角色、责任和评价

安全角色是指个人在组织内的安全实施和管理总体方案中所扮演的角色。接下来，我们概要要介绍一下企业中 6 种安全角色和责任：

■ 高级管理层：组织所有者(高层管理者)的角色被分配给最终负责组织机构安全维护和最关心保护资产的人。高层管理者必须对所有策略问题签字，高层管理者对安全策略的认同表明承认在组织机构内部实现的安全性的所有权。高层管理者对安全解决方案的总体成败负有责任，并且负责对组织机构建立安全性予以适度关注并尽职尽责。在大多数情况下，相应的责任会被委派给组织内部的安全专家。

■ 安全专家：安全专家、信息安全官或计算机应急响应团队（CIRT）的角色被分配给受过培训和经验丰富的网络工程师、系统工程师和安全工程师，他们对落实高层管理部门下达的指示负责。安全专家的职责是保证安全性，包括制定和实现安全策略。安全专家不是决策制定者， 他们只是实现者。

■ 数据所有者（Data Owner）：数据所有者的角色被分配给在安全解决方案中为了放置和保护信息而负责对信息进行分类的人。通常， 数据所有者是层次较高的、

最终负责数据保护的管理者。数据所有者一般会将实际管理数据的任务委派给数据监管者员。

- 数据监管者（Data Custodian）：数据监管者的角色被分配给负责实施安全策略和上层管理者规定的保护任务的人员。数据监管者通过执行所有必要的措施为数据提供适当的 CIA 三元组(机密性、完整性和可用性)保护，并完成上层管理者委派的要求和责任。
- 用户（User）：用户(最终用户或操作者)的角色被分配给具有安全系统访问权限的任何人。用户负责了解组织的安全策略，并遵守规定的操作过程。
- 审计人员（Auditor）：审计人员负责测试和认证安全策略是否被正确实现以及衍生的安全解决方案是否合适。审计人员要完成遵守情况报告和有效性报告，高层管理者会审查这些报告。通过这些报告发现的问题，会由高层管理者转换成下达给安全专家或数据管理员的新指示。

在前面我们讲述了管理层和安全专家在信息安全治理中不同的关注点和责任，那么怎么衡量他们以及企业中其他人是否尽职尽责呢？我们一般从以下两个方式来衡量：

- 应尽职责（Due Diligence）：一般是指调查和了解公司面临的风险，并指派相应人员去缓解风险，并保持持续的更新。
- 应尽关注（Due Care）：一般是指开发和制定了相关的安全策略、流程和标准，并采取相关的措施去保护企业中相关的信息资产。

E、开发、文档化和实施安全策略、标准、指南、基线和措施

安全策略是高级管理层（或是选定的董事会和委员会）制定的一个全面声明，它定义了安全在组织内所扮演的角色。安全策略可以是组织化策略，也可以是针对特定问题的策略。在组织化安全策略中，管理层规定了应该如何建立安全计划，制定安全计划的目标，分配责任，说明安全的战略和战术价值，并且概述了应该如何执行安全计划。这种策略必须涉及相关法律、法规、责任以及如何遵守这些规范。组织化安全策略为组织内部未来的所有安全活动提供了范围和方向，还说明了高级管理层愿意接受多大的风险。常见的针对特定问题安全策略有：风险管理策略、脆弱性管理策略、数据保护策略、访问控制策略、业务连续性策略、日志聚集和审计策略、人员安全策略、物理安全策略、安全应用程序开发策略、变更控制策略、电子邮件策略、事件响应策略

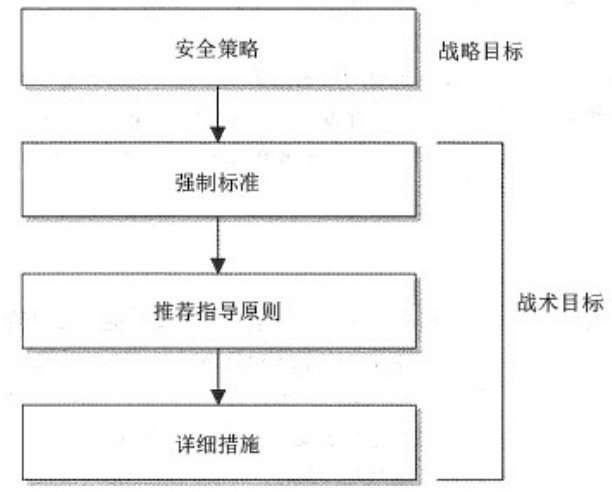
安全策略具有一些必须理解和实现的重要特征：业务目标应促进策略的制定、实现和执行。组织化安全策略应当是一份易于理解的文档，为管理层和所有员工提供参考；应当开发和用于将安全整合到所有业务功能和过程中；应当源于并支持适用于公司的所有法律法规；应当随公司的发展变化（如采用新的商业模式、与其他公司合并或者所有权发生变更）进行审核和修订；组织化安全策略的每次更迭都应当注明日期，并在版本控制下进行；受策略监管的部门和个人必须能够查看适用于他们的策略内容，并且不必阅读整个策略材料就能找到指导和答案；制定策略应以该策略一次性能够使用几年为目的。这将有助

于确保策略具有足够的前瞻性，从而能够处理将来的安全环境中可能出现的任何潜在变化；策略表述的专业水平能够强化其重要性以及遵守的必要性；策略中不应包含任何人都无法理解的语言。必须使用清楚的、易于理解和接受的陈述性声明；定期对策略进行审核，并根据自上一次审核和修订以来发生的事故加以改编。

安全策略（policies）一般由层次性的“策略链”组成，这包括信息策略（policy）、标准（standards）、指南（guidelines）、基线（baselines）和措施（procedures），其中：

- 策略/方针（policy）：是由高级管理层（或董事会）发布的关于安全一般性声明，代表着管理层对信息安全承担责任的一种承诺，一旦发布，组织全员必须遵守。
- 标准（standards）：标准是一种强制性的活动、动作和规则，能有效支撑策略该如何实施。
- 指南（guidelines）：当没有特定或强制标准来要求相关人员执行时，指南就能作为一种推荐的方式来提供参考。
- 基线（baselines）：一旦标准已经被建立，而且策略得以很好的实施，那么这时我们就能形成一个一致的参考点，这个参考点为我们的系统提供了必要的设置和保护级别。又是基线还被用于定义所需要的最低保护级别。
- 措施（procedures）：是为了达到特定目的而应当执行的详细的、分步骤的任务。措施一般说明了如何将策略、标准和指南应用到实际操作环境中。

如下图所示：策略是战略目标，是长期的；而标准、指南和措施是战术目标，一般是中短期的：



在许多企业里，我们制定了安全策略、标准、指南、基线和措施，并把它们写到了文档中，但最终这些文档最终放到了文件服务器中，而不被共享、解释或者使用。为了让这些文档能够有效，我们必须让企业中所有的人员通过培训和教育，了解这些文档涉及哪些安全问题，以及必须加以实现和实施。为了保证安全策略得以实施和保持，我们就需要审查相关人员是否尽职尽责，做到了“应尽职责”或“应尽关注”。

F、制定和执行人员安全管理

我们需要制定和执行相关的安全控制策略，来减低内部人员带来的风险，其中：

- 入职阶段：需要进行背景调查和签署保密协议
- 在职阶段：一般会开展如下活动：职责分离（Separation of duties）、工作轮换（Job rotation）、强制度假（Mandatory vacation）、须知原则（Need to Know）、最小特权原则（The Principle Of Least ）、保密协议（Non-Disclosure Agreement）、非竞争协议（Non-Complete Agreement）、监控（Monitoring）
- 离职阶段：制订一组特定的措施来管理每种解雇事件

1.3 法律、合规和道德

A、GRC 概述

GRC （ Governance, Risk Management, and Compliance)是一个日益被业界认可的通用术语，这一术语指的是企业采用一套集成的方法来应对治理、风险管理和合规三个方面的挑战。

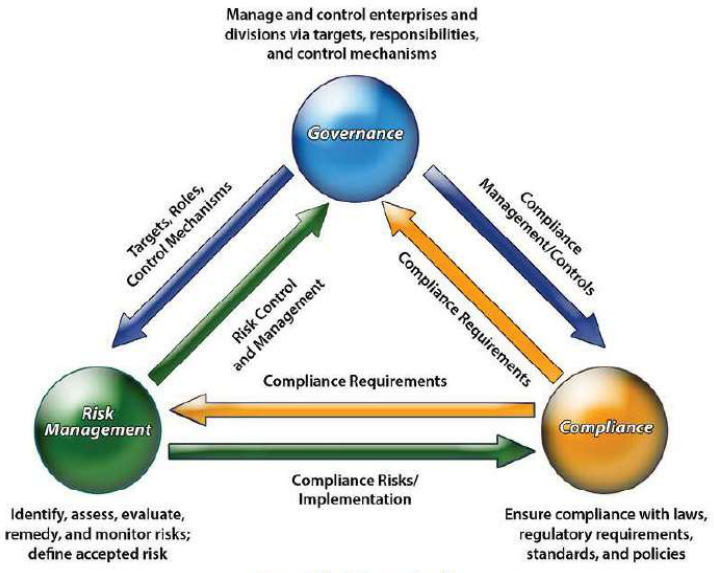


Figure 1.6 | GRC overview[8]

GRC 工作的目标是确保正确的策略和控制措施执行到位并降低风险，建立一种制衡机制，以便在新风险出现时提醒相关人员，能更有效和积极地管理业务流程。

B、知识产权

版权（Copyright）。版权覆盖许多类型的著作，如绘画、书法、音乐、戏剧、文字、哑剧、电影、雕塑、录音、建筑和源代码。版权法通常用于保护作者的作品、艺术家的画作、程序员的源代码或音乐家创作的旋律和结构。版权法不像商业秘密法那样保护特定的资源，它保护的是有资源意义的表达而不是资源本身。版权法保护原创作品的作者控制其原创作品公开发行、翻印、展览和修改的权利。

商标（Tradement）。商标和版权稍有不同，因为它用于保护一个单词、名称、符号、声音、形状、颜色、设备或这些项的组合。

专利（Patents）。专利是授予个人或公司的法律所有权，使他们能够拒绝其他人使用或复制专利所指的发明。发明必须是新奇的、有用的、非显而易见的。

商业秘密（Trade Secrets）。商业秘密是公司特有的资产，对其生存和盈利有很大作用。商业秘密法保护了这些资产不会被未授权使用或公开。

许可（Licensing）。许可协议包含与软件使用和安全相关的规定以及相应的手册。如果一个人或一家公司未能遵守或服从这些规定，那么许可证便被终止，并将根据具体行为来实施罚款。软件许可共有 4 种：

- 免费软件，是公众可以免费使用的软件，而且能够不受限制地使用、复制、研究、更改和重新分发。
- 共享软件或试用版软件，供应商使用共享软件或试用版软件来推销他们的软件产品。
- 商业软件，是一种为商业目的而销售或提供的软件。
- 学术软件，是为学术目的而提供的成本较少的软件，它可以是开放源代码软件、免费软件或商业软件。

C、隐私相关法律

欧盟《通用数据保护条例》（General Data Protection Regulation，GDPR）由欧盟推出，目的在于遏制个人信息被滥用，保护个人隐私。该条例的适用范围极为广泛，任何收集、传输、保留或处理涉及到欧盟所有成员国内的个人信息的机构组织均受该条例的约束。根据 GDPR 的规定，企业在收集、存储、使用个人信息上要取得用户的同意，用户对自己的个人数据有绝对的掌控权，包括：

- 查阅权，用户可以向企业查询自己的个人数据是否在被处理和使用，以及使用的目的，收集的数据的类型等。
- 被遗忘权，用户有权要求企业把自己的个人数据删除，如果资料已经被第三方获取，用户可以进一步要求它们删除
- 限制处理权，如果用户认为企业收集的个人数据不准确，或者使用了非法的处理

手段，但又不想删除数据的话，可以要求限制它对个人数据的使用。

- 数据移植权，用户从一家企业转投另一家企业时，可以要求把个人数据带过去。前面一家企业需要把用户数据以直观的、通用的形式给用户。

经济合作与发展组织（OECD）旨在推动和改善世界各地人民经济、社会福祉的政策。OECD 隐私原则在许多国际隐私和数据保护法中都有使用，并且在许多隐私计划和实践中也有使用。八项隐私原则如下：收集限制原则、数据质量原则、目的规范原则、使用限制原则、安全保障原则、公开原则、个人参与原则、问责原则

D、(ISC)2 道德准则

保护社会、公共利益、必要的公共信任和信心、以及基础设施。

行为得体、诚实、公正、负责和遵守法律。

为委托人提供尽职的和胜任的服务工作。

发展和保护职业声誉。

单元二：安全风险管理

2.1 风险和风险管理

A、风险概述

风险（Risk）在信息安全领域是指信息资产遭受损坏并给企业带来负面影响的潜在可能性。

风险存在于上下文环境中，NIST SP 800-39 定义了三层风险管理：

- 组织层面：关注整个业务的风险，这意味着它会构建其余的会话，并设置重要参数，如风险容忍度。
- 业务流程层面：处理组织的主要功能有是风险的，例如定义组织与其合作伙伴或客户之间的信息流的关键性。
- 信息系统层面：从信息系统的角度解决风险。虽然这是我们将重点讨论的要点，但重要的是要了解其存在于（并且必须符合）其他更为全面的风险管理工作的背景下。

B、风险相关术

资产（Asset）：是指环境中应该加以保护的任何事物。

资产估值（Asset Valuation）：指的是根据实际的成本和非货币性支出为资产分配的货币价值。

威胁（Threat）：任何可能发生的、为组织或某种特定资产带来所不希望的或不需要的结果的事情都被称为威胁。

脆弱性（Vulnerability）：IT 基础架构或组织其它方面的缺陷、漏洞、疏忽、错误、局限性、过失或敏感之处。

暴露（Exposure）：暴露是指由于威胁而容易造成资产损失。

风险（Risk）：某种威胁利用脆弱性并导致资产损害的可能性。风险可以被定义为：风险= 资产 * 威胁 * 脆弱性

防护措施或对策（Safeguard）：是指能消除脆弱性或对付一种或多种特定威胁的任何方法。

攻击（Attack）：是威胁主体对脆弱性的利用。换句话说，攻击是任何有意利用组织安全基础架构的脆弱性并导致资产的损坏、损失或泄漏的企图。攻击还可以被视为是违反或未遵守组织安全策略的任何行为。

破坏（Breach）：是指发生安全机制被威胁主体绕过或阻挠的事情。

渗透（Penetration）：指的是威胁主体通过避开安全控制获得访问组织基础架构的权力并且能够直接危及资产安全的情况。

C、风险管理概述和的重要

风险管理是一个详细的过程，包括识别可能造成数据损坏或泄漏的因素，根据数据的价值与对策的成本来评估这些因素，以及为了减轻或降低风险而实现有成本效益的解决方案。主要目的是要将风险降低到一个可以接受的级别。

风险管理的整个过程被用来制定和实施信息安全策略。这些策略的目标是减少风险和支持组织的使命。

正确地实施风险管理意味着你全面了解组织，了解它所面临的威胁，知道应该采取什么样的应对措施来处理这些威胁，并持续监控以确保风险级别处于可接受的级别。

D、风险管理策略和团队、职责

信息安全风险管理（Information System Risk Management，ISRM）策略包括以下内容：

- ISRM 团队的目标
- 公司可接受的风险级别及其定义
- 风险识别的形式化过程
- ISRM 策略与组织的战略规划过程之间的联系

- ISRM 的职责以及履行这些职责的角色
- 风险和内部控制之间的映射关系
- 为响应风险分析而改变员工行为和资源分配的方法
- 风险与业绩目标和预算之间的映射关系
- 监控控制效率的主要指标
- 信息安全风险管理策略为组织的风险管理过程及措施奠定基础并指明方向，并应解决一切信息安全问题；还为信息安全风险管理团队如何向高级管理层通报公司风险信息以及如何正确执行管理层决定的风险缓解任务提供指导

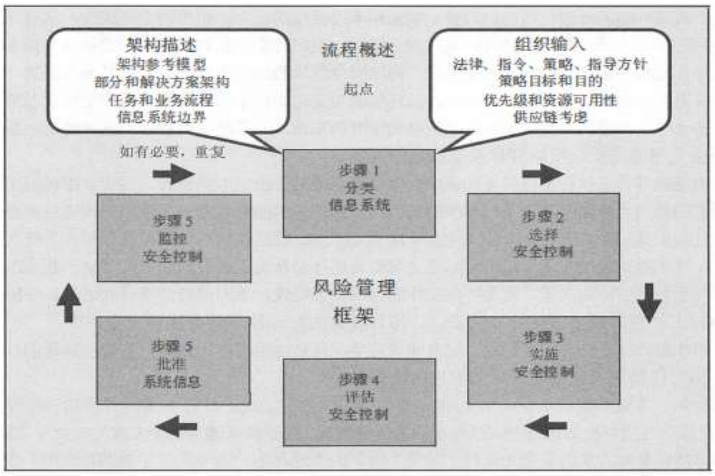
在大多数情况下，ISRM 团队成员并非由专门从事风险管理工作的员工组成，但一般一个组织可能只有一名员工负责 ISRM ，或者拥有一个协同合作的 ISRM 团队。 ISRM 团队的总体目标在于以最低预算确保公司安全，主要的工作内容和职责包括：

- 创建一个高级管理层支持的、明确的风险接受级别
- 记录风险评估过程与措施
- 识别和缓解风险的措施
- 恰当使用由高级管理层分配的资源与资金
- 对所有与信息资产有关的员工进行安全意识培训
- 如有必要，能够成立特定领域内的改进（或风险缓解）团队
- 制定法律及法规遵从要求计划，以控制和履行这些要求
- 开发衡量标准和业绩指标，以衡量和管理各种类型的风险
- 能够随环境和公司变化识别和评估风险
- 集成 ISRM 与组织的变更控制过程，保证这些变更不会形成新的脆弱性

E、风险管理框架和步骤

风险管理框架（Risk Management Framework）是有关如何评估、解决和监控风险的指南或方法。风险管理框架建立一般步骤（源自 NIST SP 800-37）包括：

- 分类：对信息系统和基于影响分析做过处理、存储和传输的系统信息进行分类
- 选择：基于安全分类选择该系统安全控制的初始化基线集；根据风险和当地情况的组织评估、调整和补充安全控制基线
- 实施：实施安全控制并描述如何在信息系统和操作环境中部署控制
- 评估：使用恰当的评估步骤评估安全系统，确定一个范围，在此范围内可以保证控制的正确实施、按计划运行且达到系统安全要求的预期效果
- 授权：基于对组织操作以及信息系统操作涉及的资金、个人、其他组织和国家风险的确定而授权信息系统操作， 并确定风险是可接受的
- 监控：不间断地监控信息系统中的安全控制，包括评估控制的有效性、记录系统变化或操作环境的变化、进行相关变化的安全影响分析以及向特定组织报告系统的安全状态



风险管理框架的特点包括：

- 通过实施强劲且持续不断的监管过程促进实时风险管理概念和不间断的信息系统授权概念的提升
- 鼓励通过自动化操作，向高层领导者提供必要的信息以帮助他们在组织信息系统方面做出基于风险且划算的决定， 以支持他们的核心任务和商业功能
- 将信息安全与公司系统结构以及系统开发生命周期（SDLC）相结合
- 强调选择、实施、评估、安全控制的监管以及信息系统的授权
- 通过风险管理(功能)将信息系统层面的风险管理过程与组织层面的风险管理过程相联系

2.2 风险评估和处置

A、风险评估定义

风险评估（风险分析），实际上是一种风险管理工具，是一种能够识别脆弱性和威胁以及评估可能造成的损失，从而确定如何实现安全防护措施的方法。风险评估主要是管理者的事情，管理者负责通过定义工作的范围和目标，启动和支持风险评估。执行风险评估的实际过程经常被委派给安全专家或评估团队。然而所有的风险评估、结果、决策和成果必须得到管理者的理解和批准并作为提供谨慎的适当关注。风险分析有下列 4 个主要目标：

- 标识资产和它们对于组织的价值
- 识别脆弱性和威胁
- 量化潜在威胁的可能性及其对业务的影响
- 在威胁的影响和对策的成本之间达到预算的平衡

B、风险评估团队

风险评估团队包括来自许多或全部部门的人员，以保证能够识别和处理所有的威胁。风险分析团队的成员可以是管理人员、应用程序编程人员、IT 人员、系统整合人员或运营部经理，事实上就是任何来自组织关键领域的关键人员。风险分析团队还必须包括了解各自部门工作流程的人，也就是每个部门中适当级别的人员。

C、风险评估流程

NIST 开发了一套执行风险评估的指导，出版在 SP 800-30 修订版 1 文档中。NIST 方法专门针对信息系统威胁及其与信息安全风险的关联方式。这种方法使用下列步骤：

1. 评估准备

2. 进行评估：a.识别威胁源和事件；b.识别威胁和诱发条件；c.确定发生的可能性；d. 确定影响的大小；e.确定风险

3. 沟通结果

4. 维持评估

FRAP，即便利的风险分析过程(Facilitated Risk Analysis Process)。这种定性方法的核心是只关注那些的确需要评估以降低成本和时间的系统。这种方法强调对活动进行筛选，从而只对最需要进行风险评估的项目进行评估。

OCTAVE（操作性关键威胁、资产和脆弱性评估）。这种方法专门为管理和指导公司内的信息安全风险评估的人员设计，它将组织内的工作人员放在权力位置，使其能够决定评估组织安全的最佳方式。

AS/NZS 4360 则采取了一种更广泛的方式来进行风险管理。这种方法可用于了解公司的财务、资本、人员安全和业务决策风险。这个方法更从商业的角度而不是安全的角度来关注公司的健康情况。

ISO/IEC27005 是一个国际标准，规定在 ISMS 框架内如何进行风险管理。如果说 NIST 风险方法主要侧重 IT 和操作层面，这个方法则侧重 IT 和较软的安全问题（文档、人员安全和培训等）。

FMEA（失效模式和影响分析）是一种确定功能、标识功能失效并通过结构化过程评估失效原因和失效影响的方法。它常用于产品开发和运营环境中，其目标是标识最容易出故障的环节，之后或者修复故障或者实施控制以降低故障的影响。

CRAMM（中央计算和电信机构风险分析与管理方法），该方法由英国创建，其自动化工具由西门子公司负责销售。该方法分为 3 个不同的阶段：定义目标、评估风险和标识对策。

D、定量和定性风险评估

定量的方法推导出具体的概率百分比。这意味着定量分析方法会创建一个报告，该报告用货币形式表明风险的级别、潜在的损失、对策的成本以及防护措施的成本。定量风险分析的六个主要步骤或阶段

1. 列出资产清单和分配资产价值（asset value 或 AV）

2. 研究每项资产，生成每个资产所有可能威胁的列表。针对列出的每个威胁，计算暴露因子（EF）和单一损失期望（SLE）

3. 执行威胁分析，计算每种风险在一年内发生的可能性，也就是年发生比率（ARO）

4. 通过计算年度损失期望（ALE），得到每个威胁可能的总损失

5. 研究每个威胁的对策，然后基于应用的对策，计算 ARO 和 ALE 的变化

6. 针对每个资产的每个威胁的每个对策执行成本/效益分析。选择对每个威胁最适用的对策

另外一种风险分析方法是定性分析，这种方法不会为各个组件和损失赋予数值和货币价值。相反，定性方法将考查各种风险可能发生的场景，并基于不同的观点对各种威胁的严重程度和各种对策的有效性进行等级排列（一个全面的分析可能包含几百种场景）。定性分析技术包括判断、最佳实践、直觉和经验。收集数据的定性分析技术示例有 Delphi、集体讨论、情节串联、焦点群体、调查、问卷、检查表、单独会谈以及采访。风险分析团队将决定对需要进行评估的威胁所使用的技术以及在分析中融入的公司和个人的文化元素。

Delphi 技术是一种群体决策方法，它用于保证每一位成员都将自己对某个特定威胁会带来的后果的真实想法表达出来。这就避免了团队中的个人在赞同其他人的想法时感到有压力，并使得他们能够以独立和匿名的方式参与工作。

定性分析矩阵。为每一个可识别的脆弱性撰写一个场景，并且研究它是如何被利用的。最熟悉某种威胁的"专家"应当复查相应的场景，以保证它反映了实际威胁发生时的情况。然后，评估能够减少这种威胁所造成损失的防护措施，并且将每种防护措施应用到场景中。暴露可能性和损失可能性既可以使用高、中、低排序，也可以使用 1~5 或 1~10 的等级排序。

定量和定性风险评估的优缺点：

特征	定性的风险分析	定量的风险分析
是否使用复杂的函数	否	是
是否使用成本/效益分析	否	是
是否得到具体的值	否	是
是否要求猜测	是	否
是否支持自动化	否	是
是否需要大量的信息	否	是
是否客观	否	是
是否使用主要意见	是	否
是否要求付出很多时间和努力	否	是
能否提供有用的和有意义的结果	是	是

E、风险处置/响应

风险评估的结果包括：

- 所有资产的完整且详细的评估；
- 所有威胁和风险、发生概率以及一旦发生的损失范围的详细列表；
- 针对特定威胁的并且标识出有效性与 ALE 的防护措施和对策列表；
- 每种防护措施的成本/效益分析。

一旦完成风险分析，管理层就必须处理每种特定的风险。对于风险有下列几种可能的响应：

- 风险缓解/降低风险（Risk Mitigation/Reducing risk）是一种消除脆弱性或阻止威胁的防护措施的实施
- 风险转让/转移风险(Assigning Risk/Transferring Risk)是把风险带来的损失转嫁给另外一个实体或组织。购买保险和外包就是转让或转移风险的常见形式
- 风险接受(Risk Acceptance)是管理层对可能采用的防护措施进行成本/效益分析评估， 并且确定对策的成本远远超过风险可能造成的损失的成本。接受风险还意味着管理层已经同意接受风险发生所造成的结果和损失。风险容忍度(risk tolerance)是组织忍受发生风险所造成损失的能力，这也是所说的风险容忍和风险偏好
- 风险威慑（Risk Deterrence）是对可能违反安全策略的人员实施威慑的过程
- 风险规避（Risk Avoidance ）是选择另外一种与相关风险关联较少的替代活动的过程
- 风险拒绝（Risk Rejection）。最后 但也是令人无法接受的对风险的反应称为拒绝风险或忽略风险。否认风险的存在以及希望风险永远不会发生， 这都未做到适度关注， 不是正确的谨慎对待风险的反应

总风险指的是在没有实现防护措施的情况下组织将要面对的风险数量。计算总风险的公式：威胁*脆弱性*资产价值=总风险

总风险和剩余风险之间的差值被称为控制间隙(controls gap)。控制间隙是指通过实现防护措施被减少的风险数量。计算剩余风险的公式是: 总风险 - 控制间隙=剩余风险

2.3 理解和应用威胁建模的概念和方法

A、威胁建模定

威胁建模是潜在威胁被识别、分类和分析的安全流程。威胁建模在设计和开发过程中可以作为一种积极主动的措施执行，而一旦产品被部署就会被作为一种被动式措施。在这

两种情况下，流程会识别潜在危害、发生的概率、问题优先级以及消除或减少威胁的手段

威胁建模的目标：减少安全相关的设计和编码缺陷的数量、降低剩余缺陷的严重程度，最终减少风险。

威胁建模的主动式方法发生于系统开发的早期阶段，特别是在初始设计和规范建立阶段。这种类型的威胁建模也被称为防御方式。这种方式基于编码和制作流程中，并对威胁的预测和特定防御进行设计，而不是依靠部署之后的更新或打补丁。大多数情况下，集成安全解决方案更符合成本效益，比后面硬塞的方案更成功。遗憾的是，并不是所有的威胁都可以在设计阶段预测出来，所以仍然需要被动式的威胁建模来解决不可预见的问题。

威胁建模的被动式方法发生在产品被创建和部署之后。此部署可以在测试或实验室环境中，或是指被部署到一般市场上。这种类型的威胁建模也被称为对抗方式。这种威胁建模的技术是道德黑客攻击、渗透测试、代码审查和模糊测试背后的核心概念。

威胁建模并不意味着是一个单独的事件，会随着时间和系统生命周期发生变化，因此要动态的进行调整。

B、威胁建模方法

威胁建模有三种通用方法，安全专业人员需要理解这三种基本方法并将其应用到特定环境，其中：

- 以攻击者为中心：这种威胁建模方法开始于确定可能对系统造成危害的各种攻击者。
- 以资产为中心：这与以攻击者为中心的方法相反，以资产为中心的威胁模型首先确定的是资产价值，然后评估资产的管理、操作、使用和存储方式，以识别攻击者可能如何危害资产。
- 以系统（软件）为中心：对于许多信息系统来说，以系统或软件为中心的方法是最有用的，在这种方法中，系统被表示为一组交互的过程，通常使用的就是数据流，然后分析人员对这些数据流图进行评估，确定控制措施是否必要、是否存在以及是否达到控制效果。

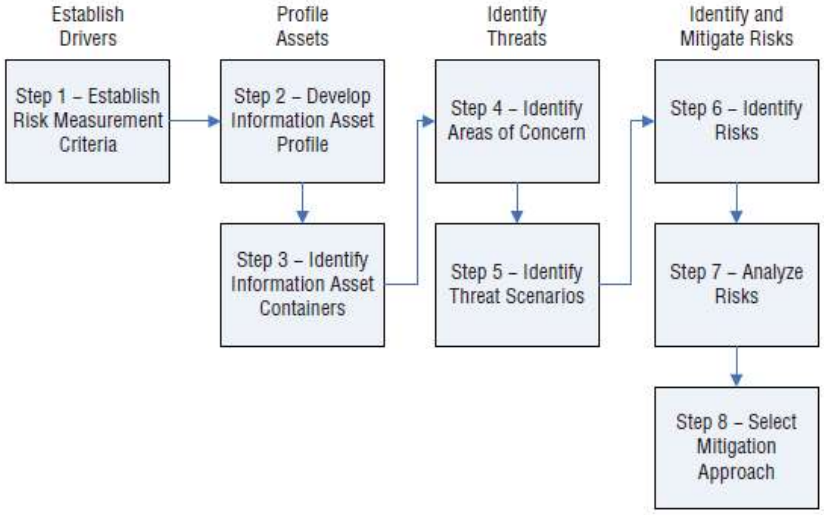
目前，有许多的威胁建模方法论（methodology），例如 STRIDE、OCTAVE、NIST 800-154 和 PASTA 其中：

1、STRIDE 是由微软开发的一种分类方案。 STRIDE 的使用经常与对应用程序或操作系统威胁的评估相关。然而，它也可以用于其它情境。STRIDE 是以下几个方面的首字母缩写：

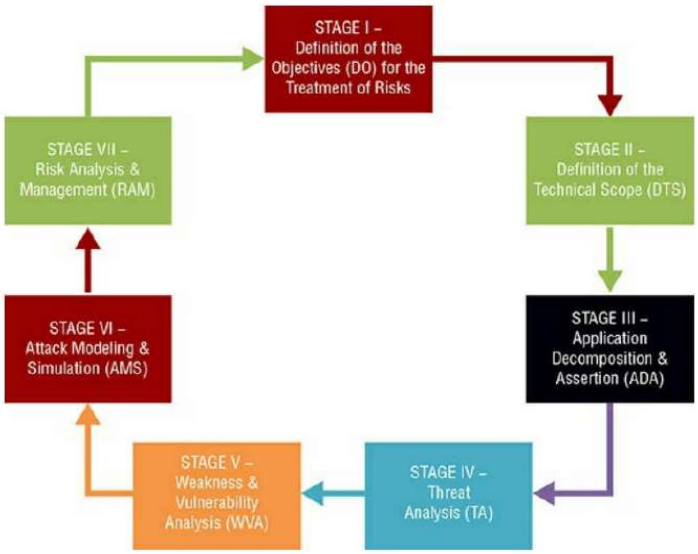
- 电子欺骗（Spoofing）： 通过使用伪造身份获得对目标系统访问的攻击行为
- 篡改（Tampering）：任何对数据进行未授权的更改或操纵的行为，不管是在传输中的还是被存储的数据。

- 否认（Repudiation）：用户或攻击者否认执行了一个动作或行为的能力。
- 信息披露（Information disclosure）：将私人、机密或受控信息揭露、传播给外部或未授权实体的行为。
- 拒绝服务（DoS）：指攻击试图阻止对资源的授权使用。
- 权限提升（Elevation of privilege）：一此攻击是指有限的用户帐号被转换成一个拥有更大特权、权力和访问权的帐户

2、OCTAVE（可操作的关键威胁、资产和薄弱点评估）用于定义一种系统的、组织范围内的评估信息安全风险的方法。然而 OCTAVE 方法重点体现的是威胁建模，同时以资产为中心的建模方法是 OCTAVE 的核心，OCTAVE 分为了四个阶段、八个步骤，如下图



3、攻击模拟和威胁分析过程（PASTA）是一个分为七个阶段的威胁建模方法 PASTA 是一种以风险为中心的方法，旨在针对受保护资产的价值选择或制定对策。

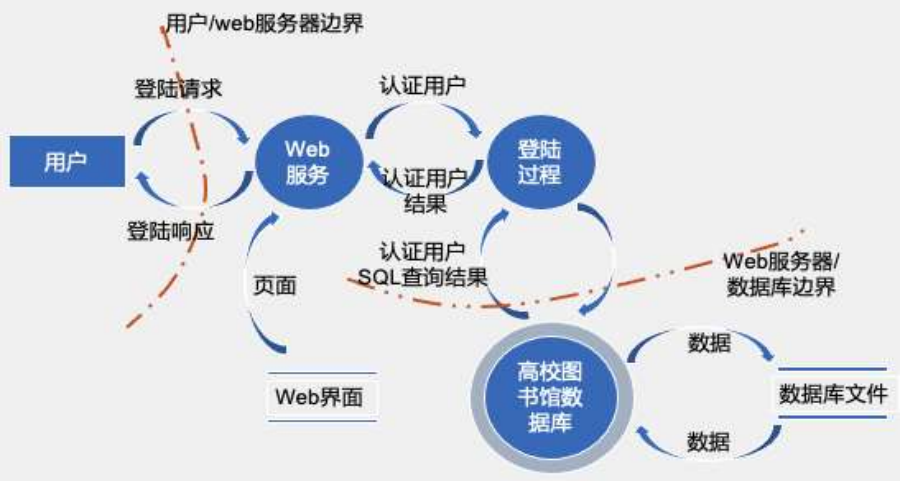


4、其他威胁建模方法包括

- TRIKE 是一种开源的威胁建模方法和工具
- 构建安全关键系统，CORAS）风险分析平台（也是开源的），它高度依赖于 UML 作为可视化威胁建模的前端
- 可视、敏捷和简单威胁建模，VAST）是一种利用敏捷概念的专有方法。

C、确定和图解潜在攻击

一旦你明白了开发项目或者部署系统架构可能面临的威胁，那么在进行威胁建模的过程中，要确定可能发生的可识别的潜在攻击概念。这通常是通过创建事务中涉及的元素、数据流和特权边界，以图示的方式来完成。如下图例子所示，这些数据流图通过可视化表示，能更好地帮助理解资源和数据流动的关系。图表流程也被称为制作架构图。创建图表有助于详述商业任务、开发流程或工作活动中每个元素功能和目的细节。一定要包括执行具体任务或操作的用户、处理器、应用程序、数据存储和所有其它的基本要素，这一点十分重要。该图表是一种高度概括，不是对编码逻辑的详细评估。然而，如果系统复杂，则需要创建多个图表，关注不同的焦点且把细节进行不同程度的放大。



接着，识别可能对图表中每个元素发起的攻击。需要记住的是：要考虑到各种形式的攻击，包括逻辑/技术、物理层面和社会层面的工具。例如，一定要包括电子欺骗、篡改和社交工程。这个过程能很快帮你进入威胁建模的下一阶段：执行降低分析。

D、执行降低分析

执行降低分析是用来分解应用程序、系统或环境的，这个任务的目的是为了更好地理解产品逻辑以及其与外部的交互元素，必须了解五个关键概念：

- 信任边界——信任或安全等级发生改变的位置
- 数据流路径——数据在两个位置之间的流动
- 输入点——接收外部输入的位置
- 特权操作——需要比标准用户帐户或流程有更大特权的任何活动，通常需要进行系统修改或改变安全性
- 安全立场和方法细节——安全策略、安全基础和安全假设的声

因为威胁要通过威胁建模进行识别，所以需要规定额外活动来完善整个流程。下一步是记录归档全部威胁。

E、优先级和响应

在文档编制中，应该对威胁的手段、目标和后果进行定义。要考虑实施某项开发可能需要的技术，以及列明潜在的对策和保障措施，还要把威胁进行排序或定级。可以利用各种技术完成这个过程，如使用概率×潜在损失的排名、高/中/低评级或 DREAD 系统，其中：

- 概率×潜在损失的排名，能产生一个风险严重性的编号，编号是从 1 到 100，100 代表可能发生的最严重的风险；
- 高/中/低的评级流程更加简单。每个威胁都会被标注这三种优先级标签中的一种；
- 设计 DREAD 评级系统是为了提供灵活的评级解决方案，其基于对每种威胁五个主要问题的回答：
  - ✓ 潜在破坏——如果威胁成真，可能造成的损失有多严重；
  - ✓ 再现性——攻击者复制这一开发会有多复杂；
  - ✓ 可利用性——实施攻击有多难；
  - ✓ 受影响用户——有多少用户可能受到攻击的影响（按百分比）
  - ✓ 可发现性——攻击者发现弱点会有多难

一旦设置了威胁的优先级，就需要确定对这些威胁的响应。应根据解决威胁的技术和流程的成本和效率对这些技术和流程进行考察权衡。响应内容应包括调整软件架构、改变操作和流程以及实施防御和检测控制。

2.4 将风险管理应用到供应链中

A、供应链中的风险

攻击者对组织供应链的破坏，也会危害到组织自身的业务。为了最大程度地减少供应

链风险，必须实施和验证适当的控制措施。如何确保第三方实际地采取相应的控制措施保护组织相关信息，是最大的挑战，常见的供应链中的风险有：

- 知识产权方面的风险。当第三方访问信息时，保护组织的知识产权不受损失或损害是一个巨大的挑战 最佳实践是确保知识产权的控制一直有效，无论在何时、何处。
- 仿冒品方面的风险。如果知识产权不小心泄露给竞争者，那么他们就会有机会制造原始产品的假冒品，并且通常质量较低或不完善。
- 恶意代码。专有的商用现货（COTS）软件的广泛使用要求客户信任供应商的安全实践。 但是，在许多实例中，这种信任被滥用，并且 COTS 供应商成为引入漏洞或损害客户数据 CIA 方面的工具。
- 未知谱系软件。标准代码库的使用、开放源代码项目的兴起以及面向对象的编程，简化了许多新系统的开发过程。但是，第三方编写的代码的质量可能相差很大。

B、供应链风险管理

供应链信息安全风险跨越了许多组织学科，包括采购，软件工程，软件保证和人员安全。许多监管和法律明确要求受监管的组织必须对供应链风险进行管理。一个明确的管理框架是解决供应链风险的最好实践。但是许多年来，风险管理领域的不断发展，管理信息系统供应链风险也越来越复杂

ISO 28000：2007，“供应链安全管理系统规范”，提供了管理供应链风险的广泛框架。尽管不是专门针对网络安全，但 ISO 28000 对于利用其他 ISO 规范（ISO 9001，ISO 27001）在供应链风险与组织的审核流程方面是一致的，以及对于寻求使用基于风险的标准化方法评估供应链的组织也是非常有用的。ISO 28000：2007 严重依赖于计划，执行，检查，采取行动（PDCA）的连续过程改进模型，以改进安全管理体系并确保组织符合安全实践。 这种方法促进了供应链风险与更广泛的组织风险管理活动的整合。

与网络安全相比，管理全球供应链涉及的风险范围更大，六个主要管理流程包括以下内容：

- 计划：平衡总需求和供应以制定最能满足采购，生产和交付要求的行动方案的过程
- 资料来源：采购货物和服务以满足计划或实际需求的过程
- 制造：将产品转换为完成状态以满足计划或实际需求的过程
- 交付：提供成品和服务以满足计划或实际需求的过程，通常包括订单管理，运输管理和分销管理
- 退货：由于任何原因与退货或接收退货相关的过程。 这些过程扩展到交付后的客

户支持

- 启用：准备，支持或处理依赖于计划和执行过程的信息或关系的过程

网络安全实践是流程领域的关键推动力之一。为了将安全整合到供应链中，并对第三方进行评估时，应考虑以下流程：

- 现场评估：访问该组织的网址 与其成员进行交谈并观察他们的操作习惯
- 公文交换和审核：调查交换数据和文档的方式以及他们执行评估和审核的正式流程
- 流程/策略审核：要求提供他们的安全策略、流程/程序、审查事件和响应文档的副本

第三方审计：根据美国注册会计师协会（AICPA）的定义，拥有独立的第三方审计员可以根据服务组织控制（SOC）报告对实体的安全基础结构进行公正的审查。认证参与标准声明（SSAE）是一项法规，定义了服务组织如何使用各种 SOC 报告来报告其合规性。

对于所有采购，需要建立最低安全要求。这些应该以组织现有的安全策略为蓝本。新硬件、软件或服务的安全要求应始终满足或超过现有基线要求的安全，并签署到合同中。使用外部服务时，请确保检查任何服务级别协议（SLA），以确保安全性是合同服务的规定组成部分。这可能包括根据组织特定需求定制的服务级别要求。

2.5 创建和维护安全意识培训和教育项目

A、安全意、培训、教育识概述

开发和发展组织有效识别和应对风险的能力，需要广泛的技能和知识。安全专家的级别需要根据每个人在组织中的角色，在重点和深度上有所不同教育、培训和意识都针对职业发展的不同方面，其中

- 教育，是一个正式的过程，需要受教育人对概念、原理和问题的进行理解，使受过教育的人有能力主动地设计程序，以解决广泛的、常常无法明确定义的问题。
- 培训，在教育是概念性的情况下，培训更为实用。培训会教特定的技能来解决已知情况。培训可能包括有关如何操作或配置系统以满足组织要求的指导。尽管培训和教育经常重叠，然后良好的教育计划更需要是对技术问题的理论理解。
- 意识，使人们对特定的问题给予关注，以便学习者可以识别异常情况并做出适当的反应。意识可能包括以用户为中心的讲座，该讲座提供有关如何识别社会工程学尝试的信息，或者可能包括电子邮件网络钓鱼活动，以识别不遵循良好电子邮件惯例的个人。

B、如何制定安全意识计划

制定安全意识计划需要有计划、持续的努力，以确保该计划有效地改善组织的安全状况。在风险级别的驱动下，该计划需要高级管理层的支持，同时要尊重组织的文化，利用可用资源以及满足组织对合规性的期望，主要步骤如下

- 现状评估。在制定意识计划时，必须评估组织的合规义务、风险环境、组织能力和资源。
- 需求评估。一旦确定了最低的合规期望，就必须进行需求评估。 需求评估将确定组织的要求与其利益相关者的能力之间的差距。 它将提供有关组织当前意识水平和首选交付方式的信息，并识别利益相关者可能具有的不同意识水平。
- 战略和计划。管理层将使用需求评估报告来制定意识战略和适当计划，以为意识内容的开发和交付提供资源。 该策略还将为评估意识计划的效果设定基准。计划本身将反映组织的培训和意识优先级，以确保解决最高风险的领域。
- 开发内容。通过意识计划，目的是塑造和强化行为。因此，意识计划的详细程度通常低于培训计划。确保内容具有相关性和意义，这对实现意识目标大有帮助。
- 传递内容。内容的传递可以以许多不同的方式发生，这样才能广泛和有效的传递。
- 监控结果。监视意识内容的传递并衡量行为变化的程度，将为改进提供重要信息。在持续流程改进模型中，生成信息成为下一轮需求评估的重要输入。
- 训练。组织的每个人需要对相关识别和应对实践进行训练，当信息安全环境的复杂性使得对信息安全所有方面的训练是非常困难的。

单元三：业务连续性计划

3.1 业务连续计划概述

A、业务连续性管理概述

为什么我们要做业务连续性和灾难恢复？虽然我们努力降低风险对组织的负面影响，但我们可以肯定的是：某种事件迟早会造成负面影响。理想情况下，损失会被遏制，且不会影响到主要业务的运营。然而，作为安全专业人员，需要为意想不到的情况制定好各种计划。在这些极端（有时是不可预测的）条件下，我们需要确保我们的组织能够继续以最低可接受的阈值运行，并迅速全面地恢复生产力。

DRP 和 BCP 都面向计划开发，而业务连续性管理（BCM）是整体的管理过程，应该包括 DRP 和 BCP。BCM 提供了一个框架，以整合恢复能力和有效应对能力的方式，保护组织中主

要利益相关者的利益。BCM 的主要目的是允许该组织继续在不同条件下进行业务操作。

B、业务连续计划（BCP）和灾难恢复计划（DRP）

什么是业务连续计划（BCP）？业务连续性计划（BCP）涉及到对组织各种过程的风险评估，还有在发生风险的情况下为了使风险对组织的影响降至最小程度而制定的各种策略、计划和措施。

什么是灾难恢复计划（DRP）？如果连续性受到破坏，那么业务过程就会停止，组织将采用灾难恢复计划，需要努力让所有关键系统重新联机。因此，灾难恢复计划（DRP）是当一切事情仍处于紧急模式下时实施的计划，组织中每个人都应该努力让所有关键系统重新联机。

业务连续性规划（BCP）采取一个更广泛的解决问题的方法。它可以包括在计划实施中对原有设施进行修复的同时在另外一个环境中恢复关键系统，使正确的人在这段时间内回到正确的位置，在不同的模式下执行业务直到常规条件恢复为止。BCP 也涉及通过不同的渠道应对客户、合作伙伴和股东，直到一切都恢复到正常。

C、业务连续计划过程和关键因素

(ISC)2 定义的业务连续性计划过程包括以下四个主要阶段：

- 项目范围和计划编制阶段
- 业务影响评估阶段
- 连续性计划阶段
- 批准和实现阶段

BCP 的关键因素包括：BCP 需要是一个活跃的实体，应当持续改进；建立和维护当前连续性计划最关键的部分是管理层支持;人员安全一直是最优先考虑的。

3.2 开发业务连续性计划项目

A、项目范围和计划

负责业务连续计划的人员首要职责之一是对业务组织进行分析，以识别与 BCP 流程具体有关的部门和个人。需要考虑：

- 负责向客户提供核心服务业务的运营部门
- 关键支持服务部门、设施和维护人员以及负责维护支持运营系统的其他团队
- 负责物理安全的公司安全团队

- 高级管理人员和对组织持续运营来说至关重要的其他人员

一旦管理层支持我们建立业务连续性计划，那么首先应该指定一个业务连续性协调员。业务连续性协调员将成为 BCP 团队的领导者，将监督连续性和灾难恢复计划的制定、实施和测试。一个领导者需要一个团队，因此需要成立一个 BCP 委员会。管理层和协调人必须共同决定和指派合格的人作为该委员会的成员。这个团队必须由熟悉公司内不同部门的人组成，因为每个部门在其功能上是独立的，并具有独特的风险和威胁。这个团队包括：业务部门、高级管理人员、IT 部门、安全部门、通信部门、法律部门。

BCP 团队确认业务组织分析结果后，就开始评估 BCP 工作的资源需求。这涉及三个不同 BCP 阶段所需的资源：

- 开发：BCP 团队需要一些资源来执行 BCP 流程的四个步骤(项目范围和计划、业务影响评估、连续性计划以及计划批准和实施)。这个阶段主要耗费人力资源，即 BCP 团队成员和召集过来协助制定计划的支持人员。
- 测试、培训和维护：在 BCP 的测试、培训和维护阶段，将需要一些硬件和软件资源；同样，这个阶段的主要资源是参与这些活动的员工付出的人力。
- 实施：当灾难发生且 BCP 团队认为有必要全面实施业务连续性计划时，将需要大量资源。这些资源包括大量实施工作(BCP 可能成为组织关注的重点)和对实际资源的消耗。出于这个原因，对 BCP 团队来说，果断、明智地使用 BCP 的能力是非常重要的。

BCP 项目的范围和目标方面都很清楚，但它并不是如此简单。由于范围从根本上影响 BCP 计划将涵盖什么方面，因此 BCP 团队应该从项目的一开始就考虑范围。BCP 应该能对高层组织的要求和分配给他们的资源进行评估。在风险评估或连续性规划开始之前，应该了解公司业务的重点和方向。一个组织需要考虑的其他重大事项包括：人员水平的变化、设施的搬迁、供应商的变化以及引入新的产品、技术或流程。在任何一个领域获得确切的数字及评估都会使 BCP 变得较为畅通。当然，由于一些信息的敏感性，一些数据可能不会提供给 BCP 团队。在这种情况下，团队应该认识到，没有得到全部的信息可能会导致其结果中的一些内容并不完全准确。

有关 BCP 的一个常见的异议是，当 BCP 一次性应用到一个组织中所有的功能时，它的范围会变得无限大，难以完成。一种替代的方法是，将 BCP 计划按照部门分成多个部分，另外把组织中一些难以完成的部分排除到 BCP 范围之外。

决定是否将组织的一个组成部分放到 BCP 范围以外以及如何放置通常会非常棘手。在某些情况下，产品、服务或分支机构可保留在范围内，但应该尽量降低资金和活动的水平。另外一种情况是，在事故发生后，重建分支机构的成本可能过高，这个时候管理层将决定是否仍将分支机构放在 BCP 的范围之外。这类决策应该由高级管理人员作出，而不是由 BCP 的管理人员和规划人员作出。

B、业务影响评估

什么是业务影响评估（BIA）？BIA 确定了能够决定组织持续发展的资源，以及对这些资源的威胁，并且还评估每种威胁实际出现的可能性以及出现的威胁对业务的影响。

我们可以通过以下两种方式来进行评估决策。第一个是定量决策：定量决策涉及使用数字和公式来作出评估决策。另一个是定性决策：定性决策考虑的是非数值因素。这种数据类型通常以优先级类别（例如高、中、低）表示。

BIA 在业务连续性规划的最初阶段实施，用来识别在灾难或者中断事件中可能会造成重大财产或者业务损失的区域。它识别公司生存所需要的关键系统，预估在灾难中公司可以容忍的中断时间（MTD）。也就是说，BIA 的目标就是当灾难发生时，重要的业务是什么，并需要最先恢复。恢复时间目标（RTO）就是当中断事件发生时，实际恢复业务所需的时间。因此 BCP 就要确保 RTO 小于 MTD。

BIA 的主要步骤包括：

- 选择单个的人员进行访谈，来完成数据收集
- 创建数据收集技术方法，例如（调查、问卷、定性和定量方法）
- 确定公司的关键业务功能
- 确定这些功能依赖的资源
- 计算缺少这些资源，业务还可以生存多久
- 确定这些功能的漏洞和所面临的威胁
- 计算每个不同业务功能的风险
- 将发现结果形成文档并报告给管理层

如何使用标准的风险评估完成业务影响评估呢？为了取得成功，组织应该系统地规划和执行一个正式的 BCP 相关风险评估。风险评估应该充分考虑到组织对业务连续性风险的承受力。风险评估也会使用到业务影响分析 BIA 里的数据来得出一致性的估计结论。

作为成功的技术指标，业务影响评估评估应当识别、评估和记录以下所有相关项：

- 组织中对时间最敏感的资源和活动的所有脆弱点
- 组织最紧迫的资源以及活动的威胁和危害
- 衡量关键的服务和产品中断的可能性、时间长度以及造成的影响
- 单点故障，也就是威胁业务连续性的关键点
- 由于关键技能的缺失造成的业务连续性风险
- 由于外包供应商和供应商造成的业务持续性风险
- BCP 计划没有涵盖本部门，或者 BCP 计划并没有很好地落实而造成的业务连续性风险

这里我们要注意，风险评估的最终目标和业务影响评估目标是不同的，风险评估的目标包括：识别和记录单点故障；制定组织特定业务流程的威胁优先级列表；为开发风险控

制管理策略汇总信息，并为解决风险制定行动方案；识别风险接受记录，或记录确认那些不会得到解决的风险。而 BCP 委员会在 BIA 中需要逐步梳理下列问题：设备出现故障或设备不可用；公用设施不可用；设施变得不可用；关键人员不可用；供应商和服务提供商变得不可用；软件和/或数据损坏。

C、编制连续性计划

BCP 开发的下一个阶段是连续性计划编制，这个阶段专注于连续性策略的开发和实现，从而最小化已发生的风险，可能对被保护资产的影响

策略开发：BCP 策略为设计和建立 BCP 的工作提供了框架和管理。该策略有助于组织通过概述 BCP 的目的理解 BCP 的重要性。它为组织及其 BCP 提供了一个原则性的概述，同时说明了 BCP 团队将如何开展工作。

预备和处理：在这个任务中，BCP 团队设计了具体的过程和机制，用于缓解在策略开发阶段中被认为不可接受的风险。

D、批准和实现阶段

计划批现：一旦 BCP 团队完成了 BCP 文档的设计阶段，那么就该申请获得高级管理层的批准了

计划实现：BCP 团队根据管理层的决策，应该共同开发一个实现项目计划，这个计划利用特定的资源，尽可能迅速地在给出过程和预备措施的目标，最终完成实施。

培训和教育：培训和教育是 BCP 实现中的一项重要内容，组织中的每个人都应当接到至少一个计划综述简报，从而使他们具有信心，确保在灾难发生时他们能够有效地完成其任务。

BCP 文档化：文档应该是一个体系化的结构，并持续修改、完善，以及妥善的保存 BCP 文档。

D2：资产安全

单元 1：资产安全概述

1.1　资产安全基本概念

A、数据相关概念

1. 数据治理

在许多大型组织中，数据治理委员会负责监督数据策略，并概述了不同职能利益相关方的角色和职责。组织应确定如何管理重要数据的创建、转换和使用。

数据治理的概念包括内部或外部正确、持续处理数据的人员、流程和 IT 组织。组织应使用一些指导原则来建立其数据治理模型，这些原则包括：

- 建立责任
- 为组织提供最佳支持的计划
- 有效获取
- 必要时确保性能
- 确保符合规则
- 确保尊重人为因素

2、数据策略

数据管理必须遵循一套广泛适用于组织的原则和程序。完善的数据策略可以指导组织仅仅收集所需的信息、确保这些信息安全，并且在不需要的时候安全的销毁它们。

完善的数据策略可指导组织在如何解决影响数据安全时，如何实践。由于资产安全性存在着动态变化，因此制定数据策略的时候也需要灵活性来适应这样的变化。

数据策略在数据治理中起着至关重要的作用。定义明确的数据策略可以为管理层在制定数据质量、格式、访问和保留有关实践和标准时提供指导。

3、数据质量

数据质量涉及数据的完整性和可靠性。在衡量数据质量时需要考虑的因素包括准确性、货币性和相关性。评估数据质量的两个方法：

- 质量保证（QA）：使用规定的标准来评估和发现数据中的不一致和其他异常情况，并应用数据净化技术来交付最终产品。QA 解决了问题：“数据是否符合目的？”
- 质量控制（QC）：根据内部标准、流程和程序进行数据质量评估，以控制和监视 QA 所告知的质量。质量控制解决了以下问题：“数据可以使用吗？”

需要减少的常规错误类型：

- 记账错误
- 遗漏错误

4、数据文档化

数据资产的文档化对于组织在管理业务流程中越来越大的数据集是非常有用的。正确的数据文档有助于确保用户有效的理解和使用数据。数据文档的组成部分一般包括：数据怎么样创建、数据的结构和内容、以及对数据所执行的任何操作。数据文档的目标如下：

- 数据寿命和重用。
- 数据用户应该了解数据的内容、上下文和限制。
- 更容易在组织内发现数据。
- 数据互操作性和数据交换。

5、数据模式

数据模式指的是：如何定义数据架构的蓝图。数据模式是一个概念，如果这是一本数据科学书籍，则将深入探讨。仅限于资产安全性主题，重要的是要注意，数据模式是数据组织的元素。有关安全控制（例如加密，访问和授权级别以及处置计划）的决定将由数据模式告知。数据模式的有效定义是它是如何构建数据库的蓝图。例如，在关系数据库中，数据模式被组织成表格。建立数据模式以记录可以输入数据库的元素或可能的最终用户感兴趣的元素。数据库通常将其架构存储在称为数据字典的参考存储库中。

B、信息资产生命周期模型

信息资产生命周期模型描述了：一个实体在其生命周期中，所经历的变化。在宏观层面上，我们可以将信息分为如下四个阶段：

1、信息获取阶段。首先组织只能通过从其他地方复制或者是从头开始创建，这两种方式中的一种来获取信息。然后，在获取到信息之后，以及在信息可以使用之前，我们有必要采取的一些步骤使信息有价值。最后，我们还必须应用一些策略性的控制。

2、使用阶段。从安全角度来看，在信息生命周期中的这一阶段，确保其机密性、完整性和可用性是最大的挑战。组织需要保持信息的可用性，而且只有正确的人在被授权的情况下，才能修改它。由于信息经常被使用，因此我们必须确保数据内部的一致性。

3、存档阶段。一方面，在我们不经常使用某些信息，且在要丢弃这些信息之前，可能由于各种原因需想要保留它，这可能会意味着如果我们不进行适当的控制，未授权或意外的对这些数据的访问和更改，就可能会在很长的一段时间都不被发现。另一个信息归档的驱动因素源自于备份需求。无论我们何种备份，在决定哪些备份需要被保护，以及如何进行保护时，参考风险评估的结论是很重要的。

保留数据多长时间的也是非常重要问题。如果我们丢弃太快，我们就得冒着由于错误

或攻击而无法恢复的危险。我们还有可能面临无法响应电子取证或是法院传票的风险。如果我们保持数据太久，我们则承担成本过高以及责任递增的风险。

4、处置阶段。处置意味着数据的销毁，但有时不仅仅是这么简单。当数据需要处置时，有两个重要的问题需要考虑：数据是否被真正销毁？是否被正确销毁。

1.2 信息资产分类分级

A、信息分类分级概述

在信息的整个生命周期中，保持和持续更新这种分类级别标签，对于确定我们需要应用的信息保护控制是很重要的。

信息分类的目的都是为了量化一个组织如果丢失了信息后可能承受多少的损失，会给组织基本业务流程带来多大的影响；一旦根据敏感程度对信息分类，公司就能够决定保护各种信息所需要的安全控制；这样可以确保信息资产得到适当级别的保护，同时分类会指明安全保护的优先顺序。因此数据分类有助于保证以成本最为低廉的方式保护数据；

每种分类都应当具有单独的处理要求和措施，以便说明如何访问、使用和销毁数据。

B、信息分类分级的级别

对于组织机构应该使用什么样的分类级别，没有硬性和快捷的规定。组织机构需要首先确定分几级才能最适应组织安全的需要，然后指定命名方案，最后定义出每个级别叫什么名称。但重要的是，不要走极端的提出大量的分类方法，这样只会给即将使用分类系统的用户带来混淆与沮丧情绪。另外，由于需要对多种类型的数据进行分类，因此分类也不应有太多限制或过于详细。每种分类都应唯一且区别于其他分类，同时不能有任何重叠。

C、信息分类分级的原则和控制

确定分类方案后，组织必须开发出一套使用准则来说明如何对信息进行分类。一般的参考准则有：数据的用途、数据的价值、数据的寿命、数据泄漏可能导致的损失级别、数据被修改或出现讹误可能导致的损失级别、保护数据的法律、法规或合约责任、数据对安全的影响、谁能够访问这些数据、由谁维护这些数据、谁能够重造这些数据、如果数据不可用或出现讹误，那么造成的机会损失有多少。

D、信息分类分级计划步骤

实施分类计划项目的必要步骤：1、定义分类级别；2、指定确定如何分类数据的准则；3、任命负责为数据分类的数据所有者；4、任命负责维护数据及其安全级别的数据看管员；5、制订每种分类级别所需的安全控制或保护机制；6、记录上述分类问题的例外情况；7、说明可用于将信息保管转交给其他数据所有者的方法；8、建立一个定期审查信息分类和所有权的措施，向数据看管员通报任何变更；9、指明信息解密措施；10、将这些问题综合为安全意识计划，让所有员工都了解如何处理不同分类级别的数据。

1.3 资产安全相关的角色和责任

A、高级管理层

高级管理层（Executive Management）持续对组织负有最终责任，因此对数据的安全也负有最终责任。他们需要制定长远规划、业务目标和保护数据的目标和目的。并且他们还需要负责确保组织在信息安全方面采取适当的应尽关注和应尽责任，这就是为什么各个企业的安全部门都获得了更多资源支持的原因。

B、数据所有者、数据监管者、系统所有者、数据管理员

数据所有者(Data Owner) (也称为信息所有者)通常是一名管理人员，他负责管理某个业务部门，对特定信息子集的保护和应用负最终责任。数据所有者具有“应尽关注”职责。数据所有者决定其负责的数据的分类，如果组织需要，那么还应改变数据的分类。他还负责确保实施必要的安全控制，定义每种分类的安全需求和备份需求，批准任何披露活动，保证应用适当的访问权限，以及定义用户访问准则。数据所有者有权准许访问请求，也可以选择将这一职权委托给业务部门经理。同时，数据所有者还要处理与其所负责数据有关的安全违规行为，以对数据进行保护。如果数据所有者工作繁忙，那么可以将数据保护机制的日常维护工作委托给数据监管者完成。

数据监管者(Data Custodian) (也称为信息监管者)负责数据的保护与维护工作。这个角色通常由 IT 或安全部门员工担任，其职责包括：实施和维护安全控制措施、执行数据的常规备份，定期验证数据的完整性，从备份介质还原数据，保存活动记录，以及实现公司关于信息安全和数据保护的信息安全策略、标准和指南所指定的需求。

系统所有者（System Owner）负责一个或多个系统，每个系统可能保存并处理由不同数据所有者拥有的数据。系统所有者负责将安全因素集成到应用程序和系统购置决策及项目开发中。他还负责通过必要的控制、密码管理、远程访问控制、操作系统配置等措施保

证足够的安全。这个角色必须确保系统的脆弱性得到正确评估，并且向事故响应团队和数据所有者报告所有的系统脆弱性。

数据管理员负责授予人员（用户）适当的访问权限，管理员未必具有全部管理员权限和特权，但具备分配权限的能力。管理员根据“最小特权”原则和“知其所需”原则分配权限，仅授予用户工作所需的权限。

C、安全管理员、审计员

安全管理员（Security Administrator）负责实施和维护企业内具体的安全网络设备和软件。安全管理员的任务往往包括创建新系统用户账户，实现新的安全软件，测试安全补丁与组件，以及发放新密码(安全管理员不能真正批准新系统用户账户，这是监督员的职责)。安全管理员必须确保为用户授予的访问权限符合公司策略和数据所有者的指示。

审计员（Auditor）的职能是定期巡查，确保组织人员正在做了该做的事情。他们确保采取并安全地维护了正确的控制措施。审计员的目标是确保组织机构遵循了自己制定的策略和适用的法律法规。组织可以拥有内部审计员和/外部审计员。外部审计员往往代表法律机构，确保组织符合法规要求。

D、其他人员：主管、变更分析员、数据分析员、用户

主管（Supervisor）也称为用户管理者，其最终负责所有用户活动和由这些用户所创建和拥有的任何资产

变更分析员（Change Control Analyst）在发生变更时，必须保证变更的安全。

数据分析员（Data Analyst）数据分析员负责保证以最佳方式存储数据，从而为需要访问和应用数据的公司与个人提供最大的便利。数据分析员与数据所有者共同合作，帮助保证建立的数据结构符合并支持公司的业务目标。

用户（User）有义务遵守操作安全措施，从而保证数据对其他人的机密性、完整性和可用性。

单元 2：保护信息

2.1 确保恰当的数据保留

A、数据保留策略

需要确保组织具有并遵循文档化的数据保留策略，而且通过定期审计。同时需要符合

法规的要求。数据保留策略用于解决三个基本问题：

保留什么数据。保留的数据包括：对业务有价值的数据、法律义务要求的数据以及与合作伙伴、第三方交易相关有价值的数据。保留数据的决定必须是谨慎、具体和可执行的。同时要注意业务需求数据与员工或客户隐私之间的平衡。

如何保留数据。为了使保留的数据有用，它必须能被及时访问到的，需要考虑以下方法：分类法、分级、标准化、索引

保留多长时间。根据业务需要，同时咨询法律顾问，符合法律的监管要求。

B、电子发现协议（e-Discovery）

电子存储信息的发现（ESI）或称电子发现是被法院或外部律师所制定的，与法律程序有关的所有 ESI 的过程。电子发现参考模型（EDRM）标识的八个步骤，它们既不一定是必需的，也不必以线性方式执行：

- 对命令所需的数据进行识别。
- 保存此数据以确保在遵照命令执行时不会意外或例行操作而被销毁。
- 从可能存在的各种存放区域收集数据。
- 确保数据及其元数据被使用正确格式所处理。
- 审查数据以确保其相关性。
- 进行适当的上下文数据分析。
- 按照请求生成最终数据集。
- 向外部受众展示数据以证明或反驳索赔。

2.2 保护隐私数据

A、隐私数据所有者和处理者

隐私数据涉及的主要人员有：数据所有者和数据处理者。隐私数据所有者的一个责任就是数据分类和批准披露的请求，隐私数据所有者间接或直接决定谁可以访问特定的数据。因此所有者通常是组织内的高级管理者。隐私数据处理者通常由那些日常保护（或危及）数据隐私的用户所组成。对于处理者关于隐私的关键问题是：他们是否理解什么是可接受的行为边界，并且（同样重要的是）知道当数据被以不符合策略的方式被意外或有意地处理时该怎么做。对于处理者在隐私保护方面的关键是培训和审计。

B、数据残留

为了应对数据残留，需要确保隐私或敏感数据被正确移除是很重要的。 一般来说，有四种方法可消除数据的残留（AIO 中提到）：

- 覆盖：覆盖数据需要使用随机或固定模式的 1 和 0 替换存储介质上代表文件内容的那些 1 和 0，以便使得原始数据无法恢复。
- 消磁：这是去除或减少常规磁盘驱动器或磁带上的磁场分布的过程。实际上强大的磁力被加载到介质后，会导致数据被擦除并且有时驱动磁盘的马达也被破坏。尽管恢复数据仍然是可能的，但是这样做通常是成本过高的。
- 加密：许多移动设备采用这种方法快速、安全的使得数据不可用。其前提是存储在介质的数据以强密钥的形式被进行加密。为了实现数据不可恢复，系统只需要安全的删除加密密钥，这比删除加密数据快许多倍。在这种情况下恢复数据完全靠计算是不实现的。
- 物理损毁：通常应对数据剩余的最好方法是简单地损毁物理介质。两种最常用的损毁介质方法是将其粉碎或使其放置到腐蚀性化学品里，使其完全不可用。另外还有一种方法是焚毁。

除了这些基本的方法外，我们还会遇到以下的具体方法（OSG 中提到）：

- 擦除（Erasing）：擦除介质上的数据就是对文件、文件选择或整个介质执行一个删除操作。在大多数情况下，删除或清除程序只是删除了目录或与目录相链接的数据。实际的数据还在驱动器中。任何人都可以使用复原工具来恢复这些数据。
- 消除（Clearing）：消除或重写是使介质可以重新使用的一个准备过程，这个过程可以确保消除的数据不会通过传统的工具恢复。
- 清除（Purging）：清除是比消除更强烈的一种形式，是指在安全性较差的环境中使介质达到可再次使用的准备过程。它确保原始数据使用任何已知方法都不会恢复。清除过程是将消除过程多次重复，并结合其他方法，如去磁法来完全清除数据。
- 解除分类（Declassification）：解除分类指在非机密情况下对介质或系统进行清除使其能够再次使用的准备过程。
- 净化（Sanitization）：净化指的是破坏介质或使用一种可靠的方法将机密数据从介质上清除但不破坏介质。它确保数据不会以任何形式恢复。
- 消磁（Degaussing）：消磁工具会建立一个强大的磁场区域，从而以消磁的方法擦除介质上的数据。技术人员通常使用消磁的方法将磁带上的数据清除，从而使其回到最初状态。
- 销毁（Destruction）：销毁是介质生命周期的最后阶段，也是清除介质数据最安全的方法。当销毁介质时，一定要确保其不能再使用或修复，并且数据不能从被

破坏的介质上提取。

C、隐私收集限制

隐私策略分为两个文档：一个涵盖员工数据的内部文档，另一个涵盖客户信息的外部文档。隐私策略在收集隐私时需要考虑以下问题：

- 收集个人的什么数据？（例如姓名，网站访问，电子邮件信息等）？
- 为什么我们收集这些数据，以及我们如何使用它们（例如，提供服务，以确保安全）？
- 我们与谁共享此数据（例如，第三方提供商，执法机构）？
- 谁拥有收集的数据（例如，主体，组织）？
- 这些数据的主体（例如，选择退出，限制）有什么权利？
- 什么时候销毁这些数据（例如，五年后，从不）？
- 有什么具体的法律或法规与这些数据相关？

2.3 确保恰当的数据安全控制

A、数据安全控制

企业资产所面临的主要威胁是盗窃、服务中断、物理损坏、系统和环境完整性受损以及未授权的访问。我们选择使用哪些控制来减少信息的风险，不仅取决于我们分配给该信息的价值，还取决于该信息的动态特点。一般来说，数据存在三种状态：

- “静态数据”是指驻留在存储设备中的数据。这种情况下保护数据简单且普遍的解决方案就是：加密。
- “运动中的数据”是通过诸如互联网这样的数据网络在计算节点之间移动的数据。我们运动的数据最佳的保护是强加密，或者在关键节点之间使用信任的信道。
- “使用中的数据”是指驻留在主存储设备中数据的术语。由多个进程共享存储器的有效侧信道攻击的存在性，可导致敏感数据丢失。可以通过确保软件测试这类攻击来归结此问题。

B、介质控制

介质和设备需要各种控制，防止介质未授权访问的控制(保护机密性)，以确保不会危及介质中的数据的完整性、机密性和可用性，这可能需要物理性的、行政管理性的和技术

性的控制。介质和设备包括电子(磁盘、CD/DVD、磁带、诸如 USB 盘之类的闪盘等)和非电子(纸质)的信息形态。介质应该被清楚地标记和做记录，其完整性应该被验证，并且当不再需要时其存储的数据应该被正确地擦除，对电子介质擦除有净化、清除和破坏等方法。其他类型的信息(如纸质文件、缩影胶片和缩微平片)也需要进行安全处理。如不进行处理，会遭受到“垃圾搜索”攻击，垃圾搜索攻击是指搜索家庭或公司的垃圾箱，找到相关敏感信息。

介质管理都应包括以下属性和任务：

- 追踪(审计日志记录)。 在特定的时间内每一件介质由谁负责保管。
- 有效实现访问控制。只允许介质/介质上信息的所有者指定的人员访问每一件介质，并根据介质/介质上信息的分类强制实施适当的安全措施。
- 追踪(本地或异地)备份版本的数量和位置。为了确保在信息生命周期结束时对信息进行适当的处理，在审计过程中说明信息的位置和可访问性，以及在信息的主要来源丢失或遭到破坏时找到备份信息，这些工作是必不可少的。
- 对介质变更的历史记录归档。
- 确保环境条件不会危及介质的安全。每一种介质都很容易因为一种或几种环境条件的影响而遭到破坏。
- 确保介质的完整性。通过根据介质类型和环境适用性检验每一件介质是否仍然可用，并将依然重要的信息由即将报废的介质转移到新的介质中，从而确保介质的完整性。
- 定期清查介质。以查看是否有任何介质丢失或改变。
- 执行安全处置活动。处置包括信息的生命周期以及处理介质/信息所需的最少措施。
- 介质库中的每一件介质的内部和外部标签

C、保护其他资产

保护移动设备及其数据的保护机制：

- 列出所有移动设备（包括序列号），以便在被盗并恢复时可以正确识别。
- 通过应用安全配置的基线加固操作系统。
- 在笔记本电脑上对 BIOS 进行密码保护。
- 将所有设备注册到其各自的供应商，并在设备被盗时向供应商提交报告。 如果设备在被盗后发去进行修理，如果你已报告了盗窃，则供应商将标记该设备。
- 飞行时，请勿将移动装置作为行李托运。总是随身携带。
- 不要任移动设备无人看管，并将其放在一个不起眼的手提箱中。
- 使用符号或数字标记设备以便正确识别。

- 尽可能使用带电缆的插槽锁将笔记本电脑连接到固定的物体。
- 将移动设备上的所有数据备份到受组织控制的存储库。
- 加密移动设备上的所有数据。
- 使能远程擦除设备上数据的功能。

保护纸质记录时要考虑的一些原则：

- 教育员工正确处理纸质记录。
- 尽量减少纸质记录的使用。
- 确保工作环境保持整洁，以便易于分辨敏感文件是否暴露在外，并定期审核工作环境，以确保敏感文件不被暴露。
- 在完成后，立即将所有敏感的文件锁起来。
- 禁止将敏感的文书工作带回家
- 为所有文书工作标明其分类等级。 理想情况是，还应包括其所有者的姓名和处置（例如保留期限）说明。
- 在员工离开办公室时对员工的包进行随机搜查，以确保敏感材料不被带回家。
- 使用十字切碎纸机销毁不需要的敏感纸张。 对于非常敏感的文件，请考虑烧毁它们。

保险箱通常用于存储备份数据的磁带、原始合同或其他类型的贵重物品。保险箱应该是防渗透的并提供防火保护。

2.4 数据泄漏

A、常见的数据泄漏原因

数据泄漏的最常见原因为：转移信息不恰当；保护不周的设备，造成丢失或被盗；采用不适合于特殊用途的技术；没有确保介质中并不包含任何数据残留；以及相关人员的意识培训不足

B、数据泄漏防护（DLP）

数据泄漏防护（DLP）包括组织为防止未经授权的外部各方访问敏感数据而采取的各种行动。首先，数据必须被认为是敏感的；其次，DLP 关系到外部各方；最后，外部访问我们的敏感数据必须是未经授权的。DLP 的真正挑战涉及到我们组织的整体观，DLP 是一个计划。这个观点必须包括我们的人，我们的流程，然后是我们的信息。

关于 DLP 的一个常见错误是将该问题视为技术问题。如果我们所做的是购买或开发旨在阻止泄漏的最新技术，我们就很可能会泄漏数据。我们需要认为 DLP 是一个计划而不是

一个项目，并且我们对组织业务流程、策略、文化和人员给予应有的重视，那么就有了许多减轻大部分潜在泄漏的机会。最后，就像信息系统安全的其他一切方面那样，我们也必须承认：尽管尽了最大的努力，还是总会有不幸。能做得最好的就是坚持这个计划，使不幸的频率减少、程度减轻。

DLP 方法的关键要素包括：

- 数据清单。选择 DLP 解决方案之前查找和表征你组织中的所有数据。
- 数据流。理解在业务和 IT 之间的这个交叉点上的数据流对于实现 DLP 是至关重要的。
- 数据保护策略，数据保护策略不仅要涵盖预防攻击者的方法，而且还必须描述如何保护我们的数据免受已经存在的内部威胁代理。
- 实现，测试和调优，部署和运行工具集，选择恰当的解决方案。

网络 DLP（NDLP）是对运动中的数据应用数据保护策略。NDLP 产品通常是一些实施部署在组织的网络周边的设备。它们还可以部署在内部子网的边界处，并且可以作为一些模块被部署为带有模块化的安全设备内。NDLP 解决方案的主要缺点是它不会保护不在组织网络中的设备上的数据。

端点 DLP（EDLP）是对静态的数据和使用中的数据应用保护策略。EDLP 被部署在每个受保护的端点上以软件形式运行。EDLP 能实现通常 NDLP 无法达到的防护等级。EDLP 的主要缺点是复杂性。

混合 DLP 是在整个企业中部署 NDLP 和 EDLP。 显然这种方法是最昂贵和最复杂的。然而对于能够负担得起的组织来说，它提供了最好的安全覆盖。

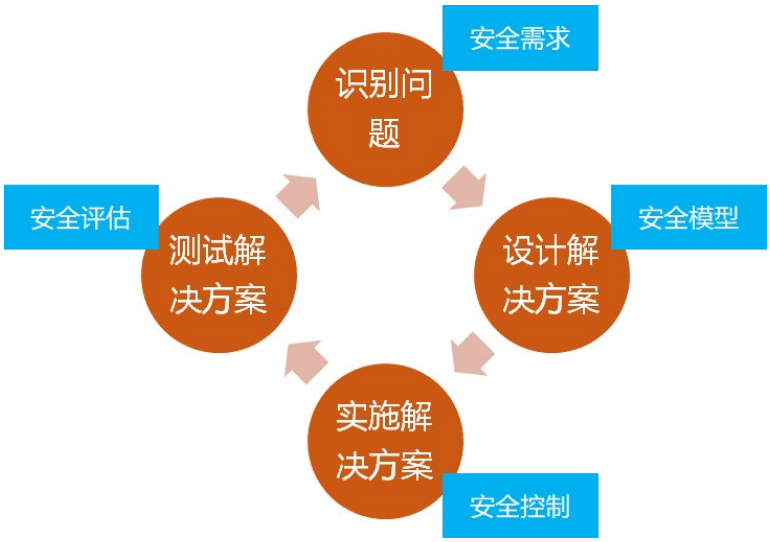
D3：安全工程

单元 1：安全架构和模型

1.1 使用安全设计原则来实施与管理工程的过程

A、工程建设生命周期和安全需求

工程建设的生命周期一般包括：需求、设计、开发、测试、上线、运营和退役。在每一个系统的开发阶段都应该考虑安全，程序员应该努力为他们开发的每一个应用程序建立安全，并把这些安全提供给关键系统应用和那些处理敏感信息的应用软件。在开发项目的早期阶段考虑安全是非常重要的，因为它比将安全添加到现有系统中更容易实现。



B、安全架构设计原则

根据一组充分考虑和定义的安全设计原则，来设计一个系统的安全控制和架构，才能更好地减少风险。

Saltzer 和 Schroeder 原则，以保护机制的体系结构为中心，探讨了计算机系统的信息保护问题，重点考察了权能和访问控制表的实现结构。Saltzer 和 Schroeder 原则，给出了信息保护机制的 8 条设计原则：

- 机制的经济性 Economy of Mechanism
- Fail Safe 默认保护 Fail Safe Defaults

- 完全仲裁 Complete Mediation
- 开放设计 Open Design
- 特权分离 Separation of Privilege
- 最小特权 Least Privilege
- 最少公共机制 Least Common Mechanism
- 心理可接受性：易用性 Psychological Acceptability：work factor and compromise recording

在 2017 年 ISO 发布了 ISO/IEC 19249，目的是描述用于促进系统和应用程序安全开发体系架构和设计原则。ISO/IEC 19249 描述的五个框架原则：域隔离、分层、封装、冗余、虚拟化。ISO/IEC 19249 描述的五个设计原则：最小特权、攻击面最小化、集中参数验证、集中通用安全服务、为错误和异常处理做准备。

我认为在 CISSP 学习中可简单的将控制技术机制分为 4 大类：

- 身份认证和访问类，主要对主体进行验证、权限进行控制的技术机制；
- 信息的安全性类，主要针对信息在机密性、完整性和可用性方面进行保护的技术机制；
- 边界隔离类，主要通过边界和隔离机制，来限制访问、使用等行为的技术机制；
- 审查类，主要是对控制措施的有效性进行监测、检测和分析的相关技术机制

C、系统架构

在设计和开发系统阶段之前，首先必须理解系统架构这个概念。系统架构描述了系统的主要组件，以及系统组件之间、系统与用户之间，以及系统与其它系统之间，如何相互交互。这个抽象架构提供了“全景”目标，并用来指导后面的设计和开发阶段。

术语“开发”是指系统的整个生命周期，包括规划、分析、设计、构建、测试、部署、维护和退役共 8 个阶段。设计阶段开始于架构工作，进一步再详细描述系统构建所需的一切。系统架构创建和使用过程是不断发展的，变得更加规范和标准化。

通常系统架构包括以下部分：

- 计算机硬件：中央处理器 CPU、存储器 Memory、输入/输出设备 Input /Output devices、总线 BUS
- 中央处理器 CPU
  - ✓ 执行类型：多任务 、多核 、多处理、多进程、多线程
  - ✓ 处理状态：单一状态、多状态
  - ✓ 保护机制：环保护
  - ✓ 操作模式：用户模式、特权模式、监管模式、系统模式、内核模式
  - ✓ 进程状态：就绪、等待、运行、监管、停止

- ✓ 系统安全模式：专有模式、系统高级模式、分割模式、多级模式

- 存储器
  - ✓ 只读存储器（ROM）：可编程只读存储器（PROM）、可擦除可编程只读存储器（EPROM）、电可擦除可编程只读存储器（ UVEPROM ）、闪存
  - ✓ 随机存取存储器（RAM）：实际存储器（主内存）、高速缓存 RAM、动态 vs 静态
  - ✓ 寄存器（Registers）
  - ✓ 存储器寻址：寄存器寻址、立即寻址、直接寻址、间接寻址、基址+偏移量寻址
  - ✓ 辅助存储器

D、系统安全架构

可信计算机系统评价标准（TCSEC）描述了相关系统应遵循的安全架构，其核心内容就是可信计算基、安全边界、引用监控器、安全内核，其中：

- 可信计算基 ：Trusted Computing Base，简称 TCB，指的是系统内提供某类安全并实施系统安全策略的所有硬件、软件和固件的组合。因此从某种意义上说，内核就是 TCB。然而，TCB 还可能包括其他组件，如能够直接与内核进行交互的可信命令、程序和配置文件。
- 安全边界(security perimeter)是划分可信与不可信的边界。并不是每一个进程和资源都会位于 TCB 内，有些资源位于安全边界之外，这是一种假想的边界。
- 引用监控器(reference monitor)是一个抽象机，是主体对客体进行所有访问的中介，定义了引用验证机制必须满足的设计要求，从而它能够正确执行系统型访问控制策略的规定。引用监控器是一个访问控制概念，而不是实际的物理概念，因此通常被称为“引用监控器概念”或“抽象机”。
- 安全内核。安全内核由位于 TCB 内的硬件、软件和固件组件构成，并且实现和实施引用监控器概念。安全内核具有以下 3 个主要要求：1. 它必须为实施引用监控器概念的进程提供隔离，并且这些进程必须不被篡改。 2. 针对每个访问企图，都必须调用安全内核，而且必须保证不回避调用。3. 它必须足够小，以便能够完整地和全面地对其进行测试和验证。

E、可信系统和保证

安全性一旦被集成到设计中， 就必须被计划、实现、测试、审计、评估、认证和最后认可。

可信系统是所有保护机制协力工作的系统，从而能够在维护稳定和安全的计算环境的情况下为许多类型的用户处理敏感数据。

保证被简单地定义为满足安全需求的置信度。保证必须被持续地维持、更新和重验证。无论可信系统经历已知的变化还是经过相当长的时间，这一点都是正确的。

可信可以通过具体的安全功能集成到系统中，而保证是在现实世界对安全功能情况可靠性和可用性的评估。

1.2 理解安全模型的基本概念

安全模型通过明确指定实现安全策略所必需的数据结构和技术，并将安全策略的抽象目标映射到信息系统的具体内容上。安全模型通常以数学和分析的理念来表示，然后映射到系统的规范说明上，再由编程人员通过编写代码开发出来。下面我们逐一对它们进行介绍。

A、Bell-LaPadula 模型

Bell-LaPadula 模型是多级安全策略的第一个算术模型，用于定义安全状态机的概念、访问的模式以及概述访问的规则。Bell-LaPadula 模型的开发是为了确保秘密被保密。Bell-LaPadula 模型中使用和实施了 4 种主要的规则：

- 简单安全规则，规定位于给定安全级别上的主体，不能读取较高安全级别驻留的数据。
- *属性规则（星属性规则），规定位于给定安全级别上的主体不能将信息写入较低的安全级别。简单安全规则称为“不能向上读”规则，*属性规则称为“不能向下写”规则。
- 第三个规则是强星属性规则，规定一个主体只能在同一安全级别上执行读写功能，在较高或较低级别都不能读写。因此，一个主体要读写一个客体，主体的许可和客体的分类必须同等。
- 第四个规则是自主安全属性，规定系统使用访问控制矩阵来实施自主访问控制。也就是说，如果我们想打破上面的三条规则，可以通过“白名单”的方式来实施。

B、Biba 模型

Biba 模式解决了系统内数据的完整性问题。Biba 模型用完整性级别来防止数据从任何完整性级别流到较高的完整性级别中。

Biba 通过 3 条主要规则来提供这种保护：

- *完整性公理规则，主体不能向位于较高完整性级别的客体写数据（被称为“不能向上写”）。
- 简单完整性公理规则，主体不能从较低完整性级别读取数据（被称为“不能向下读”）。
- 调用属性规则，主体不能请求（调用）完整性级别更高的主体的服务。

C、Clark-Wilson 模型

Clark-Wilson 模型采用一些不同的方法来保护信息的完整性。这种模型使用了下列元素：

- 用户：活动个体。
- 转换过程(TP)：可编程的抽象操作，如读、写和更改。
- 约束数据项(CDI)：只能由转换过程 TP 操纵。
- 非约束数据项(UDI)：用户可以通过简单的读写操作进行操纵。
- 完整性验证过程(IVP)：检查 CDI 与外部现实的一致性。

Clark-Wilson 模型的一个显著特点是，它专注于结构良好的事务处理和职能划分。结构良好的事务处理是指将数据项从一个一致状态转换为另一个一致状态的一系列操作。

D、无干扰方式(noninterference)

无干扰方式(noninterference)也是一种多级安全属性表达，实现这个概念是为了确保在较高安全级别中发生的任何活动不受影响，或者说干涉在较低安全级别中发生的活动。

无干扰模型的真正目的是为了处理隐蔽通道。隐蔽通道是某个实体以未授权方式接收信息的一种方式。这些通信可能很难被监测到。隐蔽通道分为两种类型：存储和计时。

E、Brewer and Nash 模型

Brewer and Nash 模型也称为 Chinese Wall 模型，这个模型规定主体只有在不能读取位于不同数据集内的某个客体时才能写另一个客体。它被创建来提供根据用户先前活动而动态改变的访问控制。这个模型的主要目标是防止用户访问被认为有利益冲突的数据。

F、其他模型实例

访问控制矩阵、取-予模型、Sutherland 模型、Graham-Denning Model、Harrison-

Ruzzo-Ullman Model。

单元 2：安全控制和评估

2.1 基于系统安全需求选择控制措施

A、安全需求

安全需要一般源自于：系统相关的任何法规或合规性要求（如：ISO 27001、SOX、GDPR、PCI DSS 等）、系统可能面临的威胁（威胁建模）、系统的风险评估。

B、控制选择

ISO 27001 是建立、实施和维持信息安全管理体系的标准，通过确定信息安全管理体系范围、制定信息安全方针、明确管理职责、以风险评估为基础，选择控制目标与控制方式等活动建立信息安全管理体系。

ISO 27002 可作为组织基于 ISO 27001 实施信息安全管理体系(ISMS) 的过程中选择控制措施时的参考，或作为组织实施通用信息安全控制措施时的指南文件。本标准包括 14 个安全控制措施的章节,共含有 35 个主要安全类别和 114 项安全控制措施。每一个主要安全控制类别包含：一个控制目标，声明要实现什么；一个或多个控制措施，可被用于实现该控制目标；实施指南为支持控制措施的实施和满足控制目标，提供更详细的信息。

2.2 理解信息系统的安全功能

大多数信息安全技术控制都基于硬件安全功能（并非所有），这些硬件安全功能就是“安全原语”。什么是“安全原语”？将原语视为构建基块，或由某种类型定义的工具。通常，“原始”一词与加密原语相关联，但我们谈论的是保持硬件安全类型的基础。安全控制技术在这些原语上实施了更详细，更复杂的安全控制。硬件安全性原语的类型将有所不同，这取决于平台。 这些可以包括：

A、封闭式系统和开放式系统

在设计和构建应用系统时，有两种不同的理念：封闭式和开放式。封闭式系统被设计用于与较小范围内的其他系统协同工作，通常所有系统都来自相同的制造厂商。封闭式系统的标准一般是专有的， 通常不对外公开。开放式系统被设计为使用统一的行业标准。这

些开放式系统比较容易与来自不同制造厂商但支持相同标准的系统集成在一起。封闭式系统很难与不同的系统集成在一起，但是它们更为安全。

B、内存保护

内存保护是核心安全组件，在操作系统中必须设计和实现。无论系统中执行哪些程序，都必须执行内存保护，否则可能导致不稳定、侵害完整性、拒绝服务和泄露等结果。内存保护用于防止活动的进程与不是专门指派或分配给它的内存区域进行交互。内存保护包括隔离、虚拟内存、分段、内存管理和保护环等。

C、虚拟化

虚拟化技术用于在单一主机的内存中运行一个或多个操作系统。这种机制几乎允许任何操作系统在任何硬件上虚拟运行。通过虚拟化技术将一台计算机虚拟为多台逻辑计算机，每个逻辑计算机可运行不同的操作系统，并且应用程序都可以在相互独立的空间内运行而互不影响。有两种虚拟化管理技术：Type1 和 Type2。

D、可信平台模块

可信平台模块（TPM）是一个安装在现代计算机主板上的微芯片，它有着专门实施的安全功能，包括对称和非对称密钥、散列、数字证书的存储和处理。

TPM 的本质在于它是一个受保护的、封装好的微控制器安全芯片，它为存储和处理密集的安全敏感数据（如密钥、密码和数字证书）提供了一个安全的避风港。TPM 内部的内存分为两个不同的部分：持久性（静态）和通用（动态）内存模块。

E、硬件安全模块(HSM)

硬件安全模块(HSM)是一种加密处理器，用于管理/存储数字加密密钥、加速加密操作、支持更快的数字签名以及改进身份验证。一般通过扩展卡或外部设备的形式直接连接到电脑或网络服务器。

F、智能卡

智能卡通常用于提供便携式安全存储，以用于身份管理（用于多因素身份验证），敏感信息（例如硬件安全模块之间的密钥）的安全传输和付款处理（例如信用卡的 EMV 标

准）。

2.3 评估与缓解安全架构、设计和解决方案要素的漏洞

A、系统评价方法

在进行正式评估时，系统通常需要经过两个阶段：第 1 阶段：对系统进行测试和技术评估，以确保系统的安全功能符合其预期使用的标准。第 2 阶段：系统应对其设计和安全标准及其实际能力和性能进行正式比较，负责此类系统安全性和准确性的人员必须决定是接受它们还是拒绝它们还是对标准进行一些修改，然后再试一次。

整个评估过程的第 1 阶段是认证（certification）。认证是对 IT 系统以及为支持认可过程而制定的其他保护措施的技术和非技术安全功能的综合评估，从而确定特定设计和实施满足一组特定安全要求的程度。认可（accreditation）一般是第 2 阶段，是管理层对系统整体安全和功能的充分性的正式认定。认证信息提交给管理层或者负责部门，由管理层来提问、复查报告和裁定结果，并且决定产品是否可以接受，以及是否需要采取任何修正措施。一旦管理层对提交的系统整体安全性表示满意，他们就会拟定一份正式的认可声明。这样一来，管理层就声明自己了解系统在当前环境下能够提供的保护等级，而且知道与安装和维护该系统相关的安全风险。

组织通常也会聘请可信的第三方来执行此类评价，这种测试最重要的结果是他们的“批准印章”(即系统符合所有基本标准)。

TCSEC 也被称为橘皮书，论述的重点是通用的操作系统，为了使它的评判方法适用于网络，后来 NCSC 在 1987 年出版了一系列有关可信计算机数据库、可信计算机网络等的指南等（俗称彩虹系列）。TCSEC 从网络安全的角度出发，解释了准则中的观点，从用户登录、授权管理、访问控制、审计跟踪、隐通道分析、可信通道建立、安全检测、生命周期保障、文本写作、用户指南均提出了规范性要求，并根据所采用的安全策略、系统所具备的安全功能将系统分为四类七个安全级别。分级主要依据四个准则：安全政策、可控性、保证能力、文档。将计算机系统的可信程度划分为 D、C1、C2、B1、B2、B3 和 A1 七个安全级别。四个类分别为：类别 A，是指已验证保护， 这是最高的安全级别；类别 B，是指强制性保护；类别 C，是指自主性保护；类别 D，是指最小化保护， 提供用于那些被评估，但不符合要求且属于其他类别的系统定级。

ITSEC 是欧洲多国安全评价方法的综合产物，军用，政府用和商用，将安全概念分为功能需求与功能评估两部分。首次提出了信息安全的保密性、完整性、可用性的概念。ITSEC 将正在被评估的系统作为评估目标（Target Of Evaluation，TOE）。所有的等级都以两种类别表示为 TOE 等级。

通用准则又被称为 CC(Common Criteria) ，ISO 将这个准则文档转换为 ISO 15408 通

用准则定义了作为评估信息技术产品和系统安全性的基础准则，全面地考虑了与信息技术安全性有关的所有因素，与 PDR（防护、检听、反应）模型和现代动态安全概念相符合的，强调安全的假设、威胁的、安全策略等安全需求的针对性，充分突出保护轮廓。仍然强调把安全需求划分为安全功能需求和安全保证需求两个独立的部分，根据安全保证需求定义安全产品的安全等级。

通用准则过程基于两个要素：保护轮廓和安全目标。保护轮廓(PP)为要评估的产品(TOE)指定安全要求和保护，这些要求和保护被认为是客户的安全要求或“客户想要的安全”。安全目标(Security Targets, ST)指定了供应商在 TOE 内构建的安全声明。ST 被认为是已实施的安全措施或是供应商的“我将提供的安全”声明。将 PP 与来自所选供应商的 TOE 中的各种 ST 进行比较，最接近或最匹配的就是客户购买的产品。

在通用准则模型中，对一件产品上进行评估时会给该产品指定一个评估保证级别（EAL）。随着级别的升高，彻底和严格的测试中面向细节的任务也逐步增加。通用准则有 7 个保证级别，其范围是从仅仅执行功能测试的 EAL1，到执行彻底的测试并验证系统设计的 EAL7。

ISO/IEC15408 是国际标准，是评估 CC 框架下产品安全属性的基础。它通常包括 3 部分：

- ISO/IEC 15408-1 介绍了 CC 评估模型的通用概念和准则。这部分定义术语、确定 TOE 的核心概念、描述评估环境和必要的参与人员。它为 PP 提供了关键概念，为安全目标提出了要求和指南。
- ISO/IEC 15408-2 定义在评估过程中要评估的安全功能要求。包括符合多数安全需求的一系列预定义的安全功能组件。这些要求按类别、属别和组件的层级结构排列。它同样也为在没有预定义的安全功能组件存在时对于个性化安全要求应如何规定提供了指南。
- ISO/IEC 15408-3 定义了保证要求，也是按类别和组件的层级结构排列。这部分概括了评估保证级别，这是考量 TOE 保证的标杆，为评估保护配置文件和安全目标提供了标准。

B、基于客户端和服务端系统

基于客户端的系统体现为运行在用户设备上的程序体现的，最常见的安全问题就是缺少认证机制，例如：Java applet 和 ActiveX、ARP、DNS 缓存中毒问题。

基于服务端的系统安全关注的重要领域是数据流控制问题，数据流是进程之间、设备之间、网络之间或通信通道之间的数据移动。

最常见的就是 Web 应用系统的漏洞，例如 OWASP 提出的 Web 应用系统十大安全漏洞（2017）。

C、数据库系统

数据库安全性是任何使用大量数据作为重要资产的组织的重要组成部分，必须关注与数据库安全性相关的几个主题包括：聚合(Aggregation)和推理（Inference）。这部分知识在 D8 中有详细描述。

D、分布式系统和端点安全

分布式系统是一个多台计算机共同完成任务的系统。由于涉及大量设备，在安全方面分布式系统受到了特殊的挑战

云计算系统是一个最常见的分布式系统，是虚拟化、互联网、分布式架构以及可随处访问数据和资源的需求的自然延伸和发展。它存在一些问题，包括隐私问题、合规困难、开源与封闭式解决方案的使用、开放标准的采用以及基于云的数据是否切实地受到保护(甚至能否保护)。

虚拟机管理程序（也称为虚拟机监视器）是创建、管理和操作虚拟机的虚拟化组件。运行虚拟机管理程序的计算机称为主机操作系统，在虚拟机管理程序支持的虚拟机中运行的操作系统称为客户操作系统。虚拟机管理程序有两种模式：

- Type-I 虚拟机管理程序是原生或裸机管理程序。在此配置中，没有主机操作系统，虚拟机管理程序直接安装到通常主机操作系统安装的硬件上。这允许最大限度地利用硬件资源，同时消除由主机 OS 引起的任何风险。
- Type-II 虚拟机管理程序是托管管理程序。在这种配置中，在硬件上安装一个标准的常规 OS，然后将虚拟机管理程序作为一个软件应用程序安装。

基础设施即服务基础设施即服务(Infrastructure as a Service, IaaS)包括计算服务、管理任务自动化、动态扩展、虚拟化服务、策略实施和管理服务以及托管过滤的互联网连接。

平台即服务平台即服务（Platform as a Service, PaaS）的概念是将计算平台和软件解决方案提供为虚拟的或者基于云的服务。

软件即服务软件即服务(Software as a Service, SaaS)提供对特定软件应用程序或套件的按需在线访问而不需要本地安装。

私有云(private cloud)是企业内部网络中的云服务并与 Internet 隔离。私有云仅供内部使用。

公有云(public cloud)是一种可供公众访问的云服务，通常通过 Internet 连接。公有云服务可能需要某种形式的订阅或按使用次数付费，或者也可能免费提供。

混合云混合 云(hybrid cloud)是私有云和公有云组件的混合体。

社区云(community cloud)是由一组用户或组织维护、使用和支付用于利益共享的云环

境，例如协作和数据交换。

云共享责任模型的概念是，当组织使用云解决方案时，提供商和客户之间存在安全性和稳定性责任的划分。不同形式的云服务(例如 SaaS、PaaS 和 laaS)可能具有不同级别或划分点的共享责任。在选择使用云服务时，重要的是要考虑管理、故障排除和安全管理的细节以及如何在云提供商和客户之间分配、划分或共享这些职责。

云访问安全代理(Cloud Access Security Broker, CASB)是一一种实施安全策略的解决方案，可在本地安装也可以基于云。CASB 的目标是在云解决方案和客户组织之间实施适当的安全措施。

安全即服务(Security as a Service, SECaaS)是一个云提供商概念，其中通过在线实体或由在线实体向组织提供安全性。SECaaS 解决方案的目的是降低在本地实施和管理安全性的成本和开销。SECaaS 通常实现为不需要专用本地硬件的纯软件安全组件。SECaaS 安全组件可包括各种安全产品，包括身份验证、授权、审计/记账、反恶意软件、入侵检测、合规性和漏洞扫描、渗透测试和安全事件管理。

网格计算是一种并行分布式处理形式，它将大量处理节点松散地分组，以实现特定处理目的。

网格计算最大的安全问题是每个工作包的内容可能会暴露给外界，另外如果中央网格服务器被控制，会被利用来攻击或欺骗网格成员。

对等网络（P2P）技术是网络和分布式应用程序解决方案，可在点对点共享任务和工作负载。P2P 主要的安全问题包括：盗版、窃听、缺乏集中监管和过滤、带宽消耗。

E、嵌入式和物联网系统

嵌入式系统是信息物理系统中最简单的形式，通常围绕微控制安装，是一种包括 CPU、内存、外设控制接口的专门设备，具有一个非常基本的操作系统。保护嵌入式系统的主要挑战是确保驱动它们的软件的安全性。

物联网（IoT）是连接嵌入式系统的全球性网络，物联网关注的安全问题包括：身份验证、数据加密、数据/补丁更新。

F、工业控制系统

工业控制系统（ICS）由专门用于控制工业过程中的物理设备的信息技术组成，包括：可编程逻辑控制器（PLC）、分布式控制系统（DCS）、管理控制与数据采集（SCADA）。过去几年，ICS 几乎没有考虑安全性。

G、移动系统

移动设备基本上是一台小型计算机，几乎具有与传统计算机一样的安全漏洞、威胁和风险，常见的安全问题有：虚拟基站、机密数据被盗、隐私问题（拍照、麦克风功能不当使用）、违反公司策略访问网络、下载恶意代码、脆弱的加密。

使用移动系统在设备安全方面的选项：全设备加密、锁屏、存储分隔、移动设备管理(MDM)、远程擦除、GPS、资产跟踪、设备访问控制、锁定(Lockout)、应用程序控制、库存控制、可移动存储、关闭不使用的功能。

使用移动系统在应用安全方面的选项：密钥管理、地理位置标记、凭据管理、加密、身份认证、应用白名单。

BYOD（自带设备）是一种策略，允许员工将自己的个人移动设备投入工作。在安全方面的注意事项有：数据所有权、所有权支撑、病毒管理、补丁管理、取证、隐私、入职/离职、公司策略遵守、用户接受度、架构/基础设施考虑、法律问题、可接受使用策略、摄像头问题等。

H、常见的架构缺陷和安全问题

隐蔽隧道是一种用于在通常不用于通信的路径上传递信息的方法。有两种基本类型：时间隐蔽隧道、存储隐蔽隧道。其它的缺陷，例如：维护陷阱（maintenance hook）、检验时间/使用时间（TOC/TOU）等，在 D8 中会有详细介绍。

单元 3：密码学基础和应用

3.1 密码学定义与概念

A、相关基本定义

明文形式存在的数据能够被人（文件）或计算机（可执行代码）所理解。一旦它转换为密文，那么在解密之前，人和机器都无法对其进行正确处理。

加密方法能够将称为明文的可读数据转换为称为密文的、看似随机和不可读的数据。

提供加密和解密的系统或产品称为密码系统(cryptosystem)，它由硬件组件和应用程序中的程序代码构成。密码系统使用加密算法（它决定加密过程的简单或复杂程度）、密钥以及必要的软件组件和协议。

算法，是一组被称为密码的规则，它规定如何加密和解密。算法包含一个密钥空间

（keyspace），它由一定范围的值组成，这些值能够用于构造密钥。

Kerckhoffs 原则指出一个密码系统唯一需要保密的部分应当是密钥。

加密方法的强度源自算法的复杂程度、密钥的机密度、密钥的长度、初始化向量以及它们如何在密码系统内协同工作。

设计加密方法的目标是使破解过程过于昂贵或十分费时。密码学强度也称为工作因数(work factor)，即对攻击者破译一个密码系统所付出的努力和资源进行估计。

密码系统服务，密码系统可以提供以下服务：

- 机密性，除了授权实体之外，其他实体无法理解提交的数据。
- 完整性，数据从创建到传输、存储都不会被未授权更改。
- 身份验证，对创建信息的用户或系统的身份进行验证。
- 授权，证明身份之后，向个体提供允许访问某些资源的密钥或密码。
- 不可否认性，确保发送方无法否认发送过消息。

密码学一般是通过密码学的方法来提供这些服务的，这些方法就是我们常说的密码算法，主要有：

- 对称系统，在一个使用对称密码学的密码系统中，发送方和接收方使用相同密钥的两个实例来加密和解密。
- 非对称系统，在对称密钥密码学中，实体之间使用单个密钥；而在非对称密钥系统中，两个实体中的每个实体都具有不同的密钥或非对称密钥。
- 散列算法，散列是一种函数，它将可变长的字符串或消息压缩变换成固定长度的值，用来检测位流从一台计算机传送到另一台计算机时是否被更改。
- 一次性密码本(one-time pad)是一种完美的加密方案，使用一个由随机值组成的密码本。
- 隐写术(steganography)是一种将数据隐藏在另一种介质中以藏匿数据的方法。

B、密钥管理

密钥管理是指密钥的生成、分发、安装、存储、更改、控制和处置，其中每个环节的缺陷都有可能导致密码系统的失效，密钥管理比密码算法更容易受到攻击。

3.2 对称加密系统

A、对称密码学概述

在一个使用对称密码学的密码系统中，发送方和接收方使用相同密钥来加密和解密。因此，这种密钥具有双重功能性，既可以完成加密，也可以完成解密。因为这种加密方法

依赖于每个用户都恰当地保护密钥不被泄露，所以对称密钥也称为秘密密钥。如果密钥落到入侵者之手，那么他就能够解密任何被截获、采用该密钥加密的消息。

对称密钥系统的优点有：比非对称系统的运算速度快得多，并且在使用大密钥时很难攻破。

对称密钥系统有的缺点包括：首先，需要一个恰当分发密钥的安全机制，来保证密钥的分发。其次，由于每对用户都需要唯一的密钥，因此如果有大量用户时，密钥数呈指数增长，密钥管理任务比较繁重。还有对称密钥系统能够提供机密性，但是不能提供真实性或不可否认性。

对称加密具有两种基本类型：替代和换位，换位也被称为置换。替代对称加密就是使用不同的位、字符或字符分组来替换原来的位、字符或字符分组。换位密码并不使用不同的文本来替换原来的文本，而是对原有的值进行置换，即重新排列原来的位、字符或字符分组以隐藏其原有意义。

B、分组密码和流密码

对称算法有两种主要类型：分组密码和流密码。当使用分组密码来加密和解密时，消息会被划分为若干位分组，这些分组随后会通过数学函数进行处理，每次一个分组。分组密码有几种操作模式，每种模式都指定一种分组密码的运作方式：

- 电子密码本（ECB）：直接将明文分组分别进行直接加密，是最简单的加密模式，它的缺点是相同的明文分组总是得到相同的密文分组，而不隐藏数据模式，它的优点是分组加密过程中的错误仅限于那一个分组，而不会影响其它分组。
- 密码分组链接模式（CBC）：在 ECB 模式中，一组明文和密钥总是生成相同的密文。CBC 并不暴露加密模式，因为算法会处理每个文本分组、密钥以及基于前一个分组的值，并将它们应用于下一个文本分组。
- 密码反馈模式(CFB)：将分组密码转换为流密码，它首先使用初始向量（IV）和密钥经过加密运算生成第一组密钥流，第一组密钥流与第一组明文进行异或运算生成第一组密文，再使用第一组密文和密钥经过加密运算生成第二组密钥流，第二组密钥流与第二组明文进行异或运算生成第二组密文，依此类推。
- 输出反馈模式(OFB)：同样将分组密码转换为流密码，它首先使用初始向量（IV）和密钥经过加密运算生成第一组密钥流，第一组密钥流与第一组明文进行异或运算生成第一组密文，再使用第一组密钥流和密钥经过加密运算生成第二组密钥流，第二组密钥流与第二组明文进行异或运算生成第二组密文，依此类推。
- 计数器模式（CTR）：与 OFB 模式非常相似，但它并不使用一个随机的唯 IV 值来生成密钥流值，而是使用一个 IV 计数器，它随需要加密的每个明文分组而递增。这个独特的计数器保证每个数据分组与唯一的密钥流值进行异或运算。

C、常见的对称密码算法

DES 是一种对称分组加密算法，每一组的分组长度是 64 位。DES 使用 64 位密钥，但只有其中 56 位为实际使用的密钥，另外 8 位则用于奇偶校验。DES 已经被一台名为 DES 破解者的专用计算机破解，现在基本已经不会被使用了。

3DES 使用了 48 轮运算（三次 DES 运算），这使得它对于差分密码分析有很强的抵御能力。3DES 可以在不同模式下运行，选择的模式决定它所使用密钥的数量和执行的功能，如下所示：

- DES-EDE3：使用 3 个不同的密钥进行加密，数据被加密、解密、再加密。
- DES-EDE2：与 DES-EDE3 相同，但只使用两个密钥，第一个和第三个加密过程使用相同的密钥。

高级加密标准（AES）是一种对称分组密码，它支持 128、192 和 256 位的密钥。这个标准也是目前我们主要使用的加密标准。

国际数据加密算法（IDEA）是一种分组密码，它处理 64 位数据分组，使用的密钥长度为 128 位。

Blowfish 属于分组密码，它处理 64 位数据分组，密钥长度为 32-448 位。

RC4 是最常用的流密码之一。

3.3 非对称加密系统

A、非对称密码学概述

在非对称（公共）密钥系统中，两个实体中的每个实体都具有不同的密钥或非对称密钥。这两个不同的非对称密钥是数学相关的。如果消息是使用其中一个密钥加密的，那么就需要另一个密钥进行解密。其中密钥中一个被称为公钥和一个被称为私钥，公钥(public key)可以被任何人所知，而私钥(private key)必须只由所有者知道和使用。非对称密钥系统的公钥和私钥是数学相关的。然而，如果某人获得了另一个人的公钥，那么他应该无法据此推断出相应的私钥。

非对称密钥系统优点包括：具有比对称系统更好的密钥分发功能，具有比对称系统更好的扩展性，还能提供身份验证和不可否认性。

非对称密钥系统缺点包括：由于非对称算法是一种数学密集型任务，运算量比较大，因此比对称系统运行要慢。

B、常见的非对称密码算法

RSA 算法是一种公钥算法，也是非对称算法中最流行的算法。RSA 是事实上的全球标准，能够用于数字签名、密钥交换和加密。

椭圆曲线密码系统（ECC）提供的功能与 RSA 相似：数字签名、安全密钥分发和加密。一个不同的因素是 ECC 的效率。ECC 比 RSA 和其他非对称算法的效率更高。

Diffie-Hellman 算法使两个系统不需要提前建立关系或预先安排就能安全地交换对称密钥。这种算法可实现密钥发送，但并不提供加密或数字签名功能。

El Gamal 是一种可用于数字签名、加密和密钥交换的公钥算法。

C、混合加密和会话密钥

混合加密系统指的是对称算法创建一个用于加密批量数据或消息的秘密密钥，非对称密钥则用于加密要传输的秘密密钥。

会话密钥(session key)是只使用一次的对称密钥，用于对通信会话期间两个用户之间的消息进行加密。会话密钥与前面介绍的对称密钥没有区别，它只是为了更好地完成用户之间的一次通信会话。

3.4 散列算法

A、散列算法概述

散列算法是一种函数，它将可变长的字符串或消息压缩变换成固定长度的值，也就是我们所说的散列值。散列函数并不保密，它是公开的。散列函数的关键是它的“单向性”这个函数只单向计算，不反向计算。散列函数本身不使用任何密钥。

良好的密码散列函数应当具有下列特征：应当对整条消息计算散列值；散列函数应当是单向函数，因此散列值不会泄露消息；给定一条消息及其散列值，要找出另一个有着同样散列值的消息应该是不可能的；散列函数应当能够抵御生日攻击。

B、常见的散列算法

MD4 是一种单向函数，也产生 128 位的消息摘要值。它应用于软件实现的快速计算环境，并为微处理器进行了优化。

MD5 是 MD4 的升级版本。MD5 仍然产生 128 位的消息摘要值，但是它的算法比较复杂，所以更难以攻破。

SHA 算法会产生 160 位的散列值或消息摘要，产生的结果随后输入非对称算法，从而为消息计算签名。SHA 改进后命名为 SHA-1。SHA-1 已经被发现容易遭受到碰撞攻击，并且不再被认为是安全的。该算法的较新版本（统称为 SHA-2 和 SHA-3 系列）已经开发和发布：SHA-256、SHA-384 和 SHA-512。SHA-2 和 SHA-3 系列被认为可以安全的使用。

C、针对单向散列函数的攻击

如果散列算法为两条不同的消息产生相同的散列值，那么我们就称之为冲突。攻击者可以试图制造冲突，这称为生日攻击。这种攻击基于标准统计学中存在的算数生日悖论。

3.5 密码学应用

A、身份认证和完整性

消息身份验证码（MAC）函数是通过以某种形式对消息应用秘密密钥而派生的一种身份验证机制，但并不表示它使用对称密钥来加密消息，有 3 种基本类型：

HMAC：如果想要使用 HMAC 函数来代替散列算法，那么需要将一个对称密钥合并在消息的后面。HMAC 使用散列算法计算已附加密钥的消息，以生成 MAC 值。

CBC-MAC：如果使用 CBC-MAC，那么就在 CBC 模式下使用对称分组密码对消息进行加密，并将最后输出的密文分组用作 MAC。发送方并不传送加密形式的消息，而是传送后面附有 MAC 值的明文消息。接收方接收到明文消息，然后在 CBC 模式下使用相同的对称分组密码对消息进行加密，计算出一个独立的 MAC 值。接收方将这个新 MAC 值与随消息一起发送的 MAC 值进行比较。这种方法并不像 HMAC 那样使用散列算法。

CMAC：是 CBC-MAC 的一种变体，它可以与 AES 和三重 DES 一起使用。

数字签名是使用发送方的私钥加密的散列值。签名的动作意味着使用私钥来加密消息的散列值。

总的来说：散列函数确保了消息的完整性，散列值的签名则提供了身份验证和不可否认性。签名动作实际上就是使用私钥加密散列值。

B、便携式设备

目前流行的操作系统版本包括磁盘加密功能，使其易于应用和管理便携式设备上的加密。例如，微软 Windows 包括 BitLocker 和加密文件系统（EFS）技术，MacOSX 包含 FileVault 加密，TrueCrypt 的开源软件包允许在 Linux，Windows 和 Mac 系统的磁盘加密。

C、保护电子邮件

电子邮件系统需要保证维护邮件或传输邮件的安全性(也就是机密性、完整性、身份认证和不可否认性)与隐私性，广泛使用的电子邮件标准有：

- 可靠隐私（PGP）。PGP 有两个可用的版本。商业版本使用 RSA 进行密钥交换，使用 IDEA 进行加解密，使用 MD5 生成消息摘要。免费版本则使用 Diffie-Hellman 进行密钥交换、CAST 128 位进行加解密算法以及 SHA-1 散列函数。许多商业机构也提供基于 PGP 的电子邮件服务作为基于 Web 的云端邮件服务、移动设备应用程序或 Web 邮件插件。
- 安全多用途互联网邮件扩展协议，简称 S/MIME 协议。这个协议使用 RSA 加密算法，并且已经得到了包括 RSA 等安全公司在内的业界主要机构的支持。S/MIME 协议依靠 X.509 证书交换密码系统密钥。这些证书包含的公钥被用于数字签名和较长通信会话中使用的对称密钥交换。RSA 是 S/MIME 支持的唯一一个公钥密码学协议，这个协议支持 AES 和 3DES 对称加密算法。

D、保护 Web 应用

加密被广泛的用于保护 Web 传输，主要是用的协议为：安全套接字(SSL)和安全传输层协议（TLS）。1999 年安全工程师在 SSL 第三版本的时候，提出了将 TLS 作为 SSL 标准的替换，现在仅仅依靠 TLS 安全。

SSL 协议提供在浏览器与 Web 服务器之间交换数字证书，并协商加密和解密参数。SSL 协议的目标是建立安全的通信通道，使整个 Web 浏览器会话保持开放。它取决于对称和非对称加密的组合。具体过程涉及以下步骤：第一步，当用户访问一个网站时，浏览器检索出服务器的证书，并从中提取服务器的公共密钥；然后，浏览器创建一个随机的对称密钥，使用服务器的公钥来加密，然后将加密的对称密钥发送到服务器上；随后，服务器使用自己的私钥解密对称密钥， 这两个系统使用对称加密密钥来交换未来的交互信息。

E、数字版权管理（DRM）

数字版权管理（DRM）软件使用加密来加强对数字媒体的版权限制。常见的数字版权管理包括：音乐 DRM、电影 DRM、电子书 DRM、电子游戏 DRM、文档 DRM。

F、线路加密

链路加密使用软件或硬件解决方案在两个点之间建立一条安全隧道，对进入隧道一端

的所有通信数据都进行加密，并且对进入隧道另一端的所有通信数据都进行解密，从而保护整个通信线路的安全。

端到端加密保护双方(例如一个客户端和一个服务器)之间的通信安全，并且可以独立于链路加密实施。

IPSec：在两个实体之间建立信息交换的安全信道。具体会在 D4 中详细介绍。

WEP：提供 64 和 128 位的加密选项， 从而保护无线 LAN 内的通信。WPA 改进了 WEP 加密，WPA2 进一步改善了 WPA 技术。具体会在 D4 中详细介绍。

G、公钥基础设施

公钥基础设施（PKI）由程序、数据格式、措施、通信协议、安全策略以及公钥密码机制组成，这些组件综合方式运行的，使得分散的人们能够以安全的、预定的方式相互通信。PKI 提供身份验证、机密性、不可否认性以及消息交换的完整性。

PKI 可能由下列实体和功能组成：CA、RA、证书存储库、证书撤消系统、密钥备份和恢复系统、自动密钥更新、密钥历史记录管理、时间标记、客户端软件。

可信的第三方（即认证授权机构（Certificate Authority，CA））创建和签发（数字签名）数字证书，每一个想加入 PKI 的人都需要一个数字证书。

数字证书是用于将公钥和唯一标识其所有者所需的组成部分关联起来的机制，证书包含序列号、版本号、身份信息、算法信息、有效期以及发行证书的授权机构的签名。

注册授权机构（RA）执行证书注册任务。RA 建立和确认个人的身份，代表终端用户启动使用 CA 的认证过程，以及执行证书生命周期管理功能。RA 不能发行证书，但是可以作为用户和 CA 之间的中间人。当需要新证书的时候..用户就会向 RA 发送请求，然后 RA 再将该请求发送给 CA。

3.6 密码分析攻击

唯密文攻击：在这种攻击中，攻击者拥有若干消息的密文，每条消息都是使用相同的加密算法加密的。攻击者的目标是找出加密过程中使用的密钥。一旦攻击者找到密钥，它就可以解密使用相同密钥加密的其他所有消息。

已知明文攻击：在已知明文攻击中，攻击者拥有一条或多条消息的明文和相对应的密文。同样，攻击者的目标是找出用于加密消息的密钥，从而能够解密和读取其他消息。

选定明文攻击:在选定明文攻击中，攻击者拥有明文和密文，不过可以选择已加密的明文来查看相应的密文。这使得他们可能更深入地理解加密过程的工作方式，从而能够获得关于正在使用的密钥的更多信息。一旦密钥被发现，使用该密钥加密的其他消息就都能够被解密。

选定密文攻击：在选定密文攻击中，攻击者选择将要解密的密文，并且可以获得解密后的明文。同样，攻击的目标是找出密钥。这是一种比前几种攻击都更为困难的攻击，攻击者可能需要控制包含密码系统的系统。

差分密码分析：差分密码分析攻击也以找出加密密钥为目标。这种攻击会查看对具有特定差异的明文进行加密而生成的密文对，并且分析这些差异的影响和结果。

线性密码分析：线性密码分析通过执行函数来确定使用分组算法的加密过程中利用某个特定密钥的最大概率。

旁路攻击：旁路攻击的原理在于不用直接攻击一台设备，而是只须监视它如何运行就可以了解其工作机制。攻击者可能会测量功率消耗、辐射排放以及进行某些数据处理的时间。借助这些信息，攻击者就可以通过逆向工程倒推处理过程，以获得加密密钥或敏感数据。功耗攻击会查看所排放的热量，攻击者已经使用这种攻击成功从智能卡中获取了机密信息。

重放攻击：重放攻击就是攻击者捕获了某些类型的数据并重新提交它，从而欺骗接收设备误以为这些是合法信息。

代数攻击：代数攻击分析算法内使用的数学原理中存在的脆弱性，并利用了其内在的代数结构。

分析式攻击：与简单穷尽全部可能性但并不注意算法特殊性的蛮力攻击相反，分析式攻击会确定算法结构上的弱点或缺陷。

统计式攻击：统计式攻击确定算法设计中的统计弱点并对其加以利用。

社会工程攻击：攻击者可以通过各种社会工程攻击类型诱使人们提供加密密钥材料。它们是非技术性的攻击，攻击者的目标是引诱人们泄露某种类型的敏感信息，这些信息可以被攻击者利用，带着这样的目标，攻击者对人们进行攻击。通过说服、强迫（软磨硬泡攻击）或者贿赂（购买密钥攻击）这些手段，可以顺利实施攻击。

单元 4：设计和实施物理安全

4.1 站点安全规划、设计和实施

A、站点规划过程

组织面临的物理方面的安全威胁：自然环境威胁、供应系统威胁、人为威胁、以政治为动机的威胁。在任何情况下，生命安全都是最重要的考虑因素。

物理安全是保护资源的人员、过程、措施和设备的组合。一个组织的物理安全计划应当涉及下列目标：

- 通过震慑预防犯罪和破坏：栅栏、保安、警示标志等。

- 通过使用延迟机制来减少损失：延缓对手行动的防御层，如锁、安全人员和屏障。
- 犯罪或破坏检测：烟雾探测器、运动探测器、CCTV 等。
- 事故评估：保安检测到的事故的反应以及破坏级别的确定。
- 响应措施：灭火机制、应急响应过程、执法通告、外部安全专家咨询。

通过环境设计来预防犯罪（CPTED）是一门学科，它研究如何正确设计通过直接影响人类行为而减少犯罪的物理环境。CPTED 提供了下列 3 种主要策略，这些策略与物理环境和社会行为组合在一起来提高总体保护：自然访问控制、自然监视以及自然区域加固。

在设计和建造一个设施时，需要从物理安全的角度考虑下列主要项：墙壁、门、天花板、窗户、地板、供暖、通风和空调、电力供应、供水和天然气管道、火灾的检测与扑灭。

B、内部支撑系统

有 3 种方法可用来保护电源：UPS、电源线连接器和备用电源。

提供洁净电源时，电力供应不会包含干扰或电压波动。可能的干扰（或者说线路噪声）类型有电磁干扰（EMI）或射频干扰（RFI），即电流通过电线时对电源产生的干扰。一些和电源相关的术语：故障(fault)、中断(blackout)、电压不足(sag)、降压(brownout)、脉冲(spike)、电涌(surge)、起动功率(inrush)、噪声(noise)、瞬时现象(transient)、平稳(clean)、接地(ground) 。

正向排空装置，即其中的容纳物只能流出而不能流入。

湿度过高会造成腐蚀，而湿度过低则可能产生过多的静电。温度过低会使机械装置运行缓慢或停止运行，温度过高则可能造成设备使用太多风扇电能并最终关闭。

火灾共有 4 种级别：A、B、C、D，也有针对这 4 种级别的灭火方式。

在我们使用喷水装置进行灭火时，一般有以下 4 种喷水系统，分别是：湿管式、干管式、提前作用式以及泛滥式等。

4.2 实施和维护物理安全

A、周边物理安全

物理访问控制的使用、监控人员、设备的进入和离开，还有审计/记录所有的物理事件，是维护整体组织安全的关键要素，包括：

- 栅栏是外围设备。栅栏被用于在受到特殊安全保护级别的区域和其他区域之间进行明确的区分。

- 大门是栅栏上受到控制的出入点。大门可由保安人员操作，在没有保安人员时，推荐使用看门狗或 CCTV。
- 旋转门是一种门，它每次只可以进一个人，并且常常限制在单方向的转动。
- 陷阱是通常由保安人员守护的双重门设置。陷阱的目的是为了牵制主体，直至其身份得到确认和验证。
- 照明的主要目的是为了阻拦那些偶然的入侵者、闯入者、小偷和希望在黑暗中实施其恶意行为的潜在窃贼。

所有的物理安全控制，无论是静止的阻碍物还是主动的检测和监视机制，最终都要依靠保安的介入来阻止实际的入侵和攻击。

B、内部物理安全

员工证、身份证或安全 ID 都是物理身份标识和/或电子访问控制设备的形式。

运动探测仪或运动传感器是在特殊区域中使用的、用于感知物体运动的设备。运动探测仪的类型有很多种，包括红外线、热能、波形、电容、光电和无源音频。

- 红外运动探测仪对被监控区域红外照明模式的显著变化进行监视。
- 热能型运动探测仪对被监控区域中的热能等级和模式的显著变化进行监视。
- 波形运动探测仪向被监控的区域发射连续的弱超声波或高频微波，并且对反射波的显著扰动或变化进行监视。
- 电容运动探测仪对被监控物体周围区域的电场或磁场变化进行探测。
- 光电运动探测仪通常在没有窗户或保持昏暗的房间内部使用。
- 无源音频运动探测仪对被监控区域中的非正常声音进行侦听。

CCTV 是一种安全机制，涉及运动探测器、传感器和报警器。

保护环境基本要素和保护人员生命是设施物理访问控制和安全维护的一个重要方面。另外安全策略必须符合行业和管辖权内的现行监管要求。

D4：网络与通信安全

单元 1：在网络架构中实施安全设计原则

1.1 OSI 参考模型

A、OSI 模型概述

OSI 参考模型将网络互联任务、协议和服务分为不同的层。当两台计算机通过网络通信时，每一层都具有自己的职责。每一层都有特定的功能，并且由那一层内工作的服务和协议来实现。

网络协议是决定系统如何在网络中通信的规则标准集。尽管本身有所不同，然而两个不同系统之所以能够相互通信和理解，其原因在于它们使用了相同的协议。这类似于两个人使用相同的语言就能相互交流和理解。

通信通过封装来完成，消息在一台计算机上的程序内构造，接着通过协议栈向下传递。每一层上的协议都在消息中添加自己的信息，这样消息的大小在沿协议栈往下传递的过程中会增大。随后，消息发送至目标计算机，封装的过程逆转，数据包将被拆开，这与在源计算机中进行封装的步骤相同。

B、OSI 模型七层

接下来，我们看一下 OSI 模型的每一层协议的特点和功能。

应用层是第七层，它工作在与用户最为接近的地方，提供文件传输、消息交换、终端会话以及更多功能。这一层并不包括实际的应用，但是包括支持这些应用的协议。应用层上的协议处理文件传输、虚拟终端、网络管理以及执行应用程序的网络请求。下面列出了在这个层上工作的一些协议：

- 文件传输协议（FTP）
- 普通文件传输协议（TFTP）
- 简单网络管理协议（SNMP）
- 简单邮件传输协议（SMTP）
- Telnet
- 超文本传输协议（HTTP）

表示层是第六层，它接收来自应用层协议的信息，然后将信息转变为所有遵循 OSI 模型的计算机都能理解的格式。这一层提供了一种其结构能被终端系统正确处理的数据表示

方式。这个层上没有协议工作，而只有服务。下面列出了表示层的一些标准：

- 美国信息交换标准编码（ASCII）
- 扩展二进制编码十进制交换模式（EBCDIC）
- 标签图像文件格式（TIFF）
- 联合图像专家组（JPEG）
- 运动图片专家组（MPEG）
- 音乐设施数字接口（MIDI）

会话层是第五层，它负责在两个应用程序之间建立连接。在数据传送过程中保持连接，以及控制这个连接的释放。会话层上的协议建立应用程序之间的连接，维持会话控制，并协商、建立、维持和撤消通信通道。下面列出了在这一层上工作的一些协议：

- 网络基本输入输出系统（Network Basic Input Output System，NetBIOS）
- 密码鉴别协议（Password Authentication Protocol，PAP）
- 端到端隧道协议（Point-to-Point Tunneling Protocol，PPTP）
- 远程过程调用（Remote Procedure Call，RPC）

传输层是第四层，提供了端对端数据传输服务，并且在两台通信计算机之间建立了一个逻辑连接。会话层和传输层的功能非常相似，它们都建立某种用于通信的会话或虚拟连接。它们之间的差异是：在会话层上工作的协议建立应用程序之间的连接，而在传输层上工作的协议则建立计算机系统之间的连接下面列出的一些协议工作在这一层：

- 传输控制协议（TCP）
- 用户数据报协议（UDP）
- 序列包交换（SPX）

网络层是第三层，其主要职责是在数据包的首部中插入信息，以便将数据正确地编址和路由，并且将数据实际路由至正确的目的地。网络层协议的职责包括网际互联服务、寻址和路由，下面列出了在这一层上工作的一些协议：

- 网际协议（Internet Protocol，IP）
- 互联网控制消息协议（Internet Control Message Protocol，ICMP）
- 互联网组管理协议（Internet Group Management Protocol，IGMP）
- 路由信息协议（Routing Information Protocol，RIP）
- 开放最短路径优先（Open Shortest Path First，OSPF）协议
- 网际数据包交换（Internetwork Packet Exchange，IPX）协议

数据链路层是第二层，继续沿协议栈向下走，我们就越接近数据要流经的实际通路（网络线缆）。数据链路层上的协议将数据转换成LAN或WAN帧进行传输，并且定义计算机访问网络的方式。这个层分为逻辑链路控制（LLC）和介质访问控制（MAC）子层。当数据链路层把最后的首部和尾部加到数据消息上时，这称为装帧。这个数据单元现在称为一个帧。下面列出了在这一层上工作的一些协议：

- 地址解析协议（ARP）
- 逆向地址解析协议（RARP）
- 点对点协议（PPP）
- 串行线路网际协议（SLIP）
- 以太网（IEEE 802.3）
- 令牌环（IEEE 802.5）
- 无线以太网（IEEE 802.1 1）

物理层（physical layer）是第一层，它将位转换为用于传送的电压。网络接口卡和驱动程序将位转换为电信号，并控制数据传输的物理方面，包括光学、电学和机械要求。下面列出了这个层上的一些标准接口：

- RS/EIA/TIA-422、RS/EIA/TIA-423、RS/EIA/TIA-449、RS/EIA/TIA-485
- 10BASE-T、10BASE2、10BASE5、100BASE-TX、100BASE-FX、100BASE-T、1000BASE-T、1000BASE-SX
- 集成服务数字网络（Integrated Services Digital Network，ISDN）
- 数字用户线路（Digital subscriber line，DSL）
- 同步光纤网络（Synchronous Optical Networking，SONET）

1.2 TCP/IP 模型与协议

A、TCP/IP 模型概述

传输控制协议/Internet 协议(TCP/IP)是控制数据从一个设备到另一个设备传送方式的协议族。除了以其命名的两个主要协议之外，TCP/IP 还包括其他协议。

TCP/IP 协议族内的协议协同工作，将应用层传递下来的数据分片，使得其能够沿着网络传输。它们与其他协议一起工作，从而将数据传送到目标计算机，然后再将数据重新组装为应用层能够理解和处理的形式。

B、TCP/IP 协议

在传输层上工作的两个主要协议是 TCP 和 UDP。TCP 是一个可靠的、面向连接的协议，这意味着它能确保数据包递送至目标计算机。如果数据包在传输过程中丢失，那么 TCP 能够标识这个问题并重新发送丢失或产生讹误的数据包。TCP 还支持包序列（能够确保接收到每一个包）、流量和拥塞控制以及错误检测和纠正。相反，UDP 是一个侧重传输效率的无连接协议，它没有包序列与流量和拥塞控制，而且目标不能确认接收每个包。如果消息正通过 TCP 传输，它就叫做“分片”；如果通过 UDP 传输，它就叫做“数据报文”

端口是用于确定其他计算机如何访问服务的机制。端口号在0~1023之间的端口称为通用端口。我们需要记住一些最常用的协议以及与它们对应的端口：

- Telnet。Telnet使用TCP 23端口，是一个终端仿真网络应用程序，支持远程连接以执行命令和运行应用程序，但不支持文件传输。
- FTP。TCP 20(被动数据)/短暂(活动数据)和21(控制连接)端口，是一个网络应用程序，支持需要匿名或特定身份验证的文件传输。
- TFTP。使用UDP 69端口，是一个支持不需要身份验证的文件传输的网络应用程序。
- SMTP。使用TCP25端口，是一种用于将电子邮件从客户端传输到电子邮件服务器以及从一个电子邮件服务器传输到另一个电子邮件服务器的协议。
- POP3。使用TCP 110端口，是一种用于将电子邮件从电子邮件服务器上的收件箱中拉到电子邮件客户端的协议。
- IMAP。使用TCP端口143，是一种用于将电子邮件从电子邮件服务器上的收件箱拉到电子邮件客户端的协议。IMAP比POP3更安全，并能从电子邮件服务器中提取标头以及直接从电子邮件服务器删除邮件，而不必先下载到本地客户端。
- DHCP。使用UDP 67和68端口，DHCP使用端口67作为服务器上的目标端口来接收客户端通信，使用端口68作为客户端请求的源端口。它用于在启动时为系统分配TCP/IP配置设置。DHCP支持集中控制网络寻址。
- HTTP。使用TCP 80端口，是将Web页面元素从Web服务器传输到Web浏览器的协议。
- SSL。使用TCP443端口(用于HTTP加密)，是一种类似于VPN的安全协议，在传输层运行。
- LPD。TCP端口515这是一种网络服务，用于假脱机打印作业和将打印作业发送到打印机。
- X Window。使用TCP 6000-6063端口，是用于命令行操作系统的GUI API。
- NFS。使用TCP 2049端口，是一种网络服务，用于支持不同系统之间的文件共享。
- SNMP。使用UDP 161端口（用于陷阱消息的是UDP 162端口），是一种网络服务，用于通过从中央监控服务器轮询监控设备来收集网络运行状况和状态信息。
- DNS是公共和专用网络中使用的分层命名方案。DNS将IP 地址和人性化的完全限定域名(FQDN)链接在一起

IP协议是一种网络层协议，它提供数据报路由服务。IP协议的主要任务是支持网络寻址和数据包路由，它是一个无连接协议，用于封装从传输层传递而来的数据。IP协议通过源IP地址和目标IP地址为数据报寻址。IPv4使用32位地址，而IPv6使用128位地址。子网划分允许将大范围的IP地址分为若干较小的、逻辑的和更易于使用的网段。IP分

类：A、B、C、D、E。无类别域间路由（CIDR），也叫做超网，允许人们在必要时灵活地增大或缩小每一类地址的范围。CIDR 是指定更灵活 IP 地址类的方法。

IPv6 也称为下一代 IP（IPng），它不仅比 IPv4 的地址空间更大，支持更多 IP 地址，而且还拥有许多 IPv4 并不具备的其他功能。这些差异如下：

- IPv6 将 IP 地址的大小从 32 位增加到 128 位，以支持更多的寻址层次结构级别、非常大的可寻址节点数以及更简单的地址自动配置。
- 通过为多播地址添加一个“作用域”字段，提高了多播路由的可扩展性。此外，还定义了一种名为任播地址的地址（anycast address），它用于向节点组中的任一节点发送数据包。
- 将 IPv4 首部中的某些字段舍弃或作为可选，以减少包处理的公共处理成本，并限制了 IPv6 首部的带宽成本。
- 改变了 IP 首部选项的编码方式，以实现更有效的转发，对选项长度的限制较为宽松，并且更适应将来可能引入的新选项。
- 添加了一个新功能，从而能够对属于用户请求特殊处理（如非默认的 QoS 或"实时"服务）的具体流量“流”的数据包进行标记。
- IPv6 还指定了支持身份验证、数据完整性以及（可选择）支持数据机密性的扩充部分。

与 UDP 类似，IP 是无连接的，是一种不可靠的数据报服务。IP 不保证数据包一定能被传送或数据包以正确顺序传送，不保证数据包只被传送一次。因此，你必须在 IP 上使用 TCP 来建立可靠和受控的通信会话。

网际控制消息协议（ICMP）用于确定网络或特定链路的运行状况，递送状态消息、报告错误、回答某些请求、报告路由信息并且常用于测试 IP 网络的连通性和排查问题。网际组管理协议（IGMP）用于向路由器报告多播组成员关系。

ARP 协议用于将 IP 地址(32 位二进制数用于逻辑寻址)解析为 MAC 地址(用于物理寻址的 48 位二进制数)。

在 OSI 模型的第 2 层帧级别确保网络流量安全是非常必要的。当帧从一个网络设备传递到另一个设备时，攻击者可以嗅探数据，修改数据包头，重定向流量，假冒流量，可以开展中间人攻击、拒绝服务攻击、重放攻击，甚至沉迷于其他恶意攻击行为。802.1 AE 是 IEEE MAC 安全标准（MACSec），它定义了一个安全基础，用来提供数据保密性、数据完整性和数据源认证。

1.3 多层、汇聚协议、SDN 以及 CDN

A、多层协议

由前面可知，作为协议套件的 TCP/IP 包含分布在各种协议栈层上的许多单独协议。因此，TCP/IP 是一种多层协议。TCP/IP 从其多层设计中获得了若干好处，这与其封装机制有关。

并非所有协议都适应 OSI 模型的分层。一些特殊的设备和网络从来就没打算与互联网有任何的交互性，所以它们往往缺乏强大的安全功能用于保护可用性、完整性和数据传输的保密性。作为信息安全专业人员，我们需要知道这些非传统的协议它们接入到网络对安全的影响。特别是，我们应该特别警惕哪些不明显的物理网络身份鉴别系统。

分布式网络协议 3（DNP3）是一种设计用于 SCADA 系统的通信协议。与其使用 OSI 七层模型，它的开发人员选择了一个简单的三层模型称为增强性能架构（EPA），大致对应 OSI 模型的 2、4 和 7 层。这种体系没有加密或认证，这是因为开发人员没有考虑到对这种设备相互连接的架构的网络攻击的可能性。

控制器区域网络总线（CAN bus）是一个设计允许微控制器和其他嵌入设备在共享总线上通讯的协议，这是一个运行在全球大部分汽车上的多层协议，几乎没有任何安全功能。

B、汇聚协议

汇聚协议是专业或专有协议和标准协议的融合。汇聚协议的主要好处是使用现有 TCP/IP 网络基础设施支持特殊或专有主机而无需特殊部署修改后的网络硬件，这能有效地节约成本。以下是汇聚协议的一些例子：

- 光纤通道以太网（FCoE）这是一个协议的封装，允许光纤通道帧（FC）通过以太网网络。
- 多协议标签交换（MPLS）经常用于其在多种 2 层协议建立 VPN 的能力。MPLS 被认为是一个汇聚协议，因为它可以封装任何更高层次的协议和隧道在各种链接。
- 互联网小型计算机系统接口（iSCSI） iSCSI 在 TCP 数据报文中封装 SCSI 数据。

C、SDN 和 CDN

软件定义网络(SDN)是一种独特的对网络进行操作、设计和管理的方法。旨在把控制层(即网络服务的数据传输管理)和基础设施层(即硬件和基于硬件的设置)分离。

内容分发网络(CDN)或内容转发网络，是资源服务的集合，被部署在互联网的许多数据中心以提供低延迟、高性能和所承载内容的高可用性。CDN 通过分布式数据主机提供客户所需的多媒体性能质量，而不是将媒体内容存储在单一位置的单一主机上，并向互联网的

其他地方进行内容分发。

1.4 网络架构和协议常见攻击

A、拒绝服务类

拒绝服务攻击是一种资源消耗型攻击，它以阻止受害系统的合法活动为主要目标。下面有两种基本的拒绝服务：

利用硬件或软件的一个漏洞进行攻击。例如死亡 Ping 攻击，这一攻击利用了一个漏洞，即许多早期的网络堆栈并没有强制执行 ICMP 包的最大长度，即 65,536 个字节。如果攻击者发送的回波请求大于最大长度，那么许多常见操作系统将变得不稳定，最终会冻结或崩溃。

通过巨量的垃圾网络流量以泛洪方式淹没受害者的通信管道。例如 SYN flood 攻击，如果攻击者向目标系统发送一个带欺骗地址的 SYN 数据包，受害系统发送一个 SYN/ACK 数据包来应答这个欺骗地址。每次受害系统接收一个这样的 SYN 数据包，它就留出一部分资源来管理这个新连接。如果攻击者发送大量 SYN 数据包给受害系统，最终导致该受害系统把它所有可用的 TCP 连接资源都分配殆尽，而不再能够处理新的请求。

B、中间人类

网络窃取或嗅探是对数据机密性的攻击，通过观察、监听、分析数据流和数据流模式，窃取敏感信息。

TCP 会话劫持（TCP session hijacking）。两个系统在 TCP 握手过程中约定的一个值是将要插入到数据包首部的序列号。一旦约定好这个序列号，如果接收系统接收的数据包中不带有预先约定好的这个值，它会忽视这个数据包。如果攻击者能正确预测两个系统将要使用的 TCP 序列号，然后她可以创建包含那些号码的数据包，欺骗接收系统，使之认为这些数据包来自授权的发送系统。然后她能够接管两个系统之间的 TCP 连接。

DNS 劫持是一种迫使受害者使用恶意 DNS 服务器而不是合法的 DNS 服务器的攻击。其中的技术很简单，可有以下三种分类：

- 基于主机。攻击者只要将受害者的电脑的 IP 设置变到流氓 DNS 服务器上即可。显然，这需要目标终端的物理或逻辑访问通道，并且通常需要管理员权限。
- 基于网络。攻击者在网络中，但不在客户机或 DNS 服务器中。攻击者能利用一种技术，如 ARP 列表缓存，将 DNS 通信重新定向到他自己的服务器上。
- 基于服务器。如果合法的 DNS 服务器配置不合理，攻击者可以分辨出这一服务器，并在他想劫持的任何域名中使自己的服务器成为授权服务器。然后，每当一

个合法服务器收到一个对劫持域名的请求，它会自动将它转发给流氓服务器。

最常见的 DNS 威胁有 DNS 欺骗、DNS 投毒。DNS 投毒和 DNS 欺骗也被称为分辨攻击。当攻击者修改在 DNS 系统中域名到 IP 地址的映射以便将流量重定向到一个假冒系统或简单地执行拒绝服务时就发生 DNS 投毒。当攻击者击败从有效的 DNS 服务器回复真正的答复并发送虚假答复给询问系统则发生 DNS 欺骗。

偷听是为了复制目的而对通信信息进行简单的侦听。将数据记录到存储设备中，或者将数据记录到尝试动态从通信流中提取出原始内容的提取程序。

假冒或伪装是指假装成某人或某事，从而获得对系统的未授权访问。这通常意味着认证证书被窃取或遭受篡改以满足(即成功地绕过)认证机制。这不同于欺骗，欺骗是提出了一个虚假的身份但没有任何证据(如错误地使用 IP 地址、MAC 地址、电子邮件地址、系统名称、域名等)。假冒往往可以通过捕获网络服务会话设置中的用户名和密码加以实现。

重放攻击是假冒攻击的分支，它可以利用通过偷听捕获的网络通信进行攻击。重放攻击企图通过对系统重放被捕获的通信来重建通信会话。一般可以使用一次性身份验证机制和序列化会话身份标识来防范重放攻击。

ARP 表中毒（ARP table poisoning），攻击者会修改系统的 ARP 表，使之包含错误的信息。ARP 欺骗，攻击者为请求的 IP 地址系统提供假的 MAC 地址，从而将通信重定向至另一个目的地。为关键系统定义静态的 ARP 映射，监控 ARP 缓存中的 MAC-IP 地址映射，或者使用 IDS 检查系统通信中的异常以及 ARP 通信中的变化，是有效的防御措施。

与 ARP 相关联的另一种攻击是超链接欺骗。这种类似于 DNS 欺骗的攻击用于将通信重定向至欺诈系统或冒名系统，或者简单地将通信发送至预定目的地之外的任何地方。超链接欺骗既可以来用 DNS 欺骗的形式，也可以只是简单地在发送给客户端的文档的 HTML 代码中修改超链接 URL。因为大多数用户并不通过 DNS 验证 URL 中的域名，而是认定超链接是合法的并进行单击，所以超链接欺骗攻击往往都会成功。

网络钓鱼是另一种经常使用超链接欺骗的攻击。网络钓鱼意味着诱骗他人上钩，从而获得信息。这种攻击可以采用很多形式，包括使用伪造的 URL。对链接欺骗的防护包括防止 DNS 欺骗、保持系统更新补丁并在使用互联网时采取同样谨慎的预防措施。

单元 2：网络组件安全

2.1 网络设备安全

A、组网类设备

中继器工作在物理层，它是将网络连接扩展到更长距离的附加设备。中继器提供最简单类型的连通性，因为它只是中继和放大线缆段之间的电信号，从而扩展一个网络。集线

器（hub）是一种多端口的中断器。集线器常常被认为是一个集中器（concentrator），因为它是允许多个计算机和设备互相通信的物理通信设备。

网桥（bridge）是一种用于连接不同 LAN 网段的 LAN 设备。它工作在数据链路层，因此处理的是 MAC 地址。

交换机实际上组合了中继器和网桥的功能。交换机是一种多端口的桥接设备，并且每个端口都为与之相连的设备提供了专门的带宽。第 2 层、第 3 层和第 4 层交换机之间的根本区别在于设备进行查看以作出转发或路由决策的首部信息（数据链路层、网络层或传输层）。

路由器是第 3 层（即网络层）设备，用于连接相似或不同的网络。路由器是一种有两个或更多接口与一个路由表的设备，因此它知道如何将数据包送到目的地。它能基于访问控制列表（ACL）过滤流量，在必要时将数据包分片。虫洞攻击是指攻击者能够在网络中的某个位置捕获数据包，并将其通过隧道传送到另一个位置。在这种攻击中，隧道（称为虫洞）两端分别有一名攻击者。

网关（gateway）是一个通用的术语，它用于在连接两个不同环境的设备上运行的软件，很多时候充当了这些环境的翻译器，或者在某种程度上限制了它们的交互。

专用交换分机（Private Branch Exchange，PBX）是用户公司所有的专用电话交换机，这个交换机执行的交换任务与电话公司交换中心执行的某些任务相同。PBX 具有到本地电话公司交换中心的专门连接，交换中心能够执行更智能的交换。

B、访问控制类设备

网络访问控制(NAC)指通过严格遵守和实施安全策略来控制对环境的访问。NAC 的目标如下：

- 防止减少零日攻击
- 在整个网络中实施安全策略
- 使用标识执行访问控制

NAC 的目标可通过使用强大、详细的安全策略来实现。这些策略定义了从客户端到服务器以及每个内部或外部通信的每个设备的安全控制、过滤、预防、检测和响应的所有方面。NAC 充当自动检测和响应系统，可实时做出反应，并在威胁发生或造成损害或破坏之前阻止威胁。

防火墙用于限制从另一个网络对特定网络的访问。防火墙包括以下几种类型：

包过滤防火墙。是一种基于网络级协议首部值作出访问决策的防火墙技术。执行包过滤进程的设备被配置上 ACL。控制着可以流进和流出特定网络的流量类型。包过滤是第一代防火墙，是所有防火墙技术中最基本的类型。包过滤也叫做无状态检查，因为这个设备不了解这些数据包工作的环境。

状态检测防火墙。状态检测防火墙维护一个状态表，以记录谁对谁发送了什么。当两个系统之间的连接开始时，防火墙调查数据包的所有层（包括：所有首部、有效荷载和尾部）。有关这个具体连接的所有必要信息都存储在状态表中（这些信息包括：源 IP 地址和目的地 IP 地址、源端口和目的端口、协议类型、首部标志、序列号和时间戳等）。一旦这个数据包通过了这个深入的检查，一切都被认为是安全的，然后防火墙会审核网络，为剩下的会话传输首部部分。每一个数据包的每个首部值都会与当前状态表中的值作对比，这个表被更新以反映通信进程的进展情况。把检查整个数据包缩减为只检查每个数据包的首部可以提高性能。

代理防火墙。代理是一个中间人的机制。在将信息递交给目标接收者之前，代理会对其进行拦截和检查。代理防火墙接受流进或流出网络的消息，检查可疑的信息，只在认为没有问题时才将数据传递至目标计算机。工作在 OSI 模型底层的代理防火墙叫做电路级代理，工作在应用层的代理防火墙叫应用级代理。SOCKS 是电路级代理网关的一个示例，它在两台计算机之间提供一个安全通道。应用级代理防火墙有如下的特征：每个被监控的协议都需要一个独特的代理；比电路级代理防火墙提供更多的保护；由于对每个包都要进行更多处理，速度比电路级代理防火墙慢。

动态包过滤防火墙。动态包过滤防火墙的优点是允许你选择任何类型的流量流出，并且只允许响应流量流入。

内核代理防火墙。内核代理防火墙被认为是第五代防火墙。与先前讨论的所有防火墙技术不同，一旦需要评估数据包，这种防火墙会建立动态的、定制的网络栈。当一个包到达内核代理防火墙时，防火墙就会针对该包创建一个新的虚拟网络栈，并只加载必要的协议代理。如果这是一个 FTP 包，那么虚拟网络栈就只加载 FTP 代理。数据包在栈的每一层都会被仔细审查。这意味着数据链路层首部、网络层首部、传输层首部、会话层信息以及应用层数据都要评估。如果在任何层发现认为不安全的信息，那么该数据包就会被丢弃。因为所有的检查和处理都在内核进行，而不需要向上传递至操作系统中的较高软件层，所以内核代理防火墙比应用级代理防火墙要快。

下一代防火墙。下一代防火墙（NGFW）结合前面讨论的防火墙最好的属性，但增加了一些重要的改进。最重要的是，它采用了基于特征的 IPS 引擎。这意味着，除了要确保传输行为按照适用的协议规则，防火墙可以在传输中寻找攻击的具体指标方面有好的表现。

虚拟防火墙。虚拟防火墙提供桥梁功能，虚拟机之间的每个流量链路都得到监控，或者它们可以集成在管理程序中。

防火墙的架构主要有 3 种：

双宿防火墙。双宿指的是一个设备具有两个接口，一个面向外部网络，另一个则面向内部网络。

被屏蔽主机（防火墙）。被屏蔽主机是一种直接与边缘路由器和内部网络通信的防火墙。来自互联网的流量首先通过外部路由器上的包过滤功能进行过滤。通过这一步的流量

发送至屏蔽主机防火墙，该防火墙对流量应用更多的规则，并丢弃拒绝的包。随后，流量移动至内部的目标主机。

被屏蔽子网（防火墙）。被屏蔽子网架构在被屏蔽主机架构的基础上又添加了一层安全性。外部的防火墙对进入 DMZ 网络的数据进行屏蔽。然而，内部路由器还可以过滤流量，而不是由防火墙将流量重定向至内部网络。这两个物理防火墙的使用就创建了一个 DMZ。在这种多层保护安全的情况下，提供的层次越多，保护就越强。

2.2 网络组网安全

A、网络拓扑

网络拓扑指的是物理连接网络以及表示资源和系统布局的方法。物理的网络拓扑与逻辑的网络拓扑之间存在差异。网络可以配置成物理上星型，但是在逻辑上以环型工作，如令牌环技术。常见的拓扑有：

- 环型拓扑（ring topology）,通过单向传输链路连接一系列设备
- 总线型拓扑（bus topology）,一根线缆跨越整个网络。节点通过这根线缆的引出点连在网络上。数据通信传遍整个介质，并且所有节点都将"查看"每个传送过来的数据包。随后，根据数据包的目标地址，每个节点会决定接受或忽略该数据包
- 星型拓扑（star topology），所有的节点连接到一台集中式设备（如交换机）。每个节点到集中式设备都有一条专用链路
- 网状型拓扑（mesh topology），所有系统和资源相互直连

B、传输介质

同轴电缆,具有由一层绝缘层包围的铜线芯，该绝缘层又由导电编织屏蔽层包围并封装在最终绝缘护套中。中心的铜芯和编织屏蔽层是两个独立的导体，因此允许通过同轴电缆进行双向通信。

双绞线与同轴电缆相比，双绞线布线非常轻便灵活。它由四对彼此缠绕在一起的电线组成，然后套在 PVC 绝缘体中。如果外部护套下面的导线周围有金属箔包装，则该导线称为屏蔽双绞线(STP)，该箔片提供额外的外部电磁干扰保护。没有箔的双绞线被称为非屏蔽双绞线(UTP)。

光缆。光缆由光源、光纤电缆和光探测器构成。因为使用玻璃，所以光纤具有更高的传输速率，并且允许将信号传送更远的距离。

C、局域网技术

以太网通过下列特征进行定义：

- 竞争型技术（所有设备都使用同样的共享通信介质）
- 使用广播和冲突域
- 使用带冲突检测的载波监听多路访问（CSMA/CD）方法
- 支持全双工通信
- 能使用同轴电缆、双绞线或光纤电缆介质

以上特征在标准 IEEE 802.3 中有相关定义描述。

无论用到什么类型的介质访问技术，网络传输通道是该网络上所有系统和设备所必须共享的主要资源。这个传输通道可以是同轴电缆上的令牌环、UTP 上的以太网、光纤上的 FDDI 或者无线电波上的 Wi-Fi。必须采取一定的方法，确保每个系统都可以访问这个通道，该系统的数据在传输过程中不被破坏以及在尖峰时刻能够控制流量。无论用到什么类型的介质访问技术，网络传输通道是该网络上所有系统和设备所必须共享的主要资源，常见的介质共享技术有：

以太网 CSMA，作为访问网络线缆的方法存在两种不同类型的 CSMA：CSMA/CD 和 CSMA/CA。

令牌环（Token Ring）技术，由 IEEE 802.5 标准所定义，是支持通信和网络资源共享的 LAN 媒介访问技术。它在星型配置的拓扑中采用令牌传递技术。名称中的"环"部分指明信号在逻辑环中传送。每台计算机都连接到称为多站访问单元（MAU）的集中式集线器。这种拓扑结构在物理上是星型的，但是信号和传输数据在逻辑环中传递。

光纤分布式数据接口（FDDI）技术由美国国家标准协会（ANSI）提出，它是一种高速的令牌传递介质访问技术。FDDI 拥有最高为 100Mbps 的数据传输速率，通常使用光纤电缆作为主干网络。FDDI 还通过第二个反向旋转光纤环路来提供默认容错。

如果数据包需要从源计算机到达一个特定的系统，那么会使用单播（unicast）传输方法。如果数据包需要到达一组特定的系统，那么发送系统会使用多播（multicast）方法。如果系统想让其子网上的所有计算机都能接收到消息，那么会使用广播（broadcast）方法。

网络地址转换（NAT）是位于一个网络和互联网（或另一个网络）之间的网关，执行透明的路由选择和地址转换。 NAT 实现的 3 种基本类型：静态映射、动态映射、端口地址转换（PAT）。

D、城域网和广域网技术

城域网（MAN）通常是一个主干网，用于将 LAN 连接到 LAN，将 LAN 连接到 WAN、互联

网和其他电信电缆网。

广域网（WAN）技术则在通信需要跨越一个更大的地域范围时使用。当一个网络上的计算机想同位于国家另一端或另一个国家的计算机通信时，就需要使用 WAN 技术。

常见的城域网和广域网技术：专用线路、帧中继、X.25、ATM、SDLC

E、无线网络技术

无线通信是指通过无线电波经由空气和空间传输信号，它也会改变空气波。这些信号可以以多种方式描述，但是通常以频率和幅度来描述。信号的频率规定所传送数据的数量与距离。频率越高，信号运载的数据越多。但是，频率越高，信号也越容易受到大气层干扰。虽然更高的频率能够运载更多的数据，但是能够传输的距离却更短。人们已开发出大量技术，以允许无线设备访问和共享有限的通信介质。主要使用的基本扩频技术有：跳频和直接序列，对于这两个技术的细节，就 CISSP 考试来说，就不用详细了解了。

无线 LAN(WLAN)使用一个称为访问点(AP)的收发器连接到以太网线缆，无线设备会使用这条链路来访问有线网络中的资源。无线网络也是被匆忙地推向了市场，它们更专注于功能，甚至是以牺牲安全性为代价的。

802.11 系列标准概括说明无线客户端和 AP 如何进行通信，列出接口的规范，规定信号的传输方式，并描述应当如何实现身份验证、合作和安全。现在有一长串的标准实际上都划归在 802.11 主标准之内。你可能看到过这个字母系列（例如 802.11a、802.11b、802.11i、802.11g、802.11h 等），字母后缀表示这些标准提出和采用的顺序，对于每个标准都有一个研究小组，每个小组都有各自的研究重点，并要求为其负责的领域研究和开发标准。IEEE 802.11i（或者称 Wi-Fi protected Access II（WPA2））的标准，应对 802.11 标准所带有的安全问题。

有线等效加密（WEP）协议，它也能对数据传输进行加密。WEP 的 3 个主要缺陷是应用静态加密密钥、初始化向量使用效率低以及缺乏数据包完整性保证。

WPA 标准使用不同的方法，从而可以比原始 802.11 标准所使用的方法提供多得多的安全和保护。这种安全提升通过特定协议、技术和算法来实现。第一个协议称为暂时密钥完整性协议(Temporal Key Integrity Protocol，TKIP)，它基于原始 802.11 标准，向后兼容 WLAN 设备。TKIP 实际上与 WEP 一起工作，向其输入密钥材料，这些材料用来生成新的动态密钥。这个新标准同样包括 802.1x 端口身份验证和 EAP 身份验证方法。802.1X 标准是一个基于端口的网络访问控制，它确保用户只有通过正确的身份验证后才能建立一个完整的网络连接。

相较于 WPA，完整的 802.11i (WPA2)有一个很大的优势,它可以提供使用 AES 算法与 CBC-MAC 计数器模式(CCM) 的加密保护,这被称为计数器模式密码块链接信息认证码协议(CCM 协议或 CCMP)。

蓝牙无线技术是 802.15 标准的一部分。蓝牙劫持（Bluejacking）是使用蓝牙技术的设备容易遭到的一种攻击。Bluesnarfing 是指通过蓝牙连接未授权地访问无线设备。

单元 3：网络信道安全

3.1 网络安全机制

A、身份验证协议

当远程系统与服务器或网络建立初始连接后，第一步工作应是验证远端用户的身份，该工作称为身份验证。如下几种身份验证协议用于控制登录证书的交换和确定在传输过程中这些证书是否需要加密：

PAP（密码身份验证协议）是一种服务于 PPP 的标准化身份验证协议。PAP 使用明文传输用户名与密码。它不提供任何形式的加密，只提供简单的传输途径，把登录证书从客户端传递到身份验证服务器。

CHAP（征询握手身份验证协议）是一种应用于点对点协议(PPP)连接上的身份验证协议。CHAP 加密用户名与密码。采用无法重放的挑战--应答对话进行验证。CHAP 在已建立的完整通信会话期间，周期性地重复验证远程系统，以确保远程用户身份持续有效。这个过程对于用户是透明的。

EAP（可扩展身份验证协议）是一种身份验证框架而不是真实协议。EAP 支持可定制的身份验证安全解决方案，如智能卡、令牌和生物身份验证。

上述三个身份验证协议最初都应用于拨号 PPP 连接中。现在，它们与许多新验证协议（如 OpenID、OAuth）及概念（如身份验证联合及 SAML）一起，都应用于大量的远程连接技术中，如宽带及 VPN，同时扩展了对传统身份验证服务（如 Kerberos、RADIUS 及 TACACS+）的支持与使用。

B、透明、机密性和完整性、日志审计

“透明性”控制，顾名思义，为确保控制对用户不可见，是服务、安全控制或是访问机制的一个特征。安全机制越透明，用户就不可能绕过它，甚至察觉不到它的存在。如果具备了透明性，也就察觉不到功能、服务或限制的存在，对于性能的影响也降至最低。

机密性和完整性机制，为验证传输的机密性，可采用对称、非对称的加密技术；为验证传输的完整性，可采用称为 hash 值的校验和技术

传输日志是一种专注于通信的审计技术。传输日志记录源地址、目的地址、时间戳、识别码、传输状态、报文数量、消息大小等详细信息。这些信息对于故障定位、追踪非法

通信，或提取系统工作的数据，都是十分有用的。

3.2 语音、多媒体、邮件等信道安全

A、语音信道安全

拨号连接。由于几乎每个家庭和办公室都已经提前安装了电话线，因此第一个远程连接技术便是充分利用这种既有的基础设施。给计算机配备上调制解调器，它便可以通过电信线路与其他计算机通信了。

战争拨号。攻击者使用执行自动拨号程序来标识能被破坏的调制解调器。他们向拨号工具中输入大量电话号码，然后该拨号工具便给每个电话号码打电话。如果有人接听电话，战争拨号工具便记录下该号码没有与计算机系统相连的情况，并把它从列表中删除。如果接通的是传真机，也这样处理。如果接通的是调制解调器，那么战争拨号工具会发送信号并试图在攻击者的系统和目标系统之间建立一个连接。如果成功建立连接的话，攻击者便可以直接访问该网络了。

有线电视公司为家庭提供电视服务已有多年，当前它们也开始为拥有线缆调制解调器并希望高速连接到互联网的用户提供数据传输服务。线缆调制解调器提供最高为 50Mbps 的高速访问，通过现有的同轴电缆或光纤访问互联网。线缆调制解调器还提供了上行和下行之间的转换。

综合业务数字网（Integrated Services Digital Network，ISDN）是一种由电话公司和 ISP 提供的技术。这种技术和必需的设备使数据、语音和其他类型的流量在介质中以数字的形式传输，而这种介质以前只用于模拟语音传输。

数字用户线路（DSL）是另一种高速连接技术，用于连接家庭（或公司）和服务提供商的交换中心。它能提供比 ISDN 和模拟技术高 6~30 倍的带宽。DSL 使用现有的电话线路，并且提供到互联网的 24 小时连接。有许多不同类型的 DSL，它们分别具有各自的特点与具体用途：

- 对称 DSL(SDSL)　数据以相同的速率上行和下行。
- 非对称 DSL(ADSL)　数据下行的速度比上行的速度更快。
- 高位率 DSL(HDSL)　在不使用中继器的情况下，可在常规铜电话线上提供 T1(1.544Mbps)的速度。
- 高数据率数字用户线路(VDSL) 基本上是数据传输速率高的 ADSL(下行速度 13 Mbps，上行速度 2Mbps)。
- 速率自适应数字用户线(RADSL)　速率自适应的功能使其能够根据线路质量和长度来调节传输速度。

一种语音通信威胁是专用交换机（PBX）欺骗与滥用。许多 PBX 系统受到恶意攻击，攻

击目的是想逃避电话费用或隐藏身份。称为“电话飞客”(phreaker)的恶意攻击者，采用与攻击计算机网络的相似手段，攻击电话系统。电话飞客可能会非法访问个人的语音信箱、重定向消息、阻塞访问以及重定向呼入与呼出电话。

VoIP（网络电话）是一种将语音封装在 IP 包中的技术，该技术支持在 TCP/IP 网络中打电话。在世界范围内，VoIP 已经成为公司及个人大众化的、廉价的电话解决方案。

SIP 是一项类似于 HTTP 的基于文本的网络传输协议，VOIP 通讯产品都采用 SIP 协议作为传输语音数据包的协议。IETF 建议使用现有的网络协议安全机制来保证 SIP 的安全运行，如 HTTP 摘要认证机制、S/MIME 机制、TLS 机制、IPsec 机制等。

黑客可采用多种技术方法来攻击 VoIP：

- 由于使用任何一种 VoIP 工具，都可以轻松伪造来电号码显示，所以黑客能够进行语音钓鱼（VoIP 钓鱼）或垃圾网络电话（SPIT）攻击。
- 呼叫管理系统及 VoIP 电话本身也易受宿主操作系统攻击及 DoS 攻击。如果设备、软件运行的主机操作系统或固件存在脆弱性，就会增加被攻击的风险。
- 通过欺骗呼叫管理器、终端连接协商过程和或响应，攻击者能执行中间人(MitM)攻击。
- 由于 VoIP 是网络流量，所以在未加密的情况下，通过窃听 VoIP 通信就可以解码 VoIP 流量内容。

SRTP（安全实时传输协议，也称为安全 RTP）是 RTP(实时传输协议)的安全改进版本，也应用于很多 VoIP 通信中。SRTP 的目的是通过健壮的加密及可靠的身份验证，尽可能降低 VoIP 遭受 DoS 攻击的风险。

B、数据信道安全

简单邮件传输协议（SMTP）作为消息传输代理来工作，将消息从用户的计算机发送到邮件服务器上。SMTP 同另外两个邮件服务器协议（POP 和 IMAP）紧密合作。

邮件服务器使用一个中继代理机制，实现从一个邮件服务器发送消息到另一个邮件服务器。中继代理机制必须正确配置，才能确保公司的邮件服务器不被恶毒团体所利用进行垃圾邮件活动。

电子邮件伪装是通过修改电子邮件头部字段来完成的，例如 From（来源）、Return-Path（回复路径）和 Reply-To（回复到）字段。SMTP 认证（SMTP authentication，SMTP-AUTH）用来在邮件传输协议中提供一个访问控制机制。

安全 MIME（S/MIME）是一种对电子邮件进行加密和数字签名以及提供安全数据传输的标准。

可靠加密（PGP）作为一种免费电子邮件保护程序而设计，它是第一个广泛使用的公钥加密程序。PGP 主要使用 RSA 公钥加密来实现密钥管理，通过使用 IDEA 加密算法来提供机

密’性，通过使用：MD5 散列算法来提供完整性，通过使用公钥证书来提供身份验证，以及通过对消息进行加密签名来提供不可否认性。PGP 使用自己的数字证书类型，而不是 PKI 中使用的数字证书类型，不过两者的目的相似。

安全套接字层（SSL）使用公钥加密，并且提供数据加密、服务器身份验证、消息完整性以及可选客户端身份验证。SSL 的开放社区版本是传输层安全（TLS）。

HTTP 安全（HTTPS）在 SSL 运行的 HTTP（HTTP 在应用层上运行，而 SSL 在传输层上运行）。

Cookie 是浏览器保存在用户硬盘上的文本文件。一些 Cookie 以文本文件的形式存储在硬盘上。这些文件应当不能包含任何敏感信息，如账号和口令。

安全外壳（SSH）在功能上类似于一种隧道机制，它为远程计算机提供终端式访问。SSH 是一种能够用于通过网络访问另一台计算机的程序。

3.3 远程访问和虚拟专用网

A、远程访问概述

远程办公或远程工作，已经成为商业计算中的常态。远程办公通常需要远程访问，也就是远程客户与网络建立起通信会话的能力。远程访问可能采取下列一些形式：

- 使用调制解调器直接拨入远程访问服务器。
- 在互联网上通过 VPN 接入网络。
- 通过瘦客户端连接接入终端服务器系统。
- 使用远程桌面服务， 如 Microsoft 的 Remote Desktop、TeamViewer. GoToMyPC、Citirx 的 XenDesktop 或 VNC,接入位于办公区的个人电脑。
- 使用基于云的桌面解决方案，例如亚马逊的 Workspace。

在规划远程访问的安全策略时，一定要解决下列问题：

- 远程连接技术每种连接都有其独特的安全问题，对于所选择连接的各个方面要进行全面检查。可能的连接包括蜂窝/移动通信、调制解调器、数字用户线路(DSL)、综合业务数字网(ISDN)、无线网络、卫星通信以及有线调制解调器。
- 传输保护有几种形式的加密协议、加密连接系统以及加密网络服务或应用。根据远程连接的需要选择合适的安全服务，可供选择的包括 VPN、SSL、 TLS、 SSH、IPsec 以及第二层隧道协议(L2TP)。
- 身份验证保护除了要保护数据流量，还要确保所有登录凭据的安全。需要采用身份验证协议以及必要的中心化远程访问身份验证系统。这可能包括密码身份验证协议(PAP)、 征询握手身份验证协议(CHAP)、 可扩展身份验证协议(EAP，或其扩展 PEAP 或 LEAP)、远程身份验证拨入用户服务(RADIUS)以及终端访问控制器访问

控制系统+（TACACS+）。

- 远程用户助手远程访问用户有时可能需要技术上的协助，所以必须提供尽可能有效的获得协助的方法。

B、虚拟专用网（VPN）

虚拟专用网（VPN）是公共网络或其他不安全环境中的安全专用连接。因为采用加密和隧道协议来确保数据在传输中的机密性与完整性，所以它是专用的连接。必须记住的是，VPN 技术需要隧道才能运作，同时还会进行加密。

点对点隧道协议（PPTP）最初目的是提供一个用 IP 网络隧道连接 PPP 的方法。使用通用路由封装（GRE）和 TCP 来封装 PPP 数据包，并通过 IP 网络延伸 PPP 连接。在 Microsoft 的实现中，隧道传输的 PPP 流量可以用 PAP、CHAP、MS-CHAP 或者 EAP-TLS 进行身份验证，PPP 有效载荷用 Microsoft 的点对点加密（MMPPE）进行加密。

后来开发的另外一个 VPN 解决方案把 PPTP 和 Cisco 的第二层转发（L2F）协议的功能结合在一起。第二层隧道协议（L2TP）用各种网络类型（IP、ATM、X.25 等）来隧道传输 PPP 流量；这样一来，不像 PPTP 那样只限于 IP 网络。PPTP 和 L2TP 的侧重点非常相似，那就是使 PPP 流量到达一个与不理解 PPP 的网络相连接的终点。和 PPTP 一样，L2TP 实际在 PPP 流量的传输过程中并不提供太多保护，只是它和提供安全功能的协议集成在一起。L2TP 继承了 PPP 的身份验证并整合 IPSec 以提供机密性、完整性，以及可能提供另外一层身份验证。

IPSec 是为专门保护 IP 流量而开发的一套协议。IPv4 没有集成任何安全，所以开发了 IPSec 来“拴住”IP 和保护协议传输的数据的安全。PPTP 和 L2TP 工作在 OSI 模型的数据链路层，IPSec 工作在网络层。IPSec 包含的主要协议及其基本功能如下：

- 身份验证首部（AH） 提供数据完整性、数据源验证和免受重放攻击的保护。
- 封装安全有效载荷（ESP） 提供机密性、数据源验证和数据完整性。
- 互联网安全连接和密钥管理协议（ISAKMP） 提供安全连接创建和密钥交换的框架。
- 互联网密钥交换（IKE） 提供验证的密钥材料以和 ISAKMP 一起使用。

TLS VPN 的最常见实现类型有两种：

第一种：TLS 门户 VPN。个体用一个标准 TLS 连接到网站上来安全地访问多个网络服务。被访问的网站一般叫做门户，因为它通过一个地点提供对其他资源的访问。远程用户使用 Web 浏览器访问 TLS VPN 网络，进行身份验证后，会呈现一个网页，作为访问其他资源的门户。

第二种：TLS 隧道 VPN。个体用 Web 浏览器通过一个 TLS 隧道来安全地访问多个网络服务，包括不是 Web 型的应用程序和协议。这通常需要进行个性化编程，从而允许服务通过

Web 型连接被访问。

我们从每个协议的特点、工作机制和工作方式，来总结一下这些隧道协议：

- 点对点隧道协议（PPTP）：工作在客户端/服务器模型中；延伸和保护了 PPP 的连接；在数据链路层上工作；只能通过 IP 网络传输
- 第二层隧道协议（L2TP）：是 L2F 和 PPTP 的混合；延伸和保护了 PPP 的连接；在数据链路层上工作；能在多种网络中传输而不仅仅是 IP 网络；为了提高安全还可以和 IPSec 相结合
- IPSec 协议：能同时处理多个 VPN 连接；能够提供安全的身份验证和加密；关注 LAN 网络间通信而非用户之间的通信；在网络层上工作，实现 IP 安全，但只支持 IP 网络
- 传输层安全（TLS）：在传输层工作，主要保护 Web 和 e-mail 流量；提供细粒化的访问控制和配置；由于 TLS 已经嵌入 Web 浏览器中，所以容易部署；仅仅能保护少数协议类型，因此不是基础设施级别的 VPN 解决方案

VPN 解决方案各有千秋，各有侧重点，例如：

- 当一个 PPP 连接需要通过 IP 网络延伸时则使用 PPTP
- 当一个 PPP 连接需要通过非 IP 网络延伸时则使用 L2TP
- IPSec 用于保护 IP 流量，常用于网关之间的连接。
- 当特定的应用层流量类型需要保护时则使用 SSL VPN

链路加密有时也称为在线加密，它通常由服务提供商提供，并且集成入网络协议。所有的信息都被加密，数据包在每一跳中都必须进行解密，这样路由器或其他中间设备才能知道数据包的下一个发送地点。路由器必须解密数据包的头部，读取头部内的路由和地址信息，然后重新加密并继续向前发送。

在端到端加密中，因为数据包的头部和尾部没有进行加密，所以数据包不需要解密，也不需要在每一跳中重新加密。起点和终点之间的设备只是读取所需的路由信息，然后将数据包向前继续发送。

D5：身份与访问管理

单元 1：身份与访问控制概述

1.1 基本概念

A、相关定义

主体是活动实体，它访问被动客体以及从客体接收信息或关于客体的数据。主体可以是用户、程序、进程、服务、计算机或可访问资源的任何其他内容。授权后，主体可修改客体。客体是一个被动实体，它向活动主体提供信息。文件、数据库、计算机、程序、进程、服务、打印机和存储介质等都是客体。

访问是在主体和客体之间进行的信息流动。访问控制给予组织机构控制、限制、监控以及保护资源可用性、完整性和机密性的能力。访问控制包含的范围很广，它涵盖了几种对计算机系统、网络和信息资源进行访问控制的不同机制，它也是防范计算机系统和资源被未授权访问的第一道防线

实施访问控制的目标和原则是什么？访问控制中 3 个主要的安全目标和原则，就是：可用性、完整性和机密性，这三个目标和原则其实也是安全的目标和原则。在访问控制中：

- 可用性指的是信息、系统和资源必须在时间上能够保证用户使用，这样才不会影响其工作效率。
- 完整性指的是信息必须是准确、完整的，并且不会受到未授权的更改。某种安全机制在提供完整性时，会保护数据或资源免受未授权的修改。
- 机密性指的是机密性能够保证信息不会泄露给未授权的个人、程序或进程。

访问控制由 3 个大的类别组成，分别是行政管理性控制、技术性控制和物理性控制。其中：

- 行政管理性控制包括： 策略和措施、人员控制、监管结构、安全意识培训和测试；
- 技术性控制包括：系统访问、网络架构、网络访问、加密和协议、和审计
- 物理性控制包括：网络分段、周边安全、计算机控制、工作区分隔、数据备份、布线和控制区

B、四个要素

身份标识描述了一种能够确保主体（用户、程序或进程）就是其所声称实体的方法。通过使用用户名或账号就能够提供身份标识。

为了能够进行正确的身份验证，主体往往需要提供进一步的凭证，这些凭证可以是密码、密码短语、密钥、个人身份号码(PIN)、 生物特征或令牌。这两种凭证项将与先前为该主体存储的信息进行比较。如果这些凭证与存储的信息相匹配，那么主体就通过了身份验证。

一旦主体提供了其凭证并且被正确标识了身份，主体试图访问的系统就需要确定该主体是否具有执行请求的动作所需的权限和特权。系统会查看某种访问控制矩阵或比较安全标签，以便验证该主体是否确实能够访问请求的资源和执行试图完成的动作。如果系统确定主体可以访问特定的资源，就会为该主体授权。

主体在一个系统或区域内的动作应当可问责。确保可问责性的唯一方法是主体能够被唯一标识，并且主体的动作被记录在案。

竞态条件是指进程按错误的顺序针对某个共享资源执行其任务。在两个或多个进程使用一个共享资源（如一个变量内的数据）时，就有可能造成竞态条件。在软件中，如果身份验证和授权步骤分为两个功能，那么攻击者就可能利用竞态条件迫使授权步骤在身份验证步骤之前完成。

1.2 标识和认证

A、身份标识

身份标识是所有访问控制的起点，没有正确的身份标识，就无法确定如何进行适当的控制。一般用：用户名、用户 ID、账号、PIN 个人身份识别码、数字识别、身份徽章 badge 等来表示一个主体的身份。

身份标识组件要求向用户发布身份标识值时，应确保以下几点：

- 每个值应当是唯一的，便于用户问责
- 应当遵循一个标准的命名方案
- 身份标识值不得描述用户的职位或任务
- 身份标识值不得在用户之间共享

B、身份验证因素

一般来说，有 3 种基本的身份验证方法、类型或因素，包括：

- 第 1 种因素，“某人知道什么（根据知识进行身份验证）”
- 第 2 种因素，“某人拥有什么（根据所有权进行身份验证）”
- 第 3 种因素，“某人是什么（根据特征进行身份验证）”

多因素身份验证是使用两个或多个因素的任何身份验证。双因素身份验证需要两个不同的因素来提供身份验证。

除了三个主要的身份验证因素外，还有其他一些因素，例如：

- 你在什么地方。根据特定的计算机识别主体的位置，主要通过 IP 地址或者来电显示识别地理位置。
- 通过物理位置控制访问。迫使主体出现在特定位置，地理定位技术可根据 IP 地址识别用户位置，并由某些身份验证系统使用。
- 上下文感知身份验证。许多移动设备管理(MDM)系统使用上下文感知身份验证来识别移动设备用户。

C、密码

密码是系统身份验证机制最常用的方式之一。密码是一个受保护的字符串，通常用于对个人进行身份验证。密码就属于类型 1“某人知道什么”，这种形式。

对于使用密码来进行验证，我们必须注意密码管理。密码是目前最常使用的身份验证机制之一，因此强化密码以及对其进行适当的管理是非常重要的。

如果一个攻击者在寻找密码，那么他可以尝试下列一些不同的技术：

- 电子监控 通过侦听网络流量来捕获信息，特别是用户向身份验证服务器发送的密码。攻击者能够复制并在任何时候使用捕获的密码，这被称为重放攻击。
- 访问密码 文件通常在身份验证服务器上执行该操作。密码文件包含许多用户的密码，如果该文件被损坏，那么会导致很大的破坏性。密码文件应当采用访问控制机制和加密方式进行保护。
- 蛮力攻击 使用工具，通过组合许多可能的字符、数字和符号来循环反复地猜测密码。
- 字典攻击使用含有成千上万单词的字典文件与用户的密码进行比较,直至发现匹配的密码。
- 社会工程攻击者让某些用户误认为他获得访问特定资源的必要授权。
- 彩虹表攻击者使用一张表，其中包含已采用散列格式的所有可能密码。

针对这些密码管理的攻击，我们可以采用以下的方式：

- 密码检查器。某些组织使用执行字典和/或蛮力攻击以检测弱密码的工具对用户选择的密码进行测试，这有助于使整个系统环境不易受到用于窃取用户密码的字典攻击和蛮力攻击的影响。

- 密码散列与加密。利用某种散列算法（通常为 MD4 或 MD5）对密码进行散列，以确保密码不以明文形式发送。
- 密码存储，密码很少以明文形式存储。相反，系统将使用诸如 SHA 的散列算法来创建密码的散列。许多系统使用更复杂的散列函数，在对密码进行散列之前向密码添加位，这些额外的位被称为盐，盐有助于阻止彩虹表攻击。
- 密码生命期。 许多系统都支持管理员设置密码的使用期限，从而强制要求用户隔一段时间就修改密码。
- 限制登录次数、 管理员可以设置操作参数，允许一定次数的失败登录，否则用户的账号就被锁定，这也称为“限幅级别（clipping level）”。

我们还可以使用感知密码、密码短语和一次性密码来增加安全性。

感知密码是基于事实或观点的信息，用于验证个人的身份。用户登记注册时，需要根据自己的生活经历来回答几个问题。

密码短语是一个比密码长的字符串(因此称为“短语”)，某些情况下，密码短语在身份验证过程中能够取代密码。用户将密码短语输入某个应用程序，应用程序会将其转换为虚密码，从而使密码短语满足应用程序所要求的长度和格式。

一次性密码（OTP）也称为动态密码，它用于身份验证，并且只能使用一次。一次性密码生成的令牌一般具有两种类型：同步和异步。

D、智能卡和令牌

智能卡和硬件令牌都是类型 2 身份验证因素(或者你拥有什么)的示例。它们很少单独使用，但通常与另一个身份验证因素相结合，提供多因素身份验证。

存储卡能够保存用户的身份验证信息，因此用户只需要输入用户 ID 或 PIN 以及提交存储卡。如果用户输入的数据与存储卡上的数据匹配，那么用户就成功通过了身份验证。

因为智能卡本身包含微处理器和集成电路，所以智能卡具有处理信息的能力。存储卡并没有这类硬件，因此没有这种功能，它们能够实现的唯一功能是简单的存储。通常，智能卡分为两类：接触式和非接触式。

令牌设备或硬件令牌是用户可随身携带的密码生成设备。令牌有两种类型，即同步动态密码令牌和异步动态密码令牌。

智能卡攻击与存储卡相比，智能卡具有更强的防篡改性。由于其中包含敏感数据，攻击者通过操纵智能卡的一些环境组件(改变输入电压、时钟频率、温度波动)来引入这些“错误”。在向智能卡引入一个错误之后，攻击者会检查某个加密函数的结果，并查看没有出现错误时智能卡执行该函数得到的正确结果。分析这些不同的结果使得攻击者能够对加密过程进行反向工程，并有望获得加密密钥。这种攻击也称为故障生成(fault generation)攻击。旁路攻击是非入侵式攻击，并用于在不利用任何形式的缺陷或弱点的情

况下找出与组件运作方式相关的敏感信息。针对智能卡的差分功率分析(查看处理过程中的功率发射)、电磁分析(查看发射出的频率)和计时(完成特定过程所需的时间)都是旁路攻击的示例。

E、生物识别技术

生物测定学属于类型 3 的验证方式，即“你是什么”。生物测定学通过分析独特的属性或行为来确认某个人的身份，它是最有效且最准确的身份标识确认方法之一。

生物测定学一般分为两种不同的类型。第一种是生理性生物测定，它指的是某个人所特有的身体特征。指纹是生物测定学系统中常用的一种生理特征。第二种是行为性生物测定，它基于个人的某种行为特点来确认其身份，例如动态签名。生理性生物测定是“你是什么”，而行为性生物测定则是“你做什么”（相对“你是什么”又弱一些）。

生物测定学系统可扫描一个人的生理属性或行为特征，然后将其与早期特征记录过程中建立的记录进行比较。因为这个系统会检查一个人的指纹、视网膜模式或者声音音调，所以它必须极为灵敏。系统必须对这个人的生理或行为特点执行准确且可重复的测量。这种类型的灵敏度很容易导致误报（false positive）或漏报（false negative）。

生物测定学系统在拒绝一个已获授权的个人时，就会出现 1 类错误(误拒绝率(False Rejection Rate，FRR))；当系统接受了一个本应该被拒绝的冒名顶替者时，就会出现 2 类错误(误接受率(False Acceptance Rate，FAR))。当比较不同的生物测定学系统时，人们使用了不同的变量，但是其中最重要的度量是交叉错误率(Crossover Error Rate，CER)。这个等级是一个百分数，它代表误拒绝率与误接受率等值的那个点。在判定系统精确度的时候，交叉错误率是非常重要的评估指标。交叉错误率(CER)也称为相等错误率(Equal Error Rate，EER)。

常见的一些生物测定方法包括指纹、手掌扫描、手部外形、虹膜扫描、动态签名、动态击键、声纹、面部扫描、手形拓扑。

生物测定学也有自己的问题。它依赖于生物体所具有的唯一且独特的特征来进行身份验证，但是这些持征可能出现问题。生物体总是在不断变化之中，这意味着他们不会在每次登录时都能提供静态的生物测定学信息。处理速度在购买生物测定学系统时，系统对用户进行身份验证所花费的实际时间也是需要考虑的一个重要因素。

1.3 授权和可问责性

A、权限、权利和特权

在授权时，经常会遇到权限（permission）、权利（right）和特权（privilege）这

几个术语。有人会交叉使用这些术语，但它们并不总是表达相同的含义。

- 权限通常是指授予主体对客体的访问权限，并确定主体可对其执行的操作。
- 权利主要是指对某个客体采取行动的能力。
- 特权是权利和权限的组合。

B、授权机制和原则

尽管身份验证和授权完全不同，但是它们需要互相配合完成两步骤操作才能确认用户是有被允许访问特定的资源。第一个步骤是身份验证，用户必须向系统证明他就是自己声称的人，即被许可的系统用户。身份验证成功之后，系统必须确认用户已被授权访问特定资源以及被许可对该资源执行哪些操作。

网络管理员和安全专家在进行保护配置时希望能够对资源进行充分的控制，使他们对每一个用户都进行非常准确的控制。知其所需这个原则确保主体只能访问他们的工作任务和工作职能必须知道的内容。主体可获得访问分类或受限数据的许可，但未获得数据授权，除非他们确实需要它来执行工作。为了满足知其所需准则，可以对各种角色、组、位置、时间和事务处理类型实施不同的访问准则。

最小特权原则确保主体仅被授予执行其工作任务和工作职能所需的权限。这通常会和“知其所需”原则混淆。唯一的区别是最小特权还包括对系统采取行动的权利。

授权蠕动是这些原则执行中最大的一个问题。当雇员在一家公司长期工作时，他们会从一个部门调动到另一个部门，因此常常被赋予越来越多的访问权限和许可。对公司而言，这可能是一个重大的风险，因为太多用户拥有访问公司资产的过多权限。针对用户账户实施最小特权应当是一项持续的工作，这意味着应对每位用户的权限进行核查，以确保公司不会置身于风险当中。

职责分离原则确保将敏感职能分为两个或多个员工执行的任务。通过创建一个检查和制衡系统来防止欺诈和错误。

访问控制机制应当默认为拒绝访问，以实现必要的安全级别并确保没有被忽略的安全漏洞。当安全机制默认为拒绝访问时，就意味着如果没有为某个用户或其所属的组明确配置权限，那么用户就应当不能访问指定的资源。

C、可问责性

审计功能确保用户的动作可问责，验证安全策略已实施，并且能够用作调查工具。审计材料和日志文件包含了大量信息，而相应的关键点往往是以一种有益且易于理解的方式来解释和呈现这些信息。我们通过记录用户、系统和应用程序的活动来跟踪可问责性。通过操作系统或应用程序内的审计功能和机制完成这些记录。

审计跟踪包含与操作系统活动、应用程序事件和用户动作相关的信息。通过检查性能信息或某些类型的错误和条件，审计跟踪可用于验证系统的健康状态。系统崩溃后，网络管理员通常会检查审计日志，将系统状态信息拼凑起来，以试图了解是哪些事件造成了系统崩溃。

审计跟踪还可用于提供有关任何可疑活动的报警，从而方便之后的调查。此外，它们还可用于准确判断攻击的范围及其已造成的破坏程度。同样，审计还可用于维持一个正确的保管链，从而确保以后要将收集到的任何数据用于刑事诉讼和调查之中时，这些数据能够正确显示。

通常，在发生安全违规、无法解释的系统活动或系统崩溃后，审计日志是非常重要的检查项。有一种实时或接近实时的审计分析方法，就是使用自动工具在创建审计信息时对其进行检查。但很多时候仍然需要手工审查。

安全信息和事件管理(SIEM)系统能够减少审计日志内信息的数量，去除普通的任务信息，并记录可能对安全专家或管理员有用的系统性能、安全和用户功能信息。

攻击者经常会删除保存其犯罪活动信息的审计日志(删除审计日志中特定犯罪数据的行为称为“擦洗(scrubbing)”)。因此应当采用严格的访问控制对审计日志加以保护，采用适当的步骤来保证审计信息的机密性和完整性不会受到任何形式的破坏。要保障只有特定的人（管理员和安全人员）才能够查看、更改和删除审计跟踪信息。

击键监控是一种能够检查和记录用户在操作过程中的键盘输入的监控行为。使用这种监控的人可以将用户输入的字符写入审计日志，以备日后检查。然而黑客也可以利用这种监控。这种监控往往会涉及隐私问题，公司应当采取这些步骤来保证不会侵犯个人的隐私，同时应向用户通告与计算机使用有关的隐私界限。

单元 2：实施身份管理

2.1 身份管理和单点登录

A、身份管理

身份管理（IDM）是一个广泛而又深入的术语，包括使用不同产品对用户进行自动化的身份标识、身份验证和授权。此外，身份管理还包括用户账户管理、访问控制、密码管理、单点登录（SSO）功能、管理用户账户的权限和特权以及设计和监控上述所有项。身份管理要求管理唯一标识的实体、它们的特征、凭证和资格。身份管理允许组织以及时和自动的方式创建并管理数字身份的生命周期（创建、维护、终止）。企业身份管理必须满足业务需求以及面向内部系统和外部系统的标准。

企业目前在控制资产访问方面需要处理的许多常见问题:

- 每位用户应当能够访问哪些内容？
- 由谁批准和允许访问？
- 访问决策如何与策略相对应？
- 离职员工是否仍然拥有访问权？
- 我们如何与动态的、不断变化的环境同步？
- 撤消访问的过程是怎样的？
- 如何对访问进行集中控制和监控？
- 为什么雇员需要记住 8 个密码？
- 我们有 5 个不同的操作平台。如果每个平台（和应用程序）都需要自己的凭证，那么如何进行集中控制？
- 我们如何控制雇员、客户和合作伙伴的访问权限？
- 如何确保我们遵守了必要的法规？

一般企业会开发或购买一套企业身份管理系统来进行身份与访问控制管理，一般功能包括：

- 用户指配。指的是为响应业务过程而创建、维护和删除存在于一个或多个系统、目录或应用程序中的用户对象与属性。
- 账户管理。账户管理负责创建所有系统中的用户账户，在必要时更改账户权限，并在不再需要时删除账户。
- 用户资料更新。大多数公司并不只是保存与用户有关的重要信息，而且要根据这些信息做出访问决策。

在准备 CISSP 考试时还应当了解一些相关技术：目录服务、访问管理、密码管理、单点登录、账户管理等内容，其中：

1、目录服务

大多数企业都使用某种类型的目录，目录中包含了与公司网络资源和用户有关的信息。多数目录遵循一种层次化的数据库格式，基于 X.500 标准和某种协议（如轻量级目录访问协议(LDAP)），允许主体和应用程序与目录进行交互。应用程序可以向目录发出一个 LDAP 请求，请求访问特定用户的相关信息；用户也可以通过类似的请求要求访问某个资源的相关信息。

目录内的客体由目录服务管理。目录服务允许管理员配置和管理如何在网络中进行身份标识、身份验证、授权和访问控制。

目录服务如何让这些实体保持有序运行呢？这就需要使用名称空间，每种目录服务都采用某种方式标识和命名它们所管理的客体。目录服务管理目录中的条目和数据，并且通过执行访问控制和身份管理功能来实施已配置的安全策略。例如，当你登入桌面终端后，目录服务（AD）将决定你能够访问网络中的哪些资源。

目录在身份管理中的角色是什么呢？ 用于身份管理的目录是一种为读取和搜索操作而进行过优化的专用数据库软件，它是身份管理解决方案的主要组件，其原因在于所有资源信息、用户属性、授权资料、角色、潜在的访问控制策略以及其他内容都存储在这一位置中。当其他身份管理软件应用程序需要执行它们的功能（授权、访问控制、分配权限）时，就能够从一个集中的位置来获取它们所需的信息。

常见的目录协议：X.500 LDAP 微软域（AD）管理

2、Web 访问管理

Web 访问管理（WAM）软件用于控制用户在使用 Web 浏览器与基于 Web 的企业资产进行交互时能够访问哪些内容。Web 访问控制管理过程的基本组件和活动：首先，用户向 Web 服务器送交凭证。然后，Web 服务器请求 WAM 平台去认证用户。WAM 对 LDAP 目录进行身份验证，并从策略数据库中检索授权。第三步，用户请求访问一个资源（客体）。最后，Web 服务器使用安全策略进行验证，并且允许用户访问请求的资源。

3、密码管理

一些最常用的密码管理方法有：密码同步、自助式密码重设和辅助式密码重设，其中：

- 密码同步。用于降低保留不同系统的不同密码的复杂性；
- 自助式密码重设。通过允许用户重新设置他们的密码，减少服务台人员收到的求助电话数量。
- 辅助式密码重设。为服务台减少有关密码问题的决策过程，这包括使用其他类型的身份验证机制（如生物测定学、令牌）进行身份验证。

B、单点登录

单点登录 SSO 技术允许用户只需要进行一次身份验证，随后不需要再次身份验证就可以访问环境中的资源。但是，如果攻击者找出某个用户的凭证，那么就可以访问这名合法用户能够访问的所有资源。SSO 解决方案还会造成瓶颈或单点故障，因此我们需要采用某种冗余或故障排除技术。

单点登录技术的常见示例包括：

- Kerberos。使用 KDC 和票证的身份验证协议，基于对称密钥密码学。
- SESAME。使用 PAS 和 PAC 的身份验证协议，基于对称和非对称密码学。
- 安全域。在相同安全策略下运行的资源，由相同的组管理。
- 目录服务。允许资源以标准化方式命名和允许访问控制被集中维护的一种技术。
- 瘦客户端。依赖一台中央服务器进行访问控制、处理和存储的终端。

Kerberos 协议是实现单点登录的一个身份验证和授权协议。它使用对称密钥密码学，并提供端对端的安全性。绝大多数 Kerberos 实现方案使用的是共享的秘密密钥。

Kerberos 协议包含几个不同的重要元素，其中

密钥分发中心密钥分发中心(KDC)，是提供身份认证服务的可信第三方。所有客户和服务器都用 KDC 做注册，所有网络成员的密钥都由 KDC 维持。Kerberos 身份认证服务器 KDC 的功能包括：票据授予服务（TGS)和身份认证服务(AS)。

票据授予票证(TGT)，TGT 提供证据证明主体已通过 KDC 进行身份认证，并有权请求票据访问其它客体。TGT 是加密的，包括对称密钥、过期时间和用户的 IP 地址。主体在请求访问客体的票据时，会出示 TGT。

票据（ST），票据是一种加密信息，提供主体有权访问客体的证据。票据有时也被称为服务票据(ST)。

Kerberos 需要一个账户数据库，这通常包含在目录服务中。这些加密票据还确保永远不会以明文形式传输登录凭证、会话密钥和身份认证消息。

Kerberos 登录过程的工作方式如下：

- 用户在客户端输入用户名和密码。
- 客户端使用 AES 加密用户名以传输到 KDC。
- KDC 根据已知凭据的数据库验证用户名。
- KDC 生成将由客户端和 Kerberos 服务器使用的对称密钥。它使用用户密码的散列对此进行加密。KDC 还生成加密的带时间戳的 TGT 。
- 然后，KDC 将加密的对称密钥和加密的带时间戳的 TGT 发送到客户端。
- 客户端安装 TGT 以供使用，直到它过期。客户端还使用用户密码的散列来解密对称密钥。

下面列举了 Kerberos 可能存在的一些弱点：

- KDC 会是一个单一故障点。如果 KDC 出现故障，那么没有人能够访问所需的资源。对于 KDC 来说，冗余是必要的。
- KDC 必须能够以实时方式处理接收到的大量请求。它必须可扩展。
- 秘密密钥临时存储在用户的工作站上，这意味着入侵者有可能获得这些密钥。
- 会话密钥被解密后驻留在用户工作站的缓存或密钥表中。同样地，入侵者也可以获取这些密钥。
- Kerberos 容易遭受密码猜测攻击。KDC 并不知道是否正在发生字典攻击。
- 如果没有应用加密功能，那么 Kerberos 不能保护网络流量。
- 如果密钥过短，那么它们可能易受蛮力攻击。
- Kerberos 要求所有客户端和服务器的时钟同步。

因此 Kerberos 必须是透明的（在后台运行，不需要用户理解）、可扩展的（在大型的异构环境中运行）、可靠的（使用分布式服务器架构来确保不会出现单点故障）和安全的（提供身份验证和机密性）。

C、管理身份和访问配置生命周期

身份和访问配置生命周期是指账户的创建、管理和删除。访问控制管理是在账户生命周期中，管理账户、访问和问责所涉及的任务和职责的集合。包含在身份和访问配置生命周期中的三个主要职责：配置、账户审核和账户撤消。

2.2 联合身份管理

A、联合身份管理概述

联合身份管理（FIM）将单一域的身份管理扩展到更多的组织。多个组织可加入联盟或组，在这些组织中，他们就共享身份的方法达成一致。每个组织中的用户可在自己的组织中登录一次，并且凭据与联合身份匹配。然后，他们可使用此联合身份访问组内任何其他组织中的资源。一般联合身份管理两种认证模式：交叉认证模式和可信第三方模式

B、SAML、SPML 和 XACML

SAML 即安全声明标记语言，是一个基于 XML 的标准，通常用于在联合组织之间交换身份验证和授权(AA)信息。SAML 数据可以通过不同类型的协议传输，但常用的一个协议是简单对象访问协议(SOAP)。SOAP 是一个规范，规定了如何以结构化方式交换与 Web 服务有关的信息。它提供了基本的消息框架，使得用户可以请求一个服务，同时，该服务也可以提供给该用户。

SPML 即服务配置标记语言，是一种新框架，它基于 XML，专门用来交换用于联合身份 SSO 目的的用户信息。它基于目录服务标记语言(DSML),它可采用 XML 格式显示基于 LDAP 的目录服务信息。

XACML 即可扩展访问控制标记语言，用于定义 XML 格式的访问控制策略。它通常将策略实现为基于属性的访问控制系统，但也可以使用基于角色的访问控制。它有助于向联盟中的所有成员提供保证，即他们授予对不同角色的相同级别的访问权限。

C、OAuth 2.0

OAuth(开放式身份验证)是一种用于访问委派的开放标准。例如，假设你有一个 Twitter 账户。然后，你下载一个名为 Acme 的应用程序，可以与你 Twitter 账户进行交互。当你尝试使用此功能时，它会将你重定向到 Twitter，如果你尚未登录，则会提示你登录 Twitter。然后，Twitter 会询问你是否要授权该应用并告诉你授予的权限。如果你批

准，Acme 应用程序可访问你的 Twitter 账户。主要好处是你永远不会将 Twitter 凭据提供给 Acme 应用程序。即使 Acme 应用程序遭受重大数据泄露暴露其所有数据，它也不会暴露你的凭据。许多在线网站都支持 OAuth 2.0，但不支持 OAuth 1.0。OAuth 2.0 与 OAuth 1.0 不向后兼容。RFC 6749 文档是关于 OAuth 2.0 的。

D、OpenID 和 OpenID 连接

OpenID 也是一个开放标准，但它由 OpenID 基金会维护，而不是作为 RFC 标准维护。它提供分散式身份验证，允许用户使用由第三方服务(称为 OpenID 提供程序)维护的一组凭据登录多个不相关的网站。当用户转到启用 OpenID 的网站(也称为依赖方)时，系统会提示他们将 OpenID 标识作为统一资源定位符(URL)提供。这两个站点交换数据并建立安全通道。然后，用户被重定向到 OpenID 提供程序，并被提示提供密码。如果正确，则将用户重定向到启用 OpenID 的站点。例如：用户要使用 OpenID 就必须先在 OpenID 身份服务器（Identity Provider， IDP）获得 OpenID 账号（比如 Google 账户），用户可以使用 OpenID 账户来登录任何一个接受 OpenID 认证的服务应用（the relying party，RP，依赖方）。OpenID 协议标准就是提供一个框架用来 IDP 和 RP 之间通信。本质而言，用户的 OpenID 是一个为用户个人所拥有的特殊 URL(比如 alice2016.openid.com)，所以有些网站甚至会提供选项让用户自己去填写 OpenID。

OpenID 连接是使用 OAuth 2.0 框架的身份验证层。与 OpenID 一样，它由 OpenID 基金会维护。它建立在使用 OpenID 创建的技术的基础上，但使用 JSON WebToken(JWT)，也称为 ID 令牌。OpenID 连接使用符合 REST 的 Web 服务来检索 JWT。除了提供身份验证之外，JWT 还可提供有关用户的配置文件信息。

E、IDaaS

云服务提供商也能提供身份认证服务，身份即服务（IDaaS）是一种软件即服务（SaaS），通常联合 IdM 和密码管理服务，并被配置用于提供单点登录（SSO）。虽然大多数 IDaaS 供应商专注于以云和网络为中心的系统，但他们也可以在企业内部网络传统平台上的 IdM 上，使用其产品。

虽然 IDaaS 在安全产业中迅速发展，但需要注意的是，它并非没有潜在的问题。首先，一些受监管的行业可能无法利用 IDaaS 并保持兼容。这是因为一个关键的功能（例如 IdM）被外包，而服务提供商可能无法符合所有的监管要求。另一个关注点是，一旦位于企业之外，一些最关键的数据将会更多地被暴露。虽然不同的云服务提供商无疑能提供与客户组织相比有相同或更好的安全性，但在做出一个使用 IDaaS 的决定之前，这仍然是一个需要讨论的重要问题。最后，还有整合的问题。基于特定的供应商和产品，一些遗留的应

用程序可能得不到支持。这也需要在签署合同之前进行讨论。

单元 3：管理授权机制

3.1 访问控制模型

A、实施纵深防御和模型概述

纵深防御策略，使用多个层级的访问控制来提供分层安全性。纵深防御的概念突出了几个重点:

- 组织的安全策略是管理访问控制之一，它通过定义安全要求为资产提供了一层防御。
- 人员是防御的关键组成部分。但他们需要适当的培训和教育来实现，遵守和支持组织安全策略中定义的安全元素。
- 管理、 技术和物理访问控制的组合提供了更强大的防御。如果仅使用管理、技术或物理控制中的一种，攻击者可能发现可利用的弱点。

B、自主访问控制

自主访问控制(DAC)模型的一个关键特征是每个客体都有一个所有者，所有者可授予或拒绝其他任何主体的访问。

在 DAC 模型中，基于为用户授予的授权限制访问。这意味着，用户被允许指定对其拥有的客体的访问类型。如果某个组织机构使用 DAC 模型，那么网络管理员能够允许资源所有者控制哪些人可以访问他们的文件。DAC 的最常见实现方式是访问控制列表（ACL），ACL 由所有者规定和设置，由操作系统实施。DAC 使得用户访问信息的能力更加动态化，这与强制访问控制（MAC）的静态特性形成对比。

C、强制访问控制

强制访问控制(MAC)模型依赖于分类标签的使用。每个分类标签代表一个安全域或安全领域。安全域是共享共同安全策略的主体和客体的集合。例如，一个安全域可以具有秘密标签，并且 MAC 模型将以相同的方式保护具有秘密标签的所有对象。当主体具有匹配的秘密标签时，主体只能访问具有相应秘密标签的客体。此外，对于所有主体，获得秘密标签的要求是相同的。

D、基于角色的访问控制

基于角色的访问控制(RBAC)模型的一个关键特征是角色或组的使用。用户账户不是直接向用户分配权限，而是放置在角色中，管理员为角色分配权限。这些角色通常由职责功能标识。如果用户账户处于某角色中，则用户具有该角色的所有权限。微软 Windows 操作系统使用组实现此模型。

E、基于规则的访问控制

基于规则的访问控制模型的一个关键特征是它采用适用于所有主体的全局规则。规则型访问控制使用特定的规则来规定主体和客体之间可以做什么，不可以做什么。例如，防火墙使用的规则允许或阻止所有用户的流量。基于规则的访问控制模型中的规则有时被称为“限制”或“过滤器”。 基于规则的访问控制模型通常是建立在传统的 RBAC 之上，因此通常也被称为规则型 RBAC（RB-RBAC）

F、基于属性的访问控制

传统的基于规则的访问控制模型包括适用于所有主体(例如用户)的全局规则。但是，基于规则的访问控制的高级实现是基于属性的访问控制(ABAC)模型。ABAC 模型使用包含规则的多个属性的策略。许多软件定义网络应用程序使用 ABAC 模型。属性可以是用户、网络和网络上的设备的任何特征。

3.2 访问控制技术、管理和方法

A、访问控制技术

访问控制实现时常用到的技术有：

- 限制性用户接口。通过不允许使用某些功能、信息或访问特定的系统资源，限制性用户接口能够限制用户的访问能力。限制性接口主要有下列 3 种:菜单和外壳、数据库视图以及物理限制接口。
- 远程访问控制技术。例如：Radius、TACACS、Diameter
- 访问控制矩阵。访问控制矩阵是包含主体、客体和分配的权限的表格。当主体尝试操作时，系统检查访问控制矩阵以确定主体是否具有执行操作的适当权限。访问控制矩阵可包括访问控制列表(ACL)和能力表(Capability Table)两种方式。
- 依赖内容的控制。依赖内容的访问控制根据客体内的内容限制对数据的访问。数

据库视图就是依赖内容的控制。视图从一个或多个表中检索特定列，从而创建虚拟表。

- 依赖上下文的控制。依赖于上下文的访问控制在授予用户访问权限之前需要特定的活动。

B、访问控制的管理和方法

访问控制实现方法由 3 个大的类别组成：行政管理性、技术性和物理性，其中

- 行政管理性控制：策略和措施、人员控制、监管结构、安全意识培训、测试
- 物理性控制：网络分段、周边安全、计算机控制、工作区分隔、数据备份、布线、控制区
- 技术性控制：系统访问、网络架构、网络访问、加密和协议、审计

访问控制管理有三种形式：集中式、分散式、混合式

3.3 针对访问控制的威胁

A、访问聚合攻击

访问聚合是指收集多条非敏感信息并将它们组合(即聚合)以获得敏感信息。换句话说，个人或团体可能收集有关系统的多个事实，然后使用这些事实来发动攻击。

侦察攻击是一种访问聚合攻击，它结合了多种工具来识别系统的多个元素，例如 IP 地址、开放的端口、运行的服务、操作系统等。攻击者还对数据库使用聚合攻击。

B、密码攻击

密码是最弱的身份验证形式，并且存在许多密码攻击。如果攻击者成功进行密码攻击，则攻击者可获得账户权限并访问授权资源。使用字典、暴力、彩虹表和嗅探方法的常见密码攻击。

C、生日攻击

生日攻击的重点是寻找碰撞。生日攻击名称来自-一个被称为生日悖论的统计现象。

D、欺骗攻击

欺骗(也称为伪装)假装成某种东西或某个人。访问控制攻击中使用的相关类型的欺骗包括电子邮件欺骗、IP 欺骗和电话号码欺骗。

E、社会工程学

社会工程学是一种利用人的弱点如人的本能反应、好奇心、信任、贪便宜等弱点进行诸如欺骗、伤害等危害手段，获取自身利益的手法。

F、网络钓鱼

网络钓鱼是一种社会工程，它试图欺骗用户放弃敏感信息，打开附件或点击链接。网络钓鱼攻击有多种变种，包括鱼叉式网络钓鱼、网络钓鲸和语音网络钓鱼。网址嫁接是另一种类似的攻击，它将受害者重定向至一个看似合法的、其实仍是伪造的 Web 站点。

G、智能卡攻击

智能卡提供比密码更好的身份验证，尤其是当它们与其他身份验证因素(如 PIN)结合使用时。但智能卡也容易受到攻击。侧信道攻击是一种被动的非侵入性攻击， 旨在观察设备的操作。攻击成功后，攻击者可了解卡中包含的有价值信息，例如加密密钥。

H、相关防御措施

控制对系统的物理访问。与安全相关的一句老话是，如果攻击者对计算机具有不受限制的物理访问权限，则攻击者就拥有了该计算机。

控制对文件的电子访问。严密控制和监控所有重要数据的电子访问，包括包含密码的文件。最终用户和非账，户管理员不需要访问密码数据库文件以执行日常工作任务。安全专业人员应立即调查任何未经授权的密码数据库文件访问。

创建强密码策略。密码策略以编程方式强制使用强密码，并确保用户定期更改其密码。攻击者需要更多时间来破解更复杂和更长的密码。如果有足够的时间，攻击者可在离线暴力攻击中发现任何密码，所以需要定期修改密码才能保证安全。更安全或更敏感的环境需要更强的密码，并要求用户更频繁地更改密码。许多组织为特权账户(如管理员账户)实施单独的密码策略，以确保它们具有更强的密码，并且管理员比常规用户更频繁地更改密码。

散列和加盐密码。使用 Bcrypt 和 PBKDF2 等协议加密密码，并考虑使用外部胡椒来进一步保护密码。结合强密码策略，使用彩虹表或其他方法很难破解加盐和加胡椒的密码。

使用密码屏蔽。确保应用程序永远不会在任何屏幕上以明文形式显示密码。而是通过显示替代字符(如*)来屏蔽密码的显示。这减少了肩窥的危害，但用户应该知道攻击者可能通过观察用户的键盘键入来收集密码。

部署多因素身份验证。部署多因素身份验证，例如使用生物识别或令牌设备。当组织使用多因素身份验证时，如果攻击者只有密码，则无法访问网络。很多在线服务(如 Google)提供多因素身份验证作为额外的保护措施。

使用账户锁定控制。账户锁定控制有助于防止在线密码攻击。在输入错误密码达到预定义次数后，他们会锁定账户。账户锁定控制通常使用削弱级别来忽略某些用户错误，但在达到阈值后执行锁定操作。对于不支持账户锁定控制的系统和服务。

使用上次登录通知。许多系统显示消息，包括上次成功登录的时间、日期和位置(例如计算机名称或 IP 地址)。如果用户注意此消息，他们可能注意到其他人是否登录了他们的账户。

用户安全培训。经过适当培训的用户可更好地了解安全性以及使用更强密码的好处。

D6：安全评估和测试

单元 1：相关概述、技术措施评估和测试

1.1 安全评估和测试概述

A、安全评估和测试的重要性

组织可以雇用最好的人，制定健全的策略和程序，并部署世界一流的技术，来确保信息系统的安全。但是，如果组织不进行定期评估这些措施的有效性，那么将无法实现长治久安。然而不幸的是，成千上万的组织往往正是在安全事件发生之后，才以这种痛苦的方式领悟到这样一个客观的事实，就是：组织当初所实施的、最为先进的控制措施早已时过境迁，并且变得不再奏效了。因此，除非组织能够持续评估和改善其安全态势，否则这些措施将随着时间的推移而逐渐失效。

B、安全评估和测试程序的构成

安全评估程序由安全测试、安全评估、安全审计三大部分构成。其中：

- 安全测试。安全测试能够验证安全控制措施运行正常。测试的方法主要包括自动扫描、工具辅助渗透测试和手动测试。测试完成时，还必须仔细审核这些测试的结果，确保每个测试是成功的。
- 安全评估。安全评估是对系统、应用程序或其他待测环境的安全性进行全面审查。在安全评估期间，经过训练的信息安全专业人员执行风险评估，识别出可能造成危害的安全漏洞，并根据需要提出修复建议。安全评估通常包括安全测试工具的使用，但不限于自动化扫描和手工渗透测试。它们还包括对威胁环境、当前和未来风险、目标环境价值的细致审查。安全评估的主要工作成果通常是向管理层提交的评估报告，报告包括以非技术语言描述的评估结果，并通常以提高待测环境安全性的具体建议作为结尾。
- 安全审计。安全审计为对信息系统内部安全控制的系统性评估，是对于特定范围的人、计算机、过程和信息的各种安全控制所实施的一个系统性评估。安全评估期间，安全审计虽然遵循许多相同技术，但必须由独立审核员执行。

1.2 技术措施评估和测试

A、技术控制措施评测概述

技术控制是通过使用 IT 资产来实现的安全控制。这种资产通常但并非总是一些以某种特定方式配置的某种软件。当我们在审计自己的技术控制时，所要测试的是：技术控制对那些我们在风险管理流程中所识别到的风险的降低能力。因为我们需要理解实施特定控制的环境，所有各种控制与那些试图降低的风险之间的联系是很重要的。

一旦我们理解了技术控制的目的，我们就能够选择合适的方法来测试其是否有效。而对于试图做代码审查而言，我们可能更适合去测试第三方软件的漏洞。作为安全专业人员，我们必须熟悉、并对最为常用的技术控制措施的评估与测试方法具备理想的经验，以便我们能为当前的工作选择合适的方法。

B、脆弱性测试

NIST 为安全社区提供安全内容自动化协议（SCAP)来描述漏洞。SCAP 组件包括:

- 通用漏洞披露(CVE): 提供一个描述安全漏洞的命名系统。
- 通用漏洞评分系统(CVSS): 提供一个描述安全漏洞严重性的标准化评分系统。
- 通用配置枚举(CCE): 提供一个系统配置问题的命名系统。
- 通用平台枚举(CPE)：提供一个操作系统、应用程序及设备的命名系统。
- 可扩展配置检查表描述格式(XCCDF)：提供一种描述 安全检查表的语言。
- 开放漏洞评估语言(OVAL)：提供一种描述安全测试过程的语言。

漏洞扫描可自动探测系统、应用程序及网络，探测可能被攻击者利用的漏洞。漏洞扫描主要分为 4 类：网络发现扫描、网络漏洞扫描、Web 应用漏洞扫描及数据库漏洞扫描。每类扫描都可以由工具来实现，其中：

网络发现扫描运用多种技术来扫描一段 IP 地址，探测存在开放网络端口的系统，常见扫描技术有：TCP SYN 扫描、TCP Connect 扫描、TCP ACK 扫描、Xmas 扫描。网络发现扫描最常用的工具是一款名为 nmap 的开源工具。

网络漏洞扫描会继续探测目标系统或网络，发现是否存在已知漏洞。误报(false positive report）：当对某个系统进行网络漏洞描时，扫描器没有获取充足信息来判定某个漏洞是否存在，即使系统实际上不存在该漏洞，扫描器也会报告存在。漏报(false negative report)：当漏洞扫描器漏过某个漏洞，未能向系统管理员报告存在危险情况。Nessus 是一种广泛应用的漏洞扫描器，但也存在许多其他种类的漏洞扫描器。开源扫描器 OpenVAS 也越来越受社区用户的欢迎。

Web 应用漏洞扫描输入及其他参数来识别 Web 应用漏洞。除了 Nessus 之外，其他常用的 Web 应用漏洞扫描工具包括商业扫描器 Acunetix、开源扫描器 Nikto 和 Wapiti，以及代理工具 Burp Suite。

数据库漏洞扫描器允许安全专业人员扫描数据库和 Web 应用程序，寻找影响数据库安全的漏洞。sqlmap 是一种常用的开源数据库漏洞扫描工具，它帮助安全专业人员探测 Web 应用程序的数据库漏洞。

采用漏洞管理系统的组织应该形成一套工作流程来管理漏洞。这套工作流程应该包括以下的基本步骤：

- 检测：通常在扫描漏洞之后，第一次发行某个漏洞。
- 验证：一旦扫描器检测到一个漏洞，管理员应该确认此漏洞，判断它是否为误报。
- 修复：此后，验证过的漏洞需要加以修复。

工作流方法的目标是确保能有条不紊地检测和修复漏洞。工作流还应该包括一系列步骤，这些步骤根据漏洞的严重性、漏洞利用的可能性、漏洞修复的可能性来决定漏洞修复顺序。

C、渗透测试

漏洞扫描只是探测漏洞是否存在，通常不会对目标系统发起攻击性行为。而执行渗透测试的安全专业人员尝试突破安全控制措施，入侵目标系统或应用来验证漏洞。渗透测试过程通常包含以下几个阶段：

- 规划阶段，包括测试范围和规则的协议。
- 信息收集和发现阶段，结合人工和自动化工具来收集目标环境的信息。
- 漏洞扫描阶段，探测系统脆弱点，结合网络漏洞扫描、Web 漏洞扫描和数据库漏洞扫描。
- 漏洞利用阶段，试图使用人工和自动化漏洞利用工具来尝试攻破系统安全防线。
- 报告阶段，总结渗透测试结果，并提出改进 系统安全的建议。

渗透测试人员通常使用一种名为 Metasploit 的工具自动对目标系统进行漏洞利用。

渗透测试人员可以是把渗透测试作为工作职责的公司员工，也可以是聘请的外部顾问。渗透测试通常划分为以下三种：

- 白盒渗透测试(White Box Penetration Test)：向攻击者提供目标系统的详细信息
- 黑盒渗透测试(Black Box Penetration Test)：攻击之前不会向测试人员透露任何信息
- 灰盒渗透测试(Gray Box Penetration Test)：也称为部分知识测试，有时是为了平衡白盒渗透测试和黑盒渗透测试的优缺点

D、日志审查

安全信息和事件管理（SIEM）工具可存储日志数据和执行自动化及人工日志审查。这些工具利用许多设备、操作系统和应用程序中存在的 syslog 功能来收集信息。日志系统还应该利用网络时间协议（NTP），确保向 SIEM 发送日志记录的系统和 SIEM 本身的时钟是同步的。信息安全管理者应该定期进行日志审查，特别是对于敏感功能，确保特权用户不会滥用其职权。

在调查安全事件时，网络流(NetFlow)日志特别有用。这些日志提供了系统连接和传输数据量的记录。

E、综合事务和真实用户监控

安全专业人员要经常参与持续安全监控中，从事性能管理、故障排除、潜在安全问题识别等活动。监测可分为两类：

真实用户监控(RUM)是一种被动监测的变体，监测工具重组单个用户的活动，追踪其与网站的交互。被动监测是一种在经网络传输或抵达服务器的过程中，通过捕获发送到系统的实际网络流量进行分析的监测的方法。被动监测提供真实监测数据，帮助管理员深入理解网络上正在发生的事情。

综合事务监测（Synthetic transactions）(或主动监测）：是对系统执行伪造的事务活动（测试脚本），从而评估其性能。综合监测可以是从系统请求一个内容来确定响应时间，也可能执行复杂的脚本来确认事务活动的结果。

F、代码审查和测试

代码审查(code review)是软件评估的基础。代码审查也称为“同行评审”（peer review），即除了编写代码的开发人员，其他开发人员审查代码是否存在缺陷。代码审查可能决定应用程序是允许移植到生产环境，还是退回给原开发人员，让其重写代码。

代码审查可采用多种不同的形式，并且不同组织之间的形式上也有所不同。最正式的代码审查过程称为范根检查法（Fagan inspections），遵循严格的审查和测试过程，包含六个步骤：规划、概述、准备、审查、返工、追查

静态测试在不运行软件的情况下，通过分析软件源代码或编译后的应用程序，评估软件的安全性。静态分析经常涉及自动化检测工具，用于检测常见的软件缺陷。

动态测试在软件运行环境下检测软件的安全性，如果组织部署他人开发的软件，这将是唯一选择。 这些情况下，测试人员无法接触到软件的底层源代码。在生产环境中，动态测试应该谨慎开展，避免服务的额外中断。

模糊测试（Fuzzing）是一种特殊的动态测试技术，向软件提供许多不同类型输入来测试其限制，发现之前未检测到的缺陷。模糊测试向软件提供无效的输入(随机产生的或特殊构造的输入)，触发已知的软件漏洞。模糊测试人员监测软件的性能，观察软件是否崩溃，是否出现缓冲区溢出或其他不可取和(或)不可预知的结果。

模糊测试主要分为两大类:

- 突变(Mutation 或 Dumb)模糊测试：从软件实际操作获取输入值，然后操纵(或变异)输入值来生成模糊输入。突变模糊测试可能改变输入的内容，在内容尾部追加字符串，或执行其他的数据操纵方法。
- 预生成(智能)模糊测试：设计数据模型，基于对软件所用数据类型的理解创建新的模糊输入。

G、误用用例测试

一些应用程序存在明显的说明示例，展示软件用户可能尝试错误使用该应用程序。软件测试人员使用一种称为误用例测试的过程，评估软件是否存在与这些已知风险相关的漏洞。

在误用例测试过程中，测试人员首先列举已知误用例。然后，尝试通过手工或自动化攻击的方法，尝试利用这些误用例来测试应用程序。

H、测试覆盖率分析

软件测试人员通常进行测试覆盖率分析，由此估计对新软件的测试程度。用以下公式计算测试覆盖率：测试覆盖率 = 已测用例的数量/全部用例的数量

测试覆盖率分析公式适用于许多不同标准。下面是五个常见标准：

- 分支覆盖率：在所有 if 和 else 条件下，每个 if 语句是否已被执行?
- 条件覆盖率：在所有输入集合下，代码中每个逻辑是否已被测试?
- 函数覆盖率：代码中每个函数是否已被调用并返回结果?
- 循环覆盖率：在导致代码执行多次、一次或零次的条件下，代码中每个循环已被执行?
- 语句覆盖率：测试期间，是否已运行过每行代码?

I、接口测试

接口测试依据接口设计规范评估模块的性能，以确保模块在所有开发工作完成时可以协同工作。在软件测试过程中，需要测试的接口分为三种类型：

- 应用编程接口（API）：开发人员对 API 进行测试，确保 API 实施了所有安全要求。
- 用户界面（UI）：包括图形用户界面（GUI）和命令行界面。UI 为终端用户提供与软件交互的能力。接口测试应该审查所有用户界面，以验证用户界面是否正常工作。
- 物理接口：存在于操作机械装置、逻辑控制器或其他物理设备的一些应用程序。软件测试人员应该谨慎测试物理接口，因为如果物理接口失效，可能导致一些潜在后果。

单元 2：管理措施评估和测试、审计和报告评审

2.1 管措措施评估和测试

A、帐户管理测试

攻击者的一种首选技巧是尽快成为他们攻击系统的“正常”特权用户。他们可以通过至少三种方式来完成此操作：盗用现有特权帐户、创建新的特权帐户、或是提升常规用户帐号的权限。帐户管理包括：通过使用强认证；通过让管理员仅在特定任务时使用特权帐户；通过密切注意用户帐号的创建、修改或误用。

主要测试方法：

- 测试所有员工都是否知道可接受使用策略（AUP）和其他适用的策略是审核用户帐号的第一步。
- 添加、删除或修改权限应该有一套被精确控制和记录的过程。因此，重要的是要有可用来测试那些定制的高级权限的过程。
- 测试对于已暂停帐户的管理控制。

B、备份验证

无论采用何种组织数据的备份方法，我们都需要定期测试，以确保备份在我们需要时能按照其预定的方式运行。备份涉及的数据类型包括用户数据文件、数据库、邮箱数据。测试数据备份的过程包括：

- 开发各种场景，以捕获那些代表着组织所面临的威胁的特定事件集。
- 制定计划，测试每个场景中的所有关键任务的数据备份。
- 利用自动化，以最小化审计师所需的工作量，并确保定期进行测试。
- 最小化，数据备份测试计划对业务流程的影响，以便其可以被定期执行。

- 确保覆盖面，以便测试到每个系统，虽然那不一定会是在同一测试中。
- 记录各种结果，以便你能知晓什么是有效的，而什么是需要加强的。
- 修复或改进你记录到的任何问题。

C、灾难恢复和业务连续性

与任何其他业务流程一样，这些流程必须定期被评估，以确保它们仍然有效。包含有灾难恢复计划（DRP）的业务连续性计划（BCP）因为环境不断变化而需要定期被测试。测试和灾难恢复演练应当至少每年进行一次，这些演练能够论证公司能否从灾难中恢复过来。主要的测试方法在第 7 章中有详细介绍。

D、关键绩效和风险指标

两个最重要的安全指标类别：关键绩效指标（KPI）和关键风险指标（KRI）。KPI 衡量目前情况的进展程度。尽管 KPI 能告诉我们当前相对于目标的位置，而关键风险指标(KRI)能告诉我们的是当前与风险偏好的关系。KRI 衡量一项活动的风险值，以便管理层能够对该活动做出明智的决定，同时也考虑到潜在的资源损失。在考虑 KRI 时，将它们与单一损失预期(SLE)方程相关联是非常有用的。

一些指标术语：

- 因子，ISMS 的一个属性，可以描述为一个随时间变化的值。因子的示例是 IDS 生成的警报的数量或事件响应(Incident Response, IR)团队所调查事件的数量。
- 测量，在一个特定时间点上因子的值。换句话说，这是一个原始数据。
- 基线，一个因子的任意值，它提供一个参考点，或表示达到某个阈值后满足了某个条件。
- 度量，标准通过在多个测量之间， 或与基准进行比较而生成的派生值。度量本身就具有比较性。
- 指标，描述 ISMS 的某些有效性的一个或多个测量的解释。换句话说，指标对管理层来说是有意义的。

2.2 安全审计

A、安全审计的重要性

尽管组织安全人员可能会定期执行安全测试和评估，但这不是安全审计。评估和测试结果仅供内部使用，旨在评估控制措施，着眼于发现潜在的改进空间。另一方面，审计是

为了向第三方证明控制措施有效性而进行的评估。在评估这些控制措施有效性时，为组织设计、实施和监控控制措施的员工存在内在的利益冲突。

B、安全审计流程

审计员(Auditor)为组织的安全控制状态提供一种客观中立的视角。他们撰写的报告与安全评估报告非常相似，但适用于不同的受众，可能包括组织的董事会、政府监管机构和其他第三方。信息系统的安全审计流程

1、确定目标，显然其他一切都取决于这一点。

2、让合适的业务部门领导参与进来，以确保业务需求能够被识别和涉及到。

3、确定范围，因为不是所有都要被测试到的。

4、选择审计团队，根据目标、范围、预算和可用的专业知识，来决定是由内部还是外部人员所组成。

5、计划审计，以确保按时、且按照预算实现所有的目标。

6、执行审计，要在坚持计划的同时，记录其中的任何偏差。

7、记录结果，因为所产生的大量信息既是有价值的，但同时也是不稳定的。

8、将结果传达给合适的领导，以实现和维持强有力的安全态势。

C、内部审计和第三方审计

内部审计。内部审计是由组织内部审计人员执行，通常适用于组织内部。内部审计人员在执行审计时，通常完全独立于所评估的职能。在许多组织中，审计负责人直接向类似总裁、首席执行官汇报，审计负责人也可直接向组织的董事会报告。内部审计好处之一是：他们熟悉组织的内部运作。缺点：在运用其他方法来保护和利用信息系统的发现能力方面，他们可能有所受限，存在着利益冲突的可能性。

第三方审计。第三方审计通常使用外部审计来执行。好处：首先，外部审计师可能已经见证并测试过不同组织中的许多信息系统；另一个优势是：他们不了解目标组织的内部动力和政治。缺点：成本相对比较高。

D、安全审计报告

SSAE 16 有三种 SOC 报告：

- SOC1 适用于财务控制
- SOC 2 适用于信任服务（安全性、可用性、保密性、过程完整性和隐私）
- SOC 3 也适用于信任服务（安全性、可用性、保密性、过程完整性和隐私）

SOC 2 和 3 之间的差异是：SOC 2 报告所产生的结果提供了适用于所列出的、信任服务控制的、非常详细的数据，这不是给一般公众的。而 SOC 3 生成的报告具有较少的细节，并且可用于一般公众性目的。SOC 2 报告包括由审计师进行过测试的描述和这些测试的结果，以及审计师对各个控制和系统有效性的意见。SOC 3 不包含测试信息和适当的控制细节，而仅报告系统是否满足特定信任服务标准的要求。SOC3 通常用作“批准证明”，并被放在服务提供商的网站和营销材料上。

SSAE 16 评估活动产生两种不同类型的报告：

- I 类报告描述了被审计组织提供的控制措施，以及审计员基于该描述所形成的意见。I 类报告适用于某个时间点，不会涉及审计员对控制措施的实际测试。
- II 类报告至少覆盖 6 个月的时间，还包括审计员根据实际测试结果对这些控制措施的有效性所形的意见。

人们通常认为 II 类报告比 I 类型报告更可靠，因为 II 类报告包括对控制措施的独立测试。类型 I 报告只是让服务组织自圆其说，控制措施已按照描述实现。

信息安全专业人员经常被要求参与内部、外部或第三方审计。他们通常必须以访谈和书面文档的方式，向审计员提供有关安全控制措施的信息。审计员还可要求安全人员参与控制评估的过程。审计员通常可全权访问组织内的所有信息，而安全人员应服从审计员的请求，如果需要可请示管理层。

2.3 报告和管理评审

A、报告

技术报告应该是针对被研究系统（system under study，SUS）具体情况的标准方法论的应用。换句话说，报告必须表明这是一个定制的审计。它必须记录所使用的方法论、其根据 SUS 所定制的方式、结果、所建议的控制或更改。原始数据和自动报告应该提供在附录中。最重要的是：报告应该说明组织的风险状况。

技术报告（除了别的内容以外）中包括不超过一页或两页的执行摘要，这样能够突出那些高级领导层需要从报告中了解的内容。而其目标是获得他们的注意，并产生所需的改变。

B、管理评审

虽然管理评审已经存在了很长的时间，但是如今在使用该术语时最好还是要基于例如 ISO 9000 系列的质量标准。这些标准定义了一个计划-执行-检测-处理的循环，如 PDCA 流程。这个持续改进的周期很好地捕获了我们在本书中涵盖的大多数主题的精华。计划阶段

主要映射到第 1 章中的内容。这一阶段是我们在 ISMS 中所要做的一切事情的基础，因为它决定了我们的目标，并驱动着我们的策略。循环中的执行阶段覆盖了多个地方，但它是第 7 章的重点。检查阶段是本章大部分内容的主要议题。最后，处理阶段是我们在管理评审中正式去做的。我们会评审从前面阶段得到的所有信息，决定我们是否需要调整目标、标准或策略，以不断改善我们的安全态势。

D7：运营安全

单元 1：安全运营概述

1.1 理解和支撑调查

A、调查概述

调查可能是简短的、非正式的确定事件；但当产生的威胁或造成的破坏足以严重到需要进行更正式的调查时，需要专业调查人员的介入和进行仔细调查。

调查的类型分为：

- 行政调查：行政调查属于内部调查，它检查业务问题或是否违反组织的政策。
- 犯罪调查：犯罪调查通常由执法者进行，是针对违法行为进行的调查。犯罪调查的结果是指控犯罪和在刑事法庭上起诉。
- 民事调查　民事调查通常不涉及执法，而涉及内部员工和外部顾问代表法律团队的工作。
- 监管调查 政府机构在他们认为个人或企业可能违法时会执行监管调查。

事故调查员经过专业的培训，并且拥有丰富的经验，能够发现其他人通常忽略的可疑或反常活动。

他们常做的评估有：

- 网络分析：流量分析、日志分析、路径追踪
- 介质分析：磁盘镜像、 时间分析(修改、访问、创建)、注册分析、松弛空间分析、隐藏的秘密信息
- 软件分析：逆向工程、恶意代码审查、漏洞审查
- 硬件/嵌入式设备分析：专用设备攻击点、固件和专用内存检查、嵌入式操作系统、虚拟软件和虚拟化管理层分析

计算机犯罪与传统犯罪的差异显而易见，即调查员必须了解技术。

罗卡交换原则，该原则认定罪犯在带走一些东西的时候会遗留下一些东西。即使在完全数字化的犯罪现场中，罗卡交换原则也能够发现谁可能是犯罪者。

计算机犯罪通常分为下面几种类型：

- 军事和情报攻击：军事和情报攻击主要用于从执法机关或军事和技术研究机构获得秘密和受限的信息。
- 商业攻击：商业攻击专门非法获取公司的机密信息。
- 财务攻击：财务攻击用于非法获得钱财和服务。

- 恐怖攻击：恐怖攻击实际上存在于社会的很多领域。
- 恶意攻击：恶意攻击可对组织或个人造成破坏。
- 兴奋攻击：兴奋攻击通常由菜鸟发起，这些攻击的动机是闯入系统带来的极度兴奋。

B、调查过程和证据

为确保以标准方式进行取证活动，取证团队必须遵循一个特殊顺序的步骤，这个步骤包括：标识、保存、收集、检查、分析、呈现、决定。

证据有自己的生命周期，包括：收集和标识、存储、保管和运输、法庭出示、将证据返还给受害者或所有者。

在法庭审理中，可使用以下几种类型的证据：书面的、口头的、计算机生成的、视觉的或听觉的。证据的真实性、完整性、充足性和可靠性是十分重要的，这些特征帮助确保证据被法律所接受。

必须建立证据链也称为监管链，这涉及所有处理证据的人，包括收集原始证据的警员、处理证据的证物技术人员以及在法庭上使用证据的律师。对证据的位置必须从被收集的时刻到出现在法庭上的时刻进行完整记录，以确保是同一证据。这需要对证据进行完整标记，记录谁在特定的时间接触过这个证据，以及要求接触证据的原因。处理证据的每个人都必须签署监管日志链，以表明直接负责处理证据的时间以及交予监管链中的下一个人的时间。监管链必须提供完整的事件序列，从而说明从证据收集开始到审问之间的过程。

调查取证中涉及到的其它术语：

- 监视：物理监视、计算机监视
- 搜索和查封：在进行搜索和查封之前，执法机构必须拥有适当的原因，并且从法官或法庭处申请一张搜查许可证。
- 访谈：只在与法律顾问磋商后才会进行
- 审讯：目的是获得用于审判的证据

1.2 理解和应用基本的安全运营概念

A、运营相关角色和职责

运营安全涉及配置、性能、容错、安全性以及问责和验证管理，其目的在于确保适当的操作标准与合规性要求得到满足。

管理层负责雇员的行为和职责。操作部门的人员负责确保系统受到保护并在预期的方式下运行。操作部门目标往往是防止反复发生问题，将硬件和软件故障降到可接受的级

别，以及减小事故或破坏的影响。这个团体应该研究任何不寻常或无法解释的事件、不定期的初始程序加载、偏离标准以及网络上其他奇怪或异常的条件。

可问责性有助于确定是否确实发生违规，系统和软件的重新配置是否有必要，并且还有助于捕获那些超出确定范围之外的活动。审计需要作为日常工作开展，需要有人负责检查审计和日志事件。

组织可以为某些类型的错误预定义门限，从而在被认为可疑的活动发生之前允许一定数量的错误。门限是违规活动的基线，在引发告警之前对用户来说这些活动可能是正常的。这条基线被称为一个限值级别(clipping level)。使用限值级别、审计和监控的目标是在发生重大损失之前发现问题，并且在网络内部可能存在攻击活动时能够及时报警。

适当的安全控制和机制必须具有一定程度的透明性。因为安全控制的存在，所以这使得用户没有必要通过额外的步骤来执行任务和职责。透明性也不能让用户对控制了解太多，这有助于防止用户发现如何避开安全控制。如果控制太过明显，那么攻击者可以发现如何更加容易地攻陷它们。

B、安全运营相关概念

“知其所需”(need to know)原则强制要求授予用户仅访问执行工作所需数据或资源的权限；最小特权原则规定，主体仅被授予完成工作所需的特权，而不再被授予更多特权。

权利(Entilement)是指授予用户权限的数量，通常在首次分配账户时指定。

- 聚合(Aggregation)。在最小特权的上下文中，聚合是指用户随时间收集的权限数量。
- 信任传递(Transitive Trust)。两个安全域之间的信任关系，允许一个域的主体访问另一个域的对象。

职责分离确保个体无法完全控制关键职能或系统确保没有任何一个人可破坏系统或安全，这种做法是必要的。相反 ，两人以上必须密谋或串通才能危害组织，这会增加这些人暴露的风险。

特权分离在概念上与职责分离相似。特权分离建立在最小特权原则的基础上，并将其应用到应用程序和流程。特权分离策略需要使用细化的权限。

任务分解(segregation of duties)类似于职责分离策略，但结合了最小特权原则。任务分解目标是确保个人未拥有过多的系统访问权限(进而可能引发利益冲突)。

双人控制(two-person control) 通常称为双人制)要求经过两个人批准后才能执行关键任务。

岗位轮换(job rotation)可进一步控制和限制特权功能。岗位轮换(有时称为职责轮换)意味着员工进行岗位轮换，或者至少将一些工作职责轮换到不同员工。岗位轮换作为一

种安全控制措施，可实现同行评审、减少欺诈并实现交叉培训。交叉培训可减少环境对任何个体的依赖。

强制休假要求员工强制休假一周或两周，这种做法提供一种同行评审形式，有助于发现欺诈和串通行为。此策略确保另一名员工至少有一周时间接管某个人的工作岗位。如果员工参与欺诈，那么接管岗位的人可能会发现。

特权账户管理确保员工没有超出所需权限，并且不会滥用这些权限。所有管理员账户都具有可提升的权限，所以应该受到监控，通常包括：访问审计日志、更改系统时间、配置接口、管理用户账户、控制系统重启、控制通信路径、备份和恢复系统、运行脚本/任务自动化工具、配置安全控制机制、使用操作系统控制命令、使用数据库恢复工具和日志文件

管理信息生命周期。根据数据分类确定保护数据的方法。安全控制需要在整个生命周期内对信息进行保护，生命周期包括：生成或捕获、分类、存储、使用、归档、销毁或清除。这些具体的内容在第 2 章中有详细介绍。

服务水平协议(SLA)是组织与外部实体(例如供应商)之间的协议。除了 SLA，组织有时还使用谅解备忘录(MOU)和/或互连安全协 ISA)。谅解备忘录记录了两个实体一起努力来达成共同目标的意愿。虽然 MOU 与 SLA 类似，但 MOU 不太正规，缺少处罚条款。如果其中一方不履行其职责，则没有任何处罚措施。

人员安全关注是安全运营的一个重要因素，组织应该实施加强人员安全的。控制措施，主要包括：胁迫；出差：敏感数据、被注入恶意软件、被监控、免费 WiFi、VPN；应急管理、安全培训与意识。

单元 2：操作安全实践

2.1 安全资源配置

A、安全资源配置概述

“配置”（Provisioning）在技术领域是一个被反复使用的术语。在 CISSP 中，配置是指为用户或用户群提供一种或多种信息服务所需的一系列活动。安全资源配置的核心是必须以安全方式提供这些服务。换言之，我们必须确保服务本身就是安全的。我们也必须确保用户或系统可以根据他们自己的授权及最低权限原则，安全地使用这些服务。

B、资产清单

保护我们信息系统最重要的是要知道我们在防护什么。我们需要：

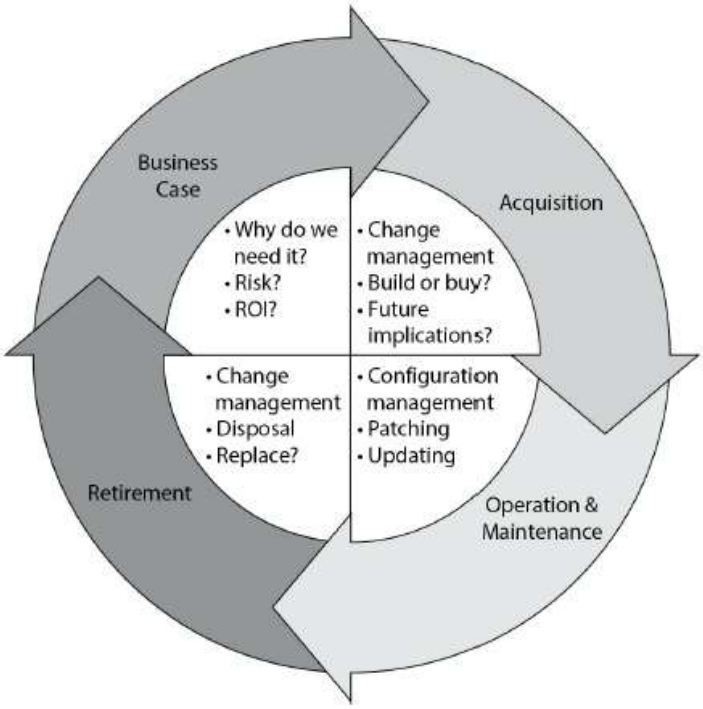
跟踪硬件。全面了解组织中有哪些设备。

跟踪软件。软件的问题包括非法和盗版软件、后门病毒、木马等。有一些被广为接受的最佳做法：

- 应用白名单。白名单是指允许在单一或成套设备中运行的一系列软件的列表。
- 使用母盘。母盘是标准镜像工作站或服务器，它包括适当配置和授权的软件。
- 执行最低权限原则。若特定的用户无法在其设备上安装任何软件，那么恶意应用程序就更难出现在我们的网络中。
- 自动扫描。应定期扫描网络中的每台设备，以确保其仅运行适当配置，以及经过批准的软件。

C、资产管理

资源配置只是资产管理生命周期过程中的一部分。资产管理生命周期可分为四个阶段：业务案例、购置、运营和维护（O&M）以及报废。



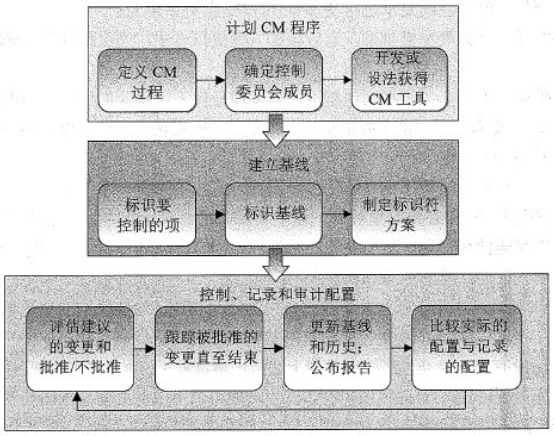
D、配置项管理和变更管理

在资产管理生命周期操作和运维阶段（O&M），我们还需要确保和掌握如何配置（configured）这些资产。

配置项管理（Configuration Management，CM）是一个操作过程，旨在确保正确配置

相应控制措施，并能及时响应当前威胁和操作环境。简单来说，配置管理（CM）是在所有系统上建立并保持基线的程序。

变更管理是一个业务流程，目的是专门用于规范业务活动（例如项目）的变化特征。变更管理控制提供一种流程，实现控制、记录、跟踪和审计所有系统变更。组织需要在所有系统的生命周期中实施变更管理流程。



变更管理流程的常见步骤如下:

1、请求变更。一旦识别出所需的变更，员工便会请求变更。

2、审核变更。组织内的专家会审核变更。

3、批准/拒绝变更。依据审核结果，这些专家然后会批准或拒绝变更。

4、测试变更。一旦批准更改，需要对变更进行测试，最好安排在非生产服务器。

5、安排并实施变更。按部就班地实施变更，以便对系统及用户造成的影响最小化。

6、记录变更。最后一步是记录变更，确保所有相关方知悉变更。

版本控制通常指软件配置管理所使用的版本控制。配置文档明确了系统的当前配置，它明确了哪些人负责系统，明确了系统的目的，并列举了基线之后的所有变更。

E、可信恢复

当一个操作系统或应用程序崩溃或死机时，不应让系统处于任何类型的不安全状态。对于系统崩溃的通常原因，首先考虑的是因为系统遇到了某些它感到不安全的或不理解的事情，并认为死机、关机和重启要比执行当前的活动更为安全。

系统崩溃后应采取的正确步骤：进入单用户或安全模式、修复问题并恢复文件、确认关键的文件和操作。

可信恢复进程中应该正确应对的安全问题：保护启动顺序、不允许绕过系统日志写入行为、不允许强迫系统关闭、不允许更改日志输出路径。

F、输入和输出控制

应用程序的输入和输出有直接的关联关系，组织需要监控输入中的任何错误和可疑的活动，实施恰当控制，这些措施包括：

- 输入到系统中的数据应格式正确并经过确证，以确保这样的数据不是恶意的；
- 事务应该是原子的，这意味着它们不能在所提供的输入和输出的过程之间中断（原子性可防止称为检验时间/使用时间，或 TOCTOU 的一类攻击）；
- 在线交易必须记录在案并添加时间标记；
- 应该防御措施来确保输出安全到达目的地；

G、系统强化

一般对信息系统进行强化的措施有：

- 确保那些传输重要信息的网络物理组件的安全。
- 开发标准加固镜像，有时也被称为母盘（GM）
- 删除环境不需要的组件
- 使用最保守的设置进行配置
- 制定一个可接受的使用策略（AUP），防止未授权用户在环境中安装未授权软件

H、远程访问安全

为利用远程访问的优势而不必承担无法接受的风险，公司必须实施可靠的远程管理一些远程管理指南：

- 为获得最佳的安全性，需要通过双因素身份验证保护的虚拟专用网络（VPN）连接。
- 不得以明文形式传送命令和数据（也就是说，应对它们进行加密）。
- 应对任何管理活动实施强身份验证。
- 应当在本地而不是远程管理真正关键的系统。
- 应当只允许少数管理员执行这种远程功能。

I、配置云资产

云配置是为用户或用户群提供一种或多种新型云资产时所需的一系列活动。云计算一般分为三种类型的服务：基础设施即服务(IaaS)、平台即服务(PaaS)以及软件即服务(SaaS)。配置每种类型的服务都会呈现其自身的一系列问题。

2.2 检测和防御类措施

A、常见攻击

安全专业人员需要充分了解各种常见攻击方法，只有这样，才能采取相关预防措施，在攻击发生时把它们识别出来以及对攻击做出适当响应。

僵尸网。计算机往往会在感染了某种恶意代码或恶意软件之后被拉进僵尸网，僵尸网中的计算机就像是机器人(被称作傀儡，有时也叫僵尸)，多个僵尸在一个网络中形成一个僵尸网，它们会依照攻击者的指令做任何事情。僵尸牧人通常是一个犯罪分子，他通过一台或多台指挥控制服务器操控僵尸网中的所有计算机。僵尸牧人通常会在僵尸网中指示僵尸发起涉及面很广的各种攻击、发送垃圾邮件和钓鱼邮件，或者将僵尸网出租给其他犯罪分子。

拒绝服务攻击。拒绝服务(DoS)攻击阻止系统处理或响应对资源和对象的合法访问或请求。DoS 攻击的一种常见形式是向服务器传送大量数据包，致使服务器不堪处理重负而瘫痪。其他形式的 DoS 攻击侧重于利用操作系统、服务或应用程序的已知缺点或漏洞。常见的攻击有：

- SYN 洪水（flood）攻击是一种常见 DoS 攻击形式。它破坏传输控制协议（TCP）用来启动通信会话的标准的三次握手。
- Smurf 攻击是洪水攻击的另一种类型，但是它用来淹没受害者的是 Internet 控制消息协议(ICMP)回声包而非 TCP SYN 包。具体来说，它是用受害者 IP 地址充当源 IP 地址的欺骗性广播 ping 请求。
- Fraggle 攻击与 Smurf 攻击相似。但 Fraggle 攻击所利用的不是 ICMP，而是在 UDP 端口 7 和端口 19 上使用 UDP 数据包。Fraggle 攻击利用欺骗性受害者 IP 地址广播 UDP 数据包，结果造成网络上的所有系统都向受害者发送通信流，情形与 Smurf 攻击一样。
- Ping 洪水攻击用 Ping 请求淹没受害者。这种攻击在以 DDoS 攻击形式通过一个僵尸网内的僵尸发起时，成千上万个系统同时向一个系统发送 Ping 请求，这个系统会在回应这些 Ping 请求而无法响应合法请求。
- 死亡之 Ping 攻击使用了超大 Ping 数据包。Ping 包通常只有 32 或 64 位，但不同的操作系统还允许使用其他大小的 Ping 包。死亡之 Ping 攻击将 Ping 包的大小改到 64KB 以上，超出许多系统的处理能力。一个系统收到的 Ping 包若大于 64KB，必然会出问题。某些情况下，系统会崩溃，而在其他情况下，系统会出现缓冲区溢出错误。
- 泪滴攻击，攻击者以一种方式将通信流分割成碎片，使系统无法将数据包重新组合到一起。大数据包通过网络发送时，通常会被分解成较小的片段，接收系统收

到后再将数据包片段重新组合成原始状态。然而，泪滴攻击会把这些数据包打碎，致使系统无法恢复。旧系统遇到这种情况时只能崩溃。

- LAND 攻击，攻击者把受害者的 IP 地址既用作源 IP 地址也用作目标 IP 地址，以这种方式向受害者发送欺骗性 SYN 包，从而形成 LAND 攻击。LAND 攻击诱骗系统不断回复自己，最终导致系统冻结、崩溃或重启。

零日利用是指利用别人还不知道的漏洞的攻击。

恶意代码是指在计算机系统上执行有害、未经授权或未知活动的任何脚本或程序。在第 8 章有详细介绍。

偷渡式下载(drive-by download)是在用户不知情的情况下把代码下载并安装到用户系统上。

中间人攻击。一名恶意用户在进行通信的两个端点之间从逻辑上占据一个位置的情况，就是发生了中间人(MITM)攻击。第 4 章有详细介绍。

蓄意破坏是指员工对自己供职的机构实施破坏的一种犯罪行为。如果员工对机构资产足够了解、有充分访问权限操纵环境的关键方面，同时又内心深感不满，便会变成一种风险。

间谍活动指收集机构专有、秘密、私有、敏感或机密信息的恶意行为。

B、防火墙

防火墙的基本功能和部署在第 4 章中有详细描述。首先，要确定防护墙的安装位置，这通常是根据防火墙能降低的风险所决定的。另外，防火墙通过执行规则来操作的，在操作上的挑战是，如何准确地跟踪当前的规则集，并制定一个程序来确定添加、修改或删除的规则。最后，需要一个计划来定期评估防火墙防御的有效性。

C、入侵检测与防御系统

IDS 通常分为基于主机和基于网络两种类型。基于主机的 IDS（Host-based IDS，HIDS）监测一台计算机或主机。基于网络的 IDS（Network-based IDS，NIDS）通过观察网络通信流模式监测网络。

IDS 评估数据，可通过两种常用方法检测恶意行为：基于知识检测和基于行为检测。简单来说，基于知识检测使用了与反恶意软件程序所用签名定义类似的签名。基于行为检测不使用签名，而将活动与正常表现基线进行对比，从中找出异常行为。

尽管基于知识的 IDS 和基于行为的 IDS 以不同方式检测事件，但它们都使用警报系统。IDS 检测到一个事件后会触发警报。然后，它会以一种被动或主动的方法做出响应。被动响应会记录事件并发出通知。而主动响应除了记录事件和发出通知之外，还会更改环

境以阻止活动。

入侵预防系统（IPS）是一种特殊类型的主动响应 IDS，可赶在攻击到达目标系统之前将其检测出来并加以拦截。与其他任何 IDS 一样，IPS 可使用基于知识检测和或基于行为检测。此外，它还可像 IDS 一样记录活动并向管理员发出通知。

D、补丁管理、漏洞管理、反恶意软件

反恶意软件（俗称杀毒软件）旨在用来检测和消除恶意软件，包括病毒、蠕虫和木马。第 8 章有更多详细描述。

补丁是纠正程序缺陷及漏洞或提高现有软件性能的所有代码类型的总称。软件可以是操作系统或应用程序。补丁有时称为更新、快速修复（quick fix）和热补丁（hotfix）。在安全方面，管理员主要关注修复系统漏洞的安全补丁。有效的补丁管理计划包含常见步骤：

- 评估补丁。当供应商公布或发布补丁时，管理员会对补丁进行评估，确定其是否适用于自己维护的系统。
- 测试补丁。管理员应尽可能在隔离的非生产系统上测试补丁，确定补丁是否导致任何不必要的副作用。
- 审批补丁。管理员测试补丁，并确认补丁是安全的，接下来便批准补丁的部署。
- 部署补丁。经过测试和审批，管理员可以着手部署补丁。
- 验证补丁。验证补丁已完成部署。

“周二补丁日”和“周三利用漏洞日”。微软在每月第二个周二定期发布补丁，攻击者意识到许多组织可能不会立即修补系统，他们使用逆向分析补丁来识别出潜在漏洞，然后构建漏洞利用的方法。

漏洞管理是指定期识别漏洞、评估漏洞并采取措施减轻漏洞相关的风险。漏洞管理计划的两个常见要素，其中：

第 1 个要素--漏洞扫描器，是测试系统和网络是否存在已知安全问题的软件工具。漏洞扫描程序配备了已知安全问题的数据库依照这个数据库来扫描系统。Nessus 是由 Tenable Network Security 管理的常见漏洞扫描器，它结合多种技术来检测各种漏洞。

第 2 个要素--漏洞评估，通常作为风险分析或风险评估的一部分执行，识别系统在某个时间点的漏洞。此外，漏洞评估可以参考其他区域来确定风险。

漏洞通常使用“通用漏洞和披露”(CVE)字典来标识。CVE 字典提供了漏洞标识的标准规约。MITRE 维护 CVE 数据库。

E、沙箱、蜜罐、蜜网

沙箱是一个应用程序的执行环境，它将执行代码与操作系统隔离，以防止危害安全行为的发生。

蜜罐是一种被开发出来的装置，目的是为了欺骗攻击者相信它是一个真实的生产系统，诱使对手对其进行攻击，然后通过监视被破坏的蜜罐，来观察和学习攻击者的行为。蜜网的整个网络都旨在吸引攻击者。一些蜜网是两个或两个以上蜜罐的简单集合；另一些而是自适应网络，它们尽可能长时间地吸引竞争者的攻击。

蜜罐的使用带来了诱惑（Enticement）与诱捕（Entrapment）的问题。如果入侵者不需要经过蜜罐主人刻意诱导就能发现蜜罐，机构可将密罐当作诱惑设备合法使用。而诱捕是非法的，当蜜罐主人主动诱导访客进入网站，然后指控他们未经授权入侵的时候，便是发生了诱捕。

“伪缺陷”是指有意将缺陷植入系统，旨在引诱攻击者的假漏洞或看起来很薄弱的环节。

填充单元系统类似于蜜罐，但是它以另一种方法进行入侵隔离。当 IDS 检测到入侵者时，入侵者会被自动转移到填充单元。填充单元具有真实网络的外观和感觉，但攻击者无法进行任何恶意活动，也无法从填充单元访问任何机密数据。

F、警示和白/黑名单

警示向用户和入侵者宣传基本安全方针策略。警示通常指出，任何在线活动都将接受审计，处于监测之下；警示往往还会提醒用户，哪些是受限活动。

白名单是一组已知良好的资源；相反，黑名单是一组已知的不良资源。最好的情况下，我们要尽量使用白名单；但如果我们不知道所有允许的资源，那就可以使用黑名单。

G、外包服务

有些机构将安全服务外包给第三方，其中可能包括许多不同类型的服务，例如：审计、渗透测试等。安全托管服务提供商（Managed Security Services Providers，MSSP）通常提供各种安全服务的专业机构，从解决方案到接管所有技术或物理安全控制措施的安装、操作和维护。在选择 MSSP 时，需要考虑以下因素：

- 需求 在开始考察潜在 MSSP 时，确定你是否知道你的需求。
- 理解 MSSP 是否理解你的业务流程。
- 声誉 需要花一些时间向一些安全专业人员了解 MSSP 的声誉
- 成本 需要在 MSSP 服务价格和能支付的费用间做出抉择

- 职责 但组织受到攻击时，尽量约定双方的职责，特别是一些在政府监管下的组织

2.3 记录和监控活动实践

A、日志记录和持续监测

日志记录是将有关事件的信息写进日志文件或数据库的过程。日志记录捕捉体现了系统上所发生的活动的事件、变化、消息和其他数据。日志通常会记录一些细节，比如发生了什么，什么时候发生的，在哪里发生的，谁做的，有时候还有是怎么发生的。

日志分多种不同类型，下面是集中在 IT 环境中常见日志类型：

- 安全日志。安全日志记录对文件、文件夹、打印机等资源的访问。
- 系统日志。系统日志记录系统事件，例如系统何时启动或关闭，或服务何时启动或关闭。
- 应用日志。这些日志记录有关具体应用程序的信息。
- 防火墙日志。防火墙日志可记录与到达防火墙的任何通信流相关的事件。
- 代理日志。代理服务器可提高用户访问互联网的效率，还可控制允许用户访问哪些网站。
- 变更日志。变更日志记录系统的变更请求、批准和实际变更，这是变更管理总流程的一个组成部分。

保护日志文件不受未经授权访问和未经授权修改侵扰至关重要。通常的做法是将日志文件拷贝到一个中央系统（例如 SIEM）中保护起来；给日志文件规定许可权，限制对文件的访问，是保护日志文件的一种手段。此外，这些策略还规定了保留日志文件的时间。

审计踪迹是在将有关事件和事发情况的信息保存到一个或多个数据库或日志文件中时创建的记录。它们提供系统活动的记录，可重建安全事件发生之前和事件发展过程中的活动。

信息安全持续监测（Information Security Continuous Monitoring，ISCM），为了保持对信息安全、漏洞和威胁的不断了解，来支撑组织风险管理决策。

日志分析是一种详细和系统化的监测形式，这种监测形式通过分析日志信息找出趋势和模式以及异常、未经授权、非法和违反策略的活动。

抽样也叫数据提取，是指从庞大数据体中提取特定元素，构成有意义的整体表述或归纳的过程。换句话说，抽样是数据压缩的一种形式，它允许安全人员只在审计踪迹中查看一小部分数据样本，便可从中收集到有价值的信息。

剪切是一种非统计抽样。它只选择超过“剪切级”的事件，而剪切级是预先定义好的一个事件阈值。在事件达到这个阈值之前，系统忽略事件。

击键监测是记录用户在物理键盘上的击键动作的行为。击键监测主要被攻击者用于恶

意目的。

B、出口监控

出口监测指对外出通信流进行监测，以防数据外泄 --- 即未经授权将数据发送到机构之外。防止数据外泄的几种常用方法包括使用数据丢失预防技术、寻求尝试隐写术以及通过水印检测未经授权的数据流出，其中：

- 数据丢失预防（DLP）系统旨在检测和阻止数据外泄企图。这些系统能够扫描未经加密的数据，从中找出关键词和数据模式。第 2 章对 DLP 有详细描述。
- 隐写术（steganography）是将一条消息嵌入一份文件的做法（例如：散列值）。
- 水印（watermarking）是将图像或图案不显眼地镶嵌到纸张或文档中的做法。数字水印是隐藏在数字文件中的标记。从出口监测的角度看，DLP 系统从这些水印中识别出敏感数据后，会阻止传输并向安全人员发出警报，可防止文件传出机构。

C、SIEM

许多组织用一种中央应用程序来自动监测网络上的系统，这个系统有好几种名称：安全信息和事件管理（SIEM）、安全事件管理（SEM）和安全信息管理（SIM），它们都是一样的。

SIEM 可在全组织范围内对系统上发生的事件进行实时分析。它们包含安装在远程系统上的代理，用于监测被称为警报触发因素的特定事件。触发因素出现时，代理会将事件报回中央监测软件。

D、效果评价审计

许多组织都制定强力、有效的安全策略。但是，仅仅策略到位并不意味着员工都知道或会遵守这些策略。组织会希望通过审计整个环境来评价安全策略和相关访问控制的执行效果。审计是指对环境进行系统化检查或审查，以确保法规得到遵守并查出异常情况、未经授权事件乃至犯罪行为。常见的效果评价审计有：

- 访问审查审计。许多机构定期进行访问审查和审计，以确保对象访问和账户管理工作将安全策略落到实处。这些审计证明，用户并不拥有过多权限，账户受到了适当管理。这确保安全流程和规程已制定出台，得到机构人员严格遵守并发挥了预期作用
- 用户权限审计。用户权限是指用户被授予的权利。用户需要得到权利和权限(特

权)才能完成自己的工作，但是他们所需要的只是有限的权限。用户权限审计可在用户拥有过多权限，违反了与用户权限相关的安全策略的时候把情况检测出来。

- 特权组审计。许多机构通过划分群组来执行基于角色的访问控制模型。对拥有高级权限的群组（例如管理员组）的成员进行资格上的限制非常重要。确保群组成员只在必要时才使用他们的高权限账号也同样重要，审计可以帮助确定人员是否遵守了这些策略。
- 安全审计。安全审计有助于帮助组织确定正确实现了安全控制。在安全操作域的上下文中， 安全审计有助于确保管理控制到位。主要内容包括：补丁管理审查、漏洞管理审查、配置管理审计、变更管理审计。
- 报告审计结果。审计报告应该有清晰、简洁和客观的结构或设计。
- 保护审计结果。审计报告通常包含敏感信息，它们应该被分配一个分类标签，只有那些有足够特权的人能够访问审计报告。
- 发布审计报告。审计报告完成后， 审计人员将按照安全策略文档中的规定， 将报告提交给指定的收件人。
- 使用外部审计人员。外部审计所表现出来的客观程度是内部审计无法达到的，它们会以一种全新的外部视角来审视内部策略、实践规范和规程。

2.4 事件管理流程

A、网络杀伤链

网络杀伤链（The Cyber Kill Chain）描述了一个七个阶段的入侵模型，此模型已成为行业标准：侦察、武器化、传送、漏洞攻击、安装、命令与控制（C&C）、在目标内的行动。

B、事件响应策略

为什么要做事件响应策略？许多公司在成为网络犯罪的受害者之后毫无头绪，不知道该找谁或者该做些什么。因此，所有公司都应当制订一个事件响应策略，以规定谁具有启动事件响应的权利，并且在事件发生之前建立支持性措施。这个策略应当由法律部门和安全部门管理。这两个部门应该协同工作，确保技术安全问题和与犯罪活动有关的法律问题都能有效得到解决。

事件响应策略和事故管理包括什么？一个事件响应团队；一套标准措施，事故处理应与灾难恢复计划紧密相关，并应成为公司灾难恢复计划的一部分；事件处理还应该与公司的安全培训及认知计划紧密联系，以确保此类不幸不会发生；应当详细说明如何报告一起

事件；

C、事件响应流程

检测：对事件做出反应的第一步，也是最重要的一步是首先意识到组织遇到的问题。

响应：在检测到事件后，下一步是确定怎么适当的响应。

缓解：在事件响应程序的这一阶段，组织应该知道发生了什么，以及认为接下来将会发生什么。下一步是缓解或控制已经或即将对最重要资产造成的损害，其次是缓解次要资产的损害。缓解的目的是阻止或减少此事件造成进一步损害，进而可以开始恢复和修复。

报告：对相关人员进行报告。

恢复：在这一阶段组织将所有系统与信息恢复到已知的良好状态。在恢复系统和信息之前收集证据十分重要。

修复：在修复阶段，要决定需要定为永久的措施（例如防火墙或 IDS/IPS 规则），以及可能需要的额外控制。修复的另一方面是确定攻击的指示（IOA）以及损害的指示（IOC），以便在未来用其实时（例如正发生时）检测攻击，它会告诉组织攻击成功的时间以及安全受到了损害。

学习：事件的终结由事件的性质或类别、期望的事件响应结果（例如业务恢复或系统还原）以及团队成功确定事件源头及根源决定。

单元 3：灾难备份与恢复

3.1 灾难备份与恢复概述

A、灾难的本质

灾难恢复计划围绕组织正常运营中断后，如何控制事件导致的混乱局面，并恢复到正常工作秩序。灾难恢复计划几乎总在高度紧张和头脑可能不那么冷静时执行。停止、阻止或中断组织执行其工作的任何事件都被视为灾难。一旦 IT 无法支持关键任务进程，就需要通过 DRP 来管理还原和恢复过程。

DRP 应该被设置为尽可能自动执行。DRP 还应当尽可能设计成在灾难期间不需要决策。应该对必要的人员进行培训，使他们在灾难发生时承担起相应的责任和任务，以及需要采取的措施，从而使组织尽快恢复运营。

B、MTD、RTO、RPO、WRT

恢复时间目标（RTO）是业务流程在灾难发生后必须恢复到指定服务级别的最长时段。RTO 值比 MTD 值小，因为 MTD 值意味着在此时间段后，如还不能恢复重要的公司业务，将给组织的声誉带来严重或者甚至是不可修复的损失。工作恢复时间（WRT）是在 RTO 已经超时后整个 MTD 值的剩余。RTO 通常指使基础设施和系统恢复运行的时间，而 WRT 指恢复数据、测试流程以及使所有事情“活”过来可以进行生产的时间。

恢复点目标（RPO）指最大可容忍的数据丢失量，用时间来衡量。这个值代表着数据必须恢复的最早时间点。数据量越大，意味着要投入的资金或者其他资源越多，才能确保在灾难事件中损失的数据越少。

平均故障间隔时间（MTBF）是我们期望一台设备能可靠运行的估计时间。平均故障间隔时间（MTBF）通常需要通过测定系统故障之间的平均时间来计算。

平均修复时间（MTTR）是指修复一台设备并使其重新投入生产预计所需的时间。对于冗余队列中的硬盘来说，MTTR 是指实际产生和发现故障后有人替换坏硬盘冗余队列并完成在新硬盘上重写信息之间的时间间隔。

C、危机管理

危机管理是一门科学和技术。如果培训预算允许，对主要员工进行危机培训，这样做至少能确保有一些员工知道如何使用正确的方法处理紧急情况，并对那些受到灾难恐吓的同事起到重要的现场领导作用。

D、应急通信

当灾难来袭时，组织能在内部与外部之间进行通信是很重要的。某些情形下，灾难可能破坏一些或所有的正常通信手段。重大灾难很容易曝光，如果组织无法与外部保持联系，及时向外部告知恢复状况，公众很容易感到害怕并往最坏处想，进而认为组织无法恢复正常。灾难期间，组织内部进行沟通也非常重要，这样员工就知道他们应该做些什么。

E、工作组恢复

在设计灾难恢复计划时，让工作组恢复到正常状态并且重新开始他们在日常工作地点的活动是非常重要的。

3.2 容错、备份和恢复能力

A、保护硬盘驱动器

在计算机中添加容错和系统恢复组件的常见方法是使用 RAID。RAID 包括两个或以上磁盘，即使其中一个磁盘损坏，大多数 RAID 也都能继续运行。一些常见配置如下：

- RAID-0 也称为条带。它使用两个或以上磁盘，它提高了磁盘子系统的性能，但不提供容错能力。
- RAID-1 也称为镜像。它使用两个磁盘，每个磁盘保存相同的数据。如果一个磁盘损坏，另一个磁盘仍保存完整的数据，这样在一个磁盘损坏后，系统仍能继续运行。
- RAID-5 也称为奇偶校验。它使用三个或更多磁盘，相当于一个磁盘， 其中包含奇偶校验信息。如果一个磁盘损坏，磁盘阵列会继续运行，但速度会慢一些。
- RAID-10 也被称为 RAID1+0 或条带镜像，是在条带(RAID-0)配置上再配置两个或以上的镜像(RAID-1)。它至少需要 4 个磁盘，当然也可以更多，增加磁盘数以偶数计。即使多个磁盘损坏，只要每个镜像中有一个驱动器是好的，它就能继续运行。

B、高可用

高可用性(HA)是保证一些业务始终正常运行的一种技术和流程的结合。具体业务可能是一个数据库、一个网络、一个应用程序、一个电源等。

可通过故障转移集群将容错功能添加到关键服务器中。故障转移集群含有两个或以上的服务器，如果其中一台服务器出现故障，集群中的其他服务器可通过称为故障转移的自动化过程接管其负载。故障转移集群可包含多台服务器(不只是两台)，它们可为多个服务或应用提供容错功能。

C、数据备份和恢复

完全备份（full backup）就是对所有数据进行备份，并将其保存在某种存储介质上。

差量过程（differential process）对最近完全备份以来发生改变的文件进行备份。

增量过程（incremental process）对最近完全备份或增量备份以来发生改变的所有文件进行备份。

用于创建远程数据库内容备份的三种主要技术手段：

- 电子链接。在电子链接这种情况中，数据库备份通过批量传送的方式转移到远处的某个场所。
- 远程日志处理。远程日志处理以一种更快的方式传输数据，与电子链接不同，在

数据库备份文件被转移时，远程日志处理设置传输数据库事务日志的副本，其中包括从上次批量传输以来发生的事务。

- 远程镜像。远程镜像是最先进的数据库备份解决方案，也是费用最昂贵的。使用远程镜像时，实时数据库服务器在备份站点进行维护，将数据库修改应用于主站点的生产服务器时，远程服务器同时收到副本。

D、可替代的工作站点

热站点（hot site）一般配置比较完善，在几个小时内就可以投入运行。热站点唯一缺乏的资源是数据（数据要从一个备份站点检索得到）和处理数据的人员。这里的设备和系统软件必须与从主站点还原的数据完全兼容，并且绝不能导致任何负面的互用性问题。

温站点（warm site）只进行了部分配置，使用了一些设备（如 HVAC）和基础设施组件，并非实际的计算机。换句话说，温站点可以说成是一个没有配备昂贵设备（如通信设备和服务器）的热站点。

冷站点（cold site）提供基本的环境、电源线路、空调、管道和地板，但不提供设备或其他服务。冷站点基本上就是一个空数据中心。

冗余站点（redundant site），即一个设备和配置与主站点完全相同的站点，并将其作为一个冗余环境。两个站点的业务处理能力可以完全一样。这些场所由公司所有，并且是原始产品环境的镜像。

滚动热站点（rolling hot site）或移动站点，这种方法将一辆大型卡车或拖车的后部转变成一个数据处理或工作区域。这是一个移动的、自给自足的数据设施。拖车内配备必要的电源、通信和系统，以便能立即进行处理工作。拖车可停放在公司停车场或其他地方。拖车必须被带到新站点，数据也需要恢复，必要的人员也需要到位。

服务局拥有额外的空间和能力，以及能提供应用程序和诸如呼叫中心的服务。公司可按月付费租用这些空间和服务，也可在出现突发事件（如灾害和紧急情况）时再付费。

云计算，许多组织现在把云计算作为首选的灾难恢复选项。希望保留自己数据中心的公司，可以选择使用这些 IaaS 服务作为备份服务提供商。在云中存储准备运行的镜像是经济实惠的，在云站点激活前能节省大部分运营成本。

互惠协议也称为相互援助协议（MAA），在灾难恢复的文章中非常流行，但在真实世界中很少被实施。理论上，相互援助协议提供了优秀的可供选择的方案。在 MAA 下，两个组织承诺在灾难发生时通过共享计算设施或其他技术资源彼此援助。在事实上，相互援助协议存在许多缺点：

- MAA 很难强制实施。协议参与各方要彼此信任，在灾难发生时能给予实际的支持。但当真正出现灾难时，非受害方可能会拒绝履行协议，受害方只能通过法律手段取得赔偿，但这样对灾难恢复工作并没有任何帮助。

- 出于对保密性的考虑，公司通常会阻止将自己的数据交给其他公司。

3.3 灾难恢复计划制定

A、为计划制定目标

建立目标对业务连续性和恢复计划尤为重要。定义目标有助于指导资源和任务的合理分配，制定必要的战略，以及对计划和程序的整体经济性作出合理判断。一旦设定目标，它们就能为计划的实际制定过程提供指导。确定目标能使人们不会脱离正轨，确保我们所做的努力最终得到回报。实用的计划目标必须包括以下关键信息：

- 责任。每个参与恢复和连续性计划的个人都应将他们的责任以书面形式列出，以便在混乱时能够明确自己的责任。每项任务都应当分配给在逻辑上最适合于处理它的人员。这些人员必须了解他们的职责，而这需要通过培训、演练、通信和文档来培养意识。
- 权威。在危急时刻，知道由谁负责很重要。明确的权威有助于减少混乱，促进合作。
- 优先级别。了解哪些是关键工作、哪些是次要工作也极为重要。总体的优先级别应在各部门和 IT 员工的帮助下由管理层来制定。
- 实现与测试。一旦制定了连续性计划，就必须将它付诸实现。公司需要将其文本化，并存放在危急时刻容易取得的地方。公司需要对那些被分配特殊任务的人员进行培训，教导他们如何执行这些任务，同时需要进行模拟演习，以帮助人们适应各种不同的状况。一年至少应该进行一次演习，整个计划应该不断进行更新和完善。

B、人员角色

BCP（或 DRP）协调员需要组建几个不同的团队，并对它们进行正确培训。下面是组织机构可能需要组建的一些团队示例：破坏评估团队、法律团队、媒体关系团队、恢复团队、重新部署团队、重建团队、救援团队、安全团队等。BCP（或 DRP）协调员应当了解公司组建并培训各种团队的需要，应根据员工的知识和技能将他们分配到特定的团队。重建团队(restoration team)应当负责使备用站点投入运行，而救援团队(Salvage team)应当负责开始恢复原始站点。BCP 必须概括说明这些特殊的团队、它们的责任和通知措施。计划还必须指出在营业时间和营业时间以外联系团队主管的方法。

C、破坏评估

一旦发生灾难，还需要设立一个角色或建立一个团队来完成评估破坏工作。

评估程序应当正确记录在文档中，应包括以下步骤:

- 确定灾难的成因。
- 确定进一步破坏的可能性。
- 标识受到影响的业务功能和领域。
- 标识关键资源的可用程度。
- 标识必须立即替换的资源。
- 估计需要多久才能恢复关键功能。
- 如果还原过程超过了事先估计的 MTD 值，那么应立即声明为灾难，并且立即启动 BCP。

因为组织机构间的业务推动力和关键功能各不相同，所以不同的组织机构具有不同的准则。这个准则可能包括以下一些或所有元素：

- 对人员生命的威胁。
- 对州/省或国家安全的威胁。
- 对设施的破坏。
- 对关键系统的破坏。
- 公司将经历的估计停工时间。

D、恢复阶段

完成破坏评估并启动恢复计划后，就必须对各种团队进行部署，这标志着公司进入恢复阶段。每个团队都有自己的任务，为使组织机构尽快恢复正常运作，恢复过程必须尽可能有组织地进行。

实际执行比在书面上进行陈述面临更大困难，这也是书面过程十分关键的原因。在 BIA 期间，关键功能及其资源会被标识。所有团队需要团结协作，首先恢复这些关键功能和资源。

当公司开始搬回它原来的场所或搬进一个新设施时，公司即进入再造阶段（reconstitution phase）。直到公司在它原来的主站点或一个建立起来替代主站点的新设施内恢复运作,公司才脱离紧急状态，因为如果在一个备用设施中运作，那么往往易于受到攻击。

E、BCP 和 DRP

BCP 团队完成下列步骤：

1、提出连续性规划策略声明。

- 说明 BCP 的作用域和目标以及 BCP 团队的职责。

2、执行业务影响分析(Business Impact Analysis, BIA)。

- 标识关键业务功能、它们的资源和 MTD 值。
- 标识威胁并计算这些威胁的影响。
- 确定解决方案。
- 向管理层提交结果。

3、确定和实现预防性控制。

- 实施控制， 降低公司已标识的风险。
- 购买保险。
- 加固基础设施 。
- 提出数据备份解决方案。
- 安装冗余和容错机制。

4、制定恢复战略。

- 在必要时实现使公司恢复正常运作的过程。
- 组建必要的团队。
- 为每个团队制定目标和措施。
- 建立通告步骤和计划启动准则，
- 确定备用的备份解决方案等。

5、测试和培训

6、持续维护计划

DRP 团队完成下列步骤：

1、起始阶段

- 目标声明
- 概念概述
- 角色与团队定义
- 任务定义

2、启动阶段

- 通告步骤
- 破坏评估
- 计划启动

3、恢复阶段

- 转移到备份站点
- 重建过程
- 恢复步骤

4、再造阶段

- 还原设施
- 测试环境
- 转移操作

5、附录

- 联系信息
- 其他计划类型
- 图表
- 系统需求

3.4 灾难恢复计划测试

A、灾难恢复计划测试方法

每一种灾难恢复计划都必须定期进行测试，以确保计划的条款是可行的并且符合组织变化的需要。可以实施的测试类型依赖于能够使用的恢复设施的类型、企业文化和灾难恢复团队成员的可用性。5 种主要的测试类型：

- 通读测试。在这类测试中，只需要向灾难恢复团队成员分发灾难恢复清单的副本，并要求他们审查。
- 结构化演练。在这种经常称为“桌面练习”的测试类型中，灾难恢复团队成员聚集在一间大会议室中，不同的人扮演灾难发生时的不同角色。成员通过参考灾难恢复计划对特定的灾难进行讨论，进而得出适当的响应办法。
- 模拟测试。模拟测试与结构化演练类似。模拟测试向灾难恢复团队成员呈现情景并要求他们做出适当的响应措施。与前面讨论的测试不同，其中某些响应措施随后会被测试。这种测试可能会中断非关键的业务活动并使用某些操作人员。
- 并行测试。并行测试涉及将实际人员重新部署到替换的恢复场所并实施场所启用过程。被重新部署到该场所的员工，以灾难实际发生时的方式履行他们的灾难恢复职责。唯一的差别在于不会中断主要设施的运营，这个场所仍然处理组织的日常业务。
- 完全中断测试。完全中断测试与并行测试的操作方式类似，但涉及实际关闭主场所的运营并将其转移至恢复场所。这类测试有很大的风险，因为它们要求停掉主

站点的操作，并转移到恢复站点。测试完成后，在主站点执行恢复操作的反向过程。

B、了解如何维护灾难恢复计划

随着组织需求的变化，必须对灾难恢复计划进行修改以符合变化的需要。灾难恢复计划是一份灵活的文档，通过使用组织好的和协调一致的测试计划，我们会发现灾难恢复计划中需要修改的地方。大多数组织都应用正式的变更管理过程，这样在基础设施发生更改时能够更新和检查所有相关的文档，以便反映更改。

C、了解通过保险降低灾难影响损失的相关内容

在业务影响分析阶段，团队很可能发现组织机构无法预防的一些威胁。为这些威胁承担全部风险往往非常危险，这就是我们购买保险的原因。

公司可以购买不同的保险，网络保险就是其中之一。网络保险(cyber insurance)是一种新型保险项目，它为由拒绝服务攻击、恶意软件破坏、黑客、电子盗窃、与隐私有关的法律诉讼以及其他事件造成的损失提供保险。公司还可选择购买一种业务中断保险(business interruption insurance)策略。购买这种保险后，如果公司停业一段时间，那么保险公司将赔付指定的开支和损失的收入。

保险范围有其限制，如果一家公司没有采取“应尽关注”，那么一旦发生灾难，保险公司就可能会依法拒绝赔付损失。重要的是，应该阅读和理解相应的保险条款，保证自己完全了解公司的责任，而不仅是保险公司的义务。

D8：软件开发安全

单元 1：在开发生命周期中应用安全

1.1 软件开发安全的重要性

A、软件代码安全质量

在开发安全软件时，安全质量是最重要的概念。我们可以通过这样一个过程来确保软件的安全：理解应用程序的安全需求，实现正确的安全控制和安全机制，彻底测试这些安全机制以及它们在应用程序中的集成方式，遵循结构化开发方法，提供安全可靠的分发方法。

B、产生应用安全问题的原因和分析

“外强内弱”的环境。为解决安全问题，很多人都将目光投向安全控制，如防火墙、入侵检测系统(IDS)、内容过滤、防病毒软件、脆弱性扫描器等。导致人们倾向于诉诸周边设备（而不是软件开发）解决安全问题，原因在于：

- 在软件开发阶段，安全不是重要的考虑因素。因此，现在还有很多编程人员并不进行这方面的考虑。
- 很多安全从业人员往往不是软件开发人员，因此没有通盘考虑软件脆弱性问题。
- 很多软件开发人员没有将安全视为一个重点。他们通常认为功能性比安全性更重要。
- 软件供应商为了最快地把产品投入市场，往往没有给正确、安全的架构、设计和测试步骤留太多时间。
- 人们已经习惯了接受带有缺陷的软件，然后进行修补，这已经成了一个常见的且似乎可以接受的做法。
- 客户无法控制所购买软件中的缺陷，他们必须依赖周界保护

对于以上这些现状，我们可以看出：

- 不同的环境需要不同的安全。由于环境的复杂性日益增长时，跟踪错误和安全危害的任务将变得极其困难。
- 环境与应用程序。软件控制可以通过操作系统、应用程序或者数据库管理控制来实现，实际应用中通常组合了上述两种控制方式。每一种控制方式都有自己的长处和弱点，但是如果能够充分理解这些特点，并且在编程时给予足够的注意，就

可以避免许多不同类型的危害。

- 功能与安全。编程人员和应用程序设计人员需要寻找一个功能需求、安全需求以及安全机制方面之间的平衡点，这将会给本已十分复杂的应用程序开发任务增加更多复杂性。
- 实现和默认配置问题。由于软件供应商始终将用户友好性和功能性放在首位，因此其产品的默认安装往往只提供很低的安全保护级别，甚至没有。

1.2 软件开发生命周期和模型

A、软件开发生命周期（SDLC）的不同阶段

软件开发生命周期（SDLC）包括以下阶段：

1、需求收集阶段

在这个阶段，涉及的每个人都想方设法理解需要该项目的原因和该项目所涵盖的范围。在安全方面，这个阶段应该完成下列工作：

- 安全需求：产品的安全需求应该从可用性、完整性和机密性几个方面进行定义。
- 安全风险评估：应该进行初步安全风险评估，以标识潜在风险和它们相关后果。
- 隐私风险评估：进行隐私风险评估，之后进行隐私影响评级，指明可访问数据或者将要处理的数据的敏感级别。
- 风险级别验收：需要开发一个明确的风险级别验收标准来确保把减少风险工作放在首位，并对安全控制便会有一个明确的方向，在设计和开发阶段便可以遵循这个方向。

2、设计阶段

软件设计阶段是用来描述需求和软件产品内部行为的一个过程。它把这两种元素联系在一起，以显示内部行为如何真正实现已定义的需求。软件需求往往来自下面 3 种模型:

- 信息模型，规定要处理的信息类型和处理方式。
- 功能模型，概述应用程序 需要执行的任务和功能。
- 行为模型，解释在具体事务处理发生过程中和发生之后应用程序的状态。

从安全角度讲，下列事项也应该在这个阶段完成：

- 攻击面分析：攻击面是攻击者用来攻击产品的地方。攻击面分析的目的是识别和减少可以被不可信用户访问的代码和功能的数量。
- 威胁建模：威胁建模是了解不同威胁如何实现、破坏如何成功进行的系统方法。

3、开发阶段

编程人员可以使用多种计算机辅助软件工程(CASE)工具来生成代码、测试软件和进行调试活动。理解安全编码做法，并将其集成进入到 SDLC 的开发阶段非常重要。静态分析提

供了可升级的安全代码审核方法，确保遵循了安全编码策略。

4、测试/验证阶段

由于希望寻找各种潜在的缺陷，因此存在不同类型的软件测试方法。下面列出了一些最常用的测试方法：

- 动态分析
- 模糊
- 人工测试
- 单元、集成、接受和回归测试

5、发布/维护阶段

一旦开发和正确测试好软件编码，就可以发布并把它安装在预期的生产环境中。之后还会发现新问题和新漏洞，可能需要开发人员改变编码、重新测试编码和重新发布编码。

从安全角度看，几乎每天都会发现新漏洞。虽然开发人员会进行大量的安全测试，但几乎也可能在同一时间和地点识别所有安全问题。开发团队必须开发补丁、修补程序和发布新版本来解决这些问题。验证（verifiatin）判断产品是否准确体现和满足了产品规范。毕竟，开发出来的产品有可能与初始规范不匹配。这一步骤能确保正确满足了规范。确认（validation）判断产品是否为所针对的实际问题提供了必要的解决方案。

零日漏洞是目前还没有找到解决方案的漏洞。如果发现了一个脆弱性，且预先没有修补方式（补丁、配置和升级），就被成为是零日漏洞。

B、软件开发项目管理

工作声明（SOW），描述了产品和客户的要求。详细的 SOW 将有助于开发人员正确理解需求，而不是靠假想和猜测行事。

工作分解结构（WBS）是一个项目管理工具，用来定义和有序分组项目的各工作单元。这是将项目故意分解为:目标是明确定义的可交付成果的任务和子任务。应该以 WBS 格式来描述 SDLC，这样每个阶段都会得到妥善解决。

甘特图是一种显示不同时间项目和调度之间相互关系的条形图，提供了帮助计划、协调和跟踪项目中特定任务的调度图表。

计划评审技术（PERT）是一种项目调度工具，这种工具被用于在开发中判断软件产品的大小并为风险评估计算标准偏差。

C、软件开发模型

瀑布模型。瀑布模型采用的是线性生命周期方法，包括：可行性、分析、设计、实施、测试、维护。每个阶段都必须完全完成，下一阶段才可以开始。在每个阶段结束时，

要回顾一下，以确保该项目处于正确的路线上，并决定该项目是否应该继续。

V 形模型。V 形模型是在瀑布模型后开发的。在软件开发过程中不再按照平面的线性方法，而是遵循 v 型格式的步骤。这种模型强调产品在每个阶段进行验证和确认，并为每个编码阶段实施提供了正式的开发测试计划。

原型模式。在投入大量时间和资源之前，可以开发软件代码的样品或模型（原型）来探索特定问题的解决方法。一个团队可以使用原型开展工作，将可以标识可用性和设计上的问题，并能根据需要调整工作方法。在软件开发行业有 3 个主要的原型模型已经被发明和普及。它们是快速原型、演化原型和运行原型。

增量模型。如果一个开发团队遵循增量模型，这能让他们在一个软件开发的全过程进行多个开发周期。这类似于“多个瀑布”周期出现在同一个软件上，在开发阶段不断走向成熟。在第一次迭代时创建了一个版本的软件，然后它会经历下一次迭代的每个过程(需求分析、设计、编码、测试和实施)。

螺旋模型。

快速应用开发。快速应用开发模型更多地依赖于快速原型的使用，而不是大量的前期规划。快速应用开发模型结合了原型化方法和以加速软件开发过程为宗旨的法代开发方法。

敏捷模型。敏捷模型是几种开发方法论的总称。它的重点不在严格的、线性的阶梯式过程上，而在增量和迭代的开发方法上，目的是促进跨部]的团队合作和持续的反馈机制。在许多敏捷方法中，有一个值得注意的元素是他们关注用户体验。敏捷模型另一个重要特点是，开发团队可采用所有可用的 SDLC 方法，并可以根据特定项目需求以最佳方式组合它们。这些不同的组合可产生很多敏捷模型下的方法论：敏捷开发、极限编程、看板管理。

其它模型。探索型模型是一种在还没有明确定义项目目标的实例中使用的方法。联合分析开发(JAD)在一个由工作组构成的环境中，采用团队协作的方法开展应用程序开发的方法。复用模型它是一个采用先进开发模型的近似软件开发的模型。净室模型是一种方法，试图通过结构化和形式化方法的开发和测试，以防止错误或失误。

D、集成开发团队和 DevOps

集成产品开发团队（IPT）是一支多元开发团队，团队成员为各利益相关方的代表。一个全面的 IPT 包括业务主管和最终用户以及其中的每一个人。IPT 不是一种开发方法。相反，它是一种管理技术。当项目经理决定使用 IPT，那么他们就必须选择一个开发方法。近来，IPT 经常与敏捷方法联系在一起。

DevOps 是将开发、IT、质量保证（QA）工作人员组成同一软件开发项目团队的实践，这将统一他们的目标，提高他们的效率，并减少对软件产品的依赖。

E、能力成熟度模型

能力成熟度模型集成(CMMI)集成了一整套产品和软件开发指南，它涉及软件开发生命周期的不同阶段。该模型描述了软件开发流程的基本规程、原则和实践，并帮助软件公司改善软件开发过程，将一些“突发奇想”的行为变成一个有规律、可重复的步骤，从而提高软件质量，缩短开发周期，提供更好的项目管理能力。

使用的成熟度级别有下列 5 种：

第 1 级：初始 开发过程很随意，甚至非常混乱。该公司没有使用一个有效的管理流程和计划。没有一致性的保证，质量不可预测

第 2 级：可重复 正式的管理结构、变更控制和质量保证。该公司可以在不同项目中适当地重复一些过程。该公司并没有定义正式的过程模型

第 3 级：定义 有正式流程，其中描述和定义了在不同项目中的过程。该公司有方法对过程进行定量的改善

第 4 级：管理 公司有一个正式的过程， 可收集和分析定性数据。度量被定义并提供给过程改善程序

第 5 级：优化 公司对持续改善过程有了预算和整体计划

1.3 变更控制

A、软件变更的原因

有多种原因可引发变更。在开发阶段，客户可能修改需求并要求追加、删除或修改一些功能。在生产阶段，可能由于环境的变化引发变更，比如新的软件产品、系统需求、新发布的补丁或升级包。

B、变更控制和步骤

变更控制是为了控制信息系统在其生命周期中发生的特定变更，并记录必要的变更控制活动的过程。变更应加以控制，确保它们经过审批，调整得当，而不会对任何原有功能造成不利影响。变更控制是控制变化的过程，发生在系统的生命周期过程中，并能记录必要的变更控制活动。在系统审计时需要检查变更控制实施和加强的流程。以下是一些必要的变更控制过程的步骤:

1、为变更提出正式申请

2、分析这个申请，包括分析开发实现策略、计算实现成本、审查任何安全问题

3、记录变更申请

4、提交变更申请以获批准

5、开发变更。包括重新编码产品程序段，并添加或删减功能；将变更的代码链接到正式的变更控制申请中；为测试和质量审核提交软件；重复过程直到能够保障质量；记录变更版本。

6、报告结果给管理层。系统的变更可能需要新一轮的认证和认可。如果系统发生重大变化，那么在功能方面和保护级别上可能需要重新评估（认证），管理层需要批示整个系统，其中包括新的变更（认可）。

1.4 编程语言、分布式和移动代码

A、编程语言概述

编程语言有下列几种类型：

第一代：机器语言 是计算机和处理器可以理解的语言，并且可以直接执行

第二代：汇编语言 是机器级别指令的符号表示

第三代：高级语言 使用抽象陈述，抽象把多个汇编语言指令集归为一个高级语句

第四代：非常高级语言 在第三代基础上进一步改进了自然语言方法

第五代：自然语言 终极目标是无须拥有编程经验，而只是使用高级的知识型处理过程和人工智能。

汇编程序（Assemblers）将汇编语言源代码翻译成机器代码。汇编语言包括处理器理解不了的记忆术，因此需要翻译成操作指令。

编译器（Compiler）开发人员可以用高级语言一次性开发出软件代码，然后被编译得适用于各种平台。

如果编程语言被认为是“可解释的”，那么解释器(interpreter)便最终把高级代码转换成机器代码。例如用 Java 写成的程序可将它们的源代码编译成一种称为 bytecode 的中间代码，当应用程序的指令需要运行时，它们在 Java 虚拟机（JVM）中执行。JVM 有一个专门适用于它所安装的特定平台的解释器，这个解释器把 bytecode 转换成可供机器执行的形式。

C 语言是高级语言，主要问题有：C 标准软件库不检查它们默认操作的数据串的长度，因此 C 语言编写的程序非常容易出现缓冲区溢出和格式串错误。C 语言缺少自动执行垃圾收集，要求开发人员手动执行，于是就给错误以可乘之机。

B、面向对象相关概念

面向对象开发 OOP，使用了类和对象的概念。为了说明这两个概念，我们举一个实际

中例子，如一张桌子，就是一个“对象”，它是名为“家具”的一个大类中的一个成员（或实例）。

理解了 OOP 的概念后，我们需要了解 OOP 相关的特性：

- 封装。对象封装了属性值，这也就意味着信息被包装，以对象名的形式被其他对象视为一个整体进行重用。对象之间需要能够互相通信，这通过使用传递到接收对象的 API 的消息完成。
- 抽象。抽象是忽略非必要的细节而只关注重要的内在特征的能力。
- 多态。多态是不同对象以不同方式响应相同的命令、输入或消息。

数据结构是对数据元素之间逻辑关系的表示。数据结构指明了元素间关联的程度、访问方法、处理选择以及数据元素的组织。从安全角度看，不仅需要了解一款架构和设计不太精良的软件的脆弱性，还需要了解这个软件组件彼此相连的复杂性和所有数据格式的类型。

内聚（cohesion）是反映某个模块能执行多少种不同类型的任务的术语。如果某个模块只执行一个任务（减法）或几个非常相似的任务(加、减、乘)，就认为该模块高内聚。

耦合是一种度量， 表示一个模块完成其任务需要进行多少交互。如果一个模块低(松散)耦合，就表示该模块在执行其任务时不需要与太多的其他模块通信。高(紧密)耦合表示一个模块在执行其任务时需要依赖其他许多模块。

内聚和耦合的复杂程度直接关系到程序的安全性。某件东西越复杂，就越难保证其安全。开发紧密代码不仅提高效率和有效性，还能降低软件的攻击面。降低复杂性便很可能减少坏人进入的可能性。但是，变量和可移动组件越少，监管起来越方便，也容易保证其安全。

应用编程接口正是描述了一个软件组件与另一个软件组件的连接。

C、分布式计算环境和框架

分布式计算环境（DCE）是一个标准，是一个客户端/服务器框架，该框架描述了各种能力如何在异质系统之间集成和共享。DCE 提供 RPC 服务、安全服务、目录服务、时间服务、分布式文件支持等。DCE 是通过客户端/服务器模型来标准化异类系统通信的首个尝试，尽管人们很难在生产系统上发现这样的运行过程，但它为分布式计算技术提供了许多基本概念，例如：CORBA、DCOM 和 J2EE。

公共对象请求代理架构(CORBA)是由对象管理组（OMG）开发的一个开放式面向对象的标准架构，它为目前环境中大量不同的软件、平台和硬件提供互操作性。CORBA 模型包含两个主要部分：面向系统的组件（对象请求代理(ORB)和对象服务）和面向应用程序的组件(应用程序对象和通用工具)。ORB 是建立对象间客户端/服务器关系的中间件，当客户端需要访问服务器上的对象并请求该对象执行某个操作或者方法时，那么 ORB 就拦截请求并负

责寻找对象。一旦找到对象， ORB 会调用一个方法(或操作)，传递参数，并将结果返回给客户端。

组件对象模型(COM)是一种允许某个应用程序内或相同计算机系统上不同应用程序之间实现进程间通信的机制。这种模型由 Microsoft 公司创建，并列出了标准化的 API、组件命名机制和通信标准。分布式组件对象模型(DCOM)不仅支持同样的用于组件交互的模型，还支持分布式(IPC)。COM 使应用程序能使用相同系统上的组件，而 DCOM 则使应用程序能访问驻留在网络不同部分的对象。基于 COM 的操作系统和/或应用程序正是这样执行基于客户端/服务器的活动。对象链接和嵌入(OLE)为在本地个人计算机上共享对象提供了一种方式，并使用 COM 作为其基础。OLE 使对象(如图形、图片和电子表格)可嵌入文档中。一个程序调用另一个程序的能力称为链接。

Java 平台企业版本(J2EE)是基于 Java 编程语言的分布式计算模型，是一个用来开发主要用 Java 编程语言编写的企业软件的框架。它提供网络直连服务的 API、容错、安全、大型 Web 服务和多层网络应用程序。

面向服务的架构(SOA)提供了标准化访问，这样可在同一时刻访问不同应用程序中最需要的服务。它将应用程序分为不同的功能单元(称为服务)，通过这些服务之间定义良好的接口和数据共享标准联系起来。简单对象访问协议(SOAP)是一种基于 XML 的协议，它用于在网络服务环境下为信息编码，实际上定义了在 XML 模式下通信是如何发生的。SOAP XML 模式定义了对象如何直接交流。

D、移动代码

能通过网络传送并由另一端的系统或设备执行的代码称为移动代码。主要包括：

1、Java applet。Java 作为一种完全成熟的编程语言使用，并用于编写一种在用户的浏览器上运行的、名为 applet 的小程序。过程如下：

- 编程人员创建 Java applet 并在编译器上运行。
- Java 编译器将源代码转换为字节码(与处理器无关)。
- 用户下载 Java applet。
- JVM 将字节码转换为机器语言(针对具体处理器)。
- Java applet 在调用时运行。

当 applet 执行时，JVM 将在一个名为沙箱的环境中创建一个虚拟机。沙箱严格限制 applet 对任何系统资源的访问，JVM 可调节对系统资源的访问，以确保 applet 代码“行为良好”，停留在自己的沙箱内。但是如果 applet 代码在本质上就是恶意代码，可能会危害用户和用户的系统。

2、ActiveX 控件。ActiveX 是一种由 Microsoft 公司开发的技术，它由一组基于 COM 和 DCOM 的 OOP 技术 1001 与工具构成。编程人员使用这些工具创建 ActiveX 控件，这种控

件是类似于 Java applet 的独立程序。当对象链接和嵌入用来嵌入 ActiveX 控件到 Web 页面中时，ActiveX 控件共享系统上当前用户的权限，由于人人都能构建这些控件，所以恶意的 ActiveX 控件拥有充分的权限来破坏该系统和与之相连的其他系统的安全。

1.5 数据库管理

A、数据库管理系统

数据库是以某种有意义的方式存储的数据的集合，它允许用户和应用程序在需要时访问、查看和更改数据。任何类型的数据库都具有下列特征:

- 它将数据保存在网络中的几台不同服务器上，从而方便进行集中化管理。
- 它的备份过程更容易。
- 它提供事务处理持续化。
- 它提供恢复和容错。
- 它允许多个用户共享数据。
- 它提供安全控制，以实现完整性检查、访问控制和必要的机密性级别。

事务处理持续化意味着执行事务处理的数据库过程是持久可靠的。在进行事务处理后，数据库的安全状态应保持原状，同时需要确保事务处理的完整性。

数据库由能提供这些功能的软件管理，该软件还可实施访问控制限制，提供数据完整性和冗余，以及为数据操作建立不同的过程，这种软件称为数据库管理系统(DBMS)。DBMS 通常由数据库管理员控制，DBMS 与程序、用户和数据库内的数据进行交互，它帮助我们更有效地存储、组织和检索信息。

B、数据库模型和相关概念

数据库模型定义了不同数据元素之间的关系，规定了如何访问数据，并定义了可接受的数据操作、提供的数据完整性类型以及这些数据的组织方式。数据库模型不仅提供了一个使用概念化形式表示数据的正式方法，还提供数据库中存储的数据的必要操作方式。如下所示，数据库可采用若干种模型:

- 关系数据库模型：使用属性(列)和元组(行)来包含和组织信息
- 层次数据库模型：组合了在逻辑树结构中相关联的记录和字段，例如 LDAP
- 网络数据库模型：构建在层次数据库模型之上，允许每个数据元素拥有多个父节点和子记录
- 面向对象的数据库模型：可设计为管理多种不同类型的数据（图像、语音、文档和视频）

- 对象-关系数据库模型：是一种具有以面向对象编程语言编写的软件前端的关系数据库

一些重要的数据库术语：

- 记录（record） 关系数据项的集合
- 文件（file）相同类型记录的集合
- 数据库(database) 数据的交叉引用集合
- 数据库管理系统(DBMS) 管理和控制数据库
- 组（tuple） 二维数据库中的行(或记录)
- 属性（attribute） 二维数据 库中的列
- 主键（primary key）使每一行（或每一条记录）区别于其他行的列（一个表中的每一行都必须包含一个主键）。
- 视图（view）为控制主体查看特定数据而定义的虚拟关系。
- 外键(foreign key) 一个表中的某个属性，与其他表的主键相关联。
- 存储单元（cell） 行和列的交汇点。
- 模式（schema） 定义数据库的结构。
- 数据字典(data dictionary) 描述数据元素及其关系的中心存储库。

如果不能访问和处理数据，那么数据就没有用处。应用程序不仅需要与存储在数据库中的数据交互，还需要某种接口和通信机制。下面介绍一些这样的接口语言：

- 开放数据库连接(ODBC)一个应用编程接口(API)，允许应用程序与本地的或者远程的数据库通信。
- 对象链接和嵌入数据库(OLE DB)作为中间件运行在客户端或者服务器上，将数据分成多个组成部分。
- ActiveX 数据对象(ADO) 一个允许应用程序访问后端数据库系统的 API。
- Java 数据库互连(JDBC)是一个允许 Java 应用程序与数据库通信的 API。

数据库软件执行 3 种主要类型的完整性服务:

语义完整性(semantic integrity) 该机制保证结构化规则和语义规则得到遵守。这些规则与以下因素有关：数据类型、逻辑值、唯一性约束以及可能负面影响到数据库结构的操作。

参考完整性(referential integrty) 如果所有外键都参考现有的主键，那么数据库就具有参考完整性。 应通过某种机制确保没有外键引用不存在的记录的主键或者空值。

实体完整性(entity integrity) 保证了元组由主键值唯一确定。

C、数据库安全问题和措施

聚合(aggregation) 指的是组合不同来源的信息的行为。用户没有明确的权限可访问

组合得到的信息，但组合得到的信息比信息的各个组成部分拥有更高敏感性。为防止聚合，需要防止主体和代表主体的应用程序或进程获得对整个数据集合的访问权限，包括集合的各个独立组成部分。

推理（inference） 当安全级别较低的数据可描述出较高安全级别的数据时，就会发生推理攻击。为了防止，一个对策是防止主体或代表主体的应用程序和进程间接得到可推理的信息。在数据库开发过程中，往往可通过实现内容相关和上下文相关访问控制来解决这个问题。内容相关访问控制基于数据的敏感度,数据的敏感度越高，能访问这些数据的个体就越少。上下文相关访问控制指的是软件根据请求的状态和顺序来“了解”应当允许哪些动作。这就是说，用户必须跟踪用户以前的访问尝试，并知道允许的访问步骤顺序。

显而易见，根据系统所需处理数据的数量，内容相关访问控制没有上下文相关访问控制复杂。防止推理攻击的常见措施有单元抑制、数据库分隔、噪声和扰动。

- 单元抑制（cell supesion）是一种用于隐藏特定单元的技术，这些单元包含的信总能用在推理攻击中。
- 分隔（partition）数据库涉及将数据库分成不同的部分，这可使未授权用户很难访问到能用于推理攻击的相关数据。
- 噪声和扰动(noise and prbalio)是种在 数据库中插入伪造信息的技术，目的是误导和迷惑攻击者，使得实际推理攻击无法成功。

数据库视图 数据库可允许一个组或者一个特定用户访问特定信息，同时限制另一个组进行访问，这种功能通过使用数据库视图来实现。

多实例（polyinstantiation） 多实例建立了具有相同主键的多个元组和由安全线定义的实例之间的关系。当一条信息插入数据库中时，需要限制低级别用户访问这条信息。通过建立另一组数据迷惑低级别用户，使用户认为他得到的信息是真实的，而不是仅限制信息的访问。其实，多实例是通过使用不同值或其他变量填充变量来交互生成客体详细信息的过程，它常用于防止推理攻击。

联机事务处理（OLTP） 用于群集数据库以提供容错和高性能。OLTP 提供了监测问题以及在问题发生时立即进行适当处理的机制。OLTP 的主要目标是确保事务处理的正确发生或根本不发生。OLTP 要实时记录所出现的事务处理，数据库软件应该实现一种名为 ACID 测试的特征：

- 原子性（atomicity）将事务处理分成多个工作单元，并确保所有修改都生效或者没有一个修改生效。要么所有修改都提交，要么数据库回滚。
- 一致性（consistency）事务处理必须遵守为特定数据库制定的完整性策略，并确保不同数据库中所有数据的一致性。
- 隔离性（isolation） 事务处理完全隔离执行直至完成，同时事务处理之间互不影响。在事务处理完成之前，修改结果不会生效。
- 持久性（durability） 一旦事务处理在所有的系统上都被验证为是正确的，它就

会被提交，并且数据库无法回滚。

D、数据仓储和数据挖掘

数据仓库（data warehousing）指的是为了信息检索和数据分析，将多个数据库或数据源组合成一个大的数据库。数据仓库使得用户可不用查询多个数据库，而只查询一个实体。构建数据仓库的数据源用于操作目的。建立数据仓库是为了进行分析，执行分析是为了做出业务预测决策，确定营销效率、业务趋势甚至欺诈活动。

数据挖掘（data mining）是对数据仓库中的数据进行进一步处理以得到更有用信息的过程。数据挖掘工具用于发现数据的联系和相关性以生成元数据。元数据可说明不同信息子集之间存在的、先前无法看到的关系。它可揭示先前不明显的异常模式。

数据挖掘也称为**数据库知识发现**（KDD） 它组合了标识有效及有用知识的各种技巧。根据生成数据的要求所使用的不同类型的系统。

大数据是与数据仓库和数据挖掘相关联的术语，但又有所不同。大数据被广泛定义为非常大的数据集，具有不适合传统分析技术的特性。这些特性被广泛认同，包括异质性、复杂性、多变性、缺乏可靠性和容量庞大。“大数据”存储在诸如“数据仓库”的专用系统中，并使用诸如“数据挖掘”的方法加以利用，这三个术语既是相关的，又是不同的。

E、以知识为基础的人工智能系统

接下来我们看一下两种类型的以知识为基础的人工智能系统：专家系统和神经网络，以及它们的应用，和它们潜在的计算机安全问题。

专家系统，试图具体化人类在某个特殊学科累积的知识，并且以一致的方式将它们应用于将来的决定。一些研究已经表明：在正确开发和实现专家系统之后，专家系统常常能够做出比人类的常规决策更好的决定。每个专家系统都有两个主要的组件：知识库和推理引擎。

神经网络，计算单元链被用来尝试模仿人脑的生物学推理过程。在专家系统中，一系列规则被存储在知识库中，而在神经网络中则建立了互相插入和最终合计生成预期输出结果的计算决策长链。

决策支持系统(DSS)是一种知识型应用，它分析业务数据并且以更容易做出业务决策的形式提供给用户。决策支持系统更多被视为信息型应用而不是操作型应用。

专家系统和神经网络都在计算机安全领域具有很多应用。这些系统提供的一个主要优点是它们快速做出一致决策的能力。计算机安全性方面的一个主要问题是，系统管理员没有能力为了寻找异常而对大量的日志记录和审计跟踪数据进行一致的、彻底的分析。

1.6 一些安全开发实践

A、源代码中的脆弱性

“开放式 Web 应用程序安全项目（OWASP）”是一个组织，它专门处理 Web 安全问题。一下是 2017 年以来最新的 Top 10 问题清单：

A1：注入 Injection

A2：失效的身份认证 Broken Authentication

A3: 敏感数据泄露 Sensitive Data Exposure

A4: XML 外部实体 XML External Entities（XXE）

A5: 失效的访问控制 Broken Access Control

A6: 安全配置错误 Security Misconfiguration

A7: 跨站脚本攻击 Cross-Site Scripting (XSS)

A8: 不安全的反序列化 Insecure Deserialization

A9: 使用已知安全隐患组件 Using Components with Known Vulnerabilities

AIO: 不足的日志记录和监控 Insufficient Logging & Monitoring

B、安全编码实践

卡内基梅隆大学（CMU）软件工程研究所（SEI）发布了一份安全编码实践 Top 10 信条清单：

1. 验证输入。程序设计者在设计程序时必须验证来自所有不可信数据源的输入。

2. 注意编译器警告。程序员应当使用编译器的最高警告等级。

3. 根据安全策略设置软件架构。设计者应创建一个软件架构，并在设计软件的过程中实施和强化安全策略。

4. 保持程序简单。设计者要尽量使程序短小精悍。复杂的设计会增加实施、配置、使用过程中出现错误的可能性。

5. 拒绝默认访问。默认情况下，应当拒绝访问，程序的保护机制应当根据“允许谁访问”来确认访问条件。

6. 遵循最小特权原则。程序的每个处理过程在执行时，都应当仅使用为完成其工作而需要的最小特权。任何提升的许可权限都要尽量持续最短的时间。这种方法可以减少攻击者用提升的特权执行任意代码的可能性。

7. “净化”传送给其它系统的数据。所谓“净化”是指从用户输入的数据中清除恶意数据，如清除用户提交表单时的恶意的或错误的字符。

8. 实施深度防御。程序设计必须能够利用多种防御策略来管理风险。

9. 使用有效的质量保证技术。良好的质量保证技术可以有效地确认和清除漏洞。模糊测试、渗透测试、源代码审计等都可以结合起来使用，以此作为一个有效的质量保证项目的一部分。独立的安全检查可以使系统更安全。有资质的外部审查人员可以提供独立的观点。

10. 采用安全的编码标准。设定标准，并审查相关责任。

C、开发环境的安全

1、IDE 的安全性

软件开发人员一般用的开发工具是集成开发环境（IDE），不同语言有不同的 IDE（例如，Eclipse、Visual Studio、Xcode 等）。IDE 允许工程师从代码库中提取代码，对其进行编辑、测试，然后将其推入存储库中，以便团队的其他成员可以在其上进行构建。因此对于 IDE 的安全方面，我们要考虑开发客户端是否是安全的，软件部署和测试的服务器环境是否安全，代码库是否安全，以及整个流程是否安全？

2、代码库的安全性

代码库通常是版本控制系统，里面存储了组织中软件的源代码。最主要安全问题包括：源代码会被盗取，以及可能被人插入漏洞。

3、软件配置管理

当一个软件产品在其开发生命周期内发生变更时，配置管理系统就需要部署到位，从而使变更控制过程能实现自动化管理。提供软件配置管理(SCM)的软件能标识不同时间点上软件的属性值，同时可执行条理化的变更管理，以便在整个软件开发生命周期内维护软件的完整性和溯源性。

4、软件托管（Software Escrow）。

在软件托管服务框架中，第三方保存源代码的副本以及其他可能的材料，只有当特定的情况发生时，它才发布给客户，主要是开发代码的供应商倒闭了或由于某种原因不能履行其义务和责任时。这个过程能保护客户，这是因为客户为开发的软件代码向供应商支付了费用，否则，如果供应商倒闭，客户将不再有机会访问到实际的代码。这意味着客户的代码永远不会被更新或适当地维护。

单元 2：应用攻击和恶意代码

2.1 扫描和伪造攻击

A、扫描攻击

IP 探测（也称为 IP 扫描或 ping 扫描）通常是针对目标网络实施的一种网络侦察类型。通过这种技术，自动化工具试图 ping 某个范围内的所有地址。为缩小搜索范围，攻击者会使用端口扫描软件探测网络中所有存活的系统并确定每台计算机上运行的服务。nmap 是一个用来对 IP 和端口进行扫描的工具。

为了缩小搜索范围， 攻击者会使用端口扫描软件来探测网络中的所有工作系统并确定每台计算机上运行的公共服务。

一旦攻击者确定了攻击目标，他们就需要找到这个系统上可利用的漏洞，从而获得希望的访问许可权限。可从互联网获得的多种工具都能协助完成这个任务。其中比较流行的工具包括 Nessus、OpenVAS、Qualys、Core Impact 和 Nexpose。

每个组织都会产生垃圾，通常每天的日常工作会产生大量的垃圾，这里面可能有大量敏感信息。垃圾搜寻是最古老的攻击方法之一，直到今天还在被使用。

B、伪装攻击

在 IP 欺骗攻击中，怀有恶意的人重新配置他们的系统，使其具有可信系统的 IP 地址，然后试图获得访问其他资源的权限。

会话劫持攻击指的是怀有恶意的人中途拦截已授权用户与资源之间通信数据的一部分，然后使用劫持技术接管这个会话并伪装成已授权用户的身份。下面列出一些常见技术：

- 捕获客户端与服务器之间身份验证的详细信息，并使用这些信息伪装成客户端的身份。
- 欺骗客户端，使其认为攻击者的系统是与之通信的服务器，并在客户端与服务器建立合法连接时作为中间人，然后断开服务器与客户端的连接。
- 使用没有正常关闭连接的用户的 cookie 数据访问 Web 应用程序。

2.2 系统和应用软件安全

A、缓冲区溢出

缓冲区溢出漏洞存在于当开发人员没有正确验证用户的输入，以确保以适当的大小输入时。输入太大“溢出”原有的缓冲区，覆盖了内存中的其他数据。在最糟的情况下，该数据可用来覆盖系统代码，允许攻击者利用缓冲区溢出漏洞在服务器上执行任意代码。

B、TOC/TOU

检验时间到使用时间（TOCTOU 或 TOC/TOU）问题是一个时间型漏洞，当程序检查访问许可权限的时间远早于资源请求的时间时，就可能出现这种问题。D3 中已有详细介绍。

C、后门、权限提升和 rootkit

后门是没有被记录到文档中的命令序列，它们允许软件开发人员绕过正常的访问控制。除了开发商的后门外，许多恶意代码感染系统后也会创建后门，允许恶意代码的开发者远程访问受感染的系统。

攻击者一旦在一个系统上站稳脚跟，他们通常会迅速向第二个目标迈进一步，将他们的访问权限从普通账号提升为管理员权限。他们通过权限提升攻击来实现。

权限提升攻击的常见方法之一是使用 rootkit。rootkit 可从互联网上免费获得，它利用操作系统已知的漏洞。攻击者经常通过使用密码攻击或社会工程学攻击获得系统的普通账号，然后利用 rootkit 将访问权限提高到 root（或系统管理员）级别。

D、密码攻击

攻击者用于获得对系统的非法访问的最简单技术之一是：获悉已授权系统用户的用户名和密码。获取合法用户密码并访问系统的三种方法：密码猜测攻击、字典攻击、社会工程学攻击。

2.3 Web 应用安全

A、SQL 注入攻击

SQL 注入攻击利用现有应用程序，将恶意的 SQL 命令注入到后台数据库引擎执行的能力，它可以通过在 Web 表单中输入恶意 SQL 语句得到一个存在安全漏洞的网站上的数据库，而不是按照设计者意图去执行 SQL 语句。

防御 SQL 注入攻击的三种常见技术：

- 使用准备好的语句。开发人员应充分利用准备好的语句来限制应用程序执行任意代码的能力。
- 执行输入验证。输入验证能够限制用户在表单中输入的数据类型。
- 限制用户特权。Web 服务器使用的数据库账户应当只有最小的权限。

B、XSS 和 CSRF 攻击

跨站脚本攻击（XSS），攻击者嵌入恶意脚本代码到正常用户会访问到的页面中，当正常用户访问该页面时，则可导致嵌入的恶意脚本代码的执行，从而达到恶意攻击用户的目的。防御跨站脚本攻击的方法是：首先确定允许的输入类型，然后通过验证实际输入来确保其与指定的模式相匹配。

跨站请求伪造攻击，简称为 XSRF 或 CSRF 攻击，类似于跨站脚本攻击，但利用不同的信任关系。XSS 攻击利用用户在网站上执行用户计算机上的代码的信任。CSRF 攻击利用远程站点在用户系统中对用户执行命令的信任。防御跨站请求伪造攻击一种方法是创建 Web 应用程序，在链接中嵌入攻击者不知道的安全令牌。另一个保障是网站检查从最终用户接收到的请求中的引用 URL,并且只接受源于他们自己站点的请求。

C、目录遍历、Unicode 和 URL 编码

路径或目录遍历 这种攻击也称为 “点点斜线”，因为它通过在 URL 中插入几个“../”字符来回溯或遍历本不应通过 Web 访问的目录，从而实施攻击。

Unicode 编码 Unicode 是一种行业标准机制，开发它的目的是为了以一种标准的编码格式来表示世界上的 10 万多个文本字符。Web 服务器支持 Unicode 以支持不同的字符（如中文），并且许多服务器都默认支持 Unicode。因此，即使我们告诉系统禁止前面提到的“../”目录遍历请求，但是在应用 Unicode 的情况下，攻击者不使用“../”而是通过那个字符的 Unicode 表示形式就仍然可以有效地提出相同的目录遍历请求。这个请求能够悄悄避开确认规则并得到处理。

URL 编码 在 Web 浏览器的 URL 中，“ 空格”以%20 表示。实际上，%20 即表示空格，因为 URL 中禁止使用空格字符。就像使用 Unicode 字符的攻击一样，攻击者发现他们能以不同的方式表示字符，从而避开过滤并提出请求。

2.4 恶意代码

A、病毒

病毒是可感染应用程序的一个小程序或者一串代码。病毒的主要功能是复制，它需要借助一个宿主应用程序来进行复制。换句话说，病毒不能进行自我复制。

病毒常见的 4 中传播技术有主引导记录感染、文件程序感染、宏病毒和服务注入。

- 主引导记录病毒。主引导记录病毒(Master Boot Record, MBR)是已知最早的病毒感染形式。这些病毒攻击 MBR---可启动介质(例如, 硬盘、软盘或 DVD)上计算机

用于在启动过程中加载操作系统的部分。

- 文件程序感染病毒。文件程序感染病毒主要感染不同类型的可执行文件（如.exe和.com），并且在操作系统执行这些文件时被激活。
- 宏病毒。宏病毒(macro virus)是使用这些编程语言中的一种而编写的与平台无关的病毒，它们可感染模板并在文档中复制。在 Office 产品中，宏病毒十分常见。
- 服务注入病毒。服务注入病毒将自己注入可信的系统进程中，如 svchost.exe. winlogin.exe 和 explorer.exe。通过破坏这些可信进程，恶意代码可绕过主机上运行的反病毒软件的检测。

病毒为了逃避检测，一般会有 4 种类型：企图逃避检测，这 4 种类型是复合病毒、隐形病毒、多态病毒和加密病毒，其中：

- 复合病毒（Multipartite Viruses） 复合病毒使用多种传播技术试图渗透只防御其中一种方法的系统。
- 隐形病毒（Stealth Viruses） 隐形病毒通过篡改操作系统欺骗反病毒软件，使其认为一切正常，从而将自己隐藏起来。
- 多态病毒（Polymorphic Viruses） 在系统间传输时，多态病毒实际上会修改自身的代码。这种病毒的传播和破坏技术不会变化，只是每次感染新的系统后，病毒的特征都略有改变。多态病毒制造者就是希望通过连续改变特征使基于特征的反病毒软件失效。
- 加密病毒（Encrypted Viruses） 加密病毒使用加密技术来躲避检测。

B、蠕虫和木马

蠕虫不同于病毒，因为它不需要宿主程序就进行自我复制，是一种独立的病毒程序。最有名的计算机蠕是 Stuxnet，它针对的是西门子监控和数据获取（SCADA）软件和设备。

特洛伊木马(Trojan horse)是一种伪装成另一个程序的程序。远程访问特洛伊木马(RAT)是在受害系统上运行的一种恶意代码，允许入侵者远程操作受害系统。

僵尸网络（botnet）。在僵尸网络中，被特洛伊木马使所有被感染的系统成为僵尸（bot）。当黑客将这些被入侵的系统收集在一起，那么它们就被称为一个僵尸网络(network of bot)。僵尸网络一般由 Internet 上的僵尸牧人(botmaster)通过僵尸网络控制服务器来控制，并执行僵尸牧人的命令。

C、其它恶意代码

逻辑炸弹(logic bomb) 当发生特定事件时，逻辑炸弹会执行某个程序或者一段代码。

间谍软件是一种隐蔽性恶意软件，安装在目标计算机上并收集关于受害者的敏感信

息。

恶意广告软件是一种可自动生成（渲染）广告的软件。广告的目的是产生销售收入，不进行恶意活动，但一些广告使用侵入性行为，这可能导致安全和隐私问题。

D、恶意代码防护

特征型检测（也称为指纹检测）使用病毒特征来检测恶意代码。病毒特征是防病毒软件供应商建立的一个指纹，它是从病毒本身中抽取出的一个代码序列。

启发式检测（heuristic detection）会分析恶意代码的总体结构，评估编码指令和逻辑功能，并研究病毒或蠕虫内的数据类型。

行为阻止（behavior blocker） 让可疑代码在未受保护的操作系统中运行，监控它与操作系统的交互，并从中寻找可疑活动。

启发式检测和行为阻止都采取主动防御，因而能检测出新的恶意软件，有时也称为“零日攻击”。特征型检测则不能检测出新的恶意软件。

防病毒策略应该说明哪些事情应该做以及哪些事情不该做：

- 应该在每一个工作站、服务器和移动设备上安装防病毒软件。
- 每一台设备都应配置为自动更新病毒特征。
- 不允许用户禁用防病毒软件。
- 应预先制定一个病毒清除流程，并指定出现病毒感染时的联系人。
- 应自动扫描所有外部磁盘（USB 驱动器等）。
- 应扫描备份文件。
- 应每年审查防病毒策略和措施。
- 防病毒软件应当提供引导区病毒防护。
- 应对网关和每一台设备进行病毒扫描。
- 应当定期进行自动病毒扫描，不能依赖于手动扫描。
- 应从物理上对关键系统加以保护，从而使恶意软件无法从本地安装。