

领域1：安全与风险管理

保密性	保护对信息的授权限制访问与披露，包括保护手段 个人隐私和专有信息。注意——加密（传输中 - TLS）（静态数据 - AES - 256）
诚信	防止不当的信息修改或破坏并包括确保信息不可否认性和真实性。
可用性	确保及时可靠地访问和使用授权用户的信息。
*引用来源： https://www.isc2.org/Certifications/CISSP/CISSP-学生术语表	

D.A.D.		
披露	改变	毁灭
相反的保密性	正直的对立面	可用性的反义词

计划		
类型	持续时间	示例
战略规划	最多5年	风险评估
战术计划	项目预算、人员配置等最多为1年。	
运营计划	几个月	修补计算机 更新AV签名 日常网络管理

风险管理
● 任何风险都无法完全避免。 ● 风险可以被最小化并加以控制，以避免损害的影响。 ● 风险管理是识别、评估、衡量、缓解或转移风险的过程。
*引用： https://resources.infosecinstitute.com/category/certifications-training/cissp/领域/安全与风险管理/
解决方案——将风险控制在可容忍和可接受的水平。风险管理 约束条件——时间、预算

风险管理框架				
预防性的 前ISO 27001标准	威慑 前ISO 27000标准	侦探	纠正性的	恢复
安全策略	安保人员	日志	警报	备份
监控摄像头	卫兵	监控摄像头	防病毒解决方案	服务器集群
回调	监控摄像头	入侵检测系统	入侵检测系统	容错驱动系统
安全意识培训	职责分离	蜜罐	业务连续性计划	数据库影子
岗位轮换	入侵报警系统	审计追踪		防病毒软件
加密	意识培训	强制休假		
数据分类	防火墙			
智能卡	加密			

风险管理生命周期		
评估	分析	缓解/响应
分类、归类与评估资产	定性与定量	减少、转移、接受
根据 <i>NIST 800-30</i> ：	定性——判断	减少/避免
系统特性描述	定量——主要术语	转移
威胁识别	AV——资产价值	接受 / 拒绝
漏洞识别	EF – 暴露因子	<div>安全治理</div> <div>BS 7799</div> <div>ISO 17799 & 2700系列</div> <div>COBIT和COSO</div> <div>八度音阶</div> <div>I TIL</div>
控制分析	ARO——年发生率	
可能性确定	单一损失期望值 = AV * EF	
影响分析	年度预期损失 = SLE*ARO	
风险确定	风险值 = 概率 * 影响	
控制建议		
结果文档		

威胁识别模型	
<i>S.T.R.I.D.E.</i>	欺骗 - 篡改 - 抵赖 - 信息泄露 - 拒绝服务 - 权限提升
<i>D.R.E.A.D.</i>	损害 - 可重复性 - 可利用性 - 受影响程度 - 可发现性
<i>M.A.R.T.</i>	缓解 - 接受 - 拒绝 - 转移

灾难恢复 / 业务连续性计划	法律类型	知识产权
连续性计划目标	刑法	版权
重要性声明	民法	商标
优先事项声明	行政法	专利
组织声明	综合犯罪控制法案（1984年）	商业机密
责任	《计算机欺诈与滥用法案》（1986年）	许可
紧急性与时间安排声明	计算机安全法（1987年）	
风险评估	政府信息安全改革法案（2000年）	
风险接受/缓解	联邦信息安全管理办法（2002年）	

CISSP 速查表系列

comparitech

实现CIA——最佳实践					
分离 职责	强制性的 假期	工作 旋转	最少 特权	需要 知道	双重控制
可用性		, SLA			
衡量指标： RTO/MTD/RPO， MTBF					
国际航空运输协 会（IAAAA）					
识别	唯一用户识别				
认证	身份验证				
授权	权限和许可的验证 已认证用户				
问责制	只有授权用户才能访问和使用该系统。 系统相应地				
审计	用于实现和达成目标的工具、流程和活动 保持合规				

保护机制			
分层	抽象概念	数据隐藏	加密

数据分类
这包括分析组织保留的数据，确定其重要性和价值，然后将其归类。

风险术语	
资产	对公司有价值的东西。
脆弱性	一个弱点；缺乏保障措施
威胁	可能对资产全部或部分构成风险的事物
威胁代理	实施攻击的实体
利用	妥协的一个例子
风险	威胁发生的概率
引用： https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/安全与风险管理/	

风险框架类型
安全与风险管理
资产安全
安全工程
通信与网络安全
身份与访问管理
安全评估与测试
安全运营
软件开发安全

风险管理的6个步骤管理框架
分类
选择
实施
评估
授权
监控器

分类级别		典型数据保留期限		数据安全控制	
军事部门	私营部门	商业文件	7年	使用中的数据	范围界定与定制化
绝密	敏感的	发票	5年	静态数据	加密
秘密	机密	应付账款/应收账款	7年		
机密	私人	人力资源 - 招聘	7年		
敏感但未分类	公司受限的	人力资源 - 未聘用	3年	流动的数据	安全协议，例如https
	公司机密	税务记录	4年		
未分类	公众	法律函件	永久地		

数据所有权				
数据所有权	数据保管人	系统所有者	管理员	最终用户
最高层级/主要责任 数据 定义分类级别 定义控制措施以应对不同级别的问题 分类 定义基线安全标准 影响分析 决定何时销毁 信息	每日授权权限 确保遵守数据政策并 数据所有权指南 确保可访问性，维护并 监控安全 数据存档 数据文档 定期备份，恢复检查 验证 确保CIA 执行用户授权 实施安全控制措施	实施安全控制措施	授予权限 用于数据处理	Uses information for their job / tasks Adhere to security policies and guidelines

数据分类标准
价值 - 有用性 - 年龄 - 关联性
数据保留政策
佛罗里达州电子记录与档案管理实践，2010 《欧洲文件保留指南》，2012年

安全政策、标准与指南	
监管	法律和行业标准所要求的
咨询意见	非强制性，但建议执行
信息性的	作为他人的指导
信息政策	定义信息处理和使用的最佳实践 安全策略：策略的技术细节 即系统安全策略：列出硬件/软件清单 使用政策及使用步骤
标准	定义使用级别
指南	非强制性标准
程序	执行任务和政策的流程
基线	最低安全水平

数据残留	
消毒	一系列删除数据的过程，完全地
消磁	擦除磁带等介质上的数据，以确保不泄露信息。可恢复的
擦除	文件或媒体的删除
覆盖	覆盖文件，粉碎
零填充	用零覆盖硬盘上的所有数据
毁灭	数据硬件设备的物理销毁
加密	使数据在没有特殊密钥的情况下无法读取。算法

标准	
美国国家标准与技术研究院（	国家标准与技术研究院技术
NIST SP 800系列	计算机安全在多个领域的应用
800-14 NIST SP	保障信息技术安全系统
800-18 NIST	制定安全计划
800-27 NIST SP	实现安全的基线
800-88 NIST	卫生与处置指南防止数据残留
800-137	持续监测计划：定义，建立、实施、分析和报告
800-145	云计算标准
FIPS	联邦信息处理标准

领域4：网络与通信安全

OSI参考模型		
7层架构，允许层间变更，标准硬件/软件互操作性。		
提示，OSI 记忆法		
似乎所有人都需要数据处理		
P租赁DoNotThSausagePizzaA路		
层	数据	安全
申请	数据	C, I, AU, N
演示文稿	数据	C、澳大利亚、加密
会话	数据	N
运输	片段	C, AU, I
网络	数据包	C, AU, I
数据链路	框架	C
物理的	比特	C
C=机密性, AU=认证, I=完整性, N=不可否认性		

层（编号）	功能	协议	硬件 / 格式
物理（1）	电信号比特到电压		电缆，集线器，USB，DSL中继器，自动配置机
数据链路第二层	框架设置错误检测与控制检查数据包的完整性目标地址，帧在MAC地址中使用IP地址转换。	PPP - PPTP - L2TP -- ARP - RARP - SNAP - CHAP - LCP - MLP - 帧中继 - HDLC - ISL - MAC - 以太网 - 令牌环 环网 - FDDI	第二层 开关 - 桥梁
网络层	路由，第三层交换，分段，逻辑的地址。ATM。数据包。	ICMP - BGP - OSPF - RIP - IP - BOOTP - DHCP - ICMP	第三层 开关 - 路由器
运输层	段 - 连接定向的	TCP - UDP 数据报。可靠的数据端到端传输转移 - 细分 - 排序 - 以及错误检查	路由器——VPN 关注的 rs - 网关
会话层	数据、单工、半双工、全双工重复的等价对等连接。	TCP - UDP - NSF - SQL - RADIUS - 以及 RPC - PPTP - PPP	网关
演示文稿层	数据压缩/解压缩以及加密/解密	TCP - UDP 消息格式	网关 JPEG - TIFF - 中 - HTML
申请层	数据	TCP - UDP - FTP - TELNET - TFTP - SMTP - HTTP CDP - SMB - SNMP - NNTP - SSL - HTTP/HTTPS。	网关

TCP/IP模型		
层次	行动	示例协议
网络访问	数据传输在此层完成	令牌环网、帧中继、光纤分布式数据接口（FDDI） • 以太网、X.25
互联网	创建称为小数据块的数据。 要通过传输的数据报文 网络接入层	IP、RARP、ARP、IGMP、ICMP
运输	流量控制与完整性	TCP、UDP
申请	将数据转换为可读形式 格式	Telnet、SSH、DNS、HTTP、FTP • SNMP、DHCP

TCP 三次握手
SYN - SYN/ACK - ACK

局域网拓扑结构		
拓朴学	优点	缺点
巴士	• 易于设置	• 无冗余 • 单点故障 • 难以排查故障
戒指	• 容错性	• 没有中间点
开始	• 容错性	• 单点故障
网格	• 容错性	• 冗余 • 设置成本高

数字用户线路（DSL）的类型	
非对称数字用户线路（ADSL）	<ul style="list-style-type: none">• 下载速度高于上传速度 • 通过电话线最大距离可达5500米。 • 最大下载速度8Mbps， 上传速度800Kbps。
速率自适应DSL（RADSL）	<ul style="list-style-type: none">• 根据传输线路质量调整上传速度 • 在5500米以上距离，最大下载速度为7Mbps， 上传速度为1Mbps。
对称数字用户线路（SDSL）	<ul style="list-style-type: none">• 上行和下行传输速率相同。 • 距离6700米，通过铜质电话电缆传输 • 最大下载速度2.3Mbps， 上传速度2.3Mbps。
超高速率数字用户线路（VDSL）	<ul style="list-style-type: none">• 比标准ADSL更高的速度 • 最高下载速度52Mbps， 上传速度16Mbps，最高可达1200米。米制单位
高比特率DSL（HDSL）	<ul style="list-style-type: none">• 两对铜线在3650米距离下的T1速度
承诺信息速率（CIR）	<ul style="list-style-type: none">• 服务提供商提供的最低保证带宽。

局域网数据包传输	
单播	单源发送至单目的地
组播	单源发送至多个目的地
广播	源数据包发送给所有目的地。
载波侦听多路访问接入（CSMA）	一个工作站会不断重传帧，直到到达目的地工作站接收。
带冲突的CSMA检测（CSMA/CD）	在检测到冲突时终止传输。用于以太网。
带冲突的CSMA避免（CSMA/CA）	在检测到繁忙传输后，暂停并随后随机间隔重传延迟传输至尽量减少两个节点同时重传的情况。
民意调查	发送者仅在轮询系统空闲时才发送目的地。
令牌传递	发送方只有在收到表示可以发送的令牌时才能发送。发送。
广播域	接收广播的设备集合。
冲突域	一组在运行过程中可能产生碰撞的设备数据的同时传输
第二层交换机	创建VLAN
三层交换机	连接VLANs

局域网/广域网介质	
双绞线	一对绞合铜线。用于以太网。Cat5/5e/6。Cat5在100米距离内速度可达100Mbps。Cat5e/6的速度可达1000Mbps。
非屏蔽双绞线 <small>双绞线（UTP）</small>	对电磁干扰（EMI）的抵抗力较弱
屏蔽双绞线 <small>配对（STP）</small>	类似于UTP，但包含保护屏蔽层。
同轴电缆	用粗导线代替两根铜线。10BASE-T， 100BASE-T，以及1000BASE-T。
光纤	使用光作为介质来传输信号。长距离千兆速度。距离更远。更少的错误和信号丢失。抗电磁干扰。多模光纤。单模和多模。单模用于室外长距离传输。
帧中继广域网	通过公共交换网络。通过中继实现高容错性故障段恢复正常工作。
安全网络设计——组件	
网络地址 <small>网络地址转换（NAT）</small>	隐藏内部公网IP地址，防止外部互联网访问
端口地址 <small>翻译（PAT）</small>	允许内部设备共享公共IP地址 使用ISP分配的给定单一公共IP地址的应用程序
有状态NAT	跟踪源和目的地之间的数据包传输
静态NAT	在两个终端之间分配一对一私有到公共IP地址设备
动态NAT	内部IP地址池映射一个或多个公共IP地址

常见TCP协议	
港口	协议
20、21	FTP
22	SSH
23	Telnet
25	SMTP
53	DNS
110	POP3
80	HTTP
143	IMAP
389	LDAP
443	HTTPS
636	安全LDAP
445	活动目录
1433	微软 SQL
3389	RDP
137-139	NETBIOS

OSI层中的攻击	
层	攻击
申请	钓鱼攻击 - 蠕虫 - 特洛伊木马
演示文稿	钓鱼攻击 - 蠕虫 - 特洛伊木马
会话	会话劫持
运输	SYN洪水攻击 - Fraggle攻击
网络	Smurfing 洪水攻击 - ICMP欺骗 - 拒绝服务攻击
数据链路	碰撞 - DOS/DDOS -偷听
物理的	信号干扰 - 窃听

硬件设备	
枢纽	第一层设备转发 通过所有端口的帧
调制解调器	数字到模拟 转换
路由器	互联网络
桥	互联网络在 以太网
网关	流入/流出数据 网络入口点
开关	本地帧前移 网络
负载均衡器	共享网络流量 通过分配来加载 两个之间的交通 设备
代理服务器	隐藏内部公共IP 来自外部的地址 公共互联网 /连接缓存与 过滤。
VPN和VPN 集中器	用于创建VPN或 聚合VPN 连接提供 使用不同的互联网 链接

协议分析仪	捕获或监控 网络流量在 实时广告离线
统一威胁 管理	新一代 漏洞扫描 应用
虚拟局域网 (VLAN)	创建碰撞 域。路由 器单独播 出领域
入侵检测系 统/入侵防御	入侵检测与 预防。

防火墙与边界防护安全	
DMZ 非军事化区域	安全的网络连接 面向外部互联网的 内部网络
堡垒主机 - 双宿主 - 三腿式 - 屏蔽子网 - 代理服务器 - PBX - 蜜罐 锅 - IDS/IPS	

网络攻击	
病毒	恶意软件、代码和可执行文件
蠕虫	自我传播的病毒
逻辑炸弹	时间或条件锁定病毒伪装成合法软件，但实际上并非合法的代码和/或可执行程序。
特洛伊木马	恶意的
后门	未经授权的代码执行入口
萨拉米，萨拉米切片	一系列小规模攻击和网络入侵最终累积成一次大规模事件
数据篡改	规模攻击处理前对原始数据的修改
嗅探	未经授权的传输数据监控
会话劫持	监控和捕获认证会话，目的是发现并劫持这些会话证书
DDoS（分布式拒绝服务）服务	向服务器发送远超其处理能力的数据包请求，导致服务器过载。导致服务失败
SYN洪水攻击	结合DDoS攻击和TCP三次握手漏洞利用，导致拒绝服务。
蓝精灵	一种特殊的DDoS攻击，利用大量互联网控制消息。协议（ICMP）数据包
弗拉格勒	使用UDP而非TCP的蓝精灵攻击
洛基	使用常见的ICMP隧道程序在网络中建立隐蔽通道
泪滴	一种利用TCP/IP分片重组中漏洞的DDoS攻击类型。发送分片数据包以耗尽通道资源
零日漏洞	利用休眠或此前未知的软件漏洞
陆地攻击	由于发送了一个源IP和目标IP相同的报文而引起。
蓝牙劫持，蓝牙窃听	匿名发送恶意信息或通过蓝牙注入代码到范围内的未受保护设备
DNS欺骗，DNS中毒	将伪造的DNS数据引入DNS服务器的缓存中，导致其提供错误的服务腐败的IP结果
会话劫持（欺骗）	更改数据包的TCP结构，使源地址显示为可信，从而获得访问权限目标系统。
TCP 序列预测 / 数字攻击	成功预测TCP数字序列，从而获得一种能力破坏某些类型的TCP通信

LDAP（轻量级目录访问协议） 协议	基于活动目录的电子邮件认证证书管理。
SASL（简单认证与安全层 客户端SSL证书 S/MIME 证书	安全的LDAP认证。 客户端证书，用于对服务器进行身份验证。 用于单点登录（SSO）中的签名和加密电子邮件
MOSS（MIME对象安全服务）	使用 multipart/signed 和 multipart/encrypted 框架进行应用数字签名。
PEM（隐私增强邮件）	一系列关于消息安全的RFC（请求评论）文档真实性。
DKIM（域名密钥识别邮件）	验证原始信息真实性的技术。
OAuth	一种开放协议，允许使用令牌代替传统方式实现安全授权。密码。

IP地址	
公网IPv4地址空间	<ul style="list-style-type: none">• A类: 0.0.0.0 – 127.255.255.255 • B类: 128.0.0.0 – 191.255.255.255 • C类: 192.0.0.0 – 223.255.255.255
私有IPv4地址空间	<ul style="list-style-type: none">• A类: 10.0.0.0 – 10.255.255.255 • B类: 172.16.0.0 – 172.31.255.255 • C类: 192.168.0.0 – 192.168.255.255
子网掩码	<ul style="list-style-type: none">• A类: 255.0.0.0 • B类: 255.255.0.0 • C类: 255.255.255.0
IPv4	32位八位组
IPv6	128位十六进制

网络类型	
本地区域网络（局域网）	地理距离和面积仅限于一个。建筑物。通常使用铜线连接。光纤技术
校园区域网络（CAN）	多栋建筑通过光纤连接或无线
大都会区域网络（人）	城市内部的大都市网络跨度
广域网网络（广域网）	在大范围地理区域上互连局域网例如，国家或地区之间。
内网	私有内部网络
外联网	连接外部授权人员访问权限内网
互联网	公共网络

网络方法与标准	
软件定义的 网络 (SDN)	网络控制与分离 转发功能。 特点——敏捷性、集中管理 程序化配置，供应商中立。
融合的 协议 媒体传输	通过单一通道传输语音、数据、视频和图像 网络
光纤通道 通过以太网 (FCoE)	在以太网网络上运行光纤。
多协议 标签 切换 (MPLS)	根据最短路径标签传输数据 代替网络IP地址。无需使用 路由表查找。
互联网小型 计算机 接口 (ISCI)	连接数据存储站点的标准等 作为存储区域网络或存储阵列。 位置无关。
多层结构 协议	加密与不同协议在不同情况下的应用 水平。缺点是隐藏了令人垂涎的渠道 以及弱加密。
旁白 互联网 协议 (VoIP)	允许语音信号通过传输。 公共互联网连接。
异步 传输模式 (ATM)	更高性能的分组交换技术 带宽。使用53字节的固定大小单元。在 需求带宽分配。使用光纤。 在互联网服务提供商中很受欢迎
X25	数据终端设备之间的(DTE)连接 数据终端设备 (DTE)和数据电路终端设备 (DCE)
帧中继	与ISDN接口配合使用。更快，支持多路使用。 PVCs，提供CIR。性能更高。需要 在每个连接点都配备DTE/DCE。执行 纠错。
同步 数据链路 控制 (SDLC)	IBM专有协议永久使用 专用租用线路。
高级数据 链路控制 (HDLC)	使用DTE/DCE通信。扩展 SDLC协议。
域名 系统 (DNS)	将域名/主机名映射到IP地址 反之亦然。

专线服务	
T1	1.544Mbps 通过电话线
T3	通过电话线传输45Mbps
自动配置机	155Mbps
ISDN	64或128 Kbps 被xDSL取代
预留	1024-49151
BRI B通道	64 千比特每秒
BRI D通道	16 千比特每秒
PRI B和D通道	64 千比特每

CISSP 速查表系列	comparitech
端口范围	
点对点隧道协议（PPTP）	认证方法： <ul style="list-style-type: none">• PAP=明文，未加密 • CHAP=未加密，加密 • MS-CHAP=加密，加密
挑战握手认证协议（CHAP）	加密用户名/密码和定期重新认证。用于PPP。
第二层隧道协议（L2TP）	与IPsec结合使用进行加密。
认证头（AH）	提供认证和完整性，不保密性。
封装安全载荷（ESP）	加密IP数据包并保持完整性。
安全联盟（SA）	两个之间的共享安全属性网络实体
运输方式	有效载荷已受保护。
隧道模式	IP有效载荷和IP头部受到保护。
互联网密钥交换（IKE）	交换AH或ESP中的加密密钥。
远程认证拨号用户服务（RADIUS）	密码已加密，但用户明文认证。
SNMP v3	加密密码。
动态端口	49152 - 65535

远程访问服务	
Telnet	用户名/密码认证。无加密。
远程登录（rlogin）	无密码保护。
SSH（安全外壳）	安全Telnet
终端访问控制器 门禁系统 （TACACS）	用户凭证存储在一个被称为服务器的设备中。 TACACS服务器。用户认证请求 由该服务器处理。
TACACS+	TACACS的高级版本。使用双因素认证 认证
远程认证拨号用户服务 用户服务（RADIUS）	客户端/服务器协议用于启用AAA服务 远程访问服务器。
虚拟专用网络（VPN）	安全加密的通信通道 两个网络之间或用户与网络之间 网络。使用NAT进行IP地址转换。安全。 采用L2TP或IPSEC等强加密技术。

VPN 加密选项	
点对点隧道协议 (PPTP)	<ul style="list-style-type: none">• PPP 用于认证• 不支持EAP• 拨号进入• 连接建立使用明文• 数据链路层• 每次会话单连接
第二层隧道协议 (L2TP)	<ul style="list-style-type: none">• 与PPTP相同，只是更安全• 通常使用IPsec来保护L2TP数据包
互联网协议安全 (IPsec)	<ul style="list-style-type: none">• 网络层• 每个会话支持多个连接• 加密与认证• 保密性与完整性

通信硬件设备	
聚光器	将连接的设备分为一个输入信号进行传输。 通过网络输出。
多路复用器	将多个信号合并为一个信号进行传输。
枢纽	将从一个端口接收到的信号转发到所有端口。
中继器	增强信号强度。

广域网传输类型	
电路交换网络	<ul style="list-style-type: none">• 需要专用的永久电路或通信路径。• 稳定速度。延迟敏感。• 主要用于互联网服务提供商的语音通信。
分组交换网络	<ul style="list-style-type: none">• 固定大小的报文在节点之间发送并共享带宽• 延迟敏感。• 因此，使用虚拟电路成本更低。

无线网络		
无线个人区域网络（WPAN）标准		
IEEE 802.15	蓝牙	
IEEE 802.3	以太网	
IEEE 802.11	Wi-Fi	
IEEE 802.20	LTE	
Wi-Fi		
标准	速度	频率（GHz）
802.11a	54 Mbps	5
802.11b	11 Mbps	2.4
802.11g	54 Mbps	2.4
802.11n	200+ 兆比特每秒	2.4 和 5
802.11ac	1Gbps	5
• 802.11 使用CSMA/CA协议作为DSSS或FHSS		
• 802.11b 仅使用 DSSS（直接序列扩频）		

无线安全协议	
临时模式	直接连接点对点模式的客户端，无需中间设备中央接入点。
基础设施模式	客户端通过接入点集中连接。
WEP（有线等效加密） 隐私	保密性，使用RC4进行加密。
WPA（Wi-Fi保护） 访问	使用临时密钥完整性协议（TKIP）进行数据保护加密
WPA2	使用AES，密钥管理。
WPA2-企业模式	使用RADIUS
TKIP（临时密钥完整性） 协议	使用RC4流密码。
EAP（可扩展认证协议） 认证协议	采用PPP和无线认证。兼容其他加密技术。
PEAP（受保护的扩展认证协议） 认证协议	将EAP封装在加密和认证的框架内 TLS隧道。
基于端口的认证802.1x，在交换环境中与EAP配合使用	

无线扩频	
跳频（FHSS） 频谱系统	使用所有可用频率，但仅使用单一频率可以同时使用。
直接序列扩频（DSSS） 扩频技术	所有可用频率的并行使用会导致更高的效率。与FHSS相比的速率吞吐量。
OFDM（正交频分复用） 频分复用 多路复用	正交频分复用

防火墙的演进历程	
第一代 防火墙	<ul style="list-style-type: none">• 包过滤防火墙： 检查源/目的地址，入站数据包的协议和端口。允许或拒绝根据ACL。网络层，无状态。
第二代 防火墙	<ul style="list-style-type: none">• 应用层防火墙/代理服务器：隐藏源地址在数据包传输期间。运行在应用层，具有状态。
第三代 防火墙	<ul style="list-style-type: none">• 状态检测防火墙： 更快的。状态和上下文数据包被检查。• 动态数据包过滤防火墙： 动态ACL修改• 包过滤路由器： 位于DMZ或边界网络中。包括分组过滤路由器和堡垒主机。分组过滤和代理
第四代 防火墙	<ul style="list-style-type: none">• 双归属主机防火墙： 用于同时面临内部和外部威胁的网络。和外部• 屏蔽子网防火墙： 创建非军事区（DMZ）——可信与不可信之间的网络
第五代 防火墙	<ul style="list-style-type: none">• 内核代理防火墙： 通过虚拟化远程分析数据包网络
下一代 防火墙（下一代防火墙）	<ul style="list-style-type: none">• 深度包检测（DPI）与IPS： 与IPS/IDS集成

软件测试	
静态测试	被动测试代码而不运行代码：语法检查、代码审查与走查。例如：工具利用可利用的缓冲区溢出漏洞来自开源软件源代码
动态测试	使用运行环境进行分析和测试。用于第三方提供的测试软件，无访问软件代码。例如，跨站脚本攻击。SQL注入
模糊测试	使用特定输入进行动态测试的类型在压力/负载下检测缺陷。例如，输入无效测试参数
变异 / 随机模糊测试	使用已修改的输入值进行测试。
代际 / 智能模糊测试	输入预期输入模型。
误用案例测试	评估已知风险和攻击的脆弱性。
接口测试	评估软件模块的性能与...相比接口规范以验证工作正常运行状态。
应用程序编程接口（API）	测试API以验证Web应用程序是否满足所有安全要求需求。
用户界面（UI）	包括图形用户界面（GUI）和命令行界面（CLI）。用户回顾接口与需求规范。
物理接口	例如，在ATM机、读卡器等物理设备中等等。
单元测试	测试系统的一小部分以测试单元是适合集成到最终产品中。
集成级别测试	程序之间的数据和控制传输接口。
系统级测试	验证系统是否具备所有所需的规格和条件。功能。

日志管理系统	
OPSEC流程	分析日常运营并审查可能的攻击采取对策。
渗透测试	从黑客的角度测试网络安全。
端口扫描器	检查计算机中开放的任何端口或端口范围。
零环	系统的内部代码。
运营保障	验证软件是否符合安全要求。
监督模式	在内部保护环中运行的进程。

威胁评估建模	
步幅	评估针对应用程序或操作系统的威胁系统。
欺骗	使用虚假身份获取系统访问权限。可以使用IP/MAC地址、用户名、无线网络SSID。
篡改	导致传输中或存储中的数据未经授权被修改存储。导致完整性受损以及可用性。
否认	拒绝攻击者执行的行动或活动。
信息披露	私人/机密或受限信息的分布向未经授权的第三方披露信息。
权限提升	攻击导致权限级别在有限时间内提升用户账户。
定期监测 关键绩效和 风险指标包括	未修复漏洞和被利用的数量 账户、漏洞解决时间、检测数量 软件缺陷等
漏洞扫描	自动探测系统、应用程序和网络。
TCP SYN 扫描	发送一个设置了SYN标志的报文。也称为半开放扫描。
TCP连接扫描	当运行扫描的用户没有权限时执行。运行半开放扫描所需的权限。
TCP ACK 扫描	发送一个设置了ACK标志的数据包。
圣诞扫描	发送一个设置了FIN、PSH和URG标志的报文。
被动扫描	检测无线网络中的非法扫描设备。
认证扫描	用于访问配置文件的只读账户。

CISSP 速查表系列		comparitech
软件开发安全最佳实践		
WASC	Web 应用安全联盟	
OWASP	打开Web应用程序安全项目	
BSI	“内置安全”倡议	
IEC	国际电工委员会	

安全测试	
为了确保安全控制措施得到正确应用并有效使用。自动化扫描，漏洞评估和手动测试。	
软件威胁	
病毒	隐形病毒 • 多态病毒 • 宏病毒 • 间谍软件/广告软件 • 僵尸网络 • 蠕虫病毒
Rootkit	内核模式rootkit • 引导程序rootkit • 用户模式rootkit • 虚拟根套件 • 固件根套件
源代码问题	缓冲区溢出 • 权限提升 • 后门
恶意软件防护	防病毒软件 • 反恶意软件 • 安全政策

考虑因素	
• 资源可用性 • 被测系统的关键性和敏感性水平 • 技术故障 • 控制配置错误导致安全漏洞 • 安全攻击风险 • 性能变化的风险 • 对正常运营的影响	
验证与确认	
• 验证——SDLC设计输出符合要求 • 验证——测试以确保软件满足需求	
安全软件	
• 反恶意软件和反病毒——扫描并记录恶意软件和病毒检测结果 • IDS/IPS = 实时和混杂模式监控攻击 • 基于网络的入侵检测系统 • 本地网络监控和被动及头部级别扫描。不进行主机级别扫描。	

• 基于主机的 • 使用事件日志监控主机 • 入侵防御系统（IPS）——攻击检测与防御 • 远程访问软件应通过VPN访问 • 漏洞评估软件——应更新并打补丁 • 路由器——基于策略的访问控制	
日志	
网络流量	网络流量捕获
审计日志记录	与硬件设备登录和访问相关的事件
网络时间协议（NTP）	应在整个网络中同步以确保正确性 日志和设备流量中的时间是一致的。
系统日志	设备事件消息日志标准。
事件类型	错误、警告、信息、成功审计、失败
简单网络管理协议（SNMP）	支持思科等不同设备。

监控与审计	
定义一个裁剪级别。又称基线。 • 审计追踪——事件/交易日期/时间，事件的作者/所有者 • 可用性——日志归档 • 日志分析——检查日志	

代码审查与测试	
由代码编写者/开发者以外的其他人检查代码以发现错误	
法根检查——步骤	规划 • 概述 • 准备 • 检查 • 返工 • 后续跟进
代码覆盖率报告	测试代码结构的详细信息
用例	测试代码占总用例的百分比
代码审查报告	手动代码测试报告创建
黑盒测试	外部测试，不测试内部结构
动态测试	运行时测试代码
白盒测试	通过访问代码和内部结构进行详细测试
CVE	常见漏洞与暴露字典
CVSS	通用漏洞评分系统
NVD	国家漏洞数据库
回归测试	验证测试所需的安装是否没有出现问题 运行系统中的任何问题
集成测试	使用两个或多个组件一起测试

<div><div><div><div><div><div></div></div></div><div><div><div></div></div><div><div></div></div></div><div><div><div></div></div><div><div></div></div></div><div><div><div></div></div><div><div></div></div></div></div></div></div> <div><div><div></div></div><div><div></div></div></div> <div><div><div></div></div><div><div></div></div></div>
--

