CIS 控制项	CIS 子控制项	资产类型	安全功能	标题	描述
1				**硬件资产的库存和控制**	
1	1.1	设备	识别	使用主动发现工具	利用主动发现工具识别连接到组织网络的设备并更新硬件资产清单。
1	1.2	设备	识别	使用被动发现工具	利用被动发现工具识别连接到组织网络的设备，并自动更新组织的硬件资产清单。
1	1.3	设备	识别	使用DHCP日志记录更新资产清单	在所有DHCP服务器或IP地址管理工具上使用动态主机配置协议（DHCP）日志记录来更新组织的硬件资产清单。
1	1.4	设备	识别	维护详细的资产清单	维护所有技术资产的准确和最新清单，并有可能存储或处理信息。此清单应包括所有硬件资产，无论是否连接到组织的网络。
1	1.5	设备	识别	维护资产库存信息	确保硬件资产清单记录每个资产的网络地址，硬件地址，计算机名称，数据资产所有者和部门，以及是否已批准硬件资产连接到网络。
1	1.6	设备	响应	标记未经授权的资产	确保未经授权的资产从网络中删除，隔离或及时更新库存。
1	1.7	设备	防护	部署端口级访问控制	根据802.1x标准，利用端口级访问控制来控制哪些设备可以对网络进行身份验证。认证系统应绑定到硬件资产清单数据中，以确保只有授权设备才能连接到网络。
1	1.8	设备	防护	利用客户端证书来验证硬件资产	使用客户端证书对连接到组织的可信网络的硬件资产进行身份验证。
2				**软件资产的库存和控制**	
2	2.1	应用	识别	维护授权软件清单	维护企业在任何业务系统中出于任何业务目的所需的所有授权软件的最新列表。
2	2.2	应用	识别	确保供应商支持软件	确保仅将软件供应商当前支持的软件应用程序或操作系统添加到组织的授权软件清单中。不支持的软件应在库存系统中标记为不受支持。
2	2.3	应用	识别	使用软件清单工具	利用整个组织中的软件清单工具自动化业务系统上所有软件的文档。
2	2.4	应用	识别	跟踪软件库存信息	软件清单系统应跟踪所有软件的名称，版本，发布者和安装日期，包括组织授权的操作系统。
2	2.5	应用	识别	集成软件和硬件资产库存	软件库存系统应与硬件资产库存相关联，以便从单个位置跟踪所有设备和相关软件。
2	2.6	应用	响应	识别和标记非授权软件	确保删除未经授权的软件或及时更新库存
2	2.7	应用	防护	利用应用程序白名单	在所有资产上使用应用程序白名单技术，以确保只有授权的软件才能执行，并且所有未经授权的软件都无法在资产上执行。
2	2.8	应用	防护	实现应用程序白名单库	组织的应用程序白名单软件必须确保只允许授权的软件库（例如* .dll，* .ocx，* .so等）加载到系统进程中。
2	2.9	应用	防护	实现应用程序白名单脚本	“该组织的应用程序白名单软件必须确保只允许在系统上运行授权的，经过数字签名的脚本（例如* .ps1，* .py，宏等）。”
2	2.10	应用	防护	物理或逻辑上隔离高风险应用程序	应使用物理或逻辑上隔离的系统来隔离和运行业务运营所需的软件，但会给组织带来更高的风险。
3				**持续性漏洞管理**	
3	3.1	应用	检测	运行自动漏洞扫描工具	利用最新的符合SCAP标准的漏洞扫描工具，每周或更频繁地自动扫描网络上的所有系统，以识别组织系统中的所有潜在漏洞。
3	3.2	应用	检测	执行经过身份验证的漏洞扫描	使用在每个系统上本地运行的代理程序或使用在被测试系统上配置了提升权限的远程扫描程序执行经过身份验证的漏洞扫描。
3	3.3	用户	防护	保护专用评估账户	使用专用帐户进行经过身份验证的漏洞扫描，该扫描不应用于任何其他管理活动，并且应绑定到特定IP地址的特定计算机。
3	3.4	应用	防护	部署自动操作系统补丁管理工具	部署自动化软件更新工具，以确保操作系统运行软件供应商提供的最新安全更新。
3	3.5	应用	防护	部署自动软件补丁管理工具	部署自动化软件更新工具，以确保所有系统上的第三方软件都运行软件供应商提供的最新安全更新。
3	3.6	应用	响应	比较前后次漏洞扫描结果	定期比较背靠背漏洞扫描的结果，以验证漏洞是否已得到及时修复。
3	3.7	应用	响应	利用风险评级流程	利用风险评级流程优先处理已发现漏洞的修复。

4				**受控使用管理权限**	
4	4.1	用户	检测	维护管理账户清单	使用自动化工具清点所有管理帐户，包括域帐户和本地帐户，以确保只有经过授权的个人才能拥有提升的权限。
4	4.2	用户	防护	更改默认密码	在部署任何新资产之前，请更改所有默认密码，使其值与管理级别帐户一致。
4	4.3	用户	防护	确保使用专用管理帐户	确保具有管理帐户访问权限的所有用户都使用专用或辅助帐户进行提升的活动。此帐户仅应用于管理活动，而不能用于互联网浏览，电子邮件或类似活动。
4	4.4	用户	防护	使用唯一密码	如果不支持多因素身份验证（例如本地管理员，root或服务帐户），则帐户将使用该系统特有的密码。
4	4.5	用户	防护	对所有管理访问使用多因素身份验证	使用多重身份验证和加密通道进行所有管理帐户访问。
4	4.6	用户	防护	使用专用机器执行所有管理任务	确保管理员为所有需要管理访问权限的管理任务或任务使用专用计算机。此计算机将从组织的主网络中分段，不允许Internet访问。本机不会用于阅读电子邮件，撰写文档或浏览Internet。
4	4.7	用户	防护	限制对脚本工具的访问	将脚本工具（例如Microsoft PowerShell和Python）的访问权限限制为仅需要访问这些功能的管理或开发用户。
4	4.8	用户	检测	管理组成员身份更改的日志和警报	配置系统以在向任何分配了管理权限的组中添加或删除帐户时发出日志条目并发出警报。
4	4.9	用户	检测	记录和告警不成功的管理员账号登录尝试	配置系统以发出日志条目，并在管理帐户登录失败时发出警报。
5				**移动设备，笔记本电脑，工作站和服务器上的硬件和软件的安全配置**	
5	5.1	应用	防护	建立安全配置	为所有授权的操作系统和软件维护文档化的标准安全配置标准。
5	5.2	应用	防护	保持安全镜像	根据组织批准的配置标准，为企业中的所有系统维护安全映像或模板。任何新的系统部署或受损的现有系统都应使用其中一个图像或模板进行成像。
5	5.3	应用	防护	安全存储主镜像	将主映像和模板存储在安全配置的服务器上，并使用完整性监控工具进行验证，以确保只能对映像进行授权更改。
5	5.4	应用	防护	部署系统配置管理工具	部署系统配置管理工具，该工具将按照定期计划的时间间隔自动强制执行配置设置并将其重新部署到系统。
5	5.5	应用	检测	实施自动配置监控系统	利用符合安全内容自动化协议（SCAP）的配置监视系统来验证所有安全配置元素，目录批准的异常，以及发生未经授权的更改时的警报。
6				**审计日志的维护，监控和分析**	
6	6.1	网络	检测	利用三个同步时间源	使用至少三个同步时间源，所有服务器和网络设备定期从中检索时间信息，以便日志中的时间戳保持一致。
6	6.2	网络	检测	激活审核日志记录	确保已在所有系统和网络设备上启用本地日志记录。
6	6.3	网络	检测	启用详细日志记录	启用系统日志记录以包括详细信息，例如事件源，日期，用户，时间戳，源地址，目标地址和其他有用元素。
6	6.4	网络	检测	确保日志充足的存储空间	确保存储日志的所有系统都有足够的存储空间用于生成的日志。
6	6.5	网络	检测	中央日志管理	确保将适当的日志聚合到中央日志管理系统以进行分析和审核。
6	6.6	网络	检测	部署SIEM或日志分析工具	部署安全信息和事件管理（SIEM）或日志分析工具以进行日志关联和分析。
6	6.7	网络	检测	定期查看日志	定期检查日志以识别异常或异常事件。
6	6.8	网络	检测	定期调整SIEM	定期调整SIEM系统，以更好地识别可操作事件并降低事件噪声。
7				**电子邮件和Web浏览器保护**	
7	7.1	应用	防护	确保仅使用完全支持的浏览器和电子邮件客户端	确保只允许在组织中执行完全支持的Web浏览器和电子邮件客户端，理想情况下仅使用供应商提供的最新版本的浏览器和电子邮件客户端。
7	7.2	应用	防护	禁用不必要或未经授权的浏览器或电子邮件客户端插件	卸载或禁用任何未经授权的浏览器或电子邮件客户端插件或附加应用程序。
7	7.3	应用	防护	限制在Web浏览器和电子邮件客户端中使用脚本语言	确保只有授权的脚本语言才能在所有Web浏览器和电子邮件客户端中运行。

7	7.4	网络	防护	维护并实施基于网络的URL过滤器	实施基于网络的URL过滤器，限制系统连接到未经组织批准的网站的能力。应对每个组织的系统强制执行此过滤，无论它们是否在组织的设施中。
7	7.5	网络	防护	订阅URL-Categorization服务	订阅URL分类服务，以确保它们与最新的网站类别定义保持同步。默认情况下，应禁止未分类的网站。
7	7.6	网络	检测	记录所有URL请求	记录来自组织的每个系统的所有URL请求，无论是现场还是移动设备，以识别潜在的恶意活动并协助事件处理程序识别可能受损的系统。
7	7.7	网络	防护	使用DNS过滤服务	使用DNS过滤服务来帮助阻止对已知恶意域的访问。
7	7.8	网络	防护	实施DMARC并启用接收方验证	要降低来自有效域的欺骗或修改电子邮件的可能性，请实施基于域的邮件身份验证，报告和一致性（DMARC）策略和验证，首先实施发件人策略框架（SPF）和DomainKeys识别邮件（DKIM）标准。
7	7.9	网络	防护	阻止不必要的文件类型	如果组织的业务不需要文件类型，则阻止所有进入组织电子邮件网关的电子邮件附件。
7	7.10	网络	防护	沙箱中检测所有电子邮件附件	使用沙盒分析和阻止具有恶意行为的入站电子邮件附件。
8				**恶意软件防御**	
8	8.1	设备	防护	利用集中管理的反恶意软件	利用集中管理的反恶意软件软件，持续监控和保护组织的每个工作站和服务器。
8	8.2	设备	防护	确保更新防恶意软件和签名	确保组织的反恶意软件软件定期更新其扫描引擎和签名数据库。
8	8.3	设备	防护	启用操作系统反漏洞功能/部署反漏洞利用技术	启用操作系统中可用的反利用功能，如数据执行保护（DEP）或地址空间布局随机化（ASLR），或部署适当的工具包，这些工具包可配置为对更广泛的应用程序和可执行文件应用保护。
8	8.4	设备	检测	配置可移动设备的防恶意软件扫描	配置设备，以便在插入或连接时自动对可移动媒体进行反恶意软件扫描。
8	8.5	设备	防护	配置设备不自动运行内容	将设备配置为不从可移动媒体自动运行内容。
8	8.6	设备	检测	集中防恶意软件日志记录	将所有恶意软件检测事件发送到企业反恶意软件管理工具和事件日志服务器，以进行分析和警报。
8	8.7	网络	检测	启用DNS查询日志记录	启用域名系统（DNS）查询日志记录以检测已知恶意域的主机名查找。
8	8.8	设备	检测	启用命令行审核日志记录	为命令shell启用命令行审核日志记录，例如Microsoft Powershell和Bash。
9				**网络端口，协议和服务的限制和控制**	
9	9.1	设备	识别	将活动端口，服务和协议关联到资产清单	将活动端口，服务和协议关联到资产清单中的硬件资产。
9	9.2	设备	防护	确保仅批准的端口，协议和服务正在运行	确保仅在具有经过验证的业务需求的系统上侦听的网络端口，协议和服务正在每个系统上运行。
9	9.3	设备	检测	执行常规自动端口扫描	针对所有系统定期执行自动端口扫描，并在系统上检测到未经授权的端口时发出警报。
9	9.4	设备	防护	应用基于主机的防火墙或端口过滤	在终端系统上应用基于主机的防火墙或端口过滤工具，使用default-deny规则删除除明确允许的那些服务和端口之外的所有流量。
9	9.5	设备	防护	实施应用程序防火墙	将应用程序防火墙放在任何关键服务器的前面，以验证和验证进入服务器的流量。应阻止并记录任何未经授权的流量。
10				**数据恢复功能**	
10	10.1	数据	防护	确保定期自动后退	确保定期自动备份所有系统数据。
10	10.2	数据	防护	执行完整的系统备份	确保通过成像等流程将组织的每个关键系统备份为完整系统，以便快速恢复整个系统。
10	10.3	数据	防护	备份媒体上的测试数据	通过执行数据恢复过程来定期测试备份介质上的数据完整性，以确保备份正常工作。
10	10.4	数据	防护	确保备份保护	确保备份在存储时以及通过网络移动时通过物理安全性或加密得到适当保护。这包括远程备份和云服务。
10	10.5	数据	防护	确保备份至少有一个非连续可寻址目的地	确保所有备份至少有一个备份目标，该目标不能通过操作系统调用连续寻址。
11				**网络设备的安全配置，例如防火墙，路由器和交换机**	
11	11.1	网络	识别	维护网络设备的标准安全配置	为所有授权的网络设备维护标准的，记录的安全配置标准。

11	11.2	网络	识别	文档流量配置规则	允许流量通过网络设备的所有配置规则都应记录在配置管理系统中，其中包含每个规则的特定业务原因，负责该业务需求的特定个人名称以及预期的需求持续时间。
11	11.3	网络	检测	使用自动化工具验证标准设备配置和检测更改	将所有网络设备配置与为使用中的每个网络设备定义的已批准安全配置进行比较，并在发现任何偏差时发出警报。
11	11.4	网络	防护	在所有网络设备上安装任何与安全相关的更新的最新稳定版本	在所有网络设备上安装最新稳定版本的任何安全相关更新。
11	11.5	网络	防护	使用多重身份验证和加密会话管理网络设备	使用多重身份验证和加密会话管理所有网络设备。
11	11.6	网络	防护	使用专用机器执行所有网络管理任务	确保网络工程师使用专用计算机执行所有需要提升访问权限的管理任务或任务本机应从组织的主网络中分割出来，不允许上网。本机不得用于阅读电子邮件，撰写文档或上网。
11	11.7	网络	防护	通过专用网络管理网络基础设施	跨网络连接管理网络基础架构，这些网络连接与该网络的业务用途分离，依赖于单独的VLAN，或者最好是完全不同的物理连接，用于网络设备的管理会话。
12				**边界防御**	
12	12.1	网络	识别	维护网络边界清单	维护组织所有网络边界的最新清单。
12	12.2	网络	检测	扫描可信网络边界上的未经授权的连接	从每个可信网络边界外部执行定期扫描，以检测可通过边界访问的任何未经授权的连接。
12	12.3	网络	防护	使用已知的恶意IP地址拒绝通信	拒绝与已知的恶意或未使用的Internet IP地址进行通信，并限制仅访问组织的每个网络边界上的可信和必要的IP地址范围。
12	12.4	网络	防护	否认未经授权的端口通信	拒绝通过未经授权的TCP或UDP端口或应用程序流量进行通信，以确保只允许授权协议在组织的每个网络边界内跨越网络或跨越网络边界。
12	12.5	网络	检测	配置监控系统以记录网络数据包	配置监视系统以记录通过组织的每个网络边界的边界的网络数据包。
12	12.6	网络	检测	部署基于网络的IDS传感器	部署基于网络的入侵检测系统（IDS）传感器，以寻找异常的攻击机制，并在组织的每个网络边界检测这些系统的危害。
12	12.7	网络	防护	部署基于网络的入侵防御系统	部署基于网络的入侵防御系统（IPS），以阻止组织的每个网络边界上的恶意网络流量。
12	12.8	网络	检测	在网络边界设备上部署NetFlow集合	在所有网络边界设备上启用NetFlow和日志记录数据的收集。
12	12.9	网络	检测	部署应用层过滤代理服务器	确保进出Internet的所有网络流量都通过经过身份验证的应用层代理，该代理配置为过滤未经授权的连接。
12	12.10	网络	检测	在代理处解密网络流量	在分析内容之前，解密边界代理处的所有加密网络流量。但是，组织可以使用可以通过代理访问的允许站点的白名单，而无需解密流量。
12	12.11	用户	防护	要求所有远程登录使用多重身份验证	要求对组织网络的所有远程登录访问权限以加密传输中的数据并使用多因素身份验证。
12	12.12	设备	防护	管理所有设备远程登录内部网络	扫描所有企业设备，在访问网络之前远程登录组织的网络，以确保组织的每个安全策略都以与本地网络设备相同的方式实施。
13				**数据保护**	
13	13.1	数据	识别	维护库存敏感信息	维护组织技术系统（包括位于现场或远程服务提供商处）的技术系统存储，处理或传输的所有敏感信息的清单。
13	13.2	数据	防护	删除组织未定期访问的敏感数据或系统	从网络中删除组织未定期访问的敏感数据或系统。这些系统只能由需要偶尔使用系统的业务部门用作独立系统（与网络断开连接），或者在需要时完全虚拟化和断电。
13	13.3	数据	检测	监控和阻止未经授权的网络流量	在网络边界上部署自动化工具，监控敏感信息的未授权传输并阻止此类传输，同时提醒信息安全专业人员。

13	13.4	数据	防护	仅允许访问授权的云存储或电子邮件提供商	仅允许访问授权的云存储或电子邮件提供商。
13	13.5	数据	检测	监控并检测任何未经授权的加密使用	监控离开组织的所有流量并检测任何未经授权的加密使用。
13	13.6	数据	防护	加密所有移动设备的硬盘驱动器。	利用经过批准的全盘加密软件加密所有移动设备的硬盘。
13	13.7	数据	防护	管理USB设备	如果需要USB存储设备，则应使用可配置系统以允许使用特定设备的企业软件。应保留此类设备的清单。
13	13.8	数据	防护	管理系统外部可移动介质读/写配置	如果没有业务需要支持此类设备，请将系统配置为不将数据写入外部可移动介质。
13	13.9	数据	防护	加密USB存储设备上的数据	如果需要USB存储设备，则必须在静止时加密存储在此类设备上的所有数据。
14				**基于最小需知的受控访问**	
14	14.1	网络	防护	基于标签度对网络进行分段	根据存储在服务器上的信息的标签或分类级别对网络进行分段，找到分离的虚拟局域网（VLAN）上的所有敏感信息。
14	14.2	网络	防护	在VLAN之间启用防火墙过滤	在VLAN之间启用防火墙过滤，以确保只有经过授权的系统才能与履行其特定职责所必需的其他系统进行通信。
14	14.3	网络	防护	禁用工作站到工作站通信	禁用所有工作站到工作站的通信，以限制攻击者通过专用VLAN或微分段等技术横向移动并危及相邻系统的能力。
14	14.4	数据	防护	加密传输中的所有敏感信息	加密传输中的所有敏感信息。
14	14.5	数据	检测	利用主动发现工具识别敏感数据	利用主动发现工具识别组织技术系统存储，处理或传输的所有敏感信息，包括位于现场或远程服务提供商的技术系统，并更新组织的敏感信息清单。
14	14.6	数据	防护	通过访问控制列表保护信息	使用文件系统，网络共享，声明，应用程序或数据库特定的访问控制列表保护存储在系统上的所有信息。这些控制措施将强制执行这样的原则：只有经过授权的个人才能根据他们作为其职责的一部分访问信息的需要访问信息。
14	14.7	数据	防护	通过自动化工具实施对数据的访问控制	使用自动化工具（例如基于主机的数据丢失防护）即使在从系统复制数据时也可以对数据实施访问控制。
14	14.8	数据	防护	加密静态敏感信息	使用需要未集成到操作系统中的辅助身份验证机制的工具加密静态的所有敏感信息，以便访问信息。
14	14.9	数据	检测	强制执行详细日志记录以访问或更改敏感数据	实施详细的审计日志记录，以访问敏感数据或更改敏感数据（利用文件完整性监控或安全信息和事件监控等工具）。
15				**无线访问控制**	
15	15.1	网络	Identify	维护授权无线接入点清单	维护连接到有线网络的授权无线接入点的清单。
15	15.2	网络	Detect	检测连接到有线网络的无线接入点	配置网络漏洞扫描工具，以检测连接到有线网络的未授权无线接入点并发出警报。
15	15.3	网络	Detect	使用无线入侵检测系统	使用无线入侵检测系统（WIDS）检测连接到网络的未授权无线接入点并发出警报。
15	15.4	设备	防护	如果不需要，禁用设备上的无线访问	在没有无线访问业务目的的设备上禁用无线访问。
15	15.5	设备	防护	限制客户端设备上的无线访问	在具有基本无线业务目的的客户端计算机上配置无线访问，以允许仅访问授权的无线网络并限制对其他无线网络的访问。
15	15.6	设备	防护	禁用无线客户端上的对等无线网络功能	禁用无线客户端上的对等（adhoc）无线网络功能。
15	15.7	网络	防护	利用高级加密标准（AES）加密无线数据	利用高级加密标准（AES）加密传输中的无线数据。
15	15.8	网络	防护	使用需要相互多重身份验证的无线身份验证协议	确保无线网络使用身份验证协议，例如可扩展身份验证协议 - 传输层安全性（EAP / TLS），这需要进行相互的多因素身份验证。
15	15.9	设备	防护	禁用设备的无线外围设备访问	禁用设备（例如蓝牙和NFC）的无线外围设备访问，除非出于商业目的需要此类访问。

15	15.10	网络	防护	为个人和不受信任的设备创建单独的无线网络	为个人或不受信任的设备创建单独的无线网络。应将此网络的企业访问视为不受信任，并相应地进行过滤和审核。
16				**帐户监控**	
16	16.1	用户	识别	维护认证系统清单	维护每个组织的身份验证系统的清单，包括位于现场或远程服务提供商的系统。
16	16.2	用户	防护	配置集中认证点	通过尽可能少的集中身份验证点（包括网络，安全性和云系统）为所有帐户配置访问权限。
16	16.3	用户	防护	需要多重身份验证	对所有系统上的所有用户帐户都要求进行多重身份验证，无论是现场管理还是第三方提供商。
16	16.4	用户	防护	加密或散列所有身份验证凭据	存储时使用salt加密或散列所有身份验证凭据。
16	16.5	用户	防护	加密用户名和身份验证凭据的传输	确保使用加密通道跨网络传输所有帐户用户名和身份验证凭据。
16	16.6	用户	识别	维护账户清单	维护由身份验证系统组织的所有帐户的清单。
16	16.7	用户	防护	建立撤销访问权限的流程	建立并遵循自动流程，通过在员工或承包商终止或更改职责后立即禁用帐户来撤销系统访问权限。禁用这些帐户而不是删除帐户可以保留审计跟踪。
16	16.8	用户	响应	禁用任何无关联帐户	禁用任何无法与业务流程或业务所有者关联的帐户。
16	16.9	用户	响应	禁用休眠帐户	在一段时间不活动后自动禁用休眠帐户。
16	16.10	用户	防护	确保所有帐户都有到期日期	确保所有帐户都有一个受监控和强制执行的过期日期。
16	16.11	用户	防护	不活动后锁定工作站会话	在标准的不活动时间段后自动锁定工作站会话。
16	16.12	用户	检测	监控尝试访问已停用的帐户	监控尝试通过审核日志记录访问已停用的帐户。
16	16.13	用户	检测	帐户登录行为偏差警报	用户偏离正常登录行为时的警报，例如时间，工作站位置和持续时间。
17				**实施安全意识和培训计划**	
17	17.1	N/A	N/A	执行技能差距分析	执行技能差距分析，了解劳动力成员不遵守的技能和行为，使用此信息构建基线教育路线图。
17	17.2	N/A	N/A	提供培训以填补技能差距	提供培训以解决确定的技能差距，从而对员工的安全行为产生积极影响。
17	17.3	N/A	N/A	实施安全意识计划	为所有员工成员创建一个安全意识计划，定期完成，以确保他们理解并展示必要的行为和技能，以帮助确保组织的安全。组织的安全意识计划应以连续和引人入胜的方式进行沟通。
17	17.4	N/A	N/A	经常更新意识内容	确保组织的安全意识计划经常更新（至少每年一次），以解决新技术，威胁，标准和业务要求。
17	17.5	N/A	N/A	培训员工进行安全认证	培训员工成员了解启用和利用安全身份验证的重要性。
17	17.6	N/A	N/A	培训员工识别社会工程攻击	培训员工如何识别不同形式的社会工程攻击，例如网络钓鱼，电话诈骗和假冒电话。
17	17.7	N/A	N/A	培训敏感数据处理工作人员	培训员工如何识别和妥善存储，传输，存档和销毁敏感信息。
17	17.8	N/A	N/A	培训员工无意识数据暴露的原因	培训员工以了解无意数据泄露的原因，例如丢失其移动设备或由于电子邮件中的自动完成而向错误的人发送电子邮件。
17	17.9	N/A	N/A	培训员工识别和报告事故	培训员工能够识别事件的最常见指标并能够报告此类事件。
18				**应用软件安全**	
18	18.1	N/A	N/A	建立安全编码实践	建立适合所使用的编程语言和开发环境的安全编码实践。
18	18.2	N/A	N/A	确保对所有内部开发的软件执行显式错误检查	对于内部开发的软件，请确保对所有输入执行显式错误检查并记录，包括大小，数据类型和可接受的范围或格式。
18	18.3	N/A	N/A	验证仍然支持获取的软件	验证开发人员是否仍支持从组织外部获取的所有软件的版本，或根据开发人员安全建议进行适当强化。
18	18.4	N/A	N/A	仅使用最新且值得信赖的第三方组件	仅为组织开发的软件使用最新且受信任的第三方组件。
18	18.5	N/A	N/A	仅使用标准化和广泛评估的加密算法	仅使用标准化且经过广泛审查的加密算法。

18	18.6	N/A	N/A	确保软件开发人员受到安全编码的培训	确保所有软件开发人员接受针对其特定开发环境和职责编写安全代码的培训。
18	18.7	N/A	N/A	应用静态和动态代码分析工具	应用静态和动态分析工具来验证内部开发的软件是否遵守安全编码实践。
18	18.8	N/A	N/A	建立接受和处理软件漏洞报告的流程	建立接受和处理软件漏洞报告的流程，包括为外部实体提供与您的安全组联系的方法。
18	18.9	N/A	N/A	独立的生产和非生产系统	为生产和非生产系统维护单独的环境。开发人员不应对生产环境进行不受监控的访问。
18	18.10	N/A	N/A	部署Web应用程序防火墙（WAF）	通过部署Web应用程序防火墙（WAF）来保护Web应用程序，该应用程序防火墙检查流向Web应用程序的所有流量，以发现常见的Web应用程序攻对于非基于Web的应用程序，如果此类工具可用于给定的应用程序类型，则应部署特定的应用程序防火墙。如果流量已加密，则设备应位于加密后面或能够在分析之前解密流量。如果两个选项都不合适，则应部署基于主机的Web应用程序防火墙。
18	18.11	N/A	N/A	使用数据库的标准强化配置模板	对于依赖数据库的应用程序，请使用标准强化配置模板。还应测试作为关键业务流程一部分的所有系统。
19				**事件响应和管理**	
19	19.1	N/A	N/A	文档化事件响应程序	确保有书面事件响应计划，用于定义人员角色以及事件处理/管理阶段。
19	19.2	N/A	N/A	为事件响应分配工作标题和职责	将处理计算机和网络事件的职务和职责分配给特定的个人，并通过解决方案确保整个事件的跟踪和记录。
19	19.3	N/A	N/A	指定管理人员支持事件处理	指定管理人员和备份，他们将通过担任关键决策角色来支持事件处理流程。
19	19.4	N/A	N/A	制定全组织范围的报告事件标准	为系统管理员和其他员工成员向事件处理团队报告异常事件所需的时间，组织范围的标准，此类报告的机制以及事件通知中应包含的信息类型。
19	19.5	N/A	N/A	维护联系信息以报告安全事件	汇总和维护有关用于报告安全事件的第三方联系信息的信息，例如执法部门，相关政府部门，供应商和ISAC合作伙伴。
19	19.6	N/A	N/A	发布有关报告计算机异常和事件的信息	发布有关向事件处理团队报告计算机异常和事件的所有劳动力成员的信息。此类信息应包含在日常员工意识活动中。
19	19.7	N/A	N/A	为人员进行定期事件演练	为事件响应中涉及的员工规划和执行例行事件响应练习和场景，以保持对响应现实世界威胁的意识和舒适度。练习应使用可用的工具和数据测试沟通渠道，决策制定和事故响应者技术能力。
19	19.8	N/A	N/A	创建事件评分和优先级架构	根据对组织的已知或潜在影响创建事件评分和优先级架构。利用分数来定义状态更新和升级程序的频率。
20				**渗透测试和红队练习**	
20	20.1	N/A	N/A	建立渗透测试计划	建立渗透测试程序，包括全范围的混合攻击，例如无线，基于客户端和Web应用程序攻击。
20	20.2	N/A	N/A	定期进行外部和内部渗透测试	定期进行外部和内部渗透测试，以识别可用于成功利用企业系统的漏洞和攻击媒介。
20	20.3	N/A	N/A	执行定期红队练习	定期执行红队练习，以测试组织是否准备好识别和阻止攻击或快速有效地做出响应。
20	20.4	N/A	N/A	包括测试是否存在未受保护的系统信息和工件	包括对攻击者有用的未受保护的系统信息和工件的测试，包括网络图，配置文件，旧的渗透测试报告，电子邮件或包含密码的文档或对系统操作至关重要的其他信息。
20	20.5	N/A	N/A	为通常在生产中测试的元素创建测试床	创建一个模拟生产环境的测试平台，用于特定的渗透测试和Red Team针对通常不在生产中测试的元素的攻击，例如对监督控制和数据采集以及其他控制系统的攻击。
20	20.6	N/A	N/A	在Concert中使用漏洞扫描和渗透测试工具	一起使用漏洞扫描和渗透测试工具。漏洞扫描评估的结果应作为指导和集中渗透测试工作的起点。
20	20.7	N/A	N/A	确保使用开放的机器可读标准记录渗透测试的结果	尽可能确保使用开放的机器可读标准（例如SCAP）记录红队结果。设计一种评分方法，用于确定红队练习的结果，以便可以随时间比较结果。
20	20.8	N/A	N/A	控制和监控与渗透测试相关的帐户	应该控制和监视用于执行渗透测试的任何用户或系统帐户，以确保它们仅用于合法目的，并在测试结束后被删除或恢复到正常功能。