等保2.0体系互联网合规实践白皮书

腾讯公司

中国电子科技集团公司第十五研究所〔信息产业信息安全测评中心〕

深圳市网安计算机安全检测技术有限公司

二零二零年 十月

Tencent 腾讯 | ITSTEC | 网安检测 NST TECHNOLOGY

版权声明

编制人员

刘羽、张益、洪跃腾、黄超、郭铁涛、郑兴、华珊珊、耿琛、肖煜、姬生利、孙少波、霍珊珊、刘健、王余、练美玲、王婷、李光辉、彭成锋、刘志高、刘泽美、谢旭、朱思霖。

特别感谢

腾讯安全平台部、腾讯安全管理部、腾讯安全云鼎实验室、腾讯桌面安全产品部、腾讯产业安全运营部、腾讯云安全合规部、中国电子科技集团公司第十五研究所、深圳市网安计算机安全检测技术有限公司。

目录

1 前言

2019 年 5 月 13 日，网络安全等级保护制度 2.0（简称等保 2.0）三大核心标准（《基本要求》、《测评要求》和《设计要求》）正式发布，并于 2019 年 12 月 1 日开始实施。随着等保 2.0 标准的陆续发布与实施，中国特色社会主义建设全面深入推进, 5G、人工智能、云计算、物联网、工业互联网、大数据等新技术新应用的兴起,以及关键信息基础设施安全保护、个人信息保护和数据安全等工作不断强化,对网络安全工作提出了更高的要求。如何让业务能够安全合规的运营成为网络运营者的关键需求。

等保 2.0 标准具有以下特点：第一，基本要求、测评要求和技术要求框架统一，采用安全管理中心支持下的三重防护结构框架；通用安全要求+新型应用安全扩展要求，将云计算、移动互联、物联网、工业控制等列入标准规范。其中云计算扩展要求作为重点内容被第一个单独列出来。

此次规范的发布将等保从推荐行提升到强行性标准的层面。等保 1.0 的最高国家政策是国务院 147 号令，而等保 2.0 标准的最高国家政策是网络安全法，其中《中华人民共和国网络安全法》第二十一条要求，国家实施网络安全等级保护制度；第二十五条要求，网络运营者应当制定网络安全事件应急预案；第三十一条则要求，关键基础设施，在网络安全等级保护制度的基础上，实行重点保护；第五十九条规定的网络安全保护义务的，由有关主管部门给予处罚。因此不开展等级保护等于违法。

借此，腾讯公司、中国电子科技集团公司第十五研究所（信息产业信息安全测评中心）、深圳市网安计算机安全检测技术有限公司联合编制了《等保 2.0

体系互联网合规实践白皮书》（简称“白皮书”），将对等保 2.0 的理解和实践分享给用户和业界，以求相互学习，相互借鉴，共同推动各行业等级保护领域的发展与知识共享。

2 等级保护 2.0 技术合规要求分析和实践

2.1 可信计算合规

等级保护 2.0 中，其中一个很重的要求变化，就是已经由被动防御转变为主动防御、动态防御。而作为应对的重要安全措施之一，就是需要通过不断强化网络安全分析能力、未知威胁的检测能力实现安全防护要求，而可信计算就是其中一个实现的落地措施和方案。

等级保护 2.0 也是充分采用“一个中心三重防护”的理念，一个中心指“安全管理中心”，三重防护指“安全计算环境、安全区域边界、安全网络通信”，在落实层面也是强化了可信计算安全技术要求的使用。

通过可信计算技术来实现对系统中应用和配置文件、参数进行验证，保障系统在可信环境下运行。《网络安全等级保护基本要求》中强化了可信计算，充分体现一个中心、三重防护的理念，部分具体要求变化见下表所示：

级别	要求
一级	可基于可信根对**通信设备**的系统引导程序、系统程序等进行可信验证，并在检测到其可信性受到破坏后进行报警。
二级	可基于可信根对通信设备的系统引导程序、系统程序、**重要配置参数和通信应用程序**等进行可信验证，并在检测到其可信性受到破坏后进行报警，**并将验证结果形成审计记录送至安全管理中心。**

三级	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，**并在应用程序的关键执行环节进行动态可信验证**，在检测到其可信性受到破坏后进行报警，并将验证结果形成审。
四级	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的**所有执行环节**进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，**并进行动态关联感知。**

腾讯实践：

在当前可信计算的应用场景中，目前计算设备的可信化实践中，个人设备远超出服务器，而腾讯内部实践场景主要面向服务器层面，这在一定程度提高了可信计算在服务器端应用的门槛和技术难度。腾讯安全平台部洋葱反入侵团队、Blade Team 安全研究团队联合相关部门专家，通过一系列研究和不断优化测试，最终形成了腾讯内部可落地的可信计算实践。这里我们主要简述部分实践内容，供业界同仁参考。

对于以上等保要求的理解，并结合腾讯实际经验和内部运维场景，在实践落地中，我们将以上：

- “通讯设备”的定义理解为：机房内的业务实现、通信、存储的关键设备，主体即 x86 平台的服务器

- “重要配置参数和通信应用程序”的定义理解为：服务器上的关键配置文件与程序
- “安全管理中心相关”定义理解为：上述可信验证过程的结果不仅仅在本地可见，关键是集中上报存档
- “并在应用程序的关键执行环节进行动态可信验证”定义理解为：实现了可孤立自证的运算执行环境（SGX），保障执行环节无问题，或进行多方背靠背计算核对(区块链)
- “动态关联感知”定义理解为：针对多维度数据、异构数据进行业务事务级别上的关联，以发现异常。

在腾讯内部可信计算实践中，硬件的可信安全是我们最早关注的领域，也是此次介绍的重点。腾讯在早期实践过程中，也是遇到了困难和挑战，包括且不限于：

- 关键技术缺失：部分供应商没有适配 BootGuard，不具备硬件 TCB 的可信启动；
- 管理途径缺失：目前货架技术上的可信启动技术均为个人电脑设计，缺乏服务器大规模管理所需的管理途径，例如 secure boot 的证书管理、各种安全功能的带外开启关闭；
- 告警信息不具备上报能力：类似管理途径缺失，现有的货架技术不具备本地告警能力，更别提远程告警能力；
- 安全事件记录粒度过粗：TPM 在供应商的实现中仅具备 PCR 值的记录能力，没有实现事件日志记录，但是即便具备了事件日志记录，记

录的信息量依然不足以用于快速判定事件性质

针对以上可信计算上的挑战，腾讯从供应链与自研两方面共同着手发力，一方面转化等保相关要求传递至供应商形成落地方案，另一方评估供应商方案的局限性展开自研安全能力建设，逐一解决形成落地解决技术可行性方案：

（1）供应链方案：

- 推动供应商导入硬件可信根的货架技术
- 进行 BMC、主板固件定制改造，增加安全特性的管理路径与告警能力
- 腾讯服务器硬件安全标准，将等保要求与行业先进标准转化吸收
- 服务器供应安全自测要求，将抽象安全要求转化为落地技术指标
- 供应链方案局限性：
  - 货架技术风险覆盖有限，更新缓慢

    业界提供的 Secure boot、Bootguard 技术由多方分别实施，覆盖范围衔接过程中易出现纰漏，一旦出现漏洞，供应商响应也非常缓慢，无法快速可控的迭代安全能力，固件安全不能靠他人
  - 供应链攻击

    供应链交付的服务器未必符合约定的自测规范，可能的原因有供应链自身工作失误、供应链受到三方污染、物流链路的物理攻击等，必须有自主可控的手段一定限度上保障供应商的交付质量

（2）自研安全方案

- 自研方案实现
  - 自主研发的主板固件检测 chipsafe & chipreg，实时细粒度 UEFI

固件监控，嵌入服务器交付与投产生命周期，校验相关安全配置有效性，并申报国家技术发明专利

- 基于可信执行环境技术保护应用程序关键执行环节，并在腾讯云上架可信计算解决方案
- 集成安全管理中心，生成各类安全异常告警，推送至安全责任人，支持移动办公

（3）方案技术落地

- **方案挑战与难点**
  - 软硬件兼容

    引入硬件可信根后，主板固件版本无法回退至引入可信根以前；板卡固件需补充签名认证，否则无法启动；操作系统的部署、启动链环境、运行时板卡驱动必须实现全面兼容。
  - 供应维保体系适配

    引入各类安全措施后，服务器的生产流程需添加步骤，验收测试环境需兼容安全措施，维保板卡配件需逐步更新，维保软件需更新淘汰。
  - 无参考先例

    国内外无相关实践参考。
- **实施方案**
  - 腾讯 tlinux 改造

    tlinux 启动程序签名、tlinux 内核模块签名、tlinux 安装镜像 ISO 改

造、签名证书管理

- 服务器全生命周期流程改造

  OEM 服务器产线兼容性改造、服务器验收流程添加可信验收、操作系统部署流程兼容性改造、服务器固件管理系统适配、服务器自维保工具适配等。

- 长时间、大规模持续测试迭代

  验证测试时间超过 6 个月，软件方案测试机器超过万台，硬件落地测试机超过千台。

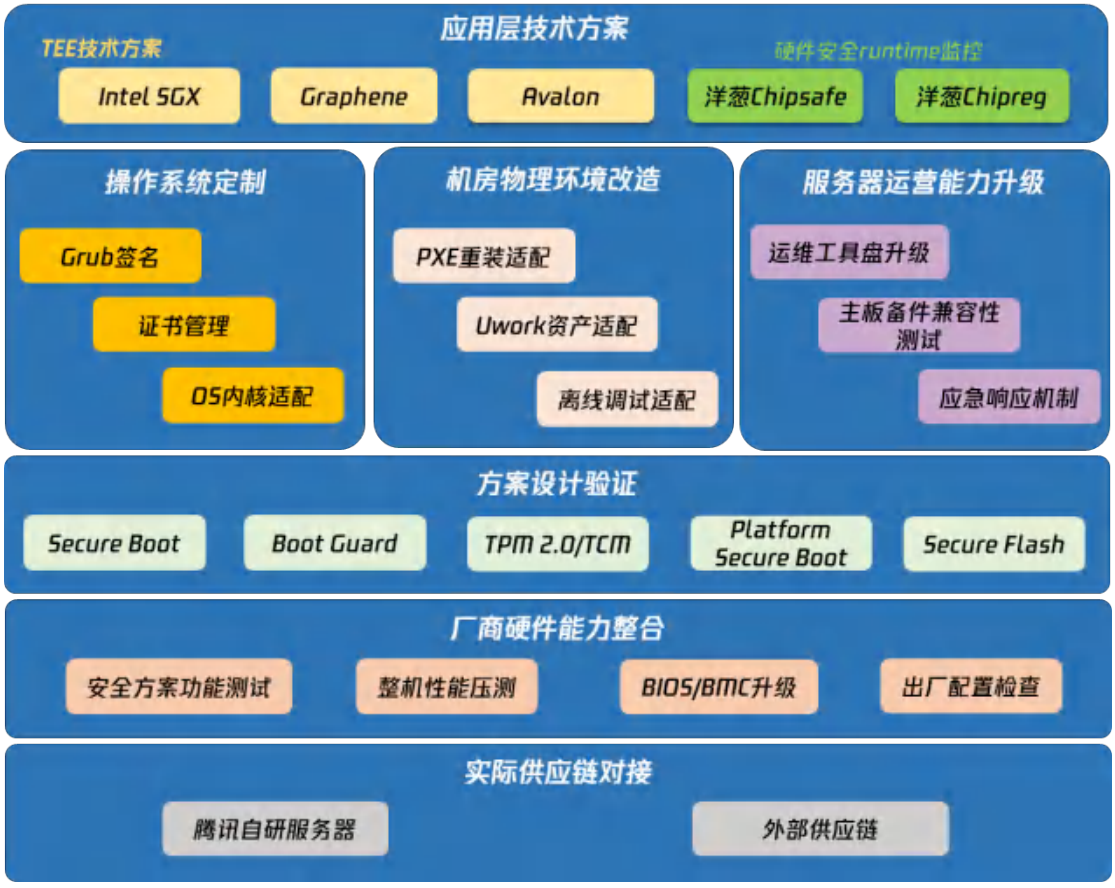


图 2.1.1 腾讯可信计算落地架构方案

未来，腾讯安全平台部也将继续在可信计算体系建设方面，积极地开展方案研究、设计与部署应用，并与上游多家供应链厂商的密切合作，力图打造国

内首个服务器安全启动成规模部署用例，并借助服务器硬件安全规范，把控厂商供应链安全水平，提升公司研发环境与云上业务对于 UEFI Bootkit、供应链攻击等底层安全威胁的免疫能力。

此外，腾讯云推出的“星星海”自研服务器由腾讯安全平台部主导进行安全能力评估建设，目前已具备可信启动的硬件防护能力。 未来，安全平台部将会持续在这个领域进行相关研发和部署。

2.2 密码技术合规

等保 2.0 标准已经在 2019 年 12 月正式开始实施。等保 2.0 标准中对密码技术做了明确的要求，密码技术主要出现在三级和四级安全要求中，主要涉及安全通信网络、安全计算环境以及安全运维管理等部分内容。随着《密码法》的颁布和实施，对等级保护对象整体安全保护能力的要求也逐步提高。密码法中也明确强调了对关键信息基础设施中密码技术的要求。

密码技术是目前世界上公认的保障信息安全最有效、最可靠的核心技术。密码法的颁布对于等保 2.0 的实施具有进一步的指导意义，等保 2.0 中定级为三级和四级的保护对象及系统，大部分也是关系国计民生的关键基础设施，这些关键基础设施中对密码技术的应用必须严格遵守密码法的规定。制定和实施密码法,就是要把密码应用和管理的基本制度及时上升为法律规范，推动构建以密码技术为核心、多种技术交叉融合的网络空间安全体系。

在等保 2.0 基本要求的《附录 B 关于等级保护对象整体安全保护能力的要求》中也提到：“本标准针对较高级别的等级保护对象，使用密码技术、可

信技术等，多数安全功能（如身份鉴别、访问控制、数据完整性、数据保密性等）为了获得更高的强度，均要基于密码技术或可信技术，为了保证等级保护对象的整体安全防护能力，应建立基于密码技术的统一支撑平台，支持高强度身份鉴别、访问控制、数据完整性、数据保密性等安全功能的实现。”因此，密码作为网络安全的基因和卫士，对于较高级别的等级保护对象的安全防护中起到了不可替代的作用。

2.2.1 等保 2.0 对密码技术的要求

密码（Cryptography，不是口令 Password）是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。密码可以完整实现网络空间身份防假冒、信息防泄密、内容防篡改、行为抗抵赖等功能，满足网络与信息系统对机密性、完整性、真实性和不可否认性等安全需求。因其解决网络安全问题的有效性，能够在基础信息网络、重要信息系统、重要工业控制系统等重要领域发挥核心作用。

本章节梳理了等保 2.0 标准下对密码技术、产品和服务的一些要求。

安全层面	安全控制点	密码技术相关要求
安全通信网络	通信传输	本项要求中密码技术相关要求包括： a）应采用密码技术保证通信过程中数据的完整性； b）应采用密码技术保证通信过程中数据的保密性； c）应在通信前基于密码技术对通信的双方进行验证或认证； d）应基于硬件密码模块对重要通信过程进行密码运算和密钥管理。
安全计算环境	身份鉴别	本项要求中密码技术相关要求包括： c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； d）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。
	数据完整性	本项要求包括： a）应采用密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别

安全层面	安全控制点	密码技术相关要求
		数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； b）应采用密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； c）在可能涉及法律责任认定的应用中，应采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的抗抵赖和数据接收行为的抗抵赖。
	数据保密性	本项要求包括： a）应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等； b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。
安全管理中心	集中管控	本项要求包括：

安全层面	安全控制点	密码技术相关要求
		b) 应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理。
安全运维管理	密码管理	应遵循密码相关的国家标准和行业标准； b) 应使用国家密码管理主管部门认证核准的密码技术和产品；
云拓展(云服务商)	镜像和快照保护	A) 应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改； B) 应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。 C) 应使用校验码或密码技术确保虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施； D) 应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程。

2.2.2 等保 2.0 如何使用密码技术

密码技术主要解决四类问题：

（1）身份鉴别

身份鉴别侧重于网络用户的身份认证，防范攻击者仿冒用户身份。典型案例包括网银 U 盾认证、手机或虚拟机环境中的协同软认证、公钥基础设施 PKI 体系以及基于 IBC 的信任体系等。真实性实现的技术方式主要包括：一是基于对称密码、公钥密码等密码技术的鉴别机制；二是基于静态口令的鉴别机制；三是基于动态口令的鉴别机制；四是基于生物特征的鉴别机制（FIDO 在线快捷身份鉴别）。

（2）传输通道的通信安全，涉及保密性和完整性

数据传输过程中的通信安全问题，主要是为了防范中间人对消息的窃听或篡改。 典型案例包括采用 SSL VPN 或 IPSec VPN 保护商业秘密信息在互联网安全传输、采用 HTTPS 保护 Web 应用数据传输安全、PGP 安全邮件收发、基于代理重加密的云上数据分发以及企业内文件授权分发等。

（3）存储过程的数据安全

数据存储的安全问题，防范攻击者对终端、服务端（包含应用系统、数据库或文件服务器等）设备数据非法访问造成的数据泄露。

实现保密性保护的方法一般可分为三类：一是访问控制方法，防止非授权用户访问敏感信息；二是信息隐藏的方法，避免恶意用户发现敏感信息的存在；三是信息加密的方法，允许敌方观测到信息，但是，无法从得到的数据提炼出有用户的信息。加密是数据通信和数据存储中实现保密性保护的一种主要机制。

可利用具有商用密码产品型号的服务器密码机、经过核准的密码服务以及内置密码模块等对重要数据进行加密保护。

实现完整性保护的方法主要包括：一是：采用消息鉴别码实现完整性。对称密码算法和杂凑算法都可以用于消息鉴别码生成。二是：采用数字签名实现完整性。虽然基于对称密码或杂凑算法的完整性保护机制能够确保接收者接收消息之前的消息完整性，但是不能防止接收者对消息的伪造，基于公钥密码技术的数字签名不仅可以防止敌手对消息进行篡改，还能防止接收者对消息进行伪造，实现消息发送行为的不可否认性。实现时，可将重要数据计算 MAC 消息鉴别码或数字签名，亦可将重要数据发送到服务器密码机等密码产品进行完整性保护后，再存放至数据库等其他介质。

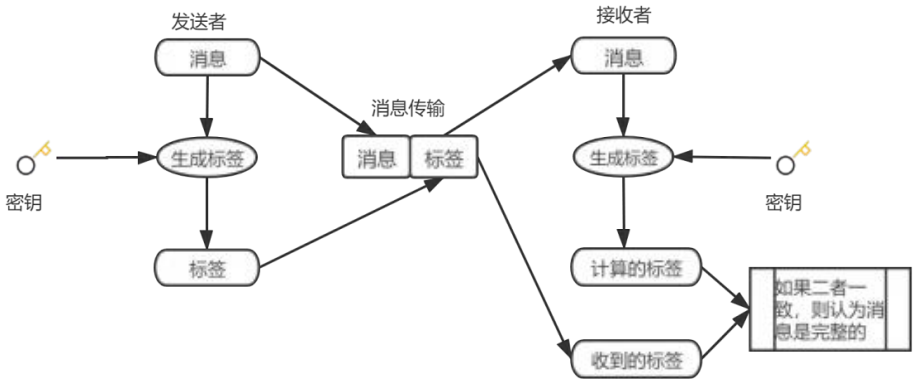


图 2.2.1 基于 MAC 消息完整性保护过程

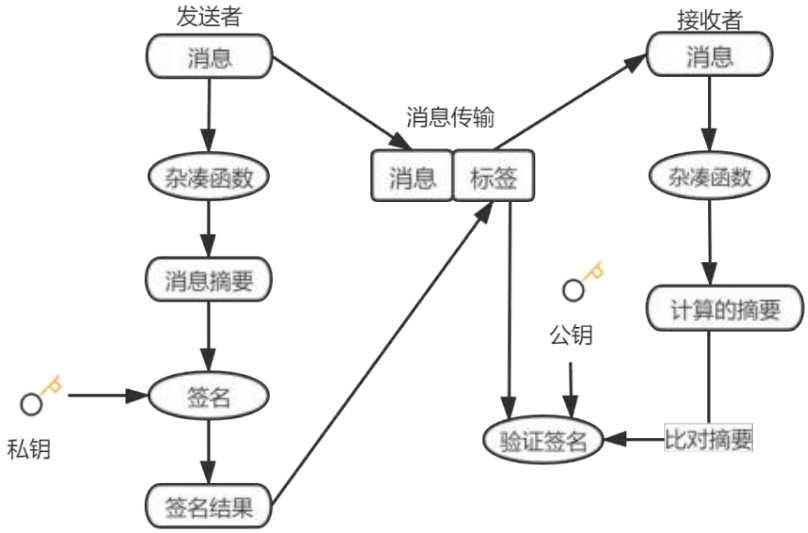


图 2.2.2 基于数字签名的消息完整性保护流程

（4）使用过程的抗抵赖安全

防护数据在分发过程中被篡改、抵赖或泄漏威胁，防范数据在共享过程中未授权的二次外发，以及访问控制被绕过后的数据访问失控。典型案例包含公钥验签技术防护、电子签章、金融密押系统防篡改、数字水印、同态加密、TDF 可信数据格式、CASB 实现密码控审一体化的防绕过安全机制等。

不可否认性实现主要包括：基于密码校验的防篡改；基于私钥签名的责任认定。

2.2.3 腾讯实践

相比等保 1.0，等保 2.0 在密码技术的应用和管理上进行了强化，包括通信传输、数据存储、身份鉴别、产品采购、使用和密钥管理中均有密码相关的要求。同时，《中华人民共和国密码法》(以下简称“密码法”）于 2019 年 10 月 26 日通过表决，2020 年 1 月 1 日起正式实施。根据《密码法》第二十七

条明确法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估。密评应与关键信息基础设施安全检测评估、网络安全等级测评制度密码相关要求相衔接。

等保 2.0 与《密码法》对我国密码技术应用提供了发展推动与规范性指引的作用，然而国内密码技术应用形势并不乐观。一是应用不广泛，密码行业尚处于产业规模化发展的初期阶段，许多企业安全管理及开发人员密码应用意识相对薄弱。2018 年有关机构对一万余个等保三级及以上的信息系统进行普查结果显示，超过 75%的系统没有使用密码；二是应用不规范，普查中对第一批 118 个重要领域的信息系统进行安全性测评发现，不符合规范的比例达到 85%；三是密码应用不安全，目前仍大量存在使用被证明不安全的密码算法的情况。

企业密码技术应用安全性合规建设势在必行，也存在固有的困难与挑战，包括密码应用合规以及密码方案建设及改造两个层面。

密码技术应用挑战与需求分析

除等保 2.0 的密码应用标准基本要求以外，根据相关法律规范要求，等保三级系统应自行或者委托商用密码检测机构开展商用密码应用安全性评估。

- **商用密码应用安全性评估**

商用密码应用安全性评估（简称“密评”）是指对采用商用密码技术、产品和服务集成建设的网络和信息系统密码应用的合规性、正确性和有效性进行评估，包括规划阶段的方案评审和建设、运行阶段的安全评估。密评具体参照

评估参照标准为 GM/T 0054-2018 《信息系统密码应用基本要求》(简称国密 0054 标准)。0054 共提出了总体要求、密码功能要求、密码技术应用要求、密钥管理和安全管理共五个部分的要求，其中也涉及到密码算法、密码技术、密码产品以及密码服务的细则要求。

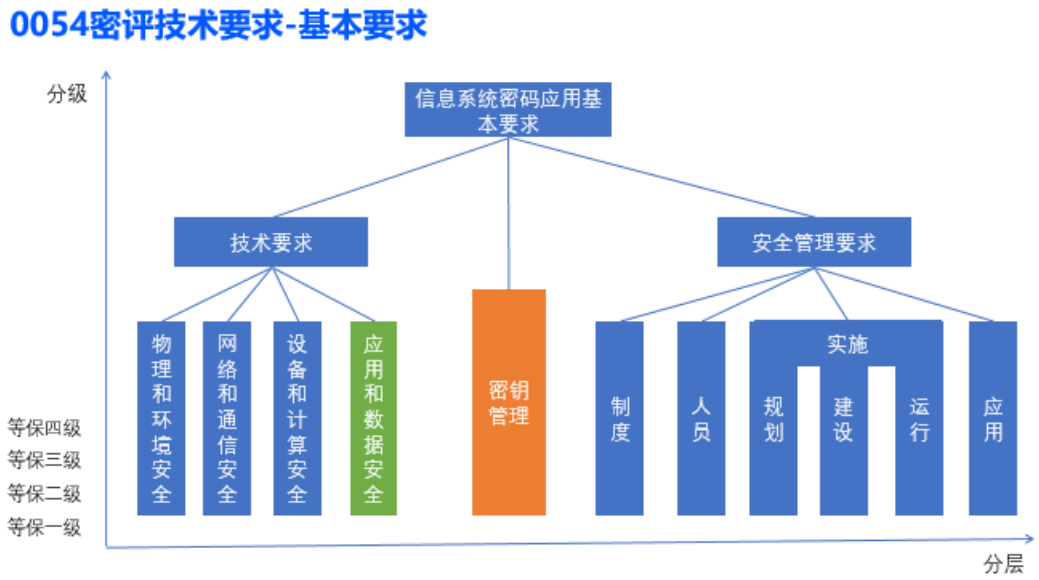


图 2.2.3 密评技术要求

- **落实合规密码技术应用面临的挑战**

在安全管理与技术应用两个层面上，密码技术的落地更为困难。即密码技术应用在使用过程中面临着三大难题，所谓“三难”就是指“难做、难用、难管”。密码产业人才短缺，开发门槛高，密码行业尚处于产业规模化发展的初期阶段是“难做”；密码算法、密码产品、密码应用三者明显脱节，用户需要大量的开发工作，因此“难用”；密码应用分散，行业缺乏统一化标准，密码技术应用及运维管理工作复杂，故而“难管。”

落实合规化密码应用实践应兼顾密码技术方案制定、密码技术与产品部署、应用开发设计以及密码方案运维多个层面的规划与设计。

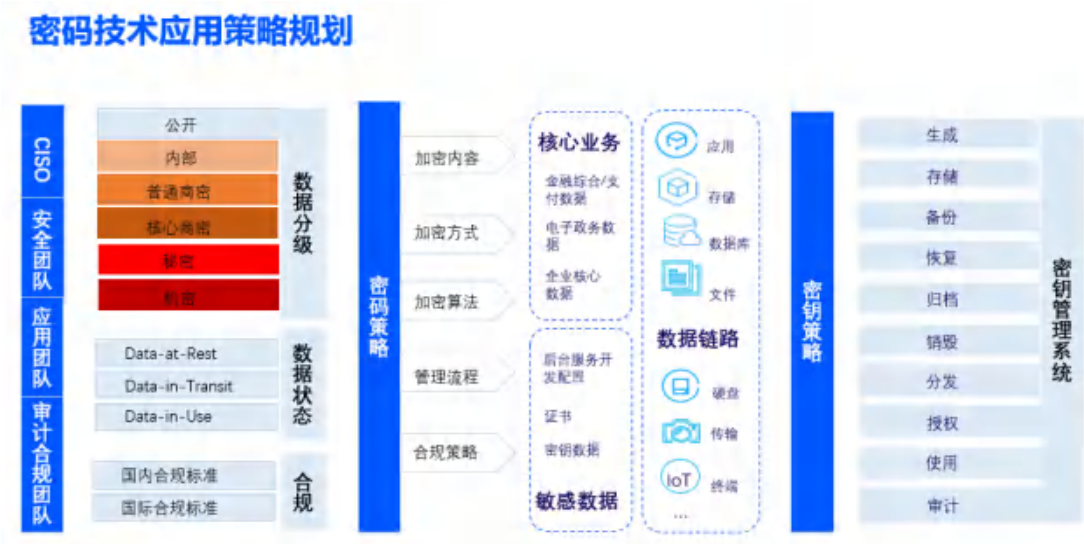


图 2.2.4 腾讯密码技术应用策略

腾讯云合规密码架构方案

作为国内最大的互联网企业之一，腾讯公司业务涵盖了社交通信、广告平台、金融科技、产业互联网等多个领域，腾讯安全在业务合规化密码技术应用上已经具备深厚的应用实践基础。以产业互联网业务腾讯云为例，腾讯安全打造了基于云平台的云数据安全中台架构，实现了端到端的云数据全生命周期安全体系，并落地了面向云平台以及云租户的密码技术应用服务。

腾讯安全云数据安全中台是基于云技术的覆盖数据全生命周期安全的极简密码服务，从学术、研究、产业、产品等各个方面共建云上密码技术应用生态，旨在为用户提供一个简单、透明、合规的密码技术服务平台。

图 2.2.5 腾讯云数据安全中台

在腾讯云密码应用架构里，基于腾讯安全云数据安全中台，以数据加密软硬件系统（CloudHSM/SEM）、密钥管理/凭据管理系统（KMS/SSM）、以及云访问安全代理（CASB）为核心，将密码运算、密码技术及密码产品以服务化、组件化的方式输出，并无缝集成至腾讯云产品中，实现从数据获取、数据处理及检索、数据分析与服务、数据访问与消费过程中的安全、合规的密码防护。

图 2.2.6 腾讯数据安全中台架构

用户可基于腾讯云数据安全中台提供的密码技术与密码产品组件、接口，或简单通过服务开通，极简化的构建业务系统合规化的密码技术应用架构，屏蔽密码技术细节，专注业务开发。

以一个典型的云业务应用场景为例，从数据产生、传输、存储、处理，到共享展示，每一个环节都涉及到密码技术应用：身份认证、网络通道的安全、配置文件和硬编码敏感信息的安全、密钥的安全管理、云上重要数据的存储安全、金融支付等敏感业务防护等。

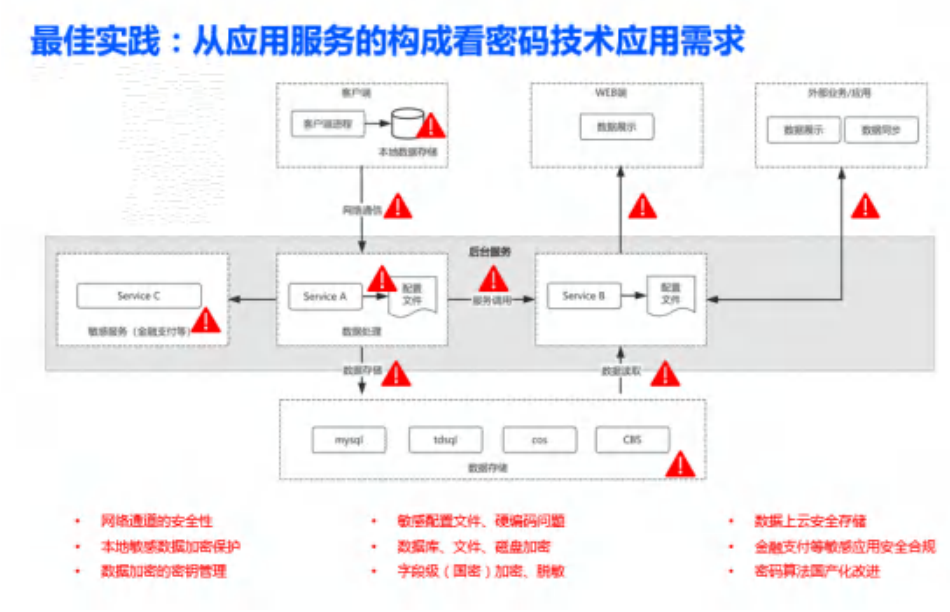


图 2.2.7 腾讯密码技术应用实践 1

针对这些问题，基于腾讯云数据安全中台提供的组件，用户可极简化的落地密码技术应用与业务安全防护。

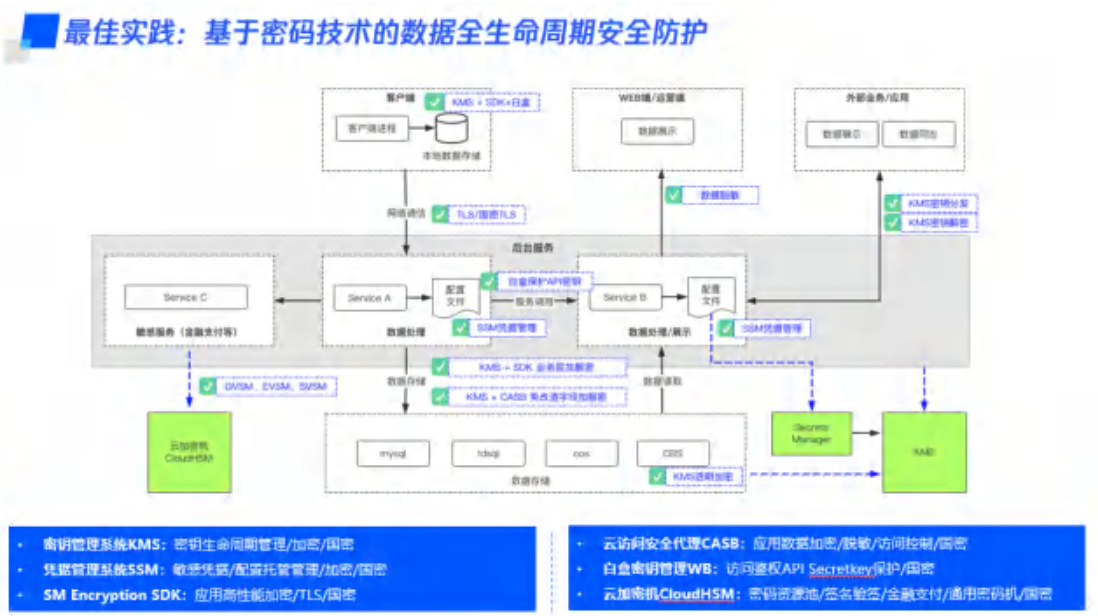


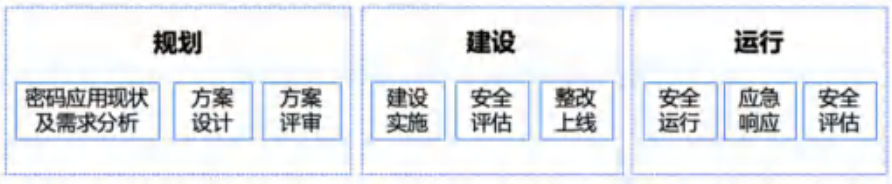
图 2.2.8 腾讯密码技术应用实践 2

中台化架构一方面解决了大规模业务系统合规密码技术应用层面的难题，另一方面也实现了密码方案规划、密码方案运维、密码管理制度的集中管控，让企业体系化的满足等保 2.0 密码技术应用要求、商用密码应用安全性评估的合规要求成为现实。

对密码技术合规实践的建议

总结来说，企事业单位应遵循《密码法》相关规定以及等保 2.0 的相关要求，对关键信息系统采用商用密码进行保护，并进行密码安全性评估，保障信息系统在密码算法、密码协议、密钥管理、密码产品和服务的合规性、正确性、有效性。可通过密码技术加持、建立数据安全中台中台等措施，为数据应用的安全与合规提供系统性的解决方案，以密码服务中心模式对外输出数据安全保护以及数据合规能力。

1） 按照规划、建设、运营模型实施密码应用，保证合规性与数据安全性；



2) 对于应用系统，依照等保 2.0 及国密 0054 标准相关的密码技术规范要求，检视是否使用了密码技术，是否合规，以及能否起到防护作用；

3) 对于云用户，应充分利用云平台提供的密码产品基础设施，构建合规化密码服务；

4) 对于新建专有云，比如政务云、金融云用户，考虑密码合规性架构，以及未来租户侧的密码应用需求，可参考腾讯云数据安全中台解决方案。

2.3 操作系统镜像等保合规

- **痛点：**

管理规定细，技术规范粗

依据《GB/T22239-2019 信息安全技术网络安全等级保护基本要求》(以下简称“基本要求”)，需要满足的基线要求包括，身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、 数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护共 11 部分，而每一部分仅提供了较粗的要求，没有给出具体的技术参数要求。

同时，针对操作系统的管理要求，也仅提供了系统和镜像加固等相关要求，并没有可落地的执行建议。

对于广大中小企业来说，在安全人员和技术能力的储备上本来就相对欠缺，

当面对等保 2.0 复杂的要求时更是一头雾水，尤其是对于操作系统的各类合规测评，往往需要进行复杂的手动配置才能满足超过 30 多个合规项的要求。

图 2.3.1 操作系统合规测评项

- **工作效果难以标准化**

在云上企业落地等保 2.0 建设中，往往 80%的人力、时间投入到 20%操作系统等配置检查上，传统企业则可能还要增加其他各类硬件设备（防火墙、网络等设备的）配置检查。

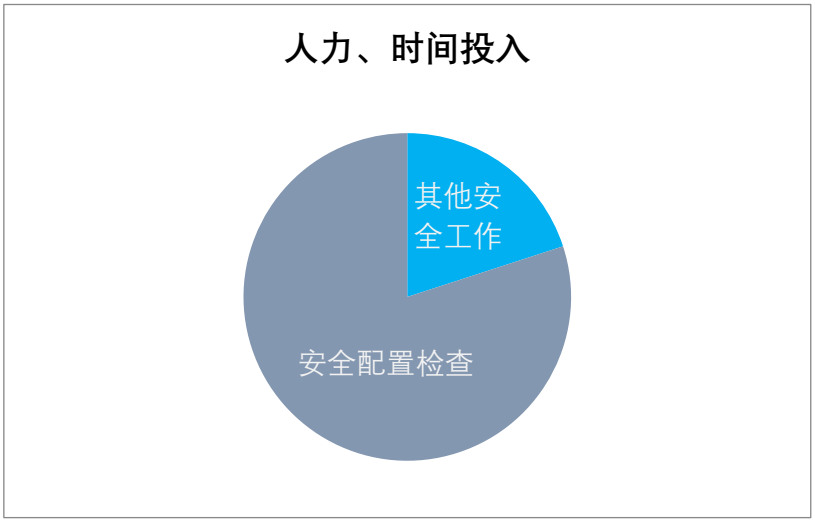


图 2.3.2 云上企业合规成本投入

与此同时，人员技术水平参差不齐，工作效果也难以标准化。

2.3.1 腾讯云操作系统等保合规实践

腾讯云每年会针对内部各类系统开展 10 次以上等保合规认证，同时也会帮助各行业用户提供等保测评支持。在这些过程中，腾讯云与专业测评机构进行了深入的交流，并且积累了丰富的自动化测评工具集和经验。

为了切实解决用户或企业在上云过程中的困扰，在专业测评机构提供基线标准支持下，云鼎实验室结合等保 2.0 最新需求，构建了多个主流操作系统等保合规基线，在保障操作系统兼容性和性能的基础上进行了等保合规适配，并且实现了工具化批量配置，可快速帮助用户摆脱复杂操作和配置的困扰，让用户无需手动操作，一键即可自动完成操作系统 90%以上的基础合规配置。

图 2.3.3 腾讯云操作系统合规标准

- **云原生场景下的默认合规实践**

由于云操作系统镜像与生俱来的可扩展性和便捷性，导致云上用户和企业

可以无需重复操作，即可复用已有操作系统环境与配置，但与此同时，很多用户也会由于操作系统镜像配置不规范或本身存在的漏洞而导致大规模安全风险，除此外，镜像的持续维护也往往需要投入较多成本。

鉴于此，腾讯云内部参考专业测评机构指导以及自身实践，构建并持续维护一套默认符合等保测评要求的系统镜像，覆盖 CentOS/Ubuntu/Windows 等主流操作系统，可免费为公有云用户提供等保需求支持。

- **云场景下的操作系统合规体系建设**

为系统性解决云环境下操作系统等保合规问题，我们结合云环境下特点，以高效、稳定、安全为主题，构建了如下自动化合规体系：

图 2.3.4 腾讯云操作系统自动化合规体系

（1）操作系统等保合规的标准和实现细节与国家专业测评机构指导和沟通，同时结合腾讯自身多年等保实践，形成了最佳配置规范和工具系统。

（2）在满足默认合规的基础上，我们结合云的特点，推出了原生合规镜像，可以批量复制默认符合等保要求的操作系统环境，为用户降低成本。

（3）在我们持续测试过程中，我们发现符合等保要求的配置只是企业脆弱性管理的一部分，操作系统面临的另外一大风险即是系统层及自带组件的安全漏洞，为此，我们针对系统默认组件进行了梳理，并对脆弱面进行分析，将发现的较大的风险点进行逐一消除或修补，以规避内、外部的潜在漏洞利用风险。

（4）考虑到系统自身也会有新的漏洞被发现，因此，我们也会对云上漏洞系统进行持续维护，来为用户提供动态可运营的合规环境。

2.3.2 对操作系统等保合规实践的建议

操作系统等保合规不仅仅是修改系统默认配置的问题，而往往需要结合企业自身环境进行构建，为此我们有如下建议：

（1）等保合规配置不应设置过于严格，建议在尽量不影响业务运行环境和运维便捷性的前提下，去构建相应基线规范；

（2）在构建等保合规自动化工具之前，建议提前了解内部业务系统类型，然后选择重点系统优先进行建设；

（3）配置是衡量系统是否满足等保合规的必备条件之一，企业需同时考虑一些安全能力的补充和运营管理，如主机 HIDS 基础安全组件部署安装和漏洞管理。

（4）操作系统等保合规建设中，如果业务对系统预置的组件或模块（如WIFI、蓝牙）没有使用场景或需求，可以默认禁用或卸载该部分模块。

（5）企业若自研主机安全入侵检测系统，可针对性的采集的等保合规配

置项参数，以便于了解等保基线配置符合率，为内部合规运营提供数据参考。

2.4 IPv6 网络安全合规实践

2.4.1 来自 IoT+5G+IPv6 新趋势下的安全算力需求

一方面，物联网、5G 网络、IPv6 越来越广泛的应用，既为广大行业的数字化演进提供了基础性支撑，也对更加广泛普遍的安全能力提出了新挑战。面对新技术新趋势下的网络数据激增，安全威胁的力度、深度、广度前所未有。

相较于一般业务，网络安全因其独有的攻防对抗属性，对算力有着更为严苛的需求。首先，黑客攻击有可能潜藏在网络里任何一个角落里，这要求企业具备足够算力来实现全面感知威胁和追踪溯源；其次，攻击方层出不穷的攻击手法和武器，迫使安全策略的量级和复杂度急剧增长，这也带来了巨大的算力开销。此外，安全对抗中，黑客攻破往往仅在毫秒之间，因此防守方需要远超一般业务的计算量来实现微秒级的实时处理能力。

在此背景下，只有做好网络安全算力储备和有效提升，才能支撑大数据并发和复杂策略处理，应对 IoT+5G+IPv6 新趋势下的安全问题，对抗拥有数据端资源优势的攻击方。

2.4.2 来自腾讯自身海量业务+全球规模的计算压力实践

当前，腾讯服务的业务规模、承载的网络流量量级均属全球第一梯队，且物联网与 5G 时代进一步引发网络数据激增，这给我们带来的安全算力挑战可以说是无出其右。在腾讯及腾讯云业务的全流量实时计算场景中，腾讯在硬件、

软件层面研发优化，持续在安全算力上深耕细作，并在众多算力需求巨大的场景实践中发挥出积极效应。

腾讯在如此大体量的分布式计算中，很多算法如果不加以优化，几乎无法在分布式环境下实现。

以一个常用的安全计算场景举例——实时计算腾讯每一台服务器每分钟的 TCP 连接会话数量。这个看似寻常的计算，实际操作起来存在诸多难点：首先，腾讯全网服务器早在 2018 年就已突破百万量级，是全球服务器总量最大的互联网企业之一，且网络流量和机房部署遍布全球。其次，每一台服务器的流量都可能从全球各个网络入口进来，并不集中。再者，对腾讯来说，单台服务器每分钟百万连接也是家常便饭，要对如此大体量的数据进行 IP 聚集，然后再对会话去重统计并且实时输出，这其实是一件相当有挑战的事情。

像这样的计算场景在智能 PaaS 上还有很多，甚至还有很多更复杂、更高维度的计算。这些都需要基于对算法的精钻细研，借助安全算力的强力支撑，并针对物理环境做针对性优化才能实现。

算力之于安全可能是掣肘，也可能是动能——匮乏的算力必然拖垮安全感知及响应能力的可靠程度，而强劲的算力则有助于构筑起坚如钢铁的安全能力，为安全防护带来巨大提升。

作为公司级智能网络流量 PaaS，平台运维着全亚洲处理流量最大的镜像集群，覆盖了腾讯自营业务和腾讯云业务的全流量。随着业务规模的急剧增长及安全场景的复杂化，平台支撑着越来越多算力需求巨大的场景和顶层应用。

在国家级省级护网、企业重保等场景中，衡量企业防护效果最重要的标尺

之一就是拦截效率，也就是阻断成功率，因此威胁实时阻断是一个刚需能力。在这方面，团队基于多年安全攻防对抗经验，巧用攻击的手段来实现防御——也就是发送伪造 RST 报文来中断双方通信，以实现 TCP 实时阻断。

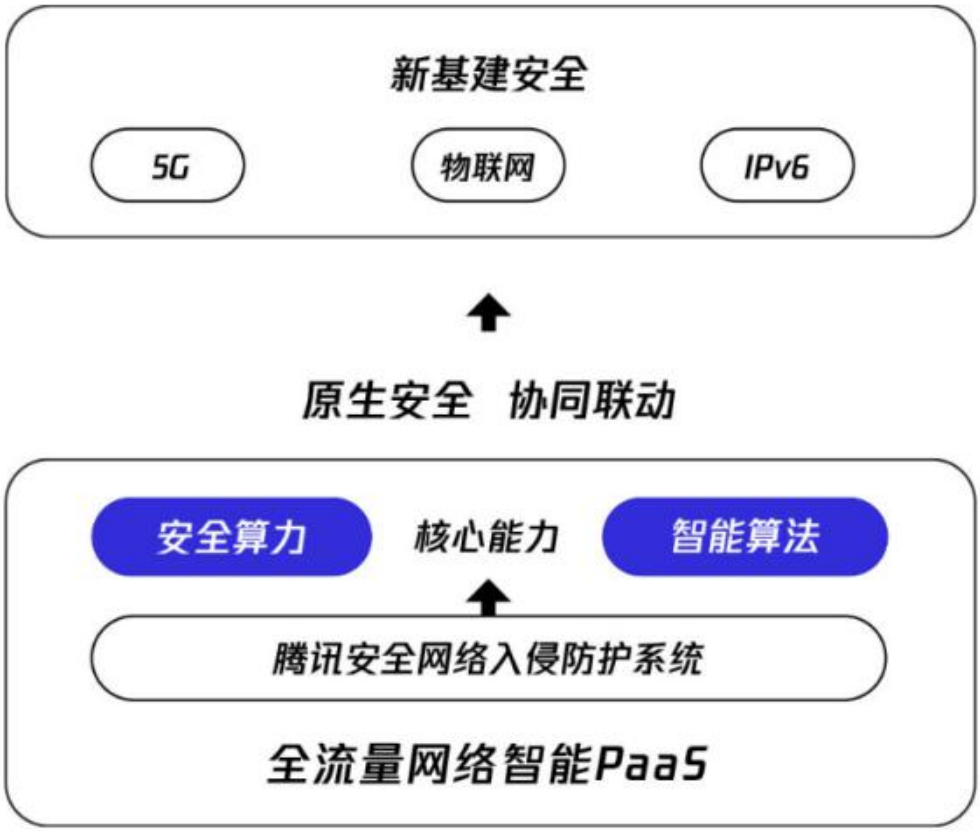


图 2.4.1 腾讯网络安全智能 PaaS 平台

而这里的核心挑战在于，为了保证阻断成功率，伪造的报文必须先于真正的报文到达客户端和服务器端。这个速度得要多快？实战告诉我们必须是 1 毫秒以内。而平台面临的是腾讯海量业务每秒 20+Tbps 的巨大流量，要在这些流量中发现各种细微的攻击报文就如同大海捞针，并且还必须在微秒之间精准捞起这根针，这对安全算力有着几近苛刻的要求。

为了能在成本不增的前提下实现如此高的算力，研发团队沿着“深入内核、贴近硬件”的思路，持续打磨平台性能：

- **深入内核**：把依赖内核才可实现的功能直接设计在内核态中，避免应用层和内核态的反复切换。
- **贴近硬件**：基于各种硬件的特性，来进行深度的 CPU 指令优化，比如 NUMA、Cache、SIMD 等。

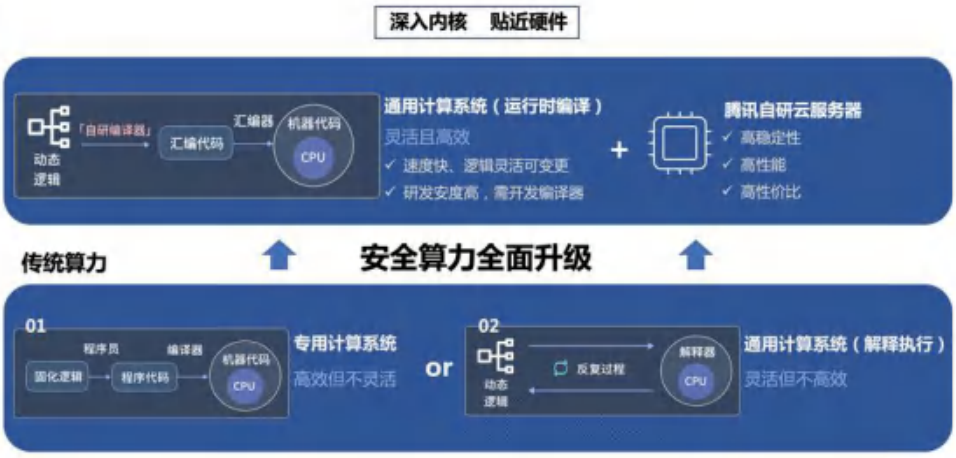


图 2.4.2 深入内核、贴近硬件

由此，基于内核协议栈和 CPU 优化带来的稳定高性能算力，实现了 RST 包的超低时延，实战阻断成功率高达 99.99%，处于业界领先水平。基于微秒级的实时阻断能力，平台支持实时、千万级域名黑名单封禁，协助腾讯云一线业务团队降低平台经营风险，提升业务运营合规性，并加强了安全能力输出和产品口碑。此外，在腾讯云大客户重保任务中，腾讯协同生态合作伙伴，通过统一的威胁阻断能力帮助建行取得了零失分的成绩，满足金融行业客户的高可靠要求。

以安全算力为核心动能

数字新基建持续推进，安全算力愈发成为产业互联网的核心动能，并在腾讯安全生态建设和攻防对抗中持续发挥强大效益。截至目前，借助星星海硬件定制及软件研发优化带来的强劲算力，天幕网络智能 PaaS 支持 TB 级跨

Region 的双向全局流量镜像，具备微秒级网络协议解析和毫秒级流量分析能力，建设覆盖百 T 每秒级的机房带宽，支撑单机计算峰值达 9 亿行/秒，支撑日处理流量达 170PB/天，持续为上层业务应用输送网络流量智能服务。

诚然，现阶段还远不是海量数据时代的巅峰，5G 网络、IPv6 时代到来后，激增数据所需的计算量呈现几何级数的增长，新兴业态的超大规模流量将对安全提出更大的算力压力。但另一方面，数字新基建也无限激发了算力潜能，算力将加速助燃互联网安全，为数字化产业护航的同时，持续输送硬核能力。

2.5 安全管理中心应用合规

等级保护 2.0 标准正式实施后，以“一个中心，三重防护”为核心框架针对云上合规进行了进一步细化，要求建立以计算环境安全为基础，以区域边界安全、通信网络安全为保障，以安全管理中心为核心的信息安全整体保障体系。安全运营中心作为安全管理中心的具体实现路径之一，得到了业界广泛的关注。

腾讯云 SOC 实践：

在此背景下，我们发布了腾讯云安全运营中心这款产品。腾讯云安全运营中心是腾讯云上的统一安全运营与管理平台，提供资产自动化盘点、互联网攻击面测绘、云安全配置风险检查、合规风险评估、流量威胁感知、泄漏监测、日志审计与检索调查、安全编排与自动化响应及安全可视等能力，帮助腾讯云上业务实现事前安全预防，事中事件监测与威胁检测，事后响应处置的一站式、可视化、自动化安全运营管理。

2.5.1 安全运营中心体系建设

图 2.5.1 安全运营中心体系图

上图为腾讯云安全运营中心的体系图-IPMDR，从识别、预防、监测、检测和响应五个方面来进行安全运营的体系建设。

识别与预防属于事前安全预防阶段，在此阶段我们对腾讯云上业务进行资产识别和动态盘点。除了传统领域的资产识别与发现外，我们也会针对云上的特有产品，将对象存储，负载均衡，云数据库等新型资产进行纳管，将腾讯云上业务所使用的资产进行全面完整的梳理和展示。预防阶段从云资产的配置风险、漏洞检测与运营、互联网攻击面测绘、合规风险自动化评估等方面进行风险检查和配置加固，提高安全水位，在攻击事件来临前保障云上的资产安全。

事中的监测与检测会收集散落在云上安全产品的数据与日志，进行集中的统一收集与存储，了解到云上资产正在遭受的威胁与风险。除主机安全威胁、网络安全威胁及应用安全威胁等，安全运营中心也会针对云上新型的威胁事件进行监测和检测，例如 API Key 的泄漏，异常 API 的调用，越权访问

等行为。实现云上安全事件的便捷统一运营管理。

事后响应处置提供了溯源调查和自动化编排的功能，通过打通各类安全产品检测的威胁数据，并通过统一的响应中心实现威胁统一响应处置，简化威胁管理难度，提升响应处置效率。安全运营中心的核心是平台和人员，将人员、流程和技术有机结合，所以我们也会有专家服务，对安全运营中心所监控到的告警和事件，进行及时的响应和处置。

最后通过安全仪表盘、安全大屏及安全报表中心实现云上安全的全局可视，实现安全态势的实时监测及安全建设成果的直观可视化呈现。

2.5.2 安全运营中心功能与架构

图 2.5.2 安全运营中心架构图

安全运营中心架构，由下到上分别为数据层、分析层、功能层和可视层。数据驱动是云时代安全运营的基本要求，数据层打通了割裂在各个云上产品中

的告警和日志。不仅包括 DDoS、WAF、云镜等云上安全产品的告警数据，同时也会打通各类云产品数据，如 CVM、负载均衡、云数据库等资产数据，为分析层提供了数据保障。分析层会将数据层提供的各类日志和告警数据进行清洗和分析，除展示原有安全产品的告警外，也会关联各个产品的日志，从中挖掘出更深层次的安全事件与风险。同时也会借助机器学习的手段，对用户基线行为进行学习，检测其中的异常行为。功能层则是将分析层发现的安全事件与风险分别分散到了安全运营中的事前、事中和事后三个阶段。事前安全预防阶段是在攻击发生之前，对云上资产进行盘点和检查，排除安全隐患，提高了安全水位。其中合规管理功能，提供了自动化的动态合规评估功能并提供相应的加固建议，可按需对云上资产的合规风险进行持续监测与评估。事中监测与检测，可以对云上的流量测威胁，主机测威胁以及云上新型的安全风险事件进行检测和告警。最上层的可视层通过仪表盘，大屏，安全评分等模块，全面的展现当前云上资产的安全风险态势，并可以方便的进行安全成果的汇报和展示。

等保 2.0 明确提出安全管理中心，针对系统管理、审计管理、安全管理、集中管控提出明确要求。腾讯云安全运营中心，作为腾讯云上安全运营和管理的统一门户平台，借助资产盘点、日志审计与检索调查、合规风险评估、流量威胁感知等功能实现云上统一安全运营与管理，完成等保 2.0 中的安全管理中心的合规要求。

2.6 个人信息保护

随着我国信息化与民众生活各方各面越来越紧密的融合，以及我国实名制

的推广，我国已经成为世界上网络数据生产量最大、数据类型最丰富的国家之一，与此同时，层出不穷的数据泄露和网络安全事件也给个人信息和隐私保护带来了新的挑战。2017 年《网络安全法》的出台对个人信息的收集、使用提出了明确的法律依据，《互联网个人信息安全保护指引》(征求意见稿)、《电信和互联网用户个人信息保护规定》、《APP 违法违规收集使用个人信息自评估指南》等一系列规定对个人信息保护提出了指导意见。目前《个人信息保护法》也在紧锣密鼓的制定中，相信后续出台后可以在法律层面更好的完善个人信息保护要求。

2.6.1 等级保护 2.0 个人信息保护要求

等级保护 2.0 基本要求中专门针对个人信息保护在安全计算环境层面增加了一个控制点，对个人信息的收集和使用进行要求；在数据保密性、数据完整性控制点对个人信息在存储和传输过程中的保密性和完整性也进行了要求：

序号	层面	控制点	测评项
1	安全计算环境	个人信息保护	a)应仅采集和保存业务必需的用户个人信息；
2			b)应禁止未授权访问和非法使用用户个人信息。
3	安全计算环境	数据完整性	a) 应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；
4	安全计算环境	数据完整性	b) 应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。
5	安全计算环境	数据保密性	a) 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；
6	安全计算环境	数据保密性	b) 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

（1）收集方面：

仅收集业务必须的用户个人信息。

1）收集的个人信息类型应与实现产品或服务的业务功能有直接关联，直

接关联是指没有该信息的参与，产品或服务的功能无法实现；

2）自动采集个人信息的频率应是实现产品或服务的业务功能所必须的最低频率；

3）间接获取个人信息的数量应是实现产品或服务的业务功能所必须的最少数量。

（2）使用方面：

采用技术措施限制对用户个人信息的非法访问和使用。

1）对被授权访问个人信息的人员，应建立最小授权的访问控制策略，使其职能访问职责所需的最少够用得个人信息，且仅具备完成职责所需的最少的数据操作权限。

2）使用个人信息时，不得超出与收集个人信息时所声称的目的具有直接或合理关联的范围。因业务需要，确需超出上述范围使用个人信息的，应再次征得个人信息主体得明示同意。

（3）传输方面：

识别出传输过程中的个人敏感信息字段，并采用密码技术进行保密性和完整性的保护。

（4）存储方面：

1）将可用于恢复识别个人的信息与去标识化后的信息分开存储。存储个人敏感信息时，应采用密码技术保证数据存储的保密性和完整性。

2）存储个人生物识别信息时，应采用技术措施确保信息安全后再进行存储，例如将个人生物识别信息的原始信息和摘要分开存储，或仅收集、存储、

使用摘要信息。

2.6.2 企业如何做到个人信息合规

保护用户个人信息正变成一种竞争优势，在后 GDPR 时代，越来越多的互联网公司意识到它们不仅是用户数据的采集者，还是用户数据的“管家”。建立和维护客户对其隐私保护能力的信任，正在成为这些依赖数据而生的互联网公司取得成功的关键因素之一。对于建立个人信息合规体系，可从以下几个方面着手：

（1）个人敏感信息的区分

《信息安全技术个人信息安全规范》界定了个人敏感信息的范围。个人的身份证件号码、生物识别信息、银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等属于个人敏感信息，对于这些个人信息，在收集时应取得信息主体的明示同意，在存储时应采取技术加密措施。

（2）个人信息的收集规则

在个人信息的收集环节，除了取得个人信息主体的授权同意外，还应向其展示隐私政策，并且收集的个人信息类型，与实现产品或服务的业务功能有直接关联，且应为所必须的最低频率。同时需要特别注意的是，相关法规和等级保护 2.0 都明确提到的，个人信息收集的最小化要求。

（3）个人信息使用规则

在个人信息的使用环节，除合法目的所必需外，应避免个人信息能够精确

定位到特定的个人；若超出个人信息授权范围使用个人信息的，还应再次征得个人信息主体明示同意。在系统运营和维护过程中，也应严格控制个人信息的访问和使用权限，遵循最小化原则。

（4）个人信息传输规则

在个人信息的传输环节对于重要个人信息应采用 SM4、AES 等加密算法进行加密，保障传输过程中数据的保密性和完整性。对于在我国境内运营中收集和产生的个人信息向境外提供的，个人信息控制者应当遵循国家相关规定和相关标准的要求；未经个人信息主体的明示同意，或法律法规明确规定，或未经主管部门同意，不得将个人信息转移给境外个人信息获得者，包括位于境外的个人或境外注册的组织和机构。

（5）个人信息存储规则

在个人信息的存储环节，个人信息保存期限应为实现目的所必需的最短时间，超出上述个人信息保存期限后，应对个人信息进行删除或匿名化处理。同时，个人信息保存也要对相关工作人员个人信息的访问进行控制。对于重要个人信息应采用 SM4、AES 等加密算法进行加密存储，保障存储过程中保密性和完整性。

（6）完善个人信息保护制度

明确个人信息的内部管理机制。包括确立保护个人信息的责任部门及人员，并明确其处理个人信息的权限，设立针对个人信息重要操作的内部审批流程、并建立个人信息岗位人员管理及培训制度等。

制定个人信息的收集、保存、使用制度。包括将个人信息区分为一般个人

信息和个人敏感信息，就一般个人信息和个人敏感信息，明确个人信息主体同意的取得方式、明确保管相关的技术措施等。

制定个人信息安全事件处置与报告制度。包括制定个人信息安全事件应急预案及进行应急演练、发生个人信息安全事件时向个人信息的告知制度等。企业个人信息合规的漫漫长路，需要大家共同铺就。

3 等级保护 2.0 安全管理合规要求分析

管理部分的核心，也偏向于上层建筑，类似国际安全体系中的 IT 治理，主要是定目标、出战略、树文化。这里目标就是企业 IT 治理的总体目标，一般理想状态是配合业务，IT 作为辅助能力实现业务目标，创造价值；战略就是根据业务目标来制定战略规划和实施计划，IT 同样也有自己的战略规划；文化是说企业文化，这点很重要，将引导企业的未来走向，如：IT 中的风险偏好、风险容忍度、对 IT 重视程度、对创新、对资源优化和风险优化的态度等。

3.1 安全管理制度

安全策略

俗话说：“人无头不走，鸟无头不飞。”凡事要有个原由和目的，这样才能做事。现在企业每日忙于各种安全工作，时而应急、时而漏洞补洞、时而策略调整，但有关企业安全的总体方针是什么，大多数 IT 负责人可能一时无法回答，只要不出事就可以了。这里以一个模板举例，供各位参考，模板并非通用，企业要结合自己的情况和业务来定方向。

第一章 总则

第一条 为规范 xxx 单位信息系统的信息安全管理，促进信息安全工作体系化、规范化，提高信息和网络服务质量，提高信息系统管理人员、使用人员的整体安全素质和水平，特制定本方针。本方针目标是为 xxx 单位信息安全管理提供清晰的策略方向，阐明信息安全建设和管理的重要原则，阐明信息安

全建设和管理所需的支持和承诺。

第二条　本方针是指导 xxx 单位信息安全工作的基本依据，信息安全相关人员依据本方针，并根据工作实际情况，制定并遵守相应的安全标准、流程和安全制度及其实施细则，做好信息安全管理工作。

第三条　信息安全是 xxx 单位信息系统管理工作的重要内容。xxx 单位管理层非常重视，大力支持信息安全工作，并给予所需的人力物力资源。

第四条　本方针的适用人员包括所有与 xxx 单位信息系统各方面相关联的人员，它适用于全部员工，集成商，软件开发商，产品提供商，顾问，临时工和使用 xxx 单位信息系统的其他第三方。

第五条　本方针适用范围包括 xxx 单位信息系统拥有的、控制和管理的所有计算机系统、数据和网络环境。

第六条　本方针主要依据国际标准 ISO17799,并遵照我国信息安全有关法律法规和相关标准。

第二章 信息安全管理的主要原则

第七条　管理与技术并重原则：信息安全不是单纯的技术问题，在采用安全技术和产品的同时，应重视管理，不断完善信息安全管理制度与管理规程，全面提高信息安全管理水平。

第八条　全过程原则：信息安全是一个系统工程，应将它落实在系统的计划组织、开发采购、实施交付、运行维护、废弃五个阶段的全生命周期管理过程中，信息安全建设管理应遵循与信息系统同步规划、同步建设、同步运行

的原则。

第九条　风险管理和风险控制原则：应进行信息安全风险管理和风险控制，将信息安全风险减低、控制在可以接受的程度内，并将其带来的危害最小化。

第十条　分级保护原则：应根据信息资产的重要程度以及面临的风险大小等因素确定各类信息资产的安全保护级别。

第十一条　统一规划、分级管理原则：信息安全管理遵循统一规划、分级管理的原则。上级主管部门信息安全领导小组负责对 xxx 单位信息安全管理工作进行统一规划，各级单位（部门）在上级主管部门信息安全领导小组的领导与监督下，负责本单位（部门）的信息安全管理工作。

第十二条　平衡原则：在 xxx 单位信息安全管理过程中，应在安全性与投入成本、安全性和操作便利性之间找到最佳的平衡点。

第十三条　动态管理原则：在 xxx 单位信息安全管理过程中，应遵循动态管理原则，针对信息系统环境的变动情况及时调整管理办法。

第三章 信息安全管理组织与职责

第十四条　建立和健全信息安全管理组织，设立由高层领导组成的信息安全领导小组，对于信息安全方面的重大问题做出决策，支持并推动信息安全管理工作在整个 xxx 单位范围内的实施。

第十五条　xxx 单位信息系统应该设置相应的信息安全管理机构，在信息安全领导小组的领导下，负责 xxx 单位的信息安全管理工作。

第十六条　xxx 单位信息安全管理机构职责如下：

1)　根据本方针制定信息系统的信息安全管理制度、管理标准规范和执行程序；

2)　组织和监督信息安全工作的贯彻和实施；

3)　考核和检查信息系统的安全管理情况，定期进行安全风险评估，并对出现的安全问题提出解决方案；

4)　负责安全管理员的选用和监督；

5)　参与信息系统新工程建设和新业务开展的方案论证，并提出相应的安全方面的建议；

6)　在信息系统工程验收时，对信息安全方面的验收测试方案进行审查并参与验收。

第四章 信息系统安全运行管理

第十七条　信息资产鉴别和分类是整个 xxx 单位信息安全管理工作的基础。

第十八条　制定信息资产鉴别和分类制度，鉴别信息资产的价值和等级，建立并维护信息资产清单。

第十九条　建立机密信息分类方法和制度，根据机密程度和重要程度对数据和信息进行分类管理。

第二十条　安全运行管理是整个信息安全管理工作的日常体现和执行环

节。应该在本方针的指导下，建立并执行信息安全管理制度与信息安全操作规程。

第二十一条　定期开展信息安全风险评估工作，通过对整个信息系统进行信息安全风险评估，确定信息系统所存在的安全隐患和安全风险，了解信息系统安全现状与信息系统安全需求之间的差异。

第二十二条　进行物理安全和环境安全的管理，建立机房管理制度。

第二十三条　对于 xxx 单位信息系统中重要业务系统、服务器和网络、安全设备，制定安全配置标准及规定，规范安全配置管理工作，建立系统变更管理制度，并进行定期的审计和检查。

第二十四条　对于外包开发的业务系统软件，应制定业务软件安全标准来进行规范，要求有完善的鉴别和认证、访问控制、日志审计功能和数据验证功能，杜绝木马和后门。建立源代码控制和软件版本控制机制。

第二十五条　建立第三方安全管理的制度和规范，严格控制第三方对 xxx 单位信息系统的访问，并在合同中规定其安全责任和安全控制要求，以维护第三方访问的安全性。

第二十六条　应该实施业务连续性管理程序，预防和恢复控制相结合，将灾难和安全故障 (可能是由于自然灾害、事故、设备故障和蓄意破坏等引起) 造成的影响降低到可以接受的水平，以防止业务活动中断，保证重要业务流程不受重大故障和灾难的影响。

第二十七条　应该分析灾难、安全故障和服务损失的后果。制定并实施

应急管理计划，确保能够在要求的时间内恢复业务流程。

第二十八条　对于意外、灾难和入侵的处理，建立包含事件鉴别、事件恢复、犯罪取证、攻击者追踪的安全事件紧急响应机制，制定并遵照正确的安全事件处理流程，尽量减小安全事件造成的损失，监督此类事件并从中总结经验。

第二十九条　制定并实施安全培训和教育计划，进行信息安全意识及信息安全技能的培训。

第五章 信息安全技术体系建设

第三十条　xxx 单位信息系统应加强信息安全技术体系建设，包含鉴别认证，访问控制，审计和跟踪，响应和恢复，内容安全等五个方面的安全技术要素。

第三十一条　建立鉴别和认证的标准和机制，建立用户和口令管理的制度和标准。

第三十二条　建立完善的信息系统的访问控制标准和机制，加强权限管理，进行网段隔离，严格控制互联网出入口，严格管理远程访问和远程维护。

第三十三条　建立有效的审计和跟踪机制，建立日志存储、管理和分析机制，提高对安全事件的审计和事后追查能力。

第三十四条　建立有效的机制和技术手段来发现、监控、分析和处理信息安全事件和信息安全违规行为，建立应急响应和恢复的标准和机制。

第三十五条　建立内容安全的标准和机制，保护软件和信息的完整性。

建立针对恶意代码和病毒的预防和查杀措施，建立并遵守软件管理策略。

第六章 附则

第三十六条　本方针由 xxx 单位信息中心负责解释。

第三十七条　本方针自发布之日起执行。

管理制度

各家企业都有一套自己的制度文件，随着时间的推移，业务的增长和标准化，制度会越来越规范，而且需求程度越来越高，自然而然会形成一套体系。如果您了解 ISO 27000 体系，对这项要求就会很熟悉——四级文档结构。体系建立之后，自然各类表单也就随之产生，因为没有过程记录，审批是走不下去的，流程无法闭环。

这里以运维为例，说下日常工作中应该有的制度和过程记录。

- 《安全运维服务流程》
- 《安全运维服务规范》
- 《安全运维方案》
- 《安全运维计划》
- 《安全运维巡检记录》
- 《安全运维监控记录》
- 《安全巡检周报》
- 《漏洞扫描报告》
- 《安全评估报告》

- 《安全审计报告》
- 《安全事件统计报告》
- 《年中总结报告》
- 《项目总结报告》
- 《验收报告》

以上这些工作期间产生的过程记录也应存档，可以是纸质文档也可以是电子文档。

此外，无论甲方乙方，很多对于项目上的里程碑节点的文档不关心，整个项目过程中，可能没有验收单，而且这种情况很普遍，在内审/外审和上级监管检查中是比较常见的问题。

制定和发布、评审和修订

企业治理和企业文化，不是标准能左右的，这里关注的包括以下几点：

- 制度无论是内部编写还是外包给别人，肯定有一个负责的部门或人，那么这个人要指定好；
- 制度写好了，发布要正式，在 OA 以通知形式全公司通告，或者通过类似的方式；
- 各类制度要有版本记录，每次修订要有记录，这些过程文档都要保留；
- 制度要定期修订，一般每年至少要修改一次，哪怕你改个日期也是修订；
- 制度修订后要有评审过程，不管高管关心不关心，让他签字，作为流程记录留存。

3.2 安全管理机构

本控制项重点关注的是企业安全管理的组织结构设计合理性以及安全管理流程的运行情况，内容看着不多但做起来却不容易。

主要检查点如下：

岗位设置

本控制点的重点是企业的安全领导小组和安全部门架构设置，必须明确主管人员，通常会指定一名高管来负责，而且要定义岗位职责。此外还会指派一名安全主管，主要负责安全工作，通常会是技术总监或者 IT 负责人，也有的会任命 CISO/CSO。

检查中要查看领导小组成立的正式文件，要查看这个文件中的组长和组员，要求文件中应有每个人的联系方式以及工作职责。因为系统最终的责任人肯定是企业的一把主管，尤其在国企和政府部门中，责任重大，会被作为安全事件的第一责任人。

对此进行测评的时候，要询问并记录安全管理责任部门、责任人、安全主管的具体名称，并要查看具体的岗位职责文件。

安全管理中的岗位设置，主要看企业有没有设立安全管理员、网络管理员、系统管理员、数据库管理员、机房管理员等职位，并且应提供专门的任职文件。通常来讲，标准着重提出安全、系统、网络这三个管理员，所以也是重点检查项。值得注意的是，一是安全管理员必须是专职的，不能由任何其他管理员兼任；二是系统管理员和数据库管理员不能为同一人。

人员配备

系统管理员、网络管理员、安全管理员的配备数量，要求是至少 1 人及以上。很多企业是达不到这种要求的，而这里的建议是用兼职来代替，但有一点要注意，安全管理员是专岗专职的，不能由其他职位人员来兼任。

授权与审批

主要考察企业流程管理情况，可能会涉及多个方面，可以是系统流程，也可以是电子流程，只要有流程而且在用，能够提供之前的审批记录即可。一般情况下企业都会存在流程不完善或缺失的情况，建议先把一些重要的活动进行审批，比如物理访问、远程控制、权限授予与变更、系统接入、需求变更等活动。其中有一条要求也正是如此，至少要具备以下审批证明材料：系统变更（包括权限变更、结构变更等）、重要操作（数据删除、权限变更、数据备份等）、物理访问（访问物理机房、访问办公环境中的敏感区域等）、系统接入（网络接入、远程控制、wifi 接入等）。审批流程中要包含申请人、审核人、批准人，某些审批单也的授权有效时间要合理，不能过快或者过久。因为遇到过授权日期已过，但授权账号还存在的情况，这是需要特别注意的。

再者便是对审批事项、审批部门、审批人的变更进行评审；定期审查、更新审批项目，审查周期不宜过长。在实际环境中，特别是在大型企业，部门很多，人员复杂，业务流程复杂，审批流程涉及人员众多。存在某一人员离岗后还在使用以前的审批流程，就会导致越权操作，所以要定期审查审批事项。

沟通与合作

此项内容可能偏向一些政府、企事业单位、国企类公司，要与多方技术单位保持沟通联系，包括监管、技术、供应商、行业专家等。一般会有一个外联单位联系表，里边有单位名称、联系人、联系方式等。

审核与检查

等保 2.0 标准中要求企业每年必须定期进行全面的安全检查。这个定期是多久没有明确规定，建议是至少每半年进行一次全面的安全评估工作。可以自己来查，也可以外包服务公司，对于发现的问题及时整改。

3.3 安全管理人员

本控制项所关注的是企业在人员管理层面的安全性考虑以及所采取的保障措施。也可以将其视为人员安全管理的生命周期，包括人员入职前，入职后，离职三个阶段以及外部人员管理。

主要检查点如下：

人员录用（入职前）

标准首先要求对于人员的管理要指定或授权专门的部门或人员，通常为企业的人力资源部。作为最基础的管理要求，企业人事部门应具备人员管理制度，包括人员录用流程、转正流程、离职流程、交接流程等，且均需具备可证明的过程记录（纸质或电子流程记录）。这里举个常规的例子，人员入职，面试时一般会有一个打分表，评价应聘者的综合素质。入职前对应聘者身份、安全背景

进行调查并记录，比如学历学位的网上验证（如学信网），相关个人证书的（如认证机构官网），电话询问历任工作单位证实工作经历真伪，并询问是否有过违法记录等，但对于此类调查不宜介入过深，以免涉及他人隐私。对于此类背景调查的结果可以表单形式留存。入职后签订的劳动合同、保密协议，涉及关键岗位的需同时提供岗位说明书，描述岗位职责。

这里引用一下国外体系对于人员管理的一些要求（摘自 CISSP OSG）：

人员安全管理措施：招聘前的需求定义与分析，对应聘者背景进行调查，签署雇佣合同和保密协议，加强在职人员的安全管理，严格控制员工离职程序。

背景调查：目的是防止因人员解雇而导致的法律诉讼、因雇佣疏忽而导致的第三方法律诉讼、雇佣不合格人员、丢失商业机密。PS：员工从一般岗位转入信息安全重要岗位，应对其进行检查。

签订保密协议：NDA（NonDisclosure Agreement 保密协议）和 NCA（NonCompete Agreement 竞业禁止协议）。协议上应有员工签名并由其保存一份副本，对于试用期员工，应签订保密承诺。第三方用户使用信息处理设施前，也要签订保密协议。

安全意识教育和培训（入职后）

根据常规安全管理要求，每年企业应至少组织两次安全相关培训，并进行考核。以企业安全资质申请的要求作为参考，每年应进行两次保密培训，至少一次安全意识培训，相应技术岗位每年应进行两次专项技能培训，并进行考核（可记入 KPI 中）。以上是必须要做的，接下来再说等保 2.0 标准中的对应要求。全员安全培训中要涵盖安全责任落实和奖惩措施的内容，让员工了解自己

与安全之间的联系，如果处置不当将会承担怎样的后果。

不同岗位的培训计划和培训课程不能相同，要与岗位职责相关定制开发，其中必须要有安全基础知识、岗位规范操作等基本内容。等保 2.0 标准中的定期技能考核，以承载三级系统的企业实际开展情况来看，每年两次基本可以满足标准的要求，如果有能力可以增加额外培训，本要求项的重点是考核而培训为次重点，意为培训是前提，考核是重点。

人员离岗（离职）

从安全的角度而非人事的角度来看员工离职流程，等保 2.0 标准中的要求项只有两条，一是权限和证件、物件的及时收回，这里重在“及时”二字。很多安全事件都是因为权限收回不够及时所造成的，因此在人员离职过程中，权限的收回要第一时间，即人员离职流程审批结束，立即收回相应权限。而后，进行物品交接，办理离职手续。这个过程都需要留存记录，比如离职审批记录，权限收回记录，物品交接单，工作交接单，离职证明等。

另一条是对离职人员调离后的保密义务进行再次确认，明确告知离职人员应承担的保密义务以及相应的法律责任等内容，此时保密协议依然生效，通常会维持人员离职后 2-3 年的时间。

相比等保 1.0 标准，等保 2.0 标准要求中不再是只针对关键岗位承诺保密义务，而是对所有离职人员而言。因为所有员工都有可能或多或少接触到一些企业的核心机密或敏感信息，都存在可能泄露信息的风险，所以“一视同仁”的策略更为合理。

外部人员访问管理

对于外部人员（也可称为第三方人员）管理，等保 2.0 标准按照人员拜访的“进——访——出”这样一个过程来要求相应的管理流程。首先，要具备外部人员访问管理制度，其中列出来访人员应如何按照流程进行申请，陪同人员应按照什么规范来引导来访人员。

通常外部人员访问会事先通过内部对接人进行申请，批准通过后登记来访人员基本信息和来访事宜，对接人为谁。拜访当日，进入企业办公园区前，应在大门进行登记，而后由被拜访人陪同方可进入企业园区（部分企业可能会在大楼入口处进行二次登记）。在进入办公区域要有专人陪同，拜访结束后由专人陪同送出至办公大楼门外。这是标准的外部人员访问流程。

对于需要接入企业受控网络访问某系统时，必须提出书面申请，公司批准后进行登记并备案。访问者需签订保密协议，承诺遵守协议中所列要求（标准中举了几个常见示例）。而后由负责该系统的专职人员来为访客建立临时账户和授予临时权限，待外部人员访问结束后，即刻清除账户及访问权限。

3.4 安全建设管理

系统定级工作在 2017 年之前并非强制要求，通常都是政府部门、事业单位会被要求必须定级。但是 2017 年 6 月《网络安全法》出台后，要求所有系统原则上都必须定级备案，政府、国企、事业、大中型私企都要定级，只有部分很小的系统和内网隔离系统，对社会影响可以忽略不计的系统可以不做定级备案。但是，如果后期业务发展，要与大公司、政府合作，或者业务规模增长到一定程度，最终还是要进行定级备案，所以基本上可以这样来总结，只要你

有在运行的系统（内部物理隔离暂且除外）就要定级备案。

对于如何定级可以参考《GB/T-22240-2020》，标准中有详细的说明，共五个级别，各级别的定义，三个客体，影响程度，定级矩阵等等。

再来看标准的要求，对于系统定级要有依据，并聘请专家（也可以组织企业内部专家评审）进行评审，出具评审报告，并将备案材料报送主管部门和公安机关。其实，上述等级保护定级和备案工作的简介，已经明确说明了如何开展等级保护工作，企业要注意这个过程中的各项流程相关工作，至少应该做到具有专家评审报告、在公安机关获得备案证明、每年开展安全等级测评并有测评机构出具的测评报告（包含整改报告）。

以上文档如都具备，则本控制点（定级和备案、等级测评）的检查要求也就符合了。

安全方案设计

本控制点要求描述没有明确具体的文件是什么，但必须有相关的配套文件，根据以往测评中所涉及到的一些关键制度，总结一下制度列表，以供参考。

《网络安全工作的总体方针和安全策略》	《机房安全管理制度》
《网络安全管理制度》	《系统安全管理制度》
《数据管理制度》	《应用安全管理制度》
《建设安全管理制度》	《运维安全管理制度》
《系统维护手册和用户操作规程》	《安全管理制度的制定、发布、评审、修订制度》
《安全机构和人员管理制度》	《网络安全教育培训管理制度》
《总体规划和安全设计方案》	《产品采购和使用管理制度》
《软件开发管理规范》	《第三方服务供应商管理制度》
《资产安全管理制度》	《介质安全管理制度》
《设备安全管理制度》	《漏洞和风险管理制度》
《设备维护管理制度》	《配置管理制度》
《密码管理制度》	《恶意代码防范管理制度》
《变更管理制度》	《备份与恢复管理制度》
《安全事件处置和报告管理制度》	《应急预案》
《外包运维管理制度》	《业务连续性管理制度》

图 4.4.1 等保 2.0 标准管理要求制度列表

通常来说，具备以上制度，基本可以满足等保 2.0 标准对于企业安全管理制度的要求，同时还需要注意的问题是，制度的评审、修订、发布都要有正式的流程的审批。比如制度的修订，要有对修订内容合理性、可行性的评审记录，可以是讨论会，也可以是管理层审议；再比如制度发布，要在企业内部公开的平台上发布，并且有高层领导的授权审批，可以通过纸质授权，也可以采用互联网公司的邮件通知形式授权。不能没有发布平台，或者没有正式通知，就开始在内部传阅，这种方式会被认定为不符合要求。

产品采购和使用

本控制点要求没有太多解释，注意尽可能采购和选用国产软硬件产品，这些产品都是符合国家规定的产品，尤其是政府机构、国企背景的企业。

自行软件开发

企业拥有研发团队的情况下，必须要有配套的制度和流程。自行软件研发控制点相比等保 1.0 标准增加了两点新要求，一是强调在开发过程中必须进行安全测试，安装（上线）前对恶意代码进行检测，其实就是要将 SDL 流程嵌入到开发流程中；二是要求开发人员必须为专职人员，不可以兼职，而且其开发相关的活动要受控制和监视。

- 梳理一下本控制点的一些关键要求：
- 开发环境与生产环境物理隔离；
- 开发部门有开发管理制度以及安全编码规范；
- 软件具备设计文档（如需求分析说明书、软件设计说明书）和使用手册；
- 对于上述文档的获取和阅读有明确的控制手段和要求；
- 测试阶段具备安全测试报告（黑盒、灰盒、渗透测试）；
- 代码仓库、文档服务器等存储开发过程文件及代码的设备，所有操作应具备相应流程，通过审批后方可执行，且对于不同版本的数据资料有明确说明和保留；
- 开发人员活动应受一定约束，不可兼职其他岗位。

总体来说，标准中首次明确提出开发流程中的安全测试要求，可以引申理解为 SDL 流程的建立和落地，可能不会像一些大型互联网公司那么完善和苛刻，可以逐步建立和改善以适应自身业务发展。另一方面，标准多次强调对开发过程文档的管控措施，因为多数文档可能涉及系统核心技术或企业内部信息，对于此类资料的管控需要引起重视。

外包开发、实施、验收、交付

这部分内容相比等保 1.0 标准有一些要求上的变化，新要求和需要企业重点关注的要求项梳理分析如下。

外包软件开发除了符合同**自行软件开发**中各项要求外，等保 2.0 标准中首次明确要求交付前的源代码审计工作，一方面开发商要自行确保代码的规范，同时还要提供源代码和代码审计报告，结合前面自行软件开发中安全测试的要求，可见等保 2.0 标准对应用系统上线前安全的重视程度明显提高，旨在避免系统带病上线。

工程实施过程中首次明确要求第三方工程监理控制项目整体实施过程。此外，项目的实施计划，实施方案（进度控制、质量控制等），交付方案，过程文档也都需要完备。

测试验收中又再次要求提供安全测试报告，后边补充说明报告中应包含密码应用安全性测试，是指商用密码应用安全性评估。

商用密码应用安全性评估

指对采用商用密码技术、产品和服务集成建设的网络和信息系统密码应用的合规性、正确性、有效性进行评估。按照商用密码应用安全性评估管理的要求，在系统规划阶段，可组织专家或委托测评机构进行评估；在系统建设完成后以及运行阶段，由测评机构进行评估。

哪些系统要做密评

《密码法》(《密码法草案》已于 2019 年 6 月 10 日经国务院常务会议讨论通过）要求“国家对关键信息基础设施的密码应用安全性进行分类分级

评估，按照国家安全审查的要求对影响或者可能影响国家安全的密码产品、密码相关服务和密码保障系统进行安全审查”。《信息安全等级保护商用密码管理办法》规定：“国家密码管理局和省、自治区、直辖市密码管理机构对第三级及以上信息系统使用商用密码的情况进行检查”。在国家密码管理局印发的《信息安全等级保护商用密码管理办法实施意见》中规定“第三级及以上信息系统的商用密码应用系统，应当通过国家密码管理部门指定测评机构的密码测评后方可投入运行”。这些制度明确了信息安全等级保护第三级及以上信息系统的商用密码应用和测评要求。此外，在新版《网络安全等级保护条例》（征求意见稿）明确要求在规划、建设、运行阶段开展密码应用安全性评估。

密评关注哪些方面

为规范商用密码应用安全性评估工作，国家密码管理局制定了《商用密码应用安全性评估管理办法》、《商用密码应用安全性测评机构管理办法》等有关规定，对测评机构、网络运营者、管理部分三类对象提出了要求，对评估程序、评估方法、监督管理等进行了明确。同时，组织编制了《信息系统密码应用基本要求》《信息系统密码测评要求》等标准，及《商用密码应用安全性评估测评过程指南（试行）》《商用密码应用安全性评估测评作业指导书（试行）》等指导性文件，指导测评机构规范有序开展评估工作。其中，《信息系统密码应用基本要求》从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、密钥管理以及安全管理六个方面提出密码应用安全性评估指标。

密评工作当前的进展

现阶段，商用密码应用安全性评估试点工作正在有序开展。经过层层评审，截止 2018 年 6 月第一批共有 10 家测评机构符合测评机构能力要求，具备独立承担并规范开展试点测评任务的能力。中科院 DCS 中心作为首批通过的优秀测评机构，正在积极参与密码应用安全性评估的各项试点工作，为我国密码事业的发展贡献自己的力量。

系统交付要求进行了简化，只保留了三项要求，如交付清单、技术人员培训等，包括采购产品、软件等，会由供应商进行相应培训。而最后要求的建设文档和运维文档，这是结合了三同步来要求的。对于应用系统的开发，设计文档以及上线后的运维记录都可以作为证明材料。

关于**密码管理**，可以参考国家相关标准。

这里给出几个能找到的密码行业标准：

GM/T 0001.2-2012 祖冲之序列密码算法：第 2 部分：基于祖冲之算法的机密性算法

GM/T 0001.3-2012 祖冲之序列密码算法：第 3 部分：基于祖冲之算法的完整性算法

GM/T 0002-2012 SM4 分组密码算法

GM/T 0003.1-2012 SM2 椭圆曲线公钥密码算法第 1 部分：总则

GM/T 0003.2-2012 SM2 椭圆曲线公钥密码算法第 2 部分：数字签名算法

GM/T 0003.3-2012 SM2 椭圆曲线公钥密码算法第 3 部分：密钥交换协议

GM/T 0003.4-2012 SM2 椭圆曲线公钥密码算法第 4 部分：公钥加密算

法

GM/T 0004-2012 SM3 密码杂凑算法

GM/T 0009-2012 SM2 密码算法使用规范

GM/T 0010-2012 SM2 密码算法加密签名消息语法规范

GM/T 0015-2012 基于 SM2 密码算法的数字证书格式规范

GM/T 0044.1-2016 SM9 标识密码算法 第 1 部分：总则

GM/T 0044.2-2016 SM9 标识密码算法 第 2 部分：数字签名算法

GM/T 0044.3-2016 SM9 标识密码算法 第 3 部分：密钥交换协议

GM/T 0044.4-2016 SM9 标识密码算法 第 4 部分：密钥封装机制和公钥加密算法

GM/T 0044.5-2016 SM9 标识密码算法 第 5 部分：参数定义

GM/T 0054-2018 信息系统密码应用基本要求

GM/T 0016-2012 智能密码钥匙密码应用接口规范

GM/T 0019-2012 通用密码服务接口规范

GM/T 0052-2016 密码设备管理 VPN 设备监察管理规范

GM/T 0046-2016 金融数据密码机检测规范

GM/T 0051-2016 密码设备管理 对称密钥管理技术规范

GM/T 0048-2016 智能密码钥匙密码检测规范

GM/T 0050-2016 密码设备管理 设备管理技术规范

GM/T 0047-2016 安全电子签章密码检测规范

GM/T 0053-2016 密码设备管理 远程监控与合规性检验接口数据规范

GM/T 0049-2016 密码键盘密码检测规范

服务供应商选择

强调对于外部供应商的管理。这里贴一下测评要求中的实施方法便于理解。

- 访谈建设负责人选择的安全服务商是否符合国家有关规定。（必须是正规公司）
- 核查与服务供应商签订的服务合同或安全责任书是否明确了后期的技术支持和服务承诺等内容。
- 核查是否具有服务供应商定期提交的安全服务报告。（安全服务项目的周报、月报等）
- 核查是否定期审核评价服务供应商所提供的服务及服务内容变更情况，是否具有服务审核报告。
- 核查是否具有服务供应商评价审核管理制度，明确针对服务供应商的评价指标、考核内容等。（这点做到的很少，Gartner 的 2019 十大安全项目中有提到类似的内容，叫做 Security rating services, SRS 即安全评级服务）

本控制点属于第三方管理范畴，至少要有供应商管理制度、供应商服务合同、服务详细说明等文档。推荐参考 ISO 27002 中 A.15 供应商关系部分的细节。

3.5 安全运维管理

安全运维管理涉及系统上线后的各类安全工作，涵盖环境、资产、设备、漏洞和风险、网络和系统、恶意代码、配置、密码、变更、灾备、应急管理等方面。

环境管理

本控制点尽管归属于安全运维管理，其实同技术部分的安全物理环境紧密相连，是从管理的角度去要求，建立制度和流程（包括记录）配合技术手段进行管理。

这里强调机房日常巡检的工作落实情况，通常机房管理室会放置一本机房巡检记录的台账，以及一本外来人员登记台账（也有可能是电子流程记录）。测评或检查时重点查看的就是巡检和访问的记录情况。比如来访登记应包括来访人员、来访时间、离开时间、来访事由、来访接待部门人员等。对于机房巡检记录通常每天都会做一次，最多不会超过一周。

在机房安全管理制度方面，通常会将制度和不允许的事宜挂在机房墙上。不过这些是结合企业自身情况的要求规定，除此之外，标准还要求管理制度中应包含物理访问、物品进出、环境安全等要求，现场会检查一些制度中要求的记录。

对于安全意识和社会工程学的检查，这些不是要求写在纸上的内容，而是在测评过程暗中检查的内容。比如办公区或会议室，白板上、桌面或是大屏幕有涉及企业核心或敏感信息的内容，有没有员工在公开场合谈论公司机密和战略规划等话题。

资产管理

标准中对于资产管理的要求可能要再定义一下，包括企业关键岗位人员、核心代码、敏感数据、Web 站点、内外网应用系统、管理制度文档，这些都可归类为资产范畴，做统计时也要一并记录。

检查中会对资产清单、分类、标识、重要性、资产所在位置/部门进行查看，

可以提供纸质或电子台账，或者是资产管理平台也可以。此外，资产管理制度要有，可以是单独的制度文档，也可以是安全管理制度的一个章节，其中明确资产管理的要求，标识方法、信息分类、信息使用、传输、存储要求等。

介质管理

介质也应算作资产的一部分，介于其用途的广泛和便捷性，需要进行独立的管理，包括磁盘、U 盘、存储卡、光盘、磁带、云存储（如 GitHub，虽然标准没要求）。传统介质，这类存储数据的媒介，通常会因为数据拥有生命周期，其也会伴随该周期经过从产生到销毁的一个过程。关键在于几个过程节点：

- 存—冗余性、保密性、完整性、专人/部门管控；
- 取—安全性控制、物理传播安全性、灾备；
- 毁—正规专业机构、脱敏、保密协议。

对于上述各节点，均有记录供查询。为确保数据安全也可以采用一些 EDR、DLP 之类的设备。

企业关于此类问题的管控应该引起重视，而对于个人其实就是随手的事，拿百度云为例，想上传资料可以，打包上传或者文件夹设置密码，分享的时候尽量只共享 1 天，或者需要共享时间较长，那么设置一个带密码的分享链接，确认对方收到后及时关闭分享。这些都是很基本的安全意识。另外，对于企业或客户的敏感信息，建议不要放在云端，存放于本地存储中是相对安全的做法。

设备维护管理

其中关于设备、线路维护的通常机房巡检中会查看，维护人员责任和审批流

程的内容都是常规要求，包括机房的设备如要带离机房必须有审批流程，关于数据安全的问题上和上节介质管理相似，这里不再重述，有兴趣的可以参考《数据安全管理办法》、《数据安全成熟度模型》，目前国内已经在进行试点，具有一定的参考性和可行性。

漏洞和风险管理

虽然只有两条要求，但这其中涵盖的东西很多。首先，从检查的角度来看，对于漏洞和风险管理，最起码要有制度，或者在方针或策略中有提到如何去管控。这其中要提供渗透测试报告、漏扫报告、修复情况说明、复测报告等，周期最好不要超过 6 个月，也就是每半年测试一次。如果你有能力做业务影响分析，那更好。除了技术层面，管理层面的测评也要去做，每年一次的等级测评通常来说不算做自评估范畴。所以，最好再做一些其他的安全评估或风险评估，也有助于企业发现存在的问题。最后就是对于发现问题修复的及时性，对于重大安全漏洞不要说影响业务，没办法打补丁。除非系统在内网，且做好了隔离，或者有其他手段可以有效控制降低风险等级。

关于漏洞管理，建议各位参考一下《网络安全漏洞管理规定》。该规定的征求意见稿刚发布时，在安全圈内引起来不小的骚动，各技术人员纷纷发表看法。

这里将管理规定的几个关键点总结一下：

1. 本规定适用国内所有企业、组织和个人；
2. 发现的漏洞，在限定时间内，相关厂商、第三方、运营方等必须做出修补，并公开漏洞细节和应对措施；
3. 发现漏洞必须提交给相关企业、厂商或漏洞平台，不得自行发表；

4. 各监管部门检查的重点可能会有所不同；

5. 不允许夸大漏洞危害，不得私自发布漏洞验证工具和方法；

6. 期限内不能整改的，要接受监管部门处罚。

网络和系统安全管理

本控制点是从管理角度将技术部分的内容做出制度流程的要求。涉及配置管理和变更管理（以下 a)、b）分别对应标准中的要求项编号)。

a）常说的“三员”（即系统管理员、网络管理员、安全管理员）以及审计管理员，通常安全管理员不可兼职其他岗位（其他部门岗位也不可以)，其他三个岗位没有明确说不能兼职，不过最好还是设立专人好一些，如果公司规模较大，每个岗位应设置多个管理员，做 AB 岗位轮换。

bc) 账户管理相关，通常会由系统管理员负责分配权限以及账户建立和删除，对于这些操作都需要通过审批才可以进行，检查时会查看账户管理制度和近半年的操作记录和审批记录，系统后台的账户相关日志记录（包括登入/登出，日常操作等)。这里说的补丁是指承载系统的主机以及系统所使用的数据库及中间件的重大安全漏洞补丁。如果对于高危风险的补丁几个月都没有修补，可以判定为高危风险点。

d）设备的安全基线配置，操作手册通常是指日常一些运维操作的详细操作步骤以及注意事项说明，便于指导新人和不熟悉系统的人进行操作。注意，这里要求的是重要设备，企业关键核心级别的设备要有相应的操作或要求文档。

ef)是关于日志记录和管理的要求，在前边各控制点中反复提到过，本要求项强调运维操作日志，包括巡检、参数设置和配置变更等操作。f)中对安全事件

的监控和预警，目前靠人工已经很难实现，更多还是结合技术手段，如 IDPS、蜜网、态势感知、SOC 等，多设备/系统联动的监控预警平台更能有效及时发现和阻断违规行为。各企业可根据自身情况和预算来取舍。

gh）是关于变更控制的要求，系统或设备进行变更时一定做好预防措施，通过上级审批，充分做好测试后再执行，期间的日志要做好留存，确保完整性。操作后的配置应备份，此时对于先前的配置备份应暂时留存，不要过早覆盖或删除。同样，运维工具接入系统也是要做好上述的各个环节，变更关注的是业务连续性，工具接入更多关注的是敏感信息泄露问题，强调了工具使用过后信息彻底清除的工作。

i)关于远程运维的要求，通常来说企业一般不会涉及这类情况，除非是供应商的售后支持可能会远程调试，需要临时开放外部接口。这种情况下，很可能会出现分配的用户具备较高权限但主要是为了调试或维修，所以口令为空或者弱口令，在维护结束后管理人员又没有及时关闭端口、删除临时用户。

j）这点同安全区域边界—边界防护中的要求类似，技术部分要求能够检测私自外联的行为并进行阻断，但究其根本很难靠纯技术手段实现。这里是从管理上进行人员的约束，定期检查员工是否有未授权私自外联的情形。

恶意代码防范管理

本控制点要求偏向于终端安全的软件，杀毒软件也可以。一方面在边界的安全设备上开启恶意代码防范功能，另一方面在终端设备（服务器、主机、系统）上安装端点防护或杀毒软件，并定期更新特征库。如果企业真的没有办法，那么在主机层安装一个 360 或者火绒，不过这是权宜之计而非推荐的做法。

等级保护 2.0 标准提出了一个新要求，即提高所有用户的防恶意代码意识，不是安全意识，而是防恶意代码意识。这就要求企业，定期开展相关培训（恶意代码防范意识培训），包括培训的通知、课件、签到（可以是电子签到、会议确认）、考核结果（不会强制要求，除非其他类培训都没有考核）。

备份与恢复管理

关于企业业务连续性计划（BCP, Business Continuity Plan）和灾难恢复计划（DRP, Disaster Recovery Plan）的相关要求。这两项计划想必多数企业都会或多或少的有在做，毕竟关系到实际业务，运维方面的事情就不再细说，主要说一下检查时的重点。对于灾难恢复需要有灾难恢复预案（或者叫灾难恢复方案）、灾难恢复演练方案以及演练的记录和总结报告。有些互联网公司此类演练都是电子流程，电子汇报，也可以在内部平台中展示记录和结果。灾难恢复演练每年至少应开展一次。

安全事件处置、应急预案管理

应急处置的内容是比较关键也比较多的，只是通常企业关注的是结果而非过程，因此大多数情况都忽略整个周期的前半部分。

按照国家要求应急响应流程包括六个阶段，如下图所示：

图 4.5.1 应急响应流程的六个阶段

对于每个阶段准有相应的要求，除去总结阶段的经验教训总结，其余五个阶段的要求如下：

准备阶段

要求企业制定《应急响应流程》和《应急响应操作规范》，其中要涵盖一些常见安全事件的处理方法，包括检测、抑制、根除和恢复操作，作为用例指导应急人员处理问题。

此外《风险管理计划》、《应急响应预案》(包括安全事件分类、上报流程等内容)、应急团队人员岗位职责。

检测阶段

企业需要制定《应急响应分析报告》、《风险告知书》、《应急响应实施方案》等。

抑制阶段

在应急响应周期中应制定并留存《应急响应抑制方案》、《应急响应变更单》(如有)、《应急响应分析报告》(抑制阶段的安全事件分析)。

根除阶段

在应急响应过程中留存《根除整改建议报告》、《根除结果确认单》。

恢复阶段

企业需要提前制定和留存《信息系统灾难恢复计划》、《信息系统灾难恢复方案》、《应急演练管理办法》、《应急响应报告》。

整体应急响应周期的流程图如下图所示：

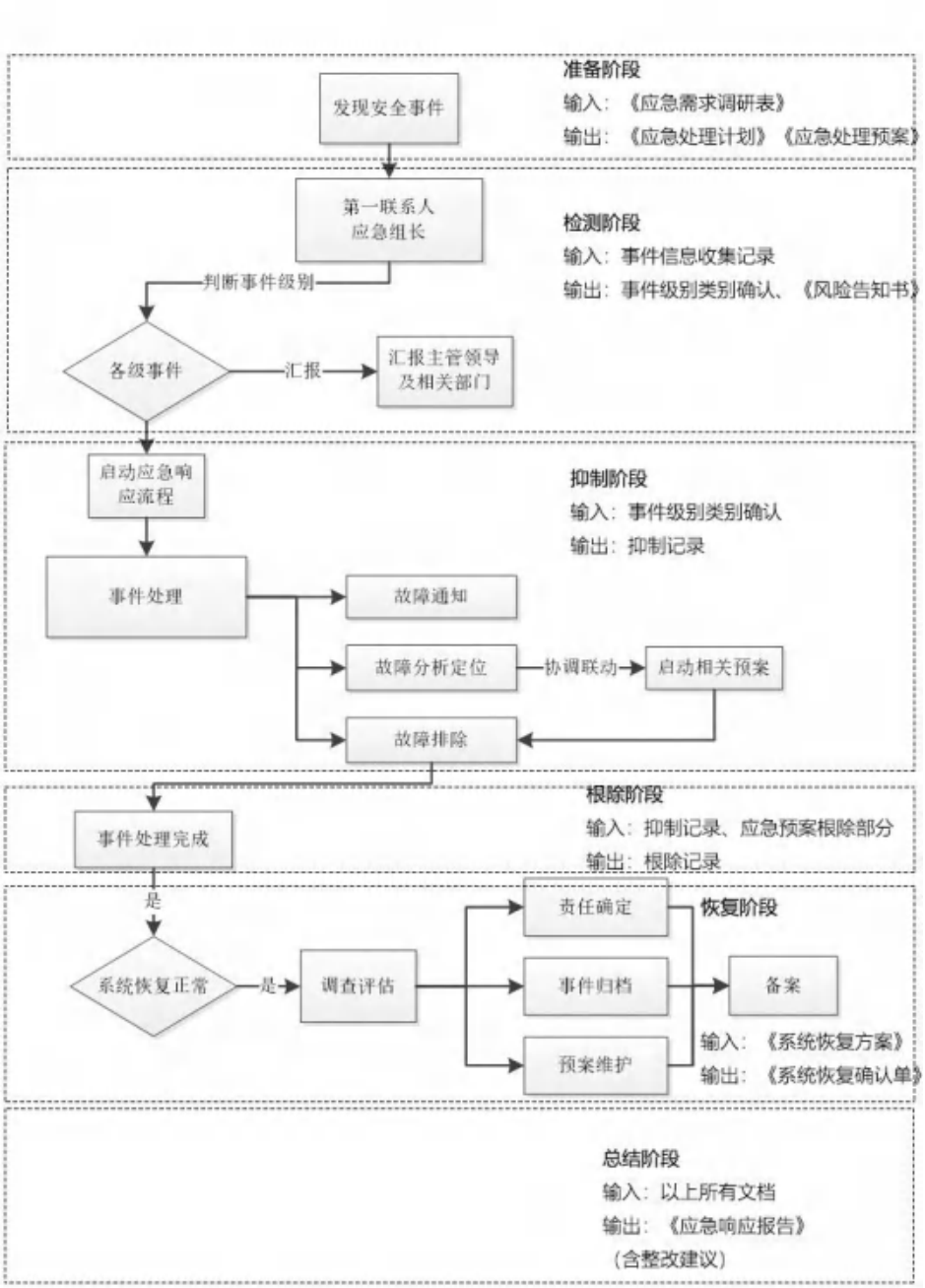


图 4.5.2 应急响应流程图

以上是根据国家标准要求的理论化的应急响应流程，这里简单介绍一下，仅供参考。

企业最基本的应该具备《应急响应流程》(可包含在应急响应管理制度或预案中)、《应急响应预案》(必须包含上报流程、事件分级)、《应急响应操作规范》，这几个文档必备。

再者是过程中的记录，包括针对安全事件的处置各阶段的分析（可包含在应急响应报告中)，抑制和根除过程的记录和确认，系统恢复操作记录，最后是整个安全事件的原因分析和经验总结。

最后是关于应急预案管理的要求，等保 2.0 标准要求每年必须开展应急响应相关培训（包括架构组成、流程、资源保障等)，不是安全意识培训，是应急培训。每年要能体现对于上一年度应急预案的评审和修改，除非系统没有变化，否则都应根据系统变化情况修改预案，而且每年应至少开展一次应急演练（可以是桌面演练、测试环境演练、真实环境演练)，并且保留演练计划和记录。

外包运维管理

新增要求，关于外包运维的管理，与 ISO 27002 供应商管理管理有些类似。

外包运维现在是比较普遍的情况，也是企业压缩成本的一种选择，只要是正规大中型运维公司通常各项执照和资质都是齐全的，所以只要不是和一些不知名或很小的公司去签订运维服务，一般都会符合国家规定。

外包运维合同或附件技术规范书/工作说明书中能够明确服务范围和内容，这部分通常不会有什么问题，都是具有法律效力的文件，都是要经过法务部门进行审核的。至于供应商的工作能力证明，只要提供对应的国家资质证书(集成类、

运维类国家认证）和成功的项目案例即可。

3.6 IPv6 合规

随着各国网络发展战略的出台，IPv6 进入快速发展阶段。2017 年 11 月中国中共中央办公厅、国务院办公厅印发了《推进互联网协议第六版(IPv6)规模部署行动计划》，提出用五至十年时间，形成下一代互联网自主技术体系和产业生态，建成全球最大规模的 IPv6 商业应用网络，实现下一代互联网在经济社会各领域深度融合应用，成为全球下一代互联网发展的重要主导力量。2020 年 3 月，为贯彻落实《推进互联网协议第六版(IPv6)规模部署行动计划》（厅字〔2017〕47 号）任务要求，加快提升 IPv6 端到端贯通能力，持续提升 IPv6 活跃用户和网络流量规模，工信部印发《2020 年 IPv6 端到端贯通能力提升专项行动的通知（工信部通信函〔2020〕57 号)》，决定于 2020 年开展 IPv6 端到端贯通能力提升专项行动。2020 年 6 月，中国人民银行印发《中国人民银行科技司关于开展金融行业 IPv6 规模部署落实情况专项摸排工作的通知（银科技[2020]13 号)》，旨在巩固金融行业 IPv6 规模部署初期阶段工作，加快推进规模贵广阶段工作，重点掌握金融机构在改造面向公众服务的各类系统的实际进展情况和存在的问题。

图 3.6.1 全球各国 IPv6 部署程度

我国目前（截止 2020 年 6 月）IPv6 部署主要集中在中央、政府、大型企业，覆盖率约在 80%左右，IPv6 活跃用户约 3.18 亿人，占比 35%。

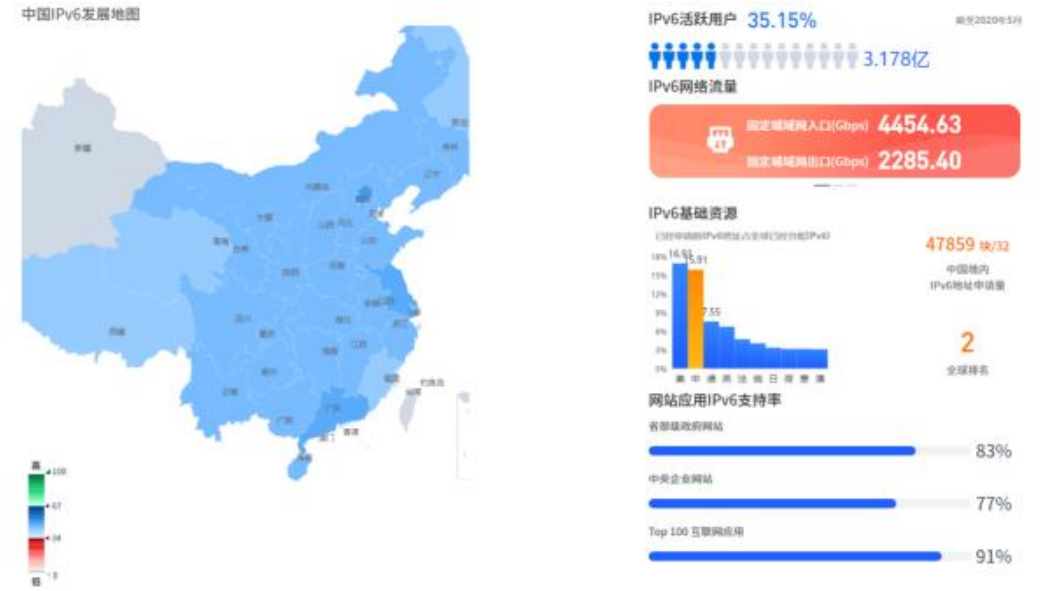


图 3.6.2 中国 IPv6 发展情况(来源：国家 IPv6 发展监测平台，2020.06)

在全球大力发展 IPv6 的同时，问题也开始逐渐显现，无论是监管部门还是政府、企事业单位，习惯了每年一次的等保和安全检查，但是在面对 IPv6 的合规性方面，目前可以说是一种不知所措的状态，尤其是企业方面。

首先应明确，该行动计划由党中央、国务院牵头开展，依据《国民经济和社会发展第十三个五年规划纲要》、《国家信息化发展战略纲要》、《“十三五”国家信息化规划》制定，其效力并不弱于《网安法》的要求，因此，政府、企事业单位应积极响应并推行。

《行动计划》有三个主要目标，五个重点工作（互联网应用、网络基础设施、应用基础设施、网络安全、关键前沿技术）。

三个主要目标

目标 1 是对 2018 年末 IPv6 改造的要求。

目标 2

- 到 2020 年末，新增网络地址不再使用 IPv4；IPv6 用户活跃数达到 5 亿，互联网用户中占比 50%（目前 3.2 亿左右，占比 35%）；
- 2020 年底以下企业需全面支持 IPv6（注：排名是指用户量排名）：
  - ✓ 国内 Top 100 商业网站及应用
  - ✓ 市地级以上政府外网网站，新闻及广播电视媒体网站系统（能力覆盖 85%+）
  - ✓ 大型 IDC（机架数量在 3000-9999 范围）
  - ✓ Top 10 CDN（支持 IPv6 节点数达 85%+）
  - ✓ Top 10 云平台 100%的云产品
  - ✓ 广电网络，5G 网络及业务，各类新增移动和固定终端

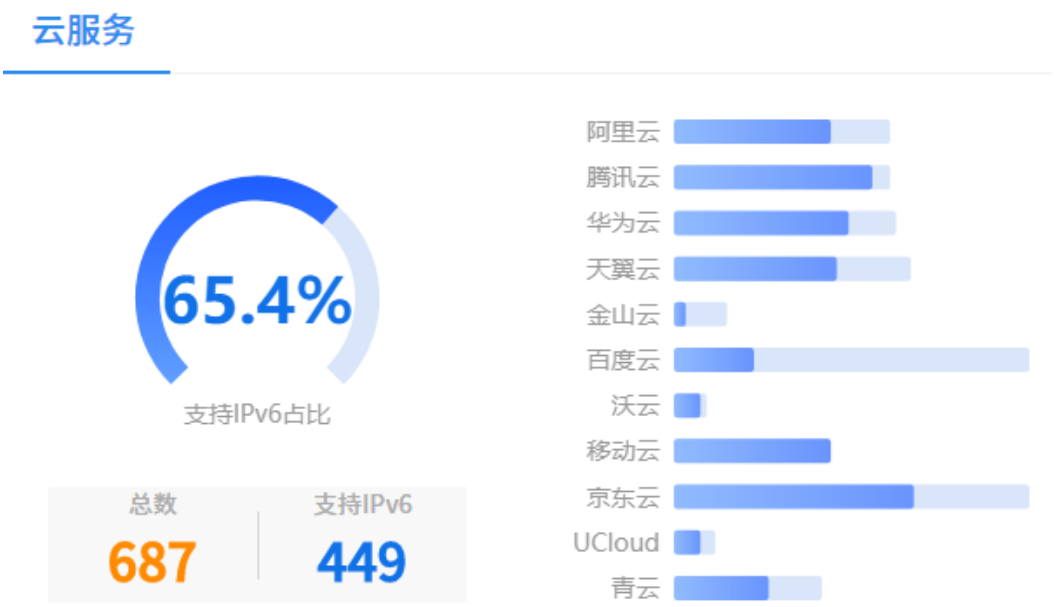


图 3.6.3 中国云产品 IPv6 支持情况(来源：国家 IPv6 发展监测平台，2020.06)

目标 3

到 2025 年末，我国 IPv6 网络规模（部署率目前第十位）、用户规模（目前第二位）、流量规模位居世界第一位，网络、应用、终端全面支持 IPv6。从 2020 年 5 月的数据来看，目标 2 的完成时间可能会推迟。那么对于政府、企事业单位（下文统称为“组织”），结合《2020 年 IPv6 端到端贯通能力提升专项行动的通知》中对完成指标的最新调整，需要关心的有几个方面：

- 现有外网网站或系统在年底前，最起码要达到 85%以上的 IPv6 支持率，在未来 1-2 年内达到 100%（国内前 100 商业网站、地市级政府网站、广电、新闻站点是强制要求）；
- 国内前 10 的内容分发网络（CDN）年底 85%以上节点要支持 IPv6；（包括：阿里云、腾讯云、网宿科技、蓝汛、金山云、百度云、华为云、京东云、帝联科技、UCloud、白山云、七牛云、鹏博士、中国移

动）

- 广电、运营商新上线系统及业务（包括移动端和固定终端）从设计到开发到商南县，需基于 IPv6 协议，不可以再用 IPv4。
- 年底前门户网站二级、三级链接的 IPv6 浓度达到 85%+；（涉及部门包括：各省（区、市）通信管理局、部属各单位、部属各高校、基础电信企业）
- App、应用、客户端、浏览器、论坛等需进行 IPv6 升级，尤其排名前 100 的网站和应用，允许 4/6 双栈连接，但优先 IPv6 连接；
- 年底前完成政务、综治、金融、医疗等领域公共管理、民生公益等服务平台改造，即 100%支持 IPv6；
- 工业互联网 IPv6 改造工作启动，没有明确要求，但需要由改造计划和阶段性成果；
- 从超大型 IDC 扩展到大型 IDC，即机架总数超过 3000 个的 IDC，年底前要完成 100%IPv6 改造；(三大运营商改造范围扩展到中小 IDC；相关企业 Q3 末要完成年报中全部数据中心的 IPv6 改造，包括阿里云、腾讯云、百度云、京东云、华为云、世纪互联、鹏博士、秦淮科技、新网互联、方正信息、西部数码、万国数据、光环新网）
- 国内排名前 10 的云服务商，年底前所有云上产品（包括：云主机、容器引擎、负载均衡、域名解析、对象存储、MySQL 云数据库、MongoDB 云数据库、API 网关、Web 应用防火墙、DDoS 高防、文件存储（NAS）、对等连接服务（VPC）、HTTPDNS、数据库审计、微服务引擎、MapReduce 服务、设备接入服务（IoT Hub）、区块链服务、视

频直播、人脸识别等）要 100%支持 IPv6（被点名企业：阿里云、天翼云、腾讯云、沃云、华为云、移动云、百度云、金山云、京东云、UCloud、青云）；

- 完善针对 IPv6 的网络安全定级备案、风险评估、通报预警、灾难备份及恢复等工作；即开始建立针对 IPv6 网络的安全评估和应急预案等文档体系。

技术合规

由于当前缺乏可参考的法规和标准，不能确定未来监管会重点检查哪些方面以及衡量指标。但是，鉴于国家对电信、广电行业的强制性要求，可以将该行业（包括地方文件）的实施指南类文档作为参考，大概预测一下 IPv6 技术合规方面需要企业关注的重点。

IPv6 部署

- 应制定 IPv6 升级改造的人员组织架构，明确责任人和各岗位职责分工；
- 组织应提前制定 IPv6 部署计划，其中充分考虑对现有系统的 IPv6 演进路径及可能影响；
- 组织应采取先试验，逐步小规模部署，在部署成熟后开始大范围推广，整个过程中应做好安全防护方案，包括割接方案及回滚方案；
- 可以采取双栈部署方式，逐渐过渡到纯 IPv6 网络，根据业务情况，逐渐淘汰或升级 IPv4 系统和终端；
- 组织核心网络设备（如防火墙、负载均衡、路由器、核心交换机等）

应支持 IPv6 协议，从长远考虑来看，组织也可以考虑支持 SRv6 的设备；

- 由于 IPv6 地址资源过于庞大，组织应合理规划地址段，细化安全域，避免后期由于地址太过分散，无法聚合，难以管理；
- 升级后网络应能支持 IPv6 组播、IPv6 的 QosS 及 DHCPv6 等协议；
- 对于遗留系统，通过评估后再进行升级计划；
- 针对公司业务主管及运维团队进行 IPv6 技术培训、割接培训，培养 IPv6 专业人才。

系统升级（以 3A 系统为例）

- 组织的 3A（或 4A）系统应能够支持 IPv6（包括业务支持、对外接口支持以及系统本身支持），主要是 Radius 报文中的属性字段（可参考 RFC3162）；
- 业务上可以区分用户 IP 类型（v4、v6 或双栈），支持 IPv6 属性，并授权相应的地址；
- 对外与其他系统交互，应能识别用户类型字段（v4、v6 或双栈），如计费系统，能够对不同类别用户的上网时长和流量提供独立记录；
- 3A 系统应能配置 IPv6 地址，能与其他设备进行 IPv6 交互；
- 新采购设备或开发系统（业务），应支持 IPv6，优先推荐 IPv6-only 项目。

网络安全合规

为贯彻落实党中央、国务院印发的《推进互联网协议第六版(IPv6)规模部

署行动计划》要求，加快下一代互联网规模部署，促进互联网演进升级和健康创新发展，应结合等保 2.0 体系要求，对 IPv6 网络进行整体而全面安全防护，保障系统安全稳定运行，确保重要数据与个人信息的完整性与保密性。

对于 IPv6 的部署和升级改造目前比较顺利，而且已经解决要求的目标，但随之而来的安全问题也开始显现。由于目前关于 IPv6 的相关标准还未出台，因此结合等保 2.0 体系总结一些当前比较典型的安全问题。

传统安全问题

尽管升级到 IPv6 网络，但是一些基于 IPv4 网络的安全问题依旧存在，组织还应继续予以关注并做好防护措施。相关合规要求示例：

- 边界设备 IPv6 安全策略与地址过滤功能；
- 边界设备 ICMPv6 过滤功能；
- DHCPv6 安全防护功能；
- IPv6 设备（包括安全设备）自身漏洞问题；
- IPv6 应用主机安全防护能力；
- IPv6 流量分析和溯源能力。

报文监听

IPv6 中可使用 IPSec 对其网络层的数据传输进行加密保护，但 RFC6434 中不再强制要求实施 IPSec，因此在未启用 IPSec 的情况下，对数据包进行监听依旧是可行的。

应用层攻击

IPv4 网络中应用层可实施的攻击在 IPv6 网络下依然可行，比如 SQL 注入、缓冲溢出等，IDPS、病毒防护、URL 过滤等应用层的防护不受网络层协

议变化影响。

泛洪攻击

在 IPv4 与 IPv6 中，向目标主机发送大量网络流量依旧有效，泛洪攻击可能会造成严重的资源消耗或导致目标崩溃，DDoS 防护依然关键。

分片攻击

在 IPv4 中，分片可以由发送主机和中间路由器执行，而 IPv6 分片只能由主机执行。这把 IPv6 路由器从昂贵的分组任务中解放了出来。

IPv6 分片的一个重要方面是对分片的支持是通过 IPv6 扩展报头(特别是片报头)实现的。前规范的 IPv6 协议(即在[RFC8200]之前的协议允许一些非正常的分片情况，比如一个包的第一个分片不包含整个 IPv6 报头链(见[RFC7112])。这种非正常分片情况可能仍然遗留，被 IPv6 实施所允许，因此可能被用来规避 IPv6 安全控制。此外，由于分片支持是通过 IPv6 扩展报头实现的，所以扩展报头的所有通用安全考虑都适用于分片报头。

地址欺骗

IPv6 使用 NDP 协议替代了 IPv4 中的 ARP 协议，但由于实现原理基本一致，因此针对 ARP 协议的 ARP 欺骗、ARP 泛洪等类似攻击方式在 IPv6 中依旧可行。

网络架构

IPv4 网络最常见的架构是内部节点使用私有 IPv4 地址，通过 NAT 设备连接到外部网络。作为转换 IPv4 地址和传输协议端口号的副作用，NAT 设备最终强制执行“只允许传出通信”的过滤策略。

虽然这不是一种安全万能方法，但它确实在许多网络场景中减少了攻击面。

由于 IPv6 网络不需要依赖于 NAT 设备，所以有时会假设 IPv6 节点造成更多的暴露面——也就是说，每个 IPv6 节点都可以从公共互联网直接访问。然而，这并不需要，通常也不应该出现这种情况。

例如，当前使用 IPv4 私有地址空间并通过 NAT 设备连接到 Internet 网络。可以通过在 IPv4 NAT 设备所在的网络拓扑的同一点部署有状态的 IPv6 防火墙来限制 IPv6 主机的暴露。IPv6 防火墙通常配置为“只允许对外通信”，这样 IPv6 过滤策略就可以与 IPv4 相对应。此外，IPv6 主机可以使用基于主机的 IPv6 防火墙，“只允许外部通信”，就像许多 IPv4 主机对 IPv4 流量所做的一样。

这种 IPv6 网络“架构”和包过滤策略是 IETF 推荐的用于 IPv6 互联网服务客户的家用默认设置之一。

IPv4 网络中的 IPv6 问题

每当一台双堆栈主机要连接到另一台主机时，它通常会使用 DNS 来获取目标主机域名的 IPv4 和 IPv6 地址。随后，它将尝试与该主机通信，方法是按顺序尝试每个地址，或者并行尝试一些地址对。

通常，IPv4-only 网络上的主机不会配置 IPv6 全局单播地址或 IPv6 默认路由，因此使用 IPv6 的通信尝试会失败，只有 IPv4 才有可能成功。

大多数现代操作系统都支持 IPv6，并且在默认情况下不管 IPv6 是否已经部署到连接节点的网络上都会启用这种支持。这意味着即使缺少全球 IPv6 连接，其仍然存在于 IPv4 专用网络中。换句话说，大多数“IPv4 专用网络”是由双栈节点组成的，当 IPv6 可用时，这些节点可以很容易地利用 IPv6 连接。因此,攻击者连接到本地子网可能触发 IPv6 网络配置(例如,通过发送伪造的路

由器通告消息),随后执行基于 IPv6 的攻击,如拒绝服务(DoS)、中间人(MITM)、触发 VPN 流量泄漏。

因此，即使是纯 IPv4 的网络，也应该实施 IPv6 安全控制。这些控制可以从减轻对自动配置和地址解析机制的攻击，到执行 IPv6 ACL 或在二层完全阻止 IPv6 流量。

新安全问题

IPv6 包结构问题

IPv6 采用固定长度的基础 IPv6 报头，可选的扩展报头形成一个菊花链包结构。希望哪个系统处理这些选项可以使用不同的选项容器，这样节点就不必解析它们无需处理的选项。然而，当需要处理整个 IPv6 报头链以访问上层协议值(如传输协议类型、传输协议端口号等)时，IPv6 包结构往往与现代路由器体系结构不相匹配。

IPv6 扩展报头存在很多安全隐患：

- 一些安全设备在执行过滤策略时不能处理整个 IPv6 报头链([RFC7113])。因此，即使只是简单地添加一个只携带“padding”选项的扩展头，也足以绕过相应的安全控制。
- 一些网络或安全设备通常可能在硬件上处理流量，但在软件中处理携带选项的包。这种情况下，IPv6 扩展头可能被用来执行 DoS 攻击。
- 在许多 IPv6 实施中发现，无法对使用 IPv6 扩展报头的包执行基本完整性检查。在某些情况下，攻击者可能通过向受害节点发送单个或持续精心设计的数据包流来导致处理节点崩溃、重新启动或无响应。

为了减轻上述的安全影响，应该执行适当的包过滤策略。通常路由器应该更宽松的放行流量(使用列入黑名单的信息包过滤方法),而更接近网络的边缘节点(例如企业边界路由器)通常应该更保守,只允许他们预期想获得的流量(即采用白名单的信息包过滤方法)。

一些网络使用扩展报头来过滤数据包，这影响了 IPv6 扩展报头在公共互联网上使用的可靠性[RFC7872]。普遍使用的丢弃包含扩展报头的 IPv6 数据包也会影响 IPsec 扩展报头。这样做的后果是，为了使 IPsec 数据包在 IPv6 互联网上存活，可能需要通过一些传输协议(例如 TCP 或 UDP)来隧道 IPsec 流量。对于某些用例，可以使用 TLS VPN 等替代技术。

海量地址“造福”攻击者

批量注册，批量薅羊毛，刷量，刷单，引流等需要操控大量的账号进行自动化攻击。在网络的攻防对抗中，动态切换 IP 来覆盖 Web 表单爆破，或者是利用工具进行 MySQL，Redis，RDP 等协议爆破，以及进行常见 Web 攻击，如 SQL 注入，0day/1day/Nday 漏洞利用等。

图 3.6.4 IPv4 与 IPv6 地址资源

对于攻击者而言，他们会想尽一切办法，来不断降低攻击成本，提高攻击效率，自动化攻击便是其中的关键方法之一。对于防守方而言，他们会实施一系列防御方法，比如累积黑/白名单，创建情报库以及部署防御策略等，来提

高攻击者的攻击成本，提高防守率。这实际上是资源的对抗，尤其是 IP 资源的对抗。企业应对秒拨 IP 技术引起重视，今早做好防护措施。

影子 IT 更难于管理

IPv6 主机通常为每个网络接口配置不同范围和属性的多个地址。这与 IPv4 形成对比，在 IPv4 中，主机通常只为每个网络接口配置一个地址。随着地址数量的增加，每个地址都具有不同属性，这为提高安全性、保密性和弹性提供了能力。

然而，由于对可用地址的不当使用，这些潜在的优点通常无法实现。可能在某些场景中，这种对可用地址的不当使用将导致意外。

IPv6 主机通常配置不同范围的多个地址，从链路本地到全局。一般来说，主机应该为每个应用程序使用尽可能小范围的地址。这种缩小的范围容易提供隔离，这层隔离是由地址范围本身所产生的（如 Vlan）。

例如，一个只能从网络内部访问的文件服务器可能只想使用 ULAs——IPv6 中相当于 IPv4 私有地址。通过使用 ULAs，有限地址范围本身可以作为与互联网隔离的一种手段。使用有限范围的地址并不排除或阻止使用其他网络防护手段，而是作为一个额外的防护。

使用有限范围的 IPv6 地址能带来额外的好处。例如，ULA 地址块(fc00::/7)足够大，几乎任何大型或复杂网络都可以从 ULA 地址空间中构建。由于 ULAs 是本地管理，因此即使上游提供程序出现故障，它们也可以提供可用的地址；也就是说，即使与上游提供程序的连接丢失，且全局地址超，仍然可以使用 ULAs 进行本地通信。

IoT 设备问题

当谈到 IPv6 和物联网，许多人认为 IPv6 是物联网释放其全部潜力的必要条件。然而，分析 IPv6——特别是全局寻址和 any to any 连接——在何种程度上与物联网想结合是很重要。

无论使用或不使用全局地址空间，是否需要 any to any 连接(包括主动入站通信)，以及它对物联网设备安全性的影响才是问题的关键。在 IPv4 中，未经请求的入站通信由于使用 NAT 会被阻断。随着 NAT 和网络过滤策略（可能）在 IPv6 中的消失，全局 any to any 通信可以提高灵活性——同时以增加攻击风险作为代价。

是否对 IPv6 和物联网设备实施同样的过滤策略将取决于相关设备的通信模型；是否期望外部实体轮询物联网设备，或是否期望物联网设备通知外部实体。如果是前者，物联网网络将需要接受入站、未经请求的通信。若是后者，传入的通信可能会被阻断，而物联网设备将能够根据需要来连接外部系统。

除了可能的物联网设备通信模式,当从外部网络向物联网网络通信是可行的,这种通信应该直接访问物联网设备，还是应该通过作为物联网和外部网络之间的网关代理来执行？显然，网关方式在安全方面可能会更好，而且在监管脆弱的物联网设备流量方面也可能处于有利地位。

物联网网关具有设备连接、协议转换、数据过滤和处理、安全、更新、管理等重要功能。物联网网关也可以作为应用程序代码平台，处理数据并成为支持边缘系统的智能部分。

IPv6 协议漏洞

有关 IPv6 的安全漏洞在逐渐被爆出,虽然可被利用的漏洞数量还不算多，但组织应该密切关注。截止今年 6 月，CVE 官方统计 IPv6 漏洞数量以超过

400 个。企业以后的漏洞扫描工具应支持 IPv6 漏洞和资产发现功能。

目前来看，“好用”已经成为当前 IPv6 规模部署工作重点（其实，目前大多数企业的要求是“能有”，还没到“好用”）。“好用”不仅是简单的用 IPv6 替代 IPv4，更要发挥基于 IPv6+的下一代互联网创新优势实现业务创新和产业赋能。IPv6+提出的 SRv6、VPN+、APN 等关键技术，为简化网络结构、优化用户体验和提升网络智能化奠定了良好的基础，与 5G、云网融合、工业互联网、车联网等应用对网络承载需求不谋而合，为进一步开展网络和业务创新提供了广阔的空间。因此，加强基于 IPv6+的下一代互联网技术创新，发展增强型“IPv6+”网络提升网络能力，从而驱动网络和业务融合创新，是下一步 IPv6 发展的必然方向。

3.7 安全建设管理安全通用要求部分责任边界举例

通用要求	安全控制点	测评指标	云平台责任	客户责任
安全通用要求	定级和备案	a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；	应单独定级，且云平台不能承载高于自身安全级别的客户应用	单独定级，不能选择低于客户应用平台级别的云平台
		b) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；	√	√
		c) 应保证定级结果经过相关部门的批准；	√	√
		d)应将备案材料	√	√

通用要求	安全控制点	测评指标	云平台责任	客户责任
		报主管部门和相应公安机关备案。		
	安全方案设计	a）应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；	√	√
		b）应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术	√	应根据 IaaS、PaaS、SaaS 不同的模式下，只设计客户应用应承担的安全要求的方案设计，其余直接采信云平台的测评结论。如 IaaS 模式下，客户无需设计对资源安全隔离、物理机房安全等方案。

通用要求	安全控制点	测评指标	云平台责任	客户责任
		相关内容，并形成配套文件；		
		c）应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。	√	√
	产品采购和使用	a）应确保网络安全产品采购和使用符合国家的有关规定；	√	如果使用的网络安全产品均为云平台提供，则可以直接使用云平台的等保测评结论；否则客户应需要单独满足要求
		b）应确保密码	√	如果使用的网络安全产品

通用要求	安全控制点	测评指标	云平台责任	客户责任
		产品与服务的采购和使用符合国家密码管理主管部门的要求；		均为云平台提供，则可以直接使用云平台的等保测评结论；否则客户应需要单独满足要求
		c）应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。	√	如果使用的网络安全产品均为云平台提供，则可以直接使用云平台的等保测评结论；否则客户应需要单独满足要求
	自行软件开发	a）应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；	√	√
		b）应制定软件开发管理制度，	√	√

通用要求	安全控制点	测评指标	云平台责任	客户责任
		明确说明开发过程的控制方法和人员行为准则；		
		c）应制定代码编写安全规范，要求开发人员参照规范编写代码；	√	√
		d）应具备软件设计的相关文档和使用指南，并对文档使用进行控制；	√	√
		e）应保证在软件开发过程中对安全性进行测试，在软件安装	√	√

通用要求	安全控制点	测评指标	云平台责任	客户责任
		前对可能存在的恶意代码进行检测；		
		f）应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制；	√	√
		g）应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。	√	√
	外包软件	a）应在软件交付前检测其中可	√	√

通用要求	安全控制点	测评指标	云平台责任	客户责任
	开发	能存在的恶意代码；		
		b）应保证开发单位提供软件设计文档和使用指南；	√	√
		c）应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。	√	√
	工程实施	a）应指定或授权专门的部门或人员负责工程实施过程的管理；	√	√
		b）应制定安全	√	√

通用要求	安全控制点	测评指标	云平台责任	客户责任
		工程实施方案控制工程实施过程；		
		c）应通过第三方工程监理控制项目的实施过程。	√	√
	测试验收	a）应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；	√	√
		b）应进行上线前的安全性测试，并出具安全测试报告，安全	√	√

通用要求	安全控制点	测评指标	云平台责任	客户责任
		测试报告应包含密码应用安全性测试相关内容。		
	系统交付	a）应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；	√	√
		b）应对负责运行维护的技术人员进行相应的技能培训；	√	√
		c）应提供建设过程文档和运行维护文档。	√	√
	等级	a）应定期进行	√	√

通用要求	安全控制点	测评指标	云平台责任	客户责任
	测评	等级测评，发现不符合相应等级保护标准要求的及时整改；		
		b）应在发生重大变更或级别发生变化时进行等级测评；	√	√
		c）应确保测评机构的选择符合国家有关规定。	√	如果使用了云平台提供的等保咨询服务，可以通过与云平台的咨询服务协议保障所选的测评机构的合规性；否则需用 单独满足
	服务供应商选择	a）应确保服务供应商的选择符合国家的有关规定；	√	√

通用要求	安全控制点	测评指标	云平台责任	客户责任
		b）应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务；	√	√
		c）应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。	√	√

4 腾讯等级保护 2.0 合规体系建设和腾讯云等级保护解决方案实践

4.1 集团等级保护合规体系建设概述

腾讯一直将把等级保护作为网络安全的基线认真对待。公司在等级保护合规体系建设工作上大概可以分为三个阶段：合规运营、体系完善和生态赋能。

合规运营（2015 年至今）是通过开展等级保护备案、测评等工作，保障公司的业务和系统持续满足《网络安全法》和相关法律法规、标准中等级保护的要求；体系完善（2016 年至今）是基于等级保护要求和攻防实际，在公司内部建立等级保护工作体系，不断加强和提升自身的安全体系建设；生态赋能（2017 年至今）是通过腾讯云把公司的等级保护安全经验和能力向生态和外界输出。

十几年前，公司就成立了集团层面的安全管理组织。聚焦于等级保护工作，从 2017 年起，公司制定了自上而下的等保工作体系，设立了“等级保护工作组”，由集团安全部门和各 BG 的相关团队一起组建，超过百人的规模，统筹推进对等级保护的法律、制度、标准跟踪，以及公司内的等级保护工作。

合规运营：从 2015 年起，公司逐步将全部核心业务纳入等级保护工作范围，并按要求备案、每年进行等级测评，保障公司业务基础安全合规，守护腾讯超过十亿用户的网络安全。体系完善：在公司等保制度方面，“等级保护工作组”在公司内发布了《腾讯集团网络安全等级保护工作实施指南》，用于指导和规范公司各团队开展等保工作。在公司内等保政策、标准宣贯和意识培训方面，“等级保护工作组”组织了多场次的等级保护专题课程和培训（每年更新，介绍最新的等保要求和工作进展），并邀请外部专家为各相关业务团队和

安全团队答疑解惑。在标准和试点应用方面，公司是多个等保 2.0 系列标准的参研单位，并积极参与了相关试点应用和专项工作；如 2016 年参与了等保 2.0 云扩展标准的测评应用；在落地实施方面，“等级保护工作组”本着基于等级保护并高于等级保护的目标，将等级保护相关法律、标准，与 ISO 27001、个人信息保护、数据安全等国内外安全要求融合打通，联合 BG 侧的安全团队，在公司内推进了多项安全专项工作，不断提升和完善等级保护安全管理和体系能力。生态赋能介绍见后续章节。

4.2 腾讯云基于等级保护的云安全合规体系建设

随着云计算技术和安全技术的不断演变，以及行业监管要求的日趋复杂，安全合规性已然成为云服务提供商面临的一大挑战。腾讯云致力于建立高效的安全内控体系，基于国内等级保护要求，并紧随不同行业、领域、国家的合规要求，从制度流程及控制活动等方面完善自身的合规基础。

腾讯云服务范围遍布全球,为保障云服务的安全性,需要满足国内外不同的合规要求,并识别各种安全威胁。腾讯云主动、积极的对国内外合规要求进行响应，并主动对各种安全威胁进行识别，确保腾讯云安全合规。

为了应对外部合规要求与威胁，腾讯云识别并采用了先进的国际和行业安全标准。整合国际和行业安全标准的要求，结合腾讯云业务实际情况，建立起一套融合的云安全合规体系，并建立了体系持续改进的机制，同时，将腾讯云安全合规体系落实到腾讯云产品的规划、开发设计、运维保障及服务支撑等整个产品生命周期的安全管控中。腾讯云安全合规体系以云安全管理章程与云安全管理手册为指引，从基础建设安全管理、互通性及可移植性、虚拟化平台管

理、身份认证管理等方面制定相应的合规标准，并细化到安全、发现与弹性三大方面的具体安全合规控制要求，通过内控监视与测量程序进行纵向管理，确保整个腾讯云安全内控体系的有效与高速运行。

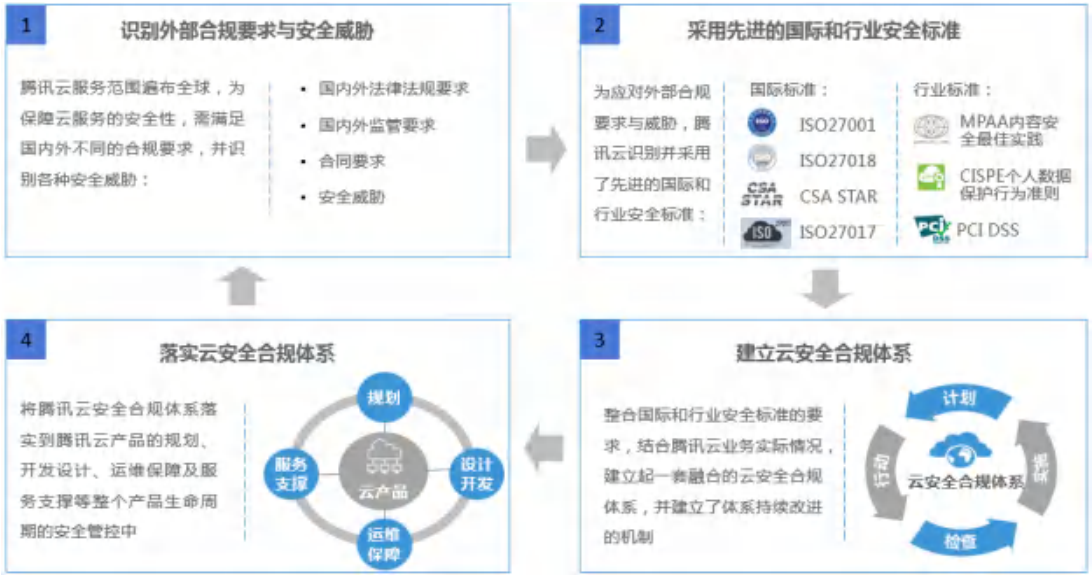


图 4.2.1 腾讯云等保 2.0 云安全合规体系

4.3 腾讯云等级保护 2.0 解决方案实践

落实网络安全等级保护制度是网络的所有者、管理者和网络服务提供者的责任与义务。通常情况，无论是在建或已运行的系统，完成一次等级保护测评的全流程需要 2-3 个月时间，有的需要半年甚至超过 1 年的也不在少数。以北京为例，等级保护备案阶段：申请与受理 4 个工作日、审查与决定 8 个工作日、制证与发证 10 个工作日。等级保护测评与整改阶段更是需要花费大量时间，一般需要 1-2 个月。

腾讯安全产业安全运营部安全专家咨询中心将腾讯公司自有重要信息系统的等级保护的经验和腾讯安全产品与解决方案结合，形成了一套可覆盖等级

保护建设与测评全生命周期的标准化服务产品，并通过对外输出等级保护最佳实践经验来赋能企事业单位等级保护建设。

如需获取腾讯安全专家咨询中心提供的等级保护咨询服务，可访问腾讯云官网安全专家服务页面。

4.3.1 等级保护测评全流程工作分解

腾讯安全专家从众多项目中总结了快速完成等级保护测评全流程的五大关键要素，即优选测评机构、系统合理定级、准备工作充分、及时跟进流程、关键路径并进。如下图所示：

图 4.3.1 等级保护测评工作流程

优选测评机构：

选择测评机构时应尽量选取企业所在地的测评机构，综合考虑其公司资质与技术能力，如测评公司具有的资质、各等级测评师人员数量、在市场中的口碑、被测评企业所属行业的测评案例等。同时明确提出本次测评的工期要求与项目预算，并采取邀请招标或公开招标的方式选择最优的测评机构。

系统合理定级：

系统定级是等级保护测评的第一步，无论是在建系统或已建系统，合理定级是关键，应参照“定级过低不允许、定级过高不可取”的原则来定级。如同为等级保护第三级可细分为 S1A3、S2A3、S3A1、S3A2、S3A3 几种类型，与之相对应的等级保护测评控制项就相差不少，将直接影响系统设计、建设、运维的方方面面。

定级完成后需由安全专家与业务专家共同对定级报告中涉及的系统业务描述、业务网络拓扑、业务受影响的风险分析进行专家评审并形成书面专家评审意见。最后定级报告与专家评审意见需上传到公安网警的等级保护备案系统中。

准备工作充分：

“磨刀不误砍柴功”，做好大量的准备工作是快速完成等保测评的先决条件。从业务系统的全生命周期角度来看，需要具备项目立项、需求说明、实施方案、验收标准、人员组织、管理制度等过程环节资料。

特别是网络安全方面，需要有网络安全的设计方案、建设实施方案、安全策略及安全检测规范、安全运营管理制度及安全建设运营过程文档（如漏洞扫描报告、渗透测试报告、代码审计报告、应急预案与演练记录、人员培训记录等）。

针对规模大或重要性要求高的业务系统其建设设计方案、安全保障方案需要聘请外部专家进行专家评审并形成书面专家评审意见。

及时跟进流程：

以广东为例，企业在公共信息网络安全综合管理系统填报前应授权一位负

责人，并由其跟进后续备案资料收集与文档扫描、系统填写与资料上传，同时关注审核反馈信息及时提交补充资料和修订资料。及时关注审核结果、获取备案证明及线下提交测评报告。

此过程中，遇到问题应及时反馈给上级领导，并协调资源推进等级保护备案流程。

关键路径并进：

加快项目进度一般可采取加班与并行赶工的方式，但前提是需要一名优秀的项目经理来分解项目实施步骤，识别并规划关键实施路径，把控管理项目实施过程风险。等级保护测评过程主要可并行的环节有商务洽谈与技术实施、系统建设与安全检测、系统测评与整改复测。

4.3.2 全生命周期等级保护建设方法论

等级保护测评是等级保护建设的重要环节，但等级保护不只是等级保护测评，它是一项长期的系统工程，等级保护建设应伴随着业务信息系统全生命周期来为业务保障护航。

腾讯总结了自身等级保护建设的经验与教训形成了如下表所示包含 7 个步实施步骤的建设方法论，并通过腾讯安全专家服务对外输出。

步骤	实施方法	腾讯安全专家服务
明确驱动因素	了解有哪些驱动因素(外因、内因)	安全咨询
定义问题	通过调研、咨询明确到了什么程度	安全咨询、安全培训
定义路线	通过调研、咨询明确要达到什么目标	安全咨询、安全培训

计划方案	参照行业最佳实践，确定要完成什么行动	安全咨询（最佳实践方案）
执行计划	通过咨询服务或采购专业的产品与服务形成解决方案与实施计划	安全集成、专项安全服务
实现效益	通过项目实施展现是否实现计划	安全集成
审查有效性	通过内、外方检查，保持有效性并推进	风险评估、安全审计

如上表所示，腾讯安全专家服务将助力您的网络安全建设工作，与广大网络运营者一起，结合自身实际来找差距、定目标、做规划、画路径、拟项目、抓落实。

创泽智能机器人集团主要产品

智能服务机器人

智能陪护机器人

安防巡检机器人

消毒机器人

智能党建机器人

智能教育机器人

智能导诊机器人

银行智能机器人

室外智能消毒机器人

多功能消毒机器人

全自动智能消毒杀菌机器人

智能医用消毒机器人

了解更多登录官网

www.chuangze.cn

扫码关注
“腾讯安全”

扫码关注
“信息产业信息安全测评中心”

扫码关注
“深圳网安检测”

扫码关注
“鹅门标局”