ZTE中兴

中兴通讯
网络安全白皮书

为客户提供安全可信的产品和服务

安 全 融 入 血 脉　透 明 增 进 信 任

中兴通讯首席安全官 **钟 宏**

2021 年 10 月

作者

本白皮书由中兴通讯各领域专家共同完成。在此，感谢对本文做出重要贡献的人：

Antonio Relvas 、曹鲲鹏、Chris Mulley、戴　恒、高瑞鑫、郝文瑞、何　英、华国红、蒋国兵、蒋　璐、李　星、李依依、刘　晖、刘日昇、马致原、Marco Costantini、平　立、宋伟强、汤可可、汪冬敏、王华刚、王玉忠、韦银星、徐国荣、杨桂荣、杨铁建、殷玲玲、俞　婷、张金鑫、张　俊、张　莉、赵　波、郑　均、朱林林。

同时，对出版本白皮书的每位贡献者，感谢你们支持！

中兴通讯首席安全官 钟宏

目录

序言

电信设备和系统作为关键基础设施，其安全性一直受到世界各国政府、运营商和用户的广泛重视。当前，5G 网络部署已经开始，凭借超高速率、超低时延和超大规模连接，5G 将重新定义从工厂车间到云端的关键基础设施运营。5G 网络引入的软件定义网络、网络功能虚拟化、网络切片、边缘计算、网络能力开放等关键技术，为智慧城市、远程手术、自动驾驶和大规模物联网连接铺平道路。然而，5G 网络的虚拟化和 IT 化增加了安全攻击面，从而引发更多的安全挑战和担忧。

根据世界经济论坛战略洞察[1]，连接设备数量的增长和敏感数据的增加需要全面的设备安全和网络安全保障措施。GSMA 2021 年发布的《移动通信安全全景》[2] 指出，5G 安全需要成为现在关注的重点，因为如果等到 5G 广泛部署后，建立安全性将变得更加困难。

为了应对这些挑战，5G 的安全性得到了前所未有的加强。从行业标准的制定和遵循，协同的漏洞响应和披露，到生产厂商的全面安全保障措施，整个行业及利益相关者都在共同努力提升网络安全。

作为全球综合通讯解决方案提供商，中兴通讯有义务、有责任最大程度地保障通信网络设备安全性，通过向客户提供安全可信的产品和服务，使全球用户享受安全可靠的网络连接，以及在此基础上的行业数字化变革。

中兴通讯在网络安全方面的原则和立场如下：

中兴通讯将安全作为产品研发和交付的最高优先级，中兴通讯根据公司发展战略规划，遵循适用的法律法规和国际国内标准，建立健全的网络安全治理架构，培养全员安全意识，确保全流程安全。

中兴通讯愿以开放、透明的方式与运营商、监管机构、合作伙伴和其他利益相关方进行沟通和合作，遵守相关法律法规、尊重客户和最终用户的合法权益，不断改善管理和技术实践，以安全可信的产品和服务回馈客户，与客户和利益相关方共同建立安全的网络环境，维护良好的网络空间安全秩序。

1. *世界经济论坛战略洞察 – 5G 安全和关键基础设施 https://intelligence.weforum.org/topics/a1G0X000006NvAbUAK/key-issues/a1G0X000006NvtqUAC*
2. *GSMA《移动通安全全景》https://www.gsma.com/security/wp-content/uploads/2021/03/id_security_landscape_02_21.pdf*

执行摘要

5G 时代已经开启，云计算、物联网、大数据、人工智能等技术得到越来越广泛的应用。在新技术应用带来新一轮产业变革的同时，网络安全形势越发严峻。一方面，全球性的网络安全威胁和网络犯罪十分猖獗，威瑞森《2021 数据泄露调查报告》[3] 深入挖掘了全球多个行业的网络安全状况，分析了 2020 年 29,207 起网络安全事件，其中 5,258 为数据泄露事件。截至 2021 年 10 月，公开批露的 CVE 漏洞达 161,750 件[4]，严重漏洞占 11.6%，高危漏洞占 20.8%。另一方面，根据 2021 年 ENISA《供应链攻击威胁态势报告》[5]，自 2020 年以来，针对供应链的攻击明显增加，这可能是由于组织的安全防护持续提升，攻击者将攻击目标转移到供应链。

中兴通讯既是网络运营商的供应商，同时也拥有广泛的供应链。在日益复杂的商业环境和全球疫情的大环境下，安全可信的弹性供应链至关重要。中兴通讯建立了健全的产品安全治理体系，重视培养全员安全意识，将安全策略和措施融入产品生命周期的每个阶段，持续强化整个供应链的安全保障，设计、开发并交付安全的产品。

本白皮书系统地介绍了中兴通讯如何通过采纳行业标准和最佳实践，实施自上而下、基于风险的网络安全治理，将其贯穿产品全生命周期：

在供应链环节，强调供应商、材料和生产制造安全可信、保证供应的持续性和弹性；

在研发环节，产品基于安全设计并通过流程规范化确保产品开发过程安全可控；

在工程服务环节，遵守规范化的操作，保障产品和服务安全交付。

在此白皮书中，中兴通讯强调了验证安全成熟度的重要性，并采纳行业技术标准、认证体系和评估框架，设立网络安全实验室，让客户、监管以及利益相关方能够便捷、有效地验证中兴通讯产品的安全性。

中兴通讯致力于向客户提供安全可信的产品和服务，保障通信网络设备安全，以实现在此基础上的数字化变革。网络空间安全需全行业以及利益相关者携手守护，让用户可以放心享受通信技术变革带来的数字化生活。

[3] 《2021 数据泄露调查报告》：https://www.verizon.com/business/resources/reports/dbir/
[4] CVE 漏洞数据：https://www.cvedetails.com/
[5] 《供应链攻击威胁态势报告》：https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

中兴通讯网络安全战略

通信网络是一个复杂庞大的系统，涉及大量软、硬件和系统数据。保证这些资产的机密性、完整性和可用性，是网络正常运行的基础。由于安全威胁多样又复杂，通信网络必须能够抵御安全攻击和干扰，具备可恢复性和弹性，这是设备供应商和运营商共同面临的挑战和责任。

中兴通讯以基于风险的方式建立了行之有效的安全治理体系，覆盖产品全生命周期。中兴通讯遵守法律法规，遵照行业标准，尊重客户需求，以“安全融入血脉，透明增进信任”为安全愿景，致力于向客户交付安全可信的产品和服务，不断追求无处不在的沟通与信任[6]。

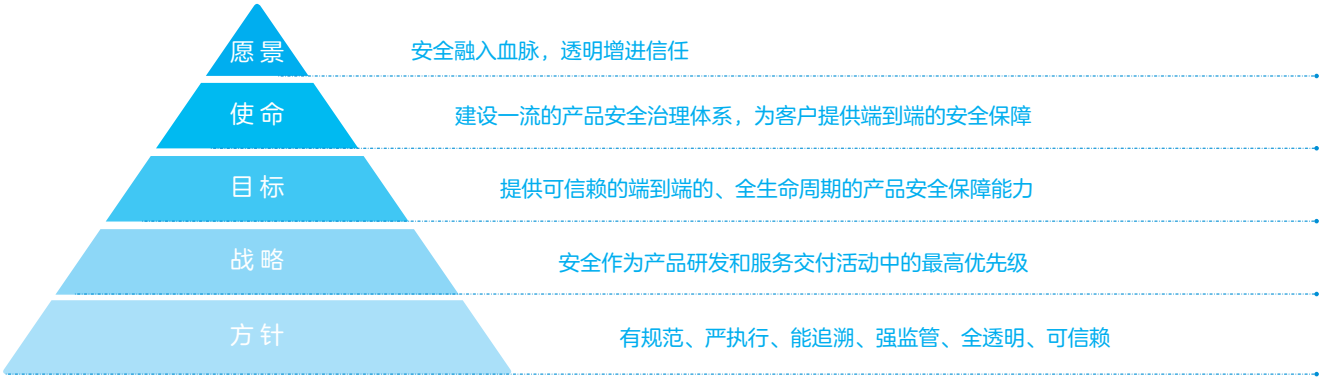


图 1 网络安全愿景和使命

[6] 中兴通讯愿景和使命：*https://www.zte.com.cn/china/about/corporate_information/vision*

基于风险的安全实践

基于三线模型的安全治理架构

企业和组织需要通过成熟的治理架构来进行高效的风险管理。国际内部审计师协会 (IIA) 发布的三线模型 [7] 帮助企业和组织确定最有助于实现目标的管理架构和流程，明确利益相关方的角色定位和职责，从而更有效地支持治理和管理风险。

中兴通讯采用基于三线模型的治理架构来推进产品安全治理工作，建立了独立于一线业务单位的安全组织，从机制上避免利益冲突，通过一线业务单位的自我检查、二线的独立安全测评、三线的独立安全审计，从多个角度和多个层次保障产品的安全性。

图 2 基于三线模型的安全治理架构

[7]《国际内部审计师协会三线模型》：https://www.iia.org.au/technical-resources/professionalGuidance/the-iia's-three-lines-model

董事会 / 审计委员会

董事会监督和指导产品安全委员会开展产品安全治理工作，内控审计定期向董事会 / 审计委员会汇报安全审计情况。

产品安全委员会

作为公司产品安全工作的决策机构，制定公司产品安全战略并保障资源，确定公司产品安全工作战略方向和目标，审议产品安全规划，决策产品安全相关重大议题。

一线

业务单位是产品安全治理的第一线。各业务单位通过产品安全的自我规划、自我执行、自我检测和自我改进，实现产品安全的自我控制。

在研发环节，将安全控制嵌入研发流程的各个阶段，项目技术评审及版本发布过程中评估安全风险并给予管控；将安全要求嵌入研发需求、设计、验证和发布流程，如设计安全 (SbD)、隐私保护设计 (PbD)；对产品进行渗透测试和定期实施安全回归测试；对产品所使用的包含开源的第三方组件安全漏洞持续跟踪分析并解决。

在供应链环节，将安全要求嵌入到验证供应商和新引入材料的过程中，通过供应商安全协议将产品安全要求传递给供应商，并定期对供应商进行审核；设立产品安全材料检测实验室对中高危材料进行抽检；在生产环境中建立专用网络用以隔离安全隐患。

在工程服务环节，通过持续对标 NIST CSF [8] 进行全业务流程的安全治理，以及组建跨领域的专业团队实现高效运作和交付安全。

二线

产品安全部是产品安全治理的第二线。作为公司产品安全委员会的常设机构，负责推动落实产品安全相关各项管理和技术实践，统筹产品安全策略规程建设，指导、检查、监督和评估一线的工作。二线为一线提供安全赋能和专业支持，协助一线管理风险，同时采用独立安全测评机制对一线安全实践进行评估和监督，从多个角度审核产品的安全性。独立安全测评包含过程评估和产品评估。前者用于评估一线安全治理执行过程的符合度和有效性；后者用于分析和评估产品和系统的安全性，包括漏洞扫描，安全编码审查，协议健壮性测试及渗透测试。独立安全测评中如发现违反产品安全红线 [9] 要求的情形，产品安全部可行使否决权，叫停业务活动，直到问题解决。同时，公司积极与第三方机构开展安全合作，对产品进行安全评估，如源代码审计、安全设计审查和渗透测试。

[8] *NIST Cybersecurity Framework: https://www.nist.gov/cyberframework*

[9] *中兴通讯产品安全红线规定中兴通讯业务过程、产品或服务的最基本安全要求，是各业务单位在开展工作过程中必须达到的标准。*

三线

内控审计是产品安全治理的第三线，对公司产品安全保障体系的健全性、合理性和有效性进行独立评价，向公司管理层以及客户等利益相关方保证产品安全策略、规范、流程得到有效执行，促使客户需求得到有效满足。内控审计负责独立审计一线和二线的工作，包括流程执行的符合性检查和产品安全检测，向董事会 / 审计委员会汇报客观独立的审计结果。内控审计可以和第三方外部审计共同对公司的产品安全执行情况进行审计。

内控审计以风险为导向，贯穿整个审计流程，中兴通讯持续不断审视公司产品安全体系的健全性和有效性，切实保障客户及利益相关方的安全需求得以满足。

产品安全规范体系

中兴通讯建立了产品安全策略、标准、流程和指导书，明确了产品安全治理的基本要求和执行规范。公司颁布了系列的安全管理规范和标准，各业务单位遵循产品安全要求一致地开展产品安全实践活动。在安全规范实际运行中，输出了相应的结果和记录，可作为证据提供给相关方进行审计。

公司的产品安全文件体系总体分为四层：

第一层：

产品安全要求总则，该标准是公司产品安全大纲，所有下层文件以此标准为基础。中兴通讯基于系统安全工程 [10] 的方法，参考法律法规、安全标准、安全最佳实践和客户要求，建立了覆盖系统全生命周期的产品安全策略，涉及到研发、供应链、工程服务、事件响应等全业务过程。公司产品安全策略作为安全治理的标尺和工具，用于内部流程规范的差距分析、评估产品安全落地的有效性。

第二层：

产品安全管理规范和流程，支撑安全策略运行的规章和流程，如研发安全规范、供应链安全管理规范、工程服务产品安全管理规范、独立安全测评管理流程、漏洞响应流程、安全事件响应流程。

第三层：

产品安全指导书，支撑规章和流程的文件，如安全设计指导书、安全编码规范、安全基线编写指导书、安全加固指导书。

第四层：

产品安全记录，执行过程和结果的记录，如源代码扫描报告、安全测评报告、漏洞分析记录、安全事件复盘报告。

[10] 系统安全工程：https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final

安全意识和安全能力提升

中兴通讯建立完善的产品安全内部宣贯体系。通过新员工意识培训、全员意识培训、应知应会考试不断提升产品安全意识。通过内部产品安全公众号持续向全员传递产品安全最新资讯、前沿技术和优秀实践；通过宣传海报、公共邮箱、易拉宝等形式向全员宣传产品安全教育内容；组织产品安全技术大会、安全开放日、安全 COP 等活动将产品安全意识教育渗透到员工的日常工作中。

中兴通讯重视安全人才队伍的专业化建设，提供了安全专职人才职业跑道和全面的培训与发展体系。公司现有五百余名产品安全专职员工，涵盖安全标准、安全规划、安全设计、安全编码、安全工具、渗透测试、安全运维。

建立“面向实战，上下贯通”的学习发展体系，安全专职人员实行岗位学分制管理，对员工从政策机制形成牵引，结合岗位安全能力要求，实现主动学习、在岗提升。

中兴通讯持续进行产品安全能力培训，课程设置上，全员课程、关键岗位课程、专题领域课程相搭配；选拔产品安全技术骨干和专家担任讲师；组织多种层面的专业技能培训，如岗位必备知识培训、岗位技能培训、产品安全专家认证、渗透测试大赛和安全编码比赛等，推动公司产品安全能力提升，形成公司产品安全文化。

中兴通讯鼓励员工通过外部培训和专业认证来提升产品安全专业能力，已有 170 余位员工持有安全专业认证，如 CISSP、CISA、CISM、CSSLP、CEH、OSCP 等，具备成熟的安全架构、安全设计、渗透测试、安全审计、安全管理等方面的安全能力。

安全保障贯穿产品生命周期

一个系统每个环节的安全都会影响到整体的安全，整体的安全强度由最薄弱的链条决定。中兴通讯的安全保障覆盖供应链、研发、工程服务、事件管理和各支撑职能领域，形成了贯穿产品生命周期的产品安全保障体系，并对标更新的行业标准和最佳实践不断改进。

安全可信的弹性供应链

供应链面临的风险与挑战

目前，许多国家和 ICT 行业已普遍认识到，相比传统行业，ICT 行业的供应链更加复杂，存在安全风险的概率更大。尤其在 5G 时代，网络的复杂化、模块化和软硬件分离的特征，使运营商客户可以多样化地选择供应商，而每个供应商的背后又是一整条供应链，其中任何一个环节出现问题，都有可能造成一系列后果。例如 FragAttacks 的 WiFi 系列漏洞就涉及多家第三方组件供应商，需要第三方组件供应商协同响应，一起进行漏洞修复。

为此，各国不断推出新的法律、法规，行业标准日益完善。例如，美国商务部 (DoC) 于 2019 年发布《确保信息和通信技术及服务供应链安全》[11]，提出了对 5G 产品和服务的新要求。行业规范 NESAS 2.0[12] 特别增加了对供应链第三方组件安全的要求，以减少设备供应商在供应链中采购和使用易受攻击、污染和不提供技术支持的第三方组件的可能性。这些新要求均对企业的供应链建设和管理带来新的挑战。

同时，客户要求越来越高，市场需求与供应大幅波动。2021 年以来，由于 COVID-19 疫情的持续影响，导致市场行情趋紧，芯片类材料供应风险凸显，材料供应周期拉长。

此外，各国监管和客户越来越将产品安全的关注范围从网络设备供应商延伸至其二级供应商、乃至三级供应商，同时，从只关注网络安全、数据安全、个人隐私保护，向关注供应安全与业务连续性方面扩展。这两个转变对供应链的安全和弹性提出了更高的要求，为供应链带来了新的挑战。

[11] 《确保信息和通信技术及服务供应链安全》：https://www.federalregister.gov/documents/2021/01/19/2021-01234/securing-the-information-and-communications-technology-and-services-supply-chain

[12] 网络设备安全保障方案：https://www.gsma.com/security/network-equipment-security-assurance-scheme/

供应链安全保障体系

对中兴通讯而言，构建安全可信的供应链，既是保障公司产品按时交付的内在需求，也是我们对客户的庄严承诺。中兴通讯先后通过了供应链安全管理体系 (ISO 28000)、信息安全管理体系 (ISO 27001)、业务连续性管理体系 (ISO 22301) 认证。2020 年，中兴通讯再次通过经认证的经营者 (AEO) 高级认证，在全球持续享有相关国家或地区快速通关的便利。

中兴通讯拥有完整的供应链业务流程框架，包括：计划、采购、制造、交付、逆向五大业务模块，聚焦客户的业务需求和安全需求，依据供应链运作参考模型 (SCOR) 将供应链范围扩大到从供应商的供应商到客户的客户。

根据安全治理重点，我们在下文将从材料安全、生产安全、交付安全三个方面介绍供应链的安全治理实践。

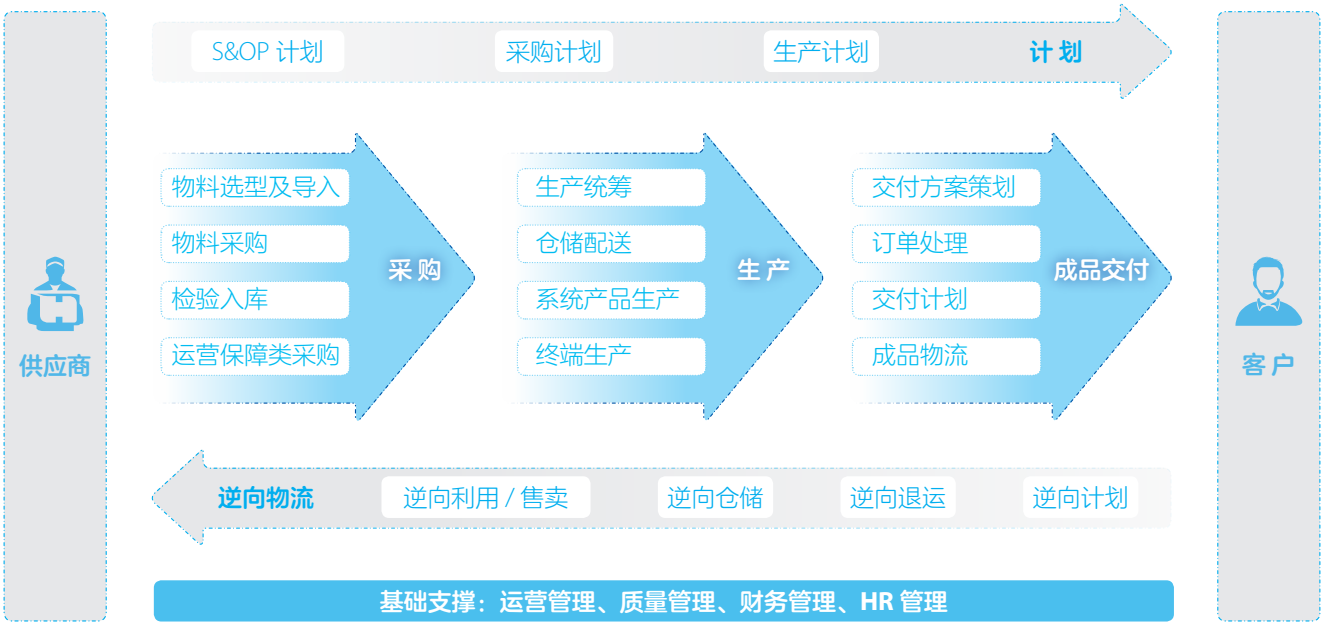


图 3 供应链业务流程框架

供应商管理和材料安全

合作伙伴是供应链的重要组成部分，分布于全球各地的数千家供应商与中兴通讯在整个产业链条上分工合作，为中兴通讯提供数万种原材料、半成品、成品或服务，是中兴通讯为客户提供产品和综合解决方案的重要组成部分。因此，中兴通讯把供应商安全管理和材料安全管理作为核心业务流程，保障材料和第三方组件的安全。

首先，选择安全可靠的供应商是保证供应链安全的第一步。中兴通讯一直非常重视供应商资源的开发与布局，建立了一整套从寻源，到资质认证，再到淘汰退出的供应商全生命周期管理机制，包括质量管理、信息安全管理、企业社会责任管理、绩效考核和问题追溯等诸多管理内容。一家潜在的供应商只有通过一系列审核，包括商务、技术、质量、财务、交付、安全、合规、企业社会责任等方面的综合评估后才能成为中兴通讯的合格供应商。

其次，在材料管理方面，中兴通讯实施品类管理，根据不同品类材料的特性，将材料的产品安全风险定义为高、中、低三个风险等级。针对高风险材料，在材料引入环节，要求提供新引入材料的产品安全检测报告。另外，中兴通讯建立了产品安全材料检测实验室，实施抽检，针对发现的安全问题实施闭环管理。对于中低风险等级的材料，通过签署供应商安全协议的形式，要求供应商进行自我管理和约束，由中兴通讯进行多种形式的安全审计。

中兴通讯要求供应商在提供产品或服务的过程中必须遵守当地的法律、法规要求，并遵守与中兴通讯签署的产品安全协议，及时发布漏洞预警和解决方案，确保将外部引入的产品安全风险降至最低。比如在安全测试或产品使用过程中若发现安全漏洞，供应商应当积极协同配合中兴通讯进行追踪和定位，并及时提供补丁，或者采取升级、替换、召回等解决方案。

中兴通讯通过每年一度的全球合作伙伴大会，把产品安全的要求传递给供应商，同时每年举行供应商集训营，把产品安全、信息安全、企业社会责任等方面的要求传递给供应商。

生产安全

参照公司对生产制造过程的安全管控要求，中兴通讯供应链制定了《制造安全管理规范》，把生产制造区域分为三类不同等级的安全管控区，管控生产制造过程中的安全风险，防止软件、硬件被篡改，包括未经授权的硬件替换、软件植入或篡改、病毒感染等。针对三类不同等级的安全管控区，采取不同的安全管控措施，其中产品安全一级、二级管控区是安全风险严管区域。在该区域，均设置安全管理员负责实施区域内的安全管控措施和日常安全监管。

为了防止病毒入侵或软件篡改，中兴通讯建设了专门的生产专用网络，与办公网络和公用网络隔离，保障生产环境的安全。同样，为了防止制造过程中对产品中软件的篡改，只有授权的工程师才能使用产品数据管理系统归档和发布软件。

成品交付安全

中兴通讯通过仓储管理系统实现在库货物全程跟踪，及时升级物流仓储 IT 系统、监控设备和安保设施，以避免仓储和货运过程中的成品或核心部件遭受损坏、替换、恶意代码植入的风险。通过货运中台系统实时监控货运轨迹，监控货运在途情况，并设有干系人预警功能。

打造弹性的供应链

面对越来越高的客户要求，以及大幅波动的市场供求带来的产品交付风险与挑战，中兴通讯供应链聚焦三大核心业务场景：材料供应、生产制造、物流货运，参照业务连续性管理体系 (ISO 22301) 的要求，采取以下措施保障供应链业务的持续稳定运行。

采购方面

中兴通讯拥有一张遍布全球的供应链网络，包括北美、欧洲的供应商，能够持续保持充足的供应。同时，我们通过深入洞察行业动态和对市场进行前瞻性供需分析，主动感知客户需求，在交付过程中依据供需关系的变化适时调整采购策略， 保证安全库存、供应资源、市场调货等，保持供应链的弹性。中兴通讯开发的可视化风险地图工具在突发事件发生时，能迅速确认波及的供应商、材料代码、产品及影响程度，第一时间完成全面风险评估。例如，2018 年 9 月日本北海道发生了 6.7 级地震，通过供应风险地图，我们在 2 小时内快速识别了受影响的 32 家供应商，65 个物料代码，及时启动了应对措施，避免了更大损失。

制造方面

中兴通讯在中国大陆布局有深圳、河源、长沙、南京、西安五大生产基地，各基地之间的生产资源可以共享，且具备产能相互备份的功能，通过灵活的产能策略，柔性保障生产的连续性和产能需求。

中兴通讯建立了产能风险扫描机制，提前规划中长期产能，满足常规需求；通过临时措施可在两周内扩充到标准产能的 120%，以满足短期需求；对于单板、家端、电源、终端等产品，始终储备有 20% 的外包产能，以保障客户交付需求。

物流货运方面

中兴通讯通过多元物流网络，保障货运安全。一方面加强与船司、航司等资源型供应商的直接合作，保证了货运资源稳定获取；另一方面，主动策划货运线路备份，包括铁运、海运、空运多种运输方案互为备份、多个启运地备份，以及同一运输方式多条线路备份等。例如，2021 年 3 月 21 号，长荣天赐号搁浅导致苏伊士运河堵塞，公司及时启用备份方案，协调中欧班列满足紧急发货需求。

产品开发过程安全可控

中兴通讯将安全作为研发的最高优先级。“安全性”必须作为产品的一项基本属性融入到产品开发全生命周期过程中，确保实现产品的设计安全和默认安全。

为满足不同客户和市场竞争条件的要求，我们持续识别网络安全威胁并与业界最佳实践保持同步，如软件安全构建成熟度模型 (BSIMM)、网络设备安全保障计划 (NESAS)、能力成熟度模型集成 (CMMI)，制定中兴通讯研发安全成熟度模型，进行组织和项目的评估，发现差距，不断改进。2020 年，中兴通讯 5G 产品的全生命周期流程经过第三方公司的 BSIMM 模型评估，安全成熟度居于业界第一梯队，并成功通过 NESAS 过程评估和 SCAS 产品测试。

流程和组织

安全嵌入的研发流程对交付高质量安全的产品至关重要。早在 2001 年，微软提出安全开发生命周期 (SDL)，该流程减少了软件中至少 50% 的漏洞[13]，大大提高了产品的安全性和开发效率，成为全世界众多公司软件开发流程的蓝本，并加以定制和发展。参考 SDL 的高效产品开发流程 (HPPD) 是中兴通讯研发领域共同遵循的流程，经过多年的发展，其成功借鉴了业界最佳实践，并在各个阶段融入安全管控措施。在该流程基础上，中兴通讯持续提升关键安全技术和研发安全成熟度，提高安全治理核心人员的专业能力。

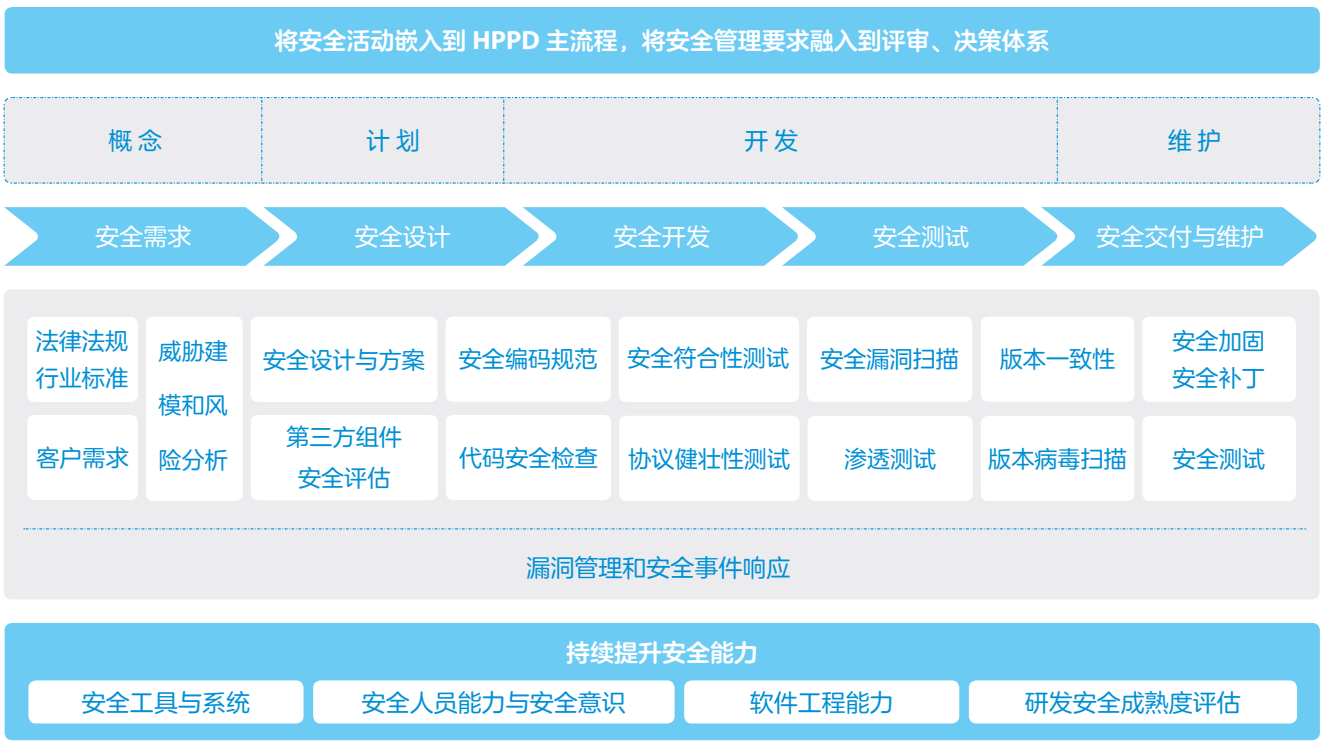


图 4 融入安全活动的 HPPD 流程持续优化演进

[13] *The Security Development Lifecycle by Michael Howard and Steve Lipner*

需求和设计

安全需求来自不同国家监管、客户、以及技术演进，中兴通讯将中长期安全需求纳入产品路标规划，短期安全需求纳入产品版本规划。

我们通过威胁建模来分析安全需求。威胁建模是安全设计中的一项核心步骤，是一种分析和解决问题的结构化方法，用来识别和量化威胁，并确定应对措施的优先级以降低风险。其目的是在产品开发过程的早期阶段识别风险并进行控制。我们参考业界最佳实践，如 ITU-T X.805，微软 STRIDE/DREAD，新思 ARA 等模型，建立了一套适合通讯产品的系统威胁建模方法，以发现威胁，识别风险，输出针对威胁的应对措施。

公司发布产品安全设计技术标准和技术栈目录，引入威胁建模工具，建立安全设计知识库，指导产品完成安全需求分析以及安全架构和特性安全设计。

对社会各届关注的隐私保护和数据合规问题，中兴通讯遵循隐私保护设计理念，将治理动作前移，在需求阶段即纳入数据保护的需求，尽早发现数据保护合规风险，有效降低风险防控成本。

开发和测试

在开发测试阶段，我们采用的安全编码标准参考自业界通用指南，如计算机安全应急响应小组 (CERT) 系列安全编码规范、开放式 Web 应用程序安全项目 (OWASP) 开发指南、通用缺陷列表 (CWE)、安全技术实施指南 (STIG)。我们持续优化中兴通讯安全编码规范，研究并替换不安全函数。我们编写的代码需通过静态检查和自动化扫描，衡量代码的质量、可靠性、安全性、可维护性。工具扫描出的缺陷采取看板化管理，监控缺陷闭环，通过控制门确保达成安全缺陷控制目标。

在开发测试阶段，我们依据安全测试规程和测试方案，对产品进行代码扫描、漏洞扫描、协议健壮性测试、渗透测试、病毒扫描等安全类测试，充分验证包含个人数据保护等安全需求的实现并修复缺陷。

发布和维护

中兴通讯制定了一套严格的发布流程，要求产品必须经过安全测试和工具扫描，通过产品安全风险评估，确保遵从中兴通讯产品安全红线，且产品必须配备安全加固手册和工具方可发布。

研发团队对现网已部署和使用中的产品制定持续的回归测试策略并执行测试，以判断新增漏洞是否影响现有版本，并且及时更新安全补丁或部署安全加固方案，确保现网产品安全风险得以消除或控制。

第三方组件安全

中兴通讯对产品使用的包含开源的第三方组件实施，包括从引入到退出的全生命周期管理，并且嵌入了 HPPD 流程，由 DevOps 工具链支撑。

在第三方组件引入阶段，充分分析和验证其功能和性能，确保达成出口管制、数据保护、开源许可等合规要求，以及公司的产品安全红线要求。同时考虑第三方组件的可替代性及供应商承诺的产品生命周期，保证其与我们产品生命周期匹配，达成对客户的服务承诺。只有通过安全合规评估并确保经过认证的可靠来源的第三方组件才能进入公司的组件管理系统，开发人员通过审批之后才能获得这些软件的访问权限，选取第三方组件以供所需产品使用。

产品所选用的第三方组件须通过安全测试，达成安全标准后才能随产品进行发布。在我们的产品生命周期内，一旦发现安全漏洞，不论发现人是客户、供应商、第三方还是我们自己，我们均会对该安全漏洞进行评估，提供解决方案或者规避措施，以及时消除风险。

在产品生命周期内，当第三方软件因为功能、性能或安全性进行版本更新、引入补丁程序，或当第三方软件生命周期终止时，我们通过组件管理系统对第三方软件进行更新或宣布停用，以确保产品所使用的第三方软件是最新的。

第三方软件的安全风险评估贯穿从组件选型、引入、测试、交付到维护的全过程，并纳入 HPPD 流程的节点管控，确保及时发现安全风险，快速评估并提供恰当的安全解决方案或规避措施。

同时，我们将第三方软件作为产品配置项纳入配置管理流程，以确保其使用可追溯。特别是当发现安全漏洞时，我们可以追踪其应用范围，彻底解决所有与第三方软件使用相关的问题。

作为开源社区的积极贡献者，中兴通讯持续跟踪社区发布的漏洞，在使用漏洞修复方案的同时贡献安全漏洞修复方案。

安全开发保障

产品持续安全的交付由稳固的配置管理系统、与开发流程相融合的DevOps工具链以及研发内部信息安全管控策略来保障。

中兴通讯的配置管理系统保证了从客户的原始需求可沿着流程的各个阶段进行追溯。从客户的原始需求正向追溯到最终产品，从最终产品逆向追溯到原始需求——覆盖包括设计、开发、测试、交付等所有流程，以及所有接触过该软件的人、工具、组件、研发和生产环境等关键要素。

中兴通讯将安全工具融合到整个 DevOps 工具链中，通过持续规划，协作开发，持续测试，发布与部署四大环节迭代串联，在代码扫描、漏洞扫描、渗透测试等安全类测试以及版本保护等关键安全活动中，确保安全工具的高效使用，形成运维监控闭环。

中兴通讯对产品的过程交付物，如代码、技术文档，进行了信息安全风险识别并实施控制举措。代码在研发云内实现编译、单元测试 / 功能测试、评审，形成交付版本。代码和文档在研发云上的流转和出云有严格的控制策略，产品在开发过程中安全受控。

交付安全的网络与服务

随着中兴通讯产品交付给客户，业务场景产生变化，新的安全风险也随之而来，需要采取适当的保护措施保证交付过程中产品和数据的完整性、机密性和可用性，实现端到端的安全。

中兴通讯交付领域在全球建立了基于风险的交付安全治理体系，全面涵盖授权管理、安全部署、远程接入管理、网络数据保护、资产安全管理、事件响应、合作伙伴管理等模块，产品安全要求已全面融入开通、验收、移交和运维阶段，确保交付行为安全可靠、网络设备安全运行，客户网络和数据得到有效的保护。此外，中兴通讯定期进行模拟演练和抽查，确保人员安全意识和规范动作到位。

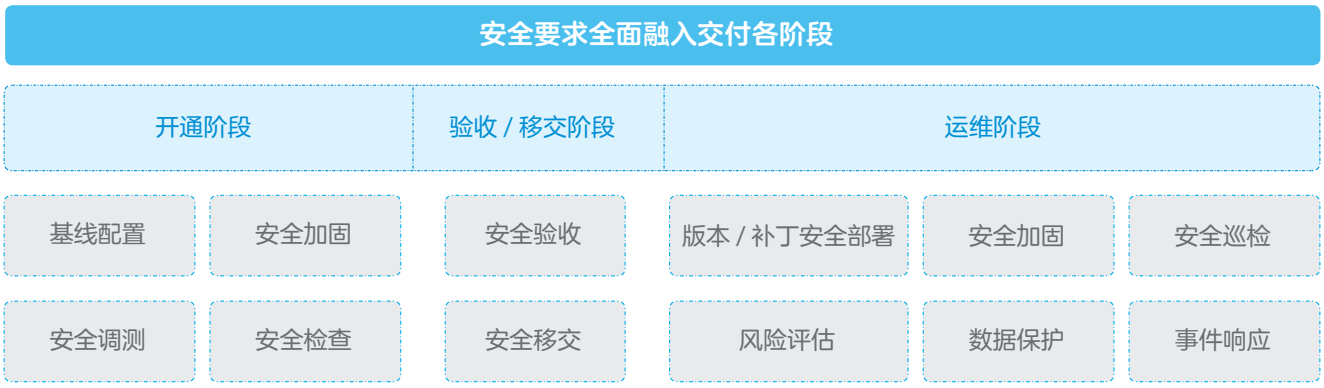


图 5 端到端的交付安全保障

授权管理

在对客户的网络和数据进行操作前，如软件升级、安全加固、网络巡检，中兴通讯事先获取客户授权，并在约定的范围和时间段完成操作，操作过程记录在案，实施操作的人员可通过日志进行追溯。

安全部署

为确保软件端到端的安全部署，中兴通讯实施严格的流程和管理制度，仅授权人员才能从支撑网站下载所需版本或补丁，下载均有记录，且所有下载的软件会在升级前进行完整性检查和病毒检查。软件部署所需的工具和软件均从指定官方渠道获取，确保安全可信和知识产权合规。

远程接入管理

为确保高效安全的远程技术支持，中兴通讯在遵循所在地法律法规和客户授权的前提下，允许产品专家通过部署的全球一张网系统 (Advanced Operations Suite, AOS)[14]、安全隔离区远程访问客户网络，进行问题排查或业务支持等。对客户网络的所有远程操作均可事后审计，确保符合客户预期的授权。

网络数据保护

为保护网络数据的安全，中兴通讯要求接入客户网络的个人移动设备做好基本的安全防护，如安装系统重要补丁和防病毒软件，仅安装授权的、与业务目的有关以及无信息安全风险的软件等。个人移动设备如需临时存储网络数据，需在客户同意后按照数据的敏感性进行相应的脱敏、加密等保护，并在遵循所在地法律法规的前提下，按照“最小范围”和“知所必需”原则进行传播。

资产安全管理

为确保客户网络设备的防护能力不会随着内外部威胁的变化而降低，中兴通讯基于合同要求定期对网络设备进行安全检查、加固和风险评估，践行对客户资产应尽的风险关注和处置义务。

事件响应

当客户网络出现安全问题时，现场工程师会立即上报至中兴通讯全球客户支持中心 (GCSC) 系统，并置上“产品安全”标签。安全问题会汇聚到产品安全事件响应团队 (PSIRT)，并根据其严重等级分发到对应的产品支持团队，确保在客户服务水平协议 (SLA) 约定的时间内得到有效解决。此外，中兴通讯定期进行重大灾害、网络攻击等突发事件的应急演练，持续提升事件响应和处置的能力。

[14] *全球一张网系统 (AOS)：AOS 是公司员工进行远程支持工作的主要门户。*

合作伙伴管理

合作伙伴是交付领域的重要力量，中兴通讯在与他们的合作中扩大了安全保护的边界，可能引入新的安全风险，应有完善的机制对合作伙伴进行安全管理，确保安全可信。中兴通讯建立了整套认证管理体系，通过认证评估、资质管理、安全管理、绩效管理和信用管理，实现对合作伙伴的进入、合作、退出全生命周期的管理机制，并基于供应商关系管理系统、财务系统和工程项目管理对合作伙伴进行端到端可视化管理。

中兴通讯制定并实施了合作伙伴认证与采购的安全基线，明确了新引入的合作伙伴必须满足的产品和服务的安全标准。潜在的合作伙伴只有通过包含产品安全及其它要素的评估后，才能正式服务于中兴通讯及其客户。所有通过认证的合作伙伴均需签署包含产品安全要求以及违约责任的《产品安全承诺书》。

中兴通讯定期对合作伙伴的服务绩效和安全情况进行综合风险评估，并根据评估结果进行分级管理和确定未来的合作机会与频率。

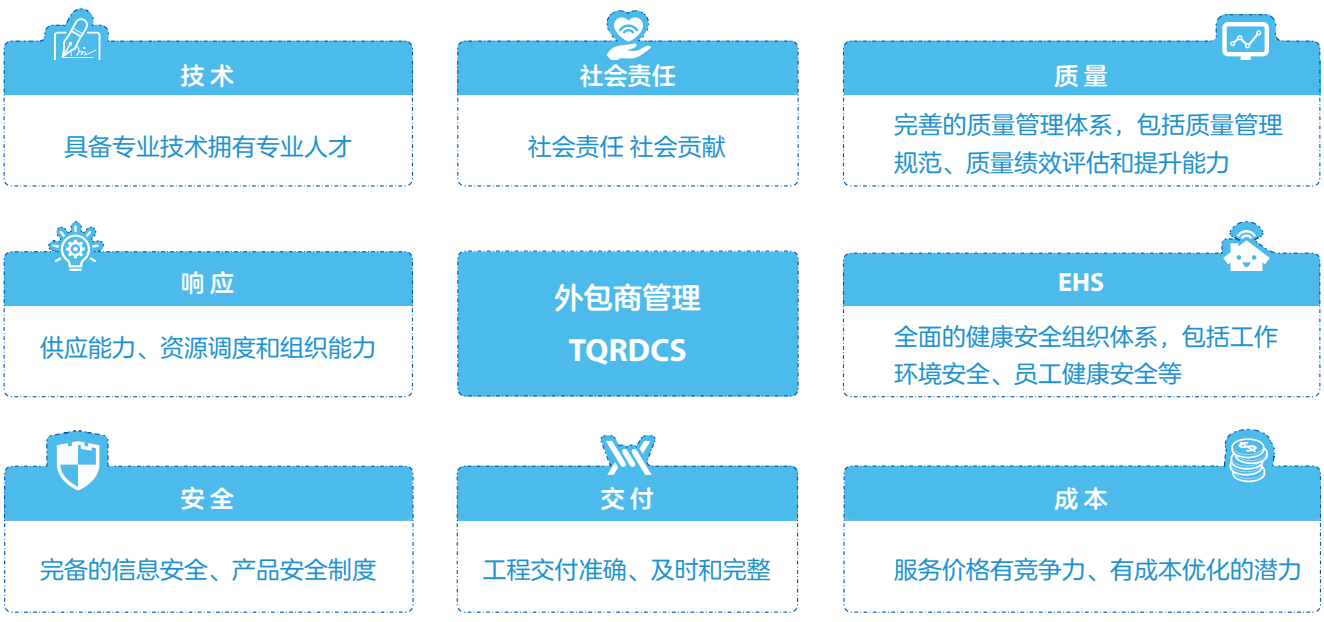


图 6 中兴通讯交付领域合作伙伴管理体系

安全事件管理

由于威胁和脆弱性会发生改变，这导致网络的安全风险不能完全消除。当安全风险转变为安全事件时，需要及时缓解，以减轻安全事件带来的不利影响。同时，消减漏洞能在很大程度上避免安全事件的发生，因此，任何已识别的产品漏洞信息应及时披露给客户，并提供漏洞处理方案。

此外，安全事件响应和漏洞处理机制有赖于利益相关方协同、高效地分享信息并及时响应，以有效缓解安全风险。

安全事件响应机制

中兴通讯事件响应机制穿透了供应链、研发和工程服务领域，由专职团队 PSIRT 负责接收、处理和披露与中兴通讯产品和解决方案相关的安全漏洞。PSIRT 协同客户和利益相关方有效合作，快速给出解决方案。对于安全事件和数据泄露建立分级响应机制，确保统一协作并快速修复，迅速恢复业务。

安全事件处理采取预防、检测、纠正和恢复、事后反馈的闭环处理机制，一旦发生安全事件，PSIRT 迅速对事件进行分析，采取必要措施控制事态发展，直到业务彻底恢复。事件得到有效控制后进行复盘改进，防止类似事件再次发生。

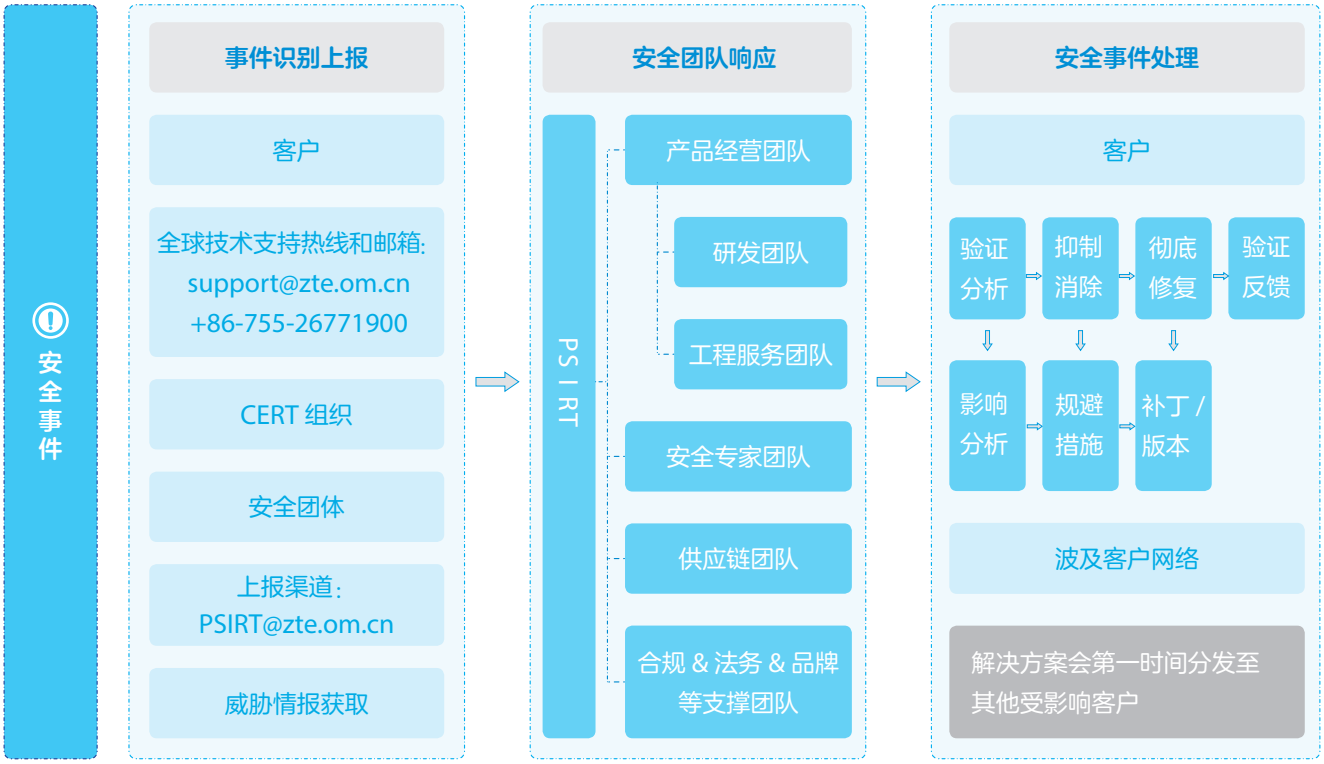


图 7 安全事件响应机制

安全漏洞处理机制

中兴通讯重视与安全组织协作，对内外部发现的漏洞，秉承公开透明的原则，结合客户及相关方的意见和要求进行负责任的披露，并提供规避措施以及解决方案。在客户实施解决方案之后，对方案的有效性进行监控，并根据反馈情况进行方案迭代，实现漏洞闭环管理。

中兴通讯是事件响应和安全团队论坛 (FIRST) 成员和 CVE 编号颁发机构 (CNA)，并参与 GSMA 协调漏洞披露 (CVD) 项目。2020 年，公司发布了新的安全漏洞奖励计划，覆盖 5G 融合核心网、5G 基站、固网、多媒体、云视频、云计算、分布式数据库及终端产品和 Web 应用系统等多个产品类别，并与知名第三方漏洞赏金平台合作，鼓励全球安全从业人员和机构反馈中兴通讯产品和服务中存在的安全漏洞。

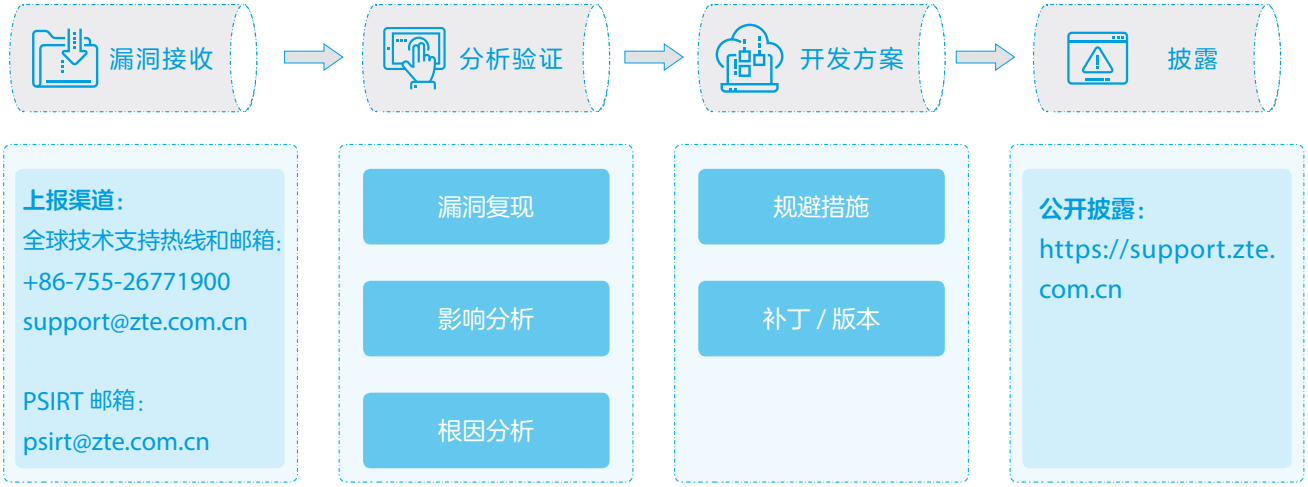


图 8 产品安全漏洞处理流程

信息安全

信息安全是保护公司资产的安全，为公司产品研发和生产运营等业务提供安全的环境。通过建立信息安全管理体系，从组织、人员、流程、技术等维度确定控制措施，保证资产的机密性、完整性和可用性，提升公司信息安全水平，为公司业务发展保驾护航。

中兴通讯建立了信息安全管理体系 (ISMS)，定义信息安全总则、安全策略、信息分级、风险评估和安全审计等管理流程，制定了信息安全红线，通过信息安全组织执行监管、调查和处理公司信息安全的违规、侵犯公司商业秘密的行为。每年对所有员工进行安全培训和考试，提高全员的安全意识，把安全、防范信息泄漏当成工作中最重要的一个环节。建立了安全举报的多种途径，在遇到风险、漏洞和信息安全异常情况时，通过邮件、电话、公司官网等举报途径，及时对信息安全异常情况进行处理，补漏，补缺安全规则。

中兴通讯通过信息定密、人员安全、物理安全和 IT 安全等一系列的安全措施，确保公司信息资产的安全，保证信息资产的保密性、完整性和可用性，提升公司信息安全水平，保障公司核心竞争力。

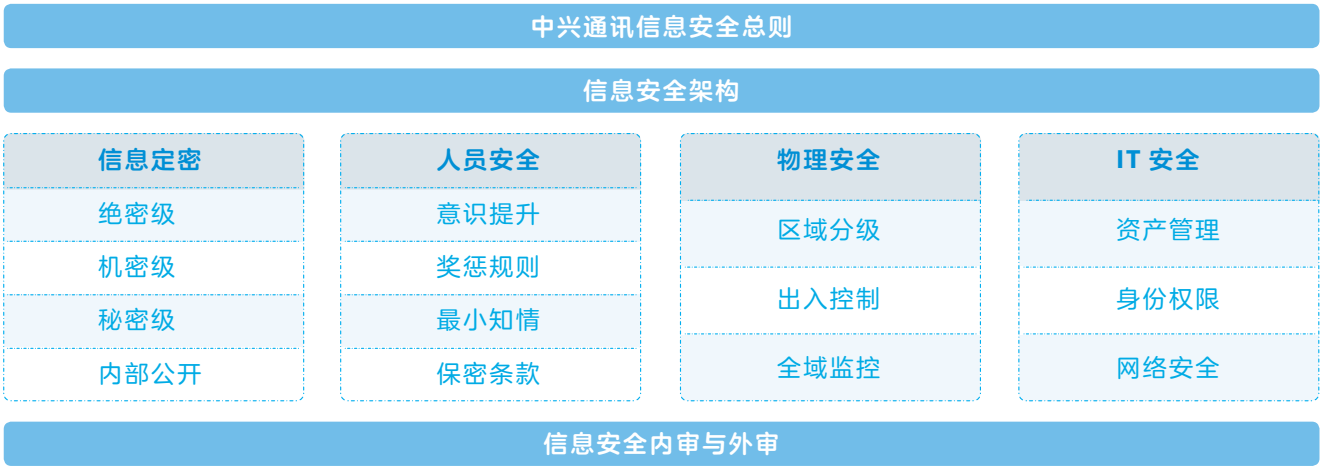


图 9 信息安全总体框架

隐私安全

大数据、人工智能、云计算、物联网和 5G 等信息通讯技术的不断发展与应用，推动社会快速进入万物互联的数字时代。数据的大规模利用带来了便利与效率，也带来了潜在的数据合规和隐私保护（以下简称“隐私保护”）隐患，可能影响到个人权益、组织商业利益、公共安全甚至国家安全。为此，全球主要国家和地区陆续出台隐私保护相关的法律法规，如欧盟《通用数据保护条例》(GDPR)，美国《加州消费者隐私法案》(CCPA)、中国《网络安全法》、《数据安全法》、《个人信息保护法》等。

中兴通讯高度重视隐私保护，将其作为公司合规战略的主要基础领域之一。中兴通讯认为，隐私保护不仅仅是应严格遵守的法律要求，也是建设行业互信，践行道德价值观的重要基石。

隐私保护体系建设

中兴通讯致力于建立适用、有效、领先的隐私保护体系，以风险为导向，从组织、人员、制度、技术等维度开展全面的体系建设。

中兴通讯建立了包括合规稽查团队、数据保护合规团队和业务单位的隐私保护管控机制进行风险防控。

中兴通讯开展了形式多样的隐私保护能力提升工作，积极传递价值导向，有效增强全体员工的隐私保护意识和能力，营造良好的隐私保护文化氛围。

中兴通讯聚焦全球主要法域的法律法规和监管要求，综合考虑其他典型国家区域的要求，结合业务分布情况进行组织环境分析，确定了公司统一的隐私保护策略和管理制度，最大限度地保证隐私保护管控要求“一次导入，全球适用”。除此之外，中兴通讯还按业务领域特点建立了针对性的业务流程和合规指引，为在业务中有效执行管控要求提供更好的支持。

为配合管理要求的有效执行，中兴通讯也积极开展隐私保护技术方面的探索。通过引入行业最佳实践，以及自研开发管理工具，持续提高整体隐私保护水平。目前，中兴通讯已获得数十项隐私保护专利。在新兴的隐私保护计算技术领域，中兴通讯也积极进行技术创新布局。

重点场景隐私保护管控

中兴通讯针对各类高风险场景构建了完善的管控机制，守护用户、客户及员工数据和隐私安全。

中兴通讯建立了数据泄露响应机制， 通过“个人数据泄露响应系统”进行管控，对应急响应过程进行跟踪和记录。

数据主体权利响应机制以中兴通讯数据保护公邮和数据主体权利响应系统为入口，便于数据主体快捷地提交权利诉求，同时确保行权过程中的个人数据安全，进而提升社会信任度。

数据跨境转移管控机制坚持授权同意和最小必要原则，根据具体场景，事前进行数据保护影响评估，确有必要的跨境转移活动需满足履行合同所必需或获取正式的授权，经过审批后方可按数据跨境管控要求实施。

中兴通讯还将隐私保护要求扩展到供应商，在供应商认证或采购时对其隐私保护能力进行充分评估，从合作源头管控风险，与全球供应商和合作伙伴共建开放、安全、可信的隐私保护生态。

隐私保护实践探索

中兴通讯积极开展隐私保护实践创新，探索安全合规的产品和服务解决方案。

中兴通讯在企业运营管理活动中，一般作为数据控制者，主要处理员工的个人数据。在对外商业活动中，在与客户接洽时，中兴通讯通常作为控制者处理客户的个人数据。当中兴通讯作为产品提供商时，通常不参与到数据处理活动中，主要应保障产品的隐私保护能力。当中兴通讯作为服务提供商时，中兴通讯通常会按客户的要求进行数据处理，主要属于数据处理者。在某些特定的运营场景中，中兴通讯也会作为数据控制者，如面向终端用户的客户支持中心、中兴自营网站、自营 APP 等。因此，在提供服务时需要遵守控制者或处理者的相关义务。

中兴通讯遵循隐私保护设计理念，聚焦用户的权益保护和数据安全，将隐私保护管控前移至产品和服务方案的设计阶段，通过将隐私保护需求导入产品和服务需求中，使数据保护成为集成到产品和服务中的默认选项，确保数据处理满足合法、公平、透明等原则，从而实现对产品和服务隐私保护的管控。

中兴通讯致力于提供可信赖的、端到端的全生命周期安全和隐私保障。2020 年，中兴通讯对标 ISO/IEC 27701:2019，在重点产品导入建立隐私信息管理体系 (PIMS) 并持续改进，获得了业内首个针对 5G 产品的 ISO/IEC 27701:2019 隐私信息管理体系认证。目前，中兴通讯已陆续获取了 5G 无线接入网、核心网、数字产品、终端等领域的多项认证证书。

作为数字经济“筑路者”，中兴通讯将契合通信行业特点，匹配内部风险偏好和外部监管环境，致力于建立适用、有效、领先的隐私保护体系，力争在隐私保护领域，成为中国企业的引领者和标杆，成为全球企业的先行者和典范。

安全成熟度是可验证的

中兴通讯相信安全成熟度是可验证的。首先，泛 IT 行业中已有众多国际公认的安全认证体系，如 ISO27000 系列、通用准则 (CC) 认证等。在更加复杂的通信行业，国际标准组织已将安全要求写入了技术规范。随着通信网络的发展，3GPP、ITU、ETSI 等标准组织均在不断更新、扩展技术标准和安全规范。其次，各国逐渐认识到 5G 网络安全的重要性，各利益相关方加强了对安全的认证和评估。欧盟致力于开发统一的通信网络安全认证，并将这一要求写入了网络安全法，欧盟 5G 工具箱进一步要求成员国对 5G 网络组件和供应商的流程采用欧盟统一的认证 [15]。同时，GSMA 代表全球数百个运营商和制造商，开发出安全评估和保障计划 NESAS，对网络设备开发流程进行审计，并与 3GPP 一同丰富 NESAS 的网络设备安全评估测试用例。欧盟以及多个国家已经将 NESAS，以及通用准则认证的网络相关部分作为统一安全认证和评估的蓝本。

这些通用的技术标准、认证体系、和评估框架，能够让我们的产品得到各方面的验证，让客户了解我们产品在开发流程以及技术方面的安全性。各个厂家遵循公认的规范，能够提高整个行业的安全水平。

中兴通讯一直致力于行业标准对标和安全验证。我们参与 GSMA 的标准制定，积极拥抱 NESAS，并和外部安全认证和评估机构合作，以验证我们的安全是否有效深入技术、产品、以及整个开发生命周期流程。从 2020 年到 2021 年，在业界顶尖安全公司的严格测试下，中兴通讯的 5G 产品线通过了 GSMA NESAS 开发和产品生命周期流程审计，8 款 5G 产品通过了以 3GPP SCAS 为测试用例的 NESAS 网络设备安全评估。此外，5G RAN 解决方案获得了 CC EAL3+[16] 认证，这是业内第一个以整个系统解决方案（包括 15 个 5G RAN 产品）作为保护轮廓获得的 EAL3+ 证书。在对标 BSIMM 模型的实践中，我们邀请新思科技对 5G 核心网和接入网产品线进行 BSIMM 评估，结果表明，我们的软件安全达到业界领先的水平。同时，我们持有一系列安全相关的 ISO 认证，包括信息安全、供应链安全、业务连续性、隐私保护等。

为了让客户、监管以及利益相关方能够更便捷、有效、透明地验证中兴通讯的产品，我们已在中国南京、意大利罗马和比利时布鲁塞尔建成三个网络安全实验室。南京实验室是中兴通讯规模最大、功能最完善的网络安全实验室，提供行业领先的全网络集成环境和评估基础设施，支持多种安全评估功能，包括源代码审查、文档审阅、渗透测试等。同时，它也是促进能力建设、在安全领域进行深入研究和探索的场所。在海外，以意大利实验室为例，我们的客户已借助设备环境丰富的实验室对多个产品进行渗透测试和源代码审计，包括 5G、家庭终端和手机等产品，而其中一部分是在意大利全国大学电信联盟 (CNIT) 的独立监督下进行的。今后，中兴通讯还会按需建立更多的网络安全实验室，开放我们的代码，迎接更多的外部监督和验证。

通过积极寻求灵活多样的对外合作和外部验证，中兴通讯不断提升流程和产品的安全成熟度。随着 5G 网络逐渐普及和发展，这一开放透明的举措还将继续，我们相信这是获取信任的最佳途径。

[15] 欧盟统一认证：参见 EU Toolbox TM09，https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

[16] CC EAL3+：EAL 是 CC 认证的评估保证等级，EAL3+ 表明认证的产品符合 EAL3 等级要求以及额外的评估要求。

开放透明共建网络安全

标准化是移动网络安全的基础，以实现互操作性和开放性。对于 5G 网络尤其如此，从 5G 安全标准的制定和实行，到跨地域、跨行业的协调漏洞披露和修复，其贡献者来自全球各地。标准组织联合通讯网络运营商和制造商共同将 5G 安全设计到标准中去。因此，开放和透明是保障 5G 安全的必要前提。只有遵循开放的标准和统一的安全保障要求，我们才能在整个移动网络中获得足够的安全性。

多年来，中兴通讯发挥其在通信网络的技术优势，积极参与国内和国际的标准化制定工作，深度参与国际主流的标准组织。目前，中兴通讯在 3GPP 担任 RAN3 工作组主席和 RAN2 副主席，同时在 3GPP 最重要的安全标准工作组 SA3 中担任报告人，主导了 5G 网间用户面安全功能安全保障评估 SCAS_5G_IPUPS 和网元能力开放功能安全保障规范 SCAS_NEF。安全保障规范 (SCAS) 作为网络设备最主要的安全标准，一直在不断扩张更新，随着 5G 及以后的网络发展，会不断迭代出更安全的规范。

在 ITU-T，中兴通讯担任 SG17 安全研究组的副主席和其中 WP5 组的主席，此外，中兴通讯还在 ETSI、GTI、GSMA 等国际组织中担任重要角色，为网络安全标准做出贡献。

中兴通讯通过多年的技术创新，在实践过程中不断积累经验，逐步具备了覆盖 5G 核心技术、安全运营和行业应用等全方位的解决方案能力。利用自身的研发优势，中兴通讯致力于实践联合国全球契约 (United Nations Global Compact)，采用更可持续的商业实践和模式，以新技术赋能行业数字化转型，实现可持续发展。至 2021 年 6 月，公司已申请专利 8 万余件，授权 4 万余件。2020 年，公司向 ETSI 披露 5G 标准必要专利声明族位列全球前三。

在 5G 时代，只有在保证安全的前提下，基于技术的行业数字化转型才能更好地实现。中兴通讯将不断投入更多的资源进行安全技术和方法的研究，持续自主创新，引入和借鉴先进的网络安全治理理念和方法，全面提升产品安全和服务能力，以满足新技术、新应用、新模式的安全保障需求。在商业环境不断变化的情况下，我们对标行业标准和最佳实践，考虑每个业务环节的安全性，不仅包括我们企业自身的安全措施，更包括上游供应链，以保持整体供应链的弹性、可靠。

中兴通讯秉持透明、开放、信任、合作的理念，与客户、合作伙伴、政府、供应商、标准组织开展更加紧密的合作，共同应对未来的安全挑战，持续为客户提供安全可信的产品和服务。

附录 A
缩略语表

缩略语	全拼或名称	说明
3GPP	3rd Generation Partnership Project	第三代合作伙伴计划
5G	Fifth generation mobile communication	第五代移动通信
AEO	Authorized Economic Operator	经认证的经营者
AOS	Advanced Operations Suite	AOS 全球一张网系统
CC	Common Criteria	通用准则
CCPA	California Consumer Privacy Act	加州消费者隐私法案
CERT	Computer Emergency Response Team	计算机安全应急响应小组
CNA	CVE Numbering Authority	CVE 编号颁发机构
CSA	Cloud Security Alliance	云安全联盟
CSC	Cyber Security Committee	产品安全委员会
CVE	Common Vulnerabilities and Exposures	通用漏洞披露
CWE	Common Weakness Enumeration	通用缺陷列表
EAL	Evaluation Assurance Level	通用准则的评估保证等级
ENISA	The European Union Agency for Cybersecurity	欧洲网络与信息安全局
ETSI	European Telecommunications Standards Institute	欧洲电信标准协会
FIRST	Forum of Incident Response and Security Teams	事件响应和安全小组论坛

缩略语	全拼或名称	说明
GCSC	Global Customer Support Center	全球客户支持中心
GDPR	General Data Protection Regulation	通用数据保护条例
HPPD	High Performance Product Development	高效产品开发
ICT	Information and Communications Technology	信息与通信技术
IETF	Internet Engineering Task Force	互联网工程任务组
IIA	Institute of Internal Auditors	国际内部审计师协会
ISO	International Organization for Standardization	国际标准化组织
ITU	International Telecommunication Union	国际电信联盟
ITU-T	ITU Telecommunication Standardization Sector	国际电联电信标准化部门
NESAS	Network Equipment Security Assurance Scheme	网络设备安全保障计划
NIST	National Institute of Standards and Technology	美国国家标准技术研究所
OWASP	Open Web Application Security Project	开放式 Web 应用程序安全项目
PbD	Privacy by Design	隐私保护设计
PSIRT	Product Security Incident Response Team	产品安全事件响应小组
RAN	Radio Access Network	无线接入网
S&OP	Sales & Operations Planning	销售与运营计划
SbD	Security by Design	设计安全
SCAS	Security Assurance Specifications	安全保障规范
SCOR	Supply-Chain Operations Reference-model	供应链运作参考模型
SDL	Security Development Lifecycle	安全开发生命周期
SEP	Standard Essential Patent	标准必要专利
STIG	Security Technical Implementation Guide	安全技术实施指南

附录 B

中兴通讯网络安全大事记

2005 年 • 中兴通讯通过 ISO 27001 信息安全管理体系认证。2021 年，中兴通讯及全球 23 家分公司均通过此认证，覆盖了公司所有业务。

2005 年 • 中兴通讯开始担任 ITU-T SG17 副主席职务。中兴通讯长期积极参与 3GPP、IETF、ITU-T 和 CSA 等国际标准化组织或安全论坛的活动，推进安全领域的标准化工作。

2011 年 • 中兴通讯 Netnumen U31 通过信息技术安全评估通用标准 (CC) EAL2 级认证。2018 年，中兴通讯累计有 12 类产品通过 CC 认证，涉及核心网、接入网、光传输、网管、路由器、基站控制器等主流产品和设备。

2013 年 • 中兴通讯成立了产品安全实验室和产品安全事件响应团队 PSIRT。

2015 年 • 中兴通讯成为国际安全论坛组织 FIRST (Forum of Incident Response and Security Teams) 成员。

2017 年 • 中兴通讯获得 ISO 28000 供应链安全管理体系认证，覆盖 26 大类电信产品的采购、制造及物流业务。

2017 年 • 中兴通讯获得海关 AEO 贸易安全认证。

2017 年 • 中兴通讯成为 CVE 编号颁发机构 CNA (CVE Numbering Authorities)。

2019 年 • 中兴通讯在全球开设了三个网络安全实验室。

2019 年 • 中兴通讯获得中国网络安全审查技术与认证中心 (CCRC) 认证的安全集成服务资质，达到信息安全服务规范的一级要求。

2020 年 • 中兴通讯获得 ISO 22301 业务连续性管理认证。

2020-2021 • 中兴通讯多个产品获得 ISO 27701 隐私信息管理体系认证，覆盖 5G RAN、核心网、数字产品和终端产品。

2020 年 • 中兴通讯的 5G NR 和 5GC 融合核心网系列产品通过网络设备安全保障计划 NESAS 的“供应商开发和产品生命周期流程的安全评估”。

2020 年 • 中兴通讯获得中国网络安全审查技术与认证中心授予的信息安全风险评估服务一级资质。

2020 年 • 中兴通讯发布新的安全漏洞奖励计划。

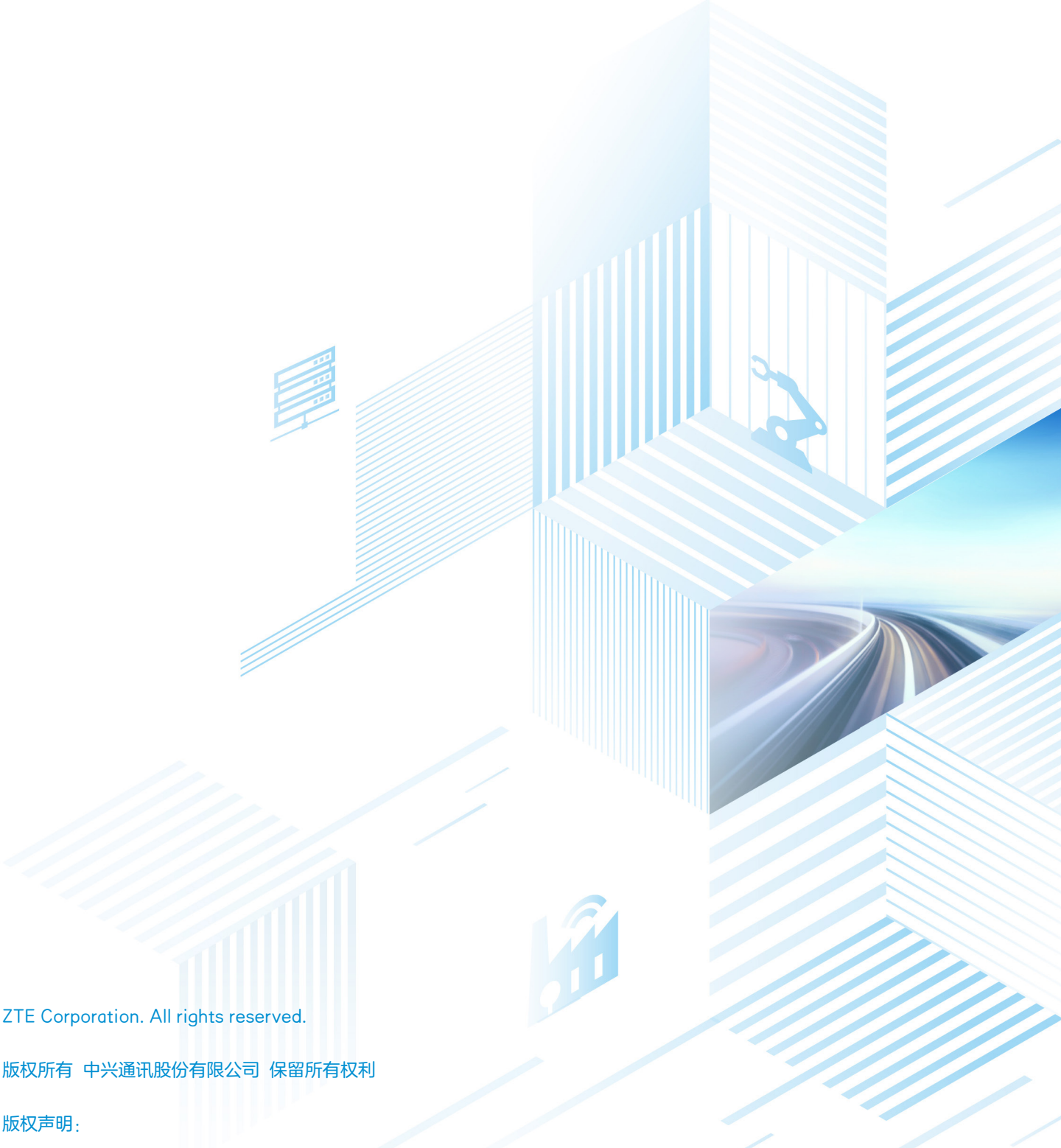
2021 年 • 中兴通讯荣获英国 bsi 隐私战略贡献奖。

2021 年 • 中兴通讯荣获联合国信息社会世界峰会 WSIS (World Summit on the Information Society) ICT 安全领域冠军奖。

2021 年 • 中兴通讯以高分完成 BSIMM 评估，其在十二项最佳实践模块中有十项获得了接近业界最佳水平的得分。

2021 年 • 中兴通讯的 5G RAN 解决方案获得 CC EAL3+ 认证，成为业内首家以 5G RAN 系列产品整套系统作为保护轮廓通过 CC EAL3+ 认证的供应商。

2021 年 • 中兴通讯的 5G NR gNodeB 和 7 个 5GC 网络设备成功通过 NESAS 网络设备产品安全评估。



ZTE中兴 中兴通讯股份有限公司 ZTE CORPORATION
地址：深圳市高新科技产业园科技南路中兴通讯大厦 邮政编码：518057
电话：+86-755-26770000 传真：+86-755-26771999 网址：www.zte.com.cn