ZTE中兴

治理 遵从 开放 透明

中兴通讯网络安全保障实践

安全融入血脉，透明增进信任

中兴通讯股份有限公司
2023年12月

作者

本白皮书由中兴通讯各领域安全专家共同完成，诚挚感谢每位编写人：

曹鲲鹏　丁　沛　何　英　蒋　璐　孔　韬　李　星　梁　平　刘佳宁

刘　磊　平　立　汤可可　唐　蕾　汪冬敏　王义华　韦银星　游世林

章乐怡　赵　波　周　杨

同时鸣谢本白皮书的每位贡献者：

曹　琦　Christopher Mulley　戴　恒　韩殿罡　华国红　黄智敏　蒋国兵

李双全　刘　晖　刘俊颜　娄爱珍　罗永红　马　伟　马致原　田　力

王华刚　王　霞　王玉忠　王　智　徐　敏　晏文德　杨桂荣　杨宇鑫

俞　婷　张金鑫　张永毅　张祥军　郑　均　周天才　朱林林

中兴通讯首席安全官　**钟　宏**

目录

1 序言

随着数字技术的发展，数字化基础设施对促进社会发展和经济增长发挥着至关重要的作用。根据全球移动通信系统协会（GSMA）预测[1]，到 2023 年底，全球 5G 连接将达到 15 亿，到 2030 年将达到 53 亿；到 2023 年底，全球联网 IoT 设备数量将增长 16%，达到 167 亿台[2]。数字化的不断发展增加了网络安全风险，根据欧盟网络安全局（ENISA）《2023 ENISA 威胁态势》[3]，网络攻击数量在全球范围持续增加，在报告观察期内，2023 年全球安全事件数量是 2022 年的两倍。

通信网络作为关键的数字基础设施，其安全性得到了前所未有的关注。从行业标准的制定和遵循，漏洞响应和协同披露，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迎接挑战。

各国政府加强了网络安全立法，促进通信及各行业的网络安全水平提升，以保护关键的基础设施。中国在《网络安全法》以及《数据保护法》等法律的基础上，出台了如《关键信息基础设施保护条例》、《网络产品安全漏洞管理规定》等细化的管理规范。欧盟《网络安全法》鼓励在设计和开发的最早阶段实施安全措施，并强调通过不断优化的治理来确保 ICT 产品、服务和流程全生命周期的安全性。欧盟《网络弹性法》强调产品安全的重要性，要求制造商在产品的整个生命周期实施安全管理，包括产品的设计安全、默认安全和漏洞处理，以防止易受攻击的产品进入市场。同时，行业网络安全标准也在不断演进，包括持续迭代的 GSMA 网络设备安全保障计划（NESAS）、即将出台的欧盟网络安全认证计划 EUCC 和 EU5G 等，中国也通过关键基础设施认证来推进安全标准化。

中兴通讯作为全球综合通信与信息技术解决方案提供商，有义务、有责任遵守法律法规、遵循行业标准，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和数字生活。

1. *5G in Context, Q1 2023: https://data.gsmaintelligence.com/research/research/research-2023/5g-in-context-q1-2023*
2. *State of IoT 2023: Number of connected IoT devices growing 16% to 16.7 billion globally https://iot-analytics.com/number-connected-iot-devices/*
3. *ENISA Threat Landscape 2023: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023*

此白皮书描述了中兴通讯安全治理架构和安全保障体系，着重强调了行之有效的治理方法和实践，即在产品全生命周期安全管控基础上，聚焦于纵深改进，包括设计安全和默认安全、第三方组件管理、事件响应和漏洞管理等。这些安全管理贯穿供应链、研发和交付业务流，并通过数字化支撑系统的不断完善实现有效落地和持续改进。

网络安全没有止境，持续改进没有终点。中兴通讯秉持开放透明，欢迎外部独立安全验证，愿与运营商、监管机构、合作伙伴和其他利益相关方密切沟通合作，不断改善管理和技术实践，共同建立安全可信的网络环境、保障数字世界安全。

2 安全保障实践框架

中兴通讯以基于风险的方式建立了覆盖产品全生命周期的安全治理体系，始终将安全作为产品研发和交付的最高优先级。

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，向客户交付安全可信的产品和服务，致力于实现“让沟通与信任无处不在”的美好未来。

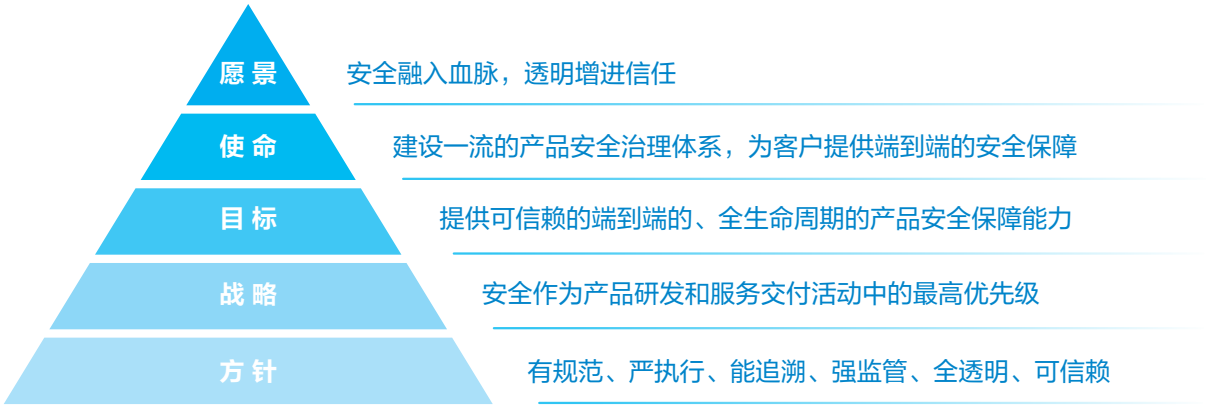

图 1 中兴通讯网络安全愿景和使命

2.1 三线架构确保有效治理

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[4]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，从而更有效地管理风险。

中兴通讯采用基于三线模型的治理架构进行产品安全治理工作，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执行和检查、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和服务的安全性。

4. *THE IIA’S THREE LINES MODEL: https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf*

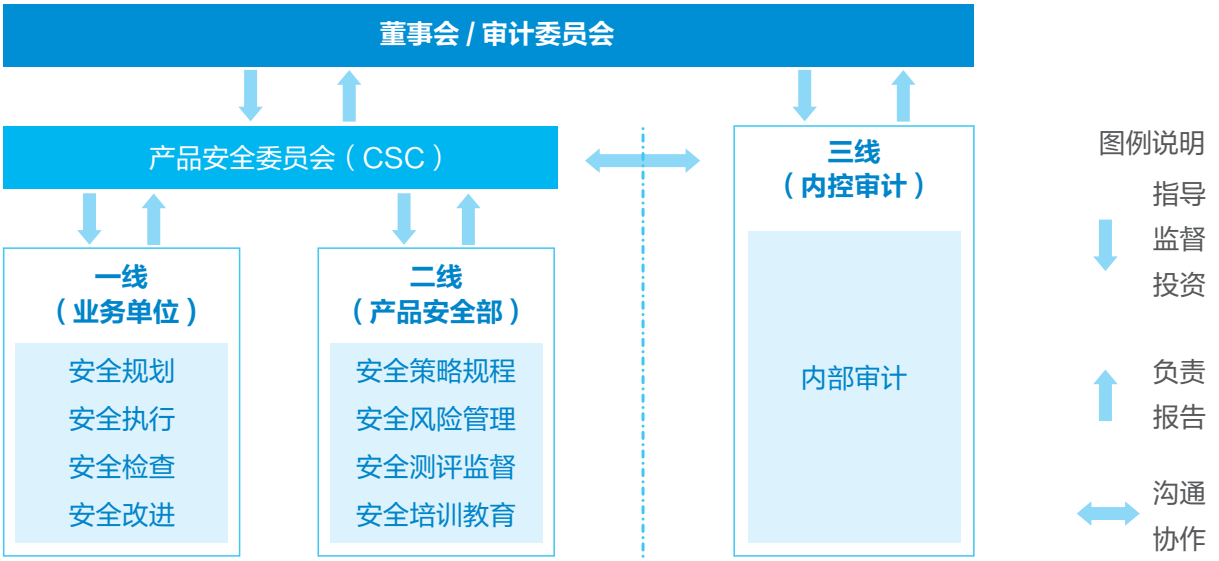

图 2 中兴通讯网络安全治理三线模型

董事会 / 审计委员会：

董事会监督和指导产品安全委员会（CSC）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。公司高层作为产品安全委员会常委，参与产品安全治理工作。

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，产品基于设计安全并通过规范化流程确保产品研发过程安全可控；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；在交付环节，遵守规范化的操作，保障产品和服务安全交付。

二线：

产品安全部是产品安全治理的第二线，采用独立安全测评机制对一线安全实践进行评估和监督。

公司设立了多个网络安全实验室，实施独立的安全测评。采用过程审计来评估一线安全治理执行过程的符合度和有效性；采用产品安全测试来评估产品的安全性，安全测试包括漏洞扫描、安全编码审查、协议健

壮性测试及渗透测试。同时，公司积极与第三方机构开展安全合作，对产品和流程进行安全评估，如过程审计、源代码审计、安全设计审查和渗透测试。

中兴通讯重视人员安全意识和能力的培养，持续开展多层面分领域的安全意识和专业技能培训，如全员安全意识培训、安全设计培训、渗透测试培训等，公司员工目前持有 230+ 国际安全认证证书。

三线：

内控审计是产品安全治理的第三线。内控审计负责独立审计一线和二线的工作，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。

一线执行、二线监督、三线审计，确保产品安全治理体系健全有效。

2.2 安全融入产品全生命周期

覆盖产品全生命周期的安全治理和管控是产品安全的基本要求。

2019 年，欧盟颁布《网络安全法》，要求通过不断发展的设计和开发流程来确保 ICT 产品和服务全生命周期的安全性。GSMA NESAS 对产品开发和全生命周期提出了安全要求，成为通信设备安全融入全流程的最佳实践。中兴通讯基于风险的安全治理覆盖供应链、研发、交付、事件响应和各支撑领域，形成了贯穿全生命周期的产品安全保障体系，并持续对标行业最新标准和最佳实践。中兴通讯研发流程（高效产品开发 HPPD）通过了 GSMA NESAS 过程评估和德国 BSI NESAS CCS-GI 过程评估。

在研发环节，将安全控制嵌入研发流程的各个阶段，例如：

- 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、隐私保护设计（Privacy by Design, PbD）；
- 对产品进行渗透测试，定期实施安全回归测试；
- 对第三方组件（含开源）的安全漏洞持续跟踪、分析并解决；
- 在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。

在供应链环节，将安全要求嵌入到验证供应商、新引入材料和生产过程中，例如：

- 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风险材料进行抽检；
- 在生产环境中建立专用网络用以隔离安全隐患。

在交付环节，采用技术和管理双重手段持续提升网络的安全性和弹性，确保始终交付安全的产品与服务。例如：

- 对接触客户网络关键设备的关键岗位人员进行安全管控和培训；
- 网络变更操作必须获得客户授权，操作有记录，行为可稽查；
- 定期进行安全事件响应应急演练，持续提升事件响应能力。

一些端到端的业务流，如第三方组件管理、漏洞管理，在 DevSecOps 工具链的支持下，打通供应链、研发、交付的端到端安全管理，快速响应安全事件和漏洞。

2.3 数字化支撑系统

中兴通讯安全治理已融入产品全生命周期各业务流程，实现了贯穿一线业务领域的产品安全数字化支撑系统。

公司建立了智能供应协同平台（ISCP）、产品研发云（RD Cloud）、全球客户支持中心（GCSC）等数字化系统，实现弹性供应、持续规划、协作开发、集成测试、发布部署、问题解决等业务环节的高效运作。配置管理系统和漏洞管理系统实现了产品安全问题的跟踪和追溯。

产品安全运用 DevSecOps 工具链实现各环节的安全管控。在材料安全测试、第三方软件安全扫描、代码扫描、漏洞扫描、版本保护、安全加固等关键安全活动中，利用安全工具自动检查产品和服务是否满足安全要求。

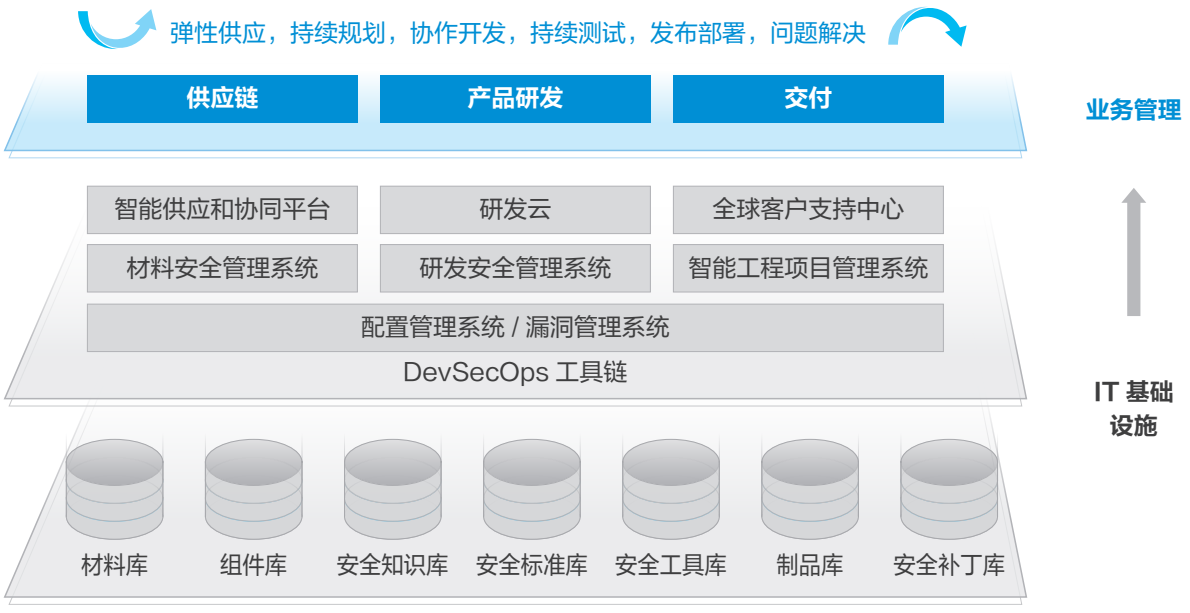

图 3 中兴通讯产品全生命周期数字化支撑系统

3 实现设计安全和默认安全

GSMA NESAS《开发和生命周期安全要求》[5] 明确提出设计安全的要求，网络产品应在整个开发和产品生命周期中通过设计实现安全性。

考虑了设计安全的产品能够合理防止恶意网络攻击，如非法访问网络设备、数据，以及连接的基础设施。网络设备制造商应进行风险评估，以识别和列举关键系统普遍存在的网络威胁，将保护措施纳入产品蓝图中。

欧盟《网络安全法》要求企业应以更高级别的安全性设计其 ICT 产品、服务或流程，让用户获得最佳安全默认配置的产品和服务。

考虑了默认安全的产品在交付时已经做了安全保护，用户可以“开箱即用”，几乎不需要额外配置。

设计安全和默认安全不仅有利于用户，也有利于制造商，能减少漏洞数量和修复漏洞的成本。

中兴通讯提倡透明和问责制，认为提供设计安全和默认安全的产品是制造商的责任。公司强调在产品开发生命周期中尽早引入安全设计原则，在产品设计阶段进行威胁分析和风险评估，建立并优化产品安全保护准则及基线。安全设计原则包括但不限于：减少攻击面、设置安全默认值、隐私保护、最小权限、纵深防御、失效安全、职责分离等。

3.1 安全设计过程

在中兴通讯的产品研发过程中，安全设计是早期的关键环节，及早识别产品威胁、合理评估风险、确立安全保护控制措施，有利于将安全风险和安全成本降到最低。将设计安全和默认安全要求纳入安全设计过程控制，可保障产品达成开箱即用和极简运维的交付目标。

5. *Official Document FS.16 – Network Equipment Security Assurance Scheme – Development and Lifecycle Security Requirement, Version 2.1*
https://www.gsma.com/security/wp-content/uploads/2022/02/FS.16-v2.1.pdf

中兴通讯持续构建具有自身特色、具备业界领先水平的安全设计过程。公司对标业界规范、技术标准、市场要求，建设“产品安全知识库”实施面向产品的威胁建模，创建“产品安全技术要求库”实施安全设计对标规划、进行风险接受决策，输出产品安全方案设计。依托 DevSecOps 工具链，实现了平台化的安全设计过程线上开发，建立了闭环度量改进机制并持续优化。

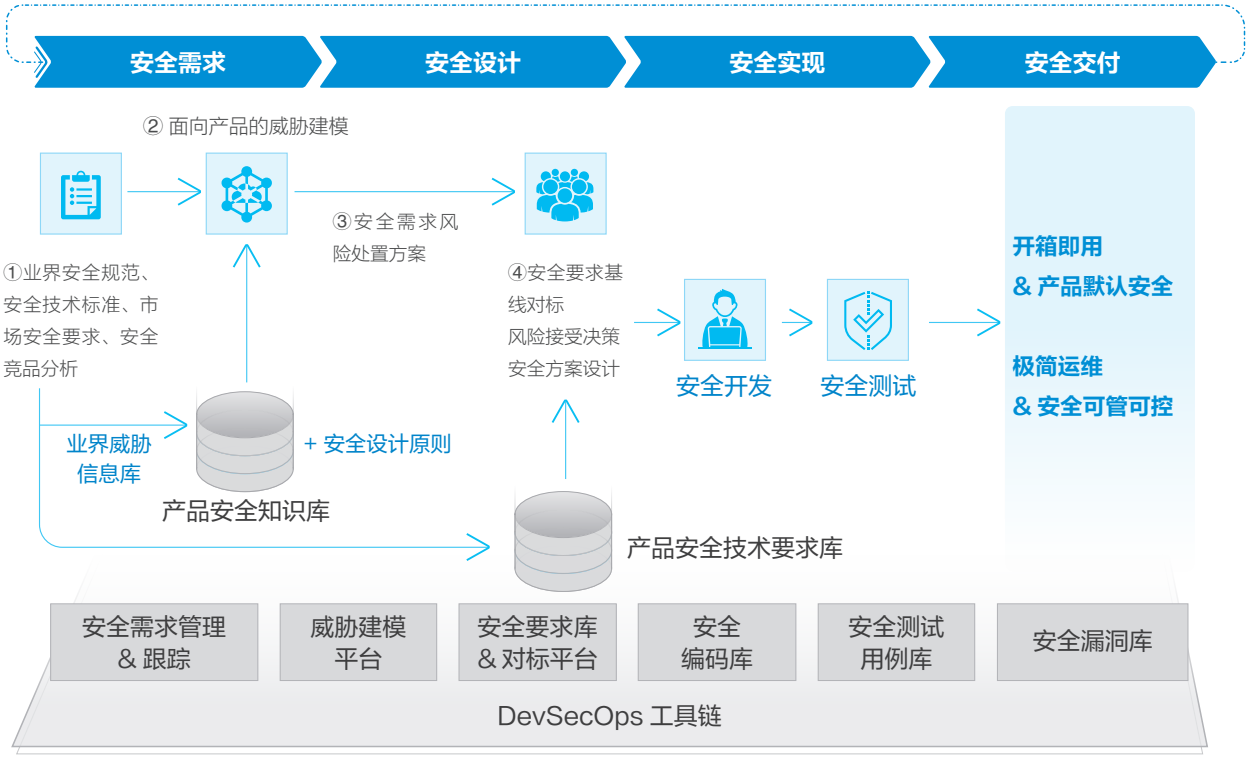

图 4 中兴通讯产品研发过程中的安全设计

3.2 安全设计实践

中兴通讯安全设计最佳实践包括：产品安全知识库、产品安全技术要求库和威胁建模平台。产品安全知识库持续积累产品安全知识经验，持续提升安全设计专业性和有效性；产品安全技术要求库对标业界安全标准规范，为安全设计提供基线化要求；威胁建模平台支持线上化、自动化和可视化的协同操作。

产品安全知识库

产品安全知识库吸纳了行业规范和最佳实践，如业界通用威胁和漏洞信息（CAPEC、ATT&CK、CWE、CVE 等）、行业安全技术标准规范（3GPP SCAS 规范、IETF RFC 标准等）、以及中兴通讯自身的产品安

全实践经验。产品安全知识库遵循结构化威胁信息表达式（STIX）规范，包含了资产、威胁、风险准则、控制措施、攻击模式、滥用案例等关键要素。

产品安全技术要求库

产品安全技术要求库包括了产品安全技术栈目录全景图和产品安全设计技术标准族。技术栈目录全景图按照“架构分层、技术分域”的原则，对产品涉及的安全技术栈进行统一分类。针对关键的安全技术栈编写了一系列的产品安全设计技术指导书，作为企业技术标准发布。中兴通讯将所有已发布的安全技术要求录入研发云（RD Cloud）的安全技术要求库和对标平台中，并在产品研发流程中嵌入安全技术要求基线对标控制点。

威胁建模平台

中兴通讯通过构建威胁建模平台，实现了资产识别、威胁分析、风险评估及处置、控制措施优选、安全追踪矩阵输出等关键威胁建模活动的数字化工序，实现了过程的标准化、规范化、自动化、层次化和可视化，威胁建模平台已集成到 DevSecOps 工具链，可支持跨团队的协同研发，灵活开展威胁建模实践。

4 安全开发和测试

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过程中。

公司产品开发和测试的安全要求对标行业标准和最佳实践，参考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），制定了产品安全成熟度模型和相应规范，定期进行组织和项目评估，发现差距，不断改进。

公司安全编码标准参考业界通用指南，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）。在开发阶段，源代码扫描是关键控制点，需通过静态检查和自动化扫描，衡量代码的质量和安全性，对工具扫描出的缺陷进行看板化闭环管理。公司注重提升开发人员的安全编码能力，通过定期评估持续提升其能力水平。

各产品项目制定安全测试规程和测试方案，在测试阶段对产品进行代码扫描、漏洞扫描、协议健壮性测试、病毒扫描等安全测试，充分验证安全需求的实现并修复缺陷。公司成立了专业的渗透测试团队，进行更深层次的漏洞挖掘。

在发布阶段，公司要求产品必须经过安全测试和安全风险评估。产品发布时，必须配备安全加固手册和工具。发布过程采用证书授权中心（CA）验证，确保传输过程的一致性和可追溯性。

在版本维护阶段，公司定期执行回归测试，以识别新增漏洞是否影响已有版本。研发团队及时更新安全补丁、制定安全加固方案，以便用户进行产品安全风险消除或控制。

5 第三方组件管理

随着 ICT 产业的不断发展，ICT 产品中包含了越来越多的第三方组件[6]，这些组件带来了新的安全威胁，例如被发现有新的漏洞、停止支持等。

管理好第三方组件对安全至关重要。监管和行业纷纷出台要求和指导，以提升第三方组件管理水平，使可能产生的风险降到最低。比如，GSMA NESAS 在 2.0 版本中新增了“第三方组件采购”，要求设备供应商制定适当的流程来确保产品生命周期内第三方组件的质量、使用受支持的第三方组件、评估第三方组件中新发现的漏洞是否会对网络造成威胁等。

5.1 第三方组件管理策略

第三方组件包括开源软件、商用组件、商用附赠软件等，是产品的组成部分，并可能被多个产品使用。公司遵循法律法规要求和行业最佳实践，在供应链管理、产品研发、交付过程中，不断积累管理实践，对第三方组件实施全生命周期管理。

中兴通讯第三方组件安全管理覆盖组件引入、使用、运维和退出各业务阶段，第三方组件管理要求已融入高效产品研发（HPPD）流程。

6. *指具有离散结构的对象，例如程序集、软件包，其源自外部实体并合并到网络产品中，Official Document FS.16 – Network Equipment Security Assurance Scheme – Development and Lifecycle Security Requirement, Version 2.1*

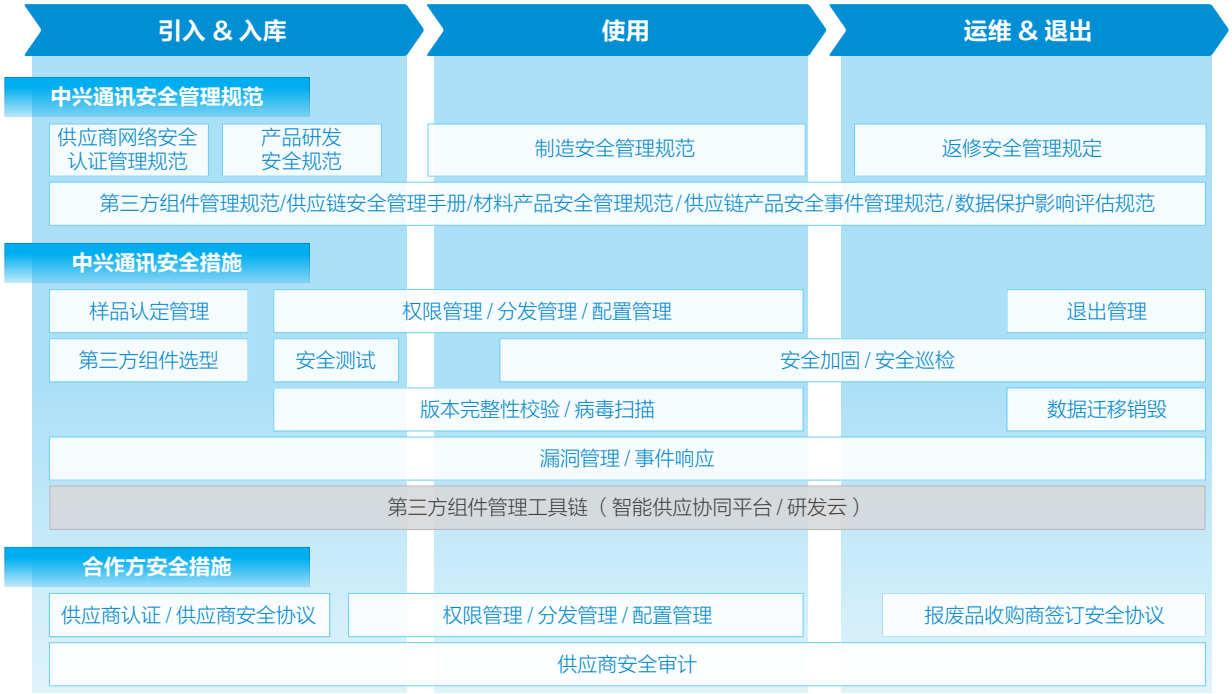

图 5 中兴通讯第三方组件管理策略

组件引入

- 第三方组件引入需进行选型认证，只有通过认证的第三方组件才能进入公司组件库（组件广场）。选型认证需要对第三方组件执行安全合规扫描，分析并验证其功能和性能，评估安全风险，确保达成出口管制、数据保护、开源许可等合规要求；此外，还需要考虑第三方组件的可替代性及生命周期。
- 完成认证的第三方组件需设置组件守护人，负责组件全生命周期管理。
- 与商用组件供应商签署安全协议，确保供应商理解并对所提供的第三方组件产品安全要求做出承诺。中兴通讯定期组织供应商赋能活动，致力于与供应商共同提升生态安全。

组件使用

- 产品只允许引用组件广场中的第三方组件。
- 在产品的方案设计、开发测试及发布的各个活动中，均嵌入第三方组件的安全风险评估，确保提供恰当的安全解决方案或规避措施。
- 产品需通过整机级安全测试，达到安全标准后才能发布。
- 第三方组件作为产品配置项以确保其使用情况可追溯。当发现第三方组件的安全漏洞时，可通过产品配置项追踪漏洞波及范围。

组件运维和退出

- 当第三方组件因为功能、性能、安全问题进行版本升级，或引入了补丁程序，组件守护人执行更新操作，确保组件库中的组件是最新的；当第三方组件提供方停止维护、组件生命周期终止时，组件守护人执行

停用操作。更新和停用自动通知到研发团队，以更新产品方案。

- 在产品交付环节，中兴通讯产品安全事件响应团队（Product Security Incident Response Team, PSIRT）与供应商和安全社区保持密切协作，及时获取第三方组件漏洞信息，协同相关团队进行波及分析、漏洞修复方案制定、验证和实施，确保快速响应和消除第三方组件带来的安全问题及风险。

开源组件管理

- 在引入时，优选安全、合规、社区活跃度高、生态系统完备、可信度高的开源组件，并建立开源组件成熟度评价模型，作为产品选型及使用的安全评估参考。
- 在使用中，使用开源软件成分分析工具和漏洞扫描工具，评估开源组件的安全性及许可证合规情况、识别并修复已知漏洞。
- 公司将开源组件安全问题和解决方案提交开源社区，共享成果。

5.2 第三方组件管理实践

中兴通讯组件广场为第三方组件的引入者、使用者、管理者提供了一个安全可信的平台，是 RD Cloud 的重要组成部分。组件广场针对产品规划、开发、测试、集成、发布及运维场景，提供同源管理、安全合规管控、调用追踪、检索、评论等功能，使第三方组件可管理、可调用、可追踪和可信任。

图 6 中兴通讯第三方组件管理实践

中兴通讯依托成熟的产品配置项管理，建立了融合第三方组件的产品全生命期漏洞管理流程。一旦感知到第三方组件出现的安全漏洞，漏洞管理系统可自动定位波及的产品和版本，实现了从第三方组件漏洞到波及产品、版本、客户的追踪和解决修复。

6 弹性供应链

相比于传统行业，ICT 行业的供应链更加复杂，存在安全风险的概率更大。网络的复杂化、模块化和虚拟化的特征，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。

《2023 ENISA 威胁态势》报告指出，在过去 12 个月，61% 的公司中受到软件供应链攻击影响，预计到 2026 年，这些攻击对企业造成的总成本将较 2023 年增长 76%。

由此，各国监管和客户将产品安全的关注范围从网络设备供应商延伸至其二级、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，向供应安全与业务连续性方面扩展。这对供应链的安全和弹性提出了更高的要求。

6.1 供应链安全

对中兴通讯而言，构建安全可信的弹性供应链[7]，既是保障公司产品安全交付的内在需求，也是公司对客户的庄严承诺。公司先后通过了 ISO 27001 信息安全管理体系认证、ISO 28000 供应链安全管理体系认证、和 ISO 22301 业务连续性管理体系认证，还通过了经认证的经营者（AEO）高级认证，在全球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，聚焦客户的业务需求和安全需求，强调供应商管理、材料、生产制造和物流货运四个方面的安全治理，支撑供应链全业务流程，依据供应链 SCOR 模型[8]，将供应链安全保障范围扩大到供应商的供应商及客户的客户。

7. *6.1、6.2 节描述的供应链，指设备供应商视角的上游供应链及自身供应链业务。*
8. *Supply-Chain Operations Reference-model，由国际供应链协会 Supply-Chain Council 开发支持。*

供应商安全

分布于全球各地的数千家供应商合作伙伴是中兴通讯供应链的重要组成部分，为中兴通讯提供数以万计原材料、半成品、成品或服务。因此，公司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。

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。公司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，提升安全管理水平，遵守双方签署的产品安全协议。对于新发现的安全漏洞，供应商应当协同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。

中兴通讯持续将产品安全、企业社会责任等要求传递给供应商，并通过年度全球合作伙伴大会和供应商集训营向供应商赋能。

材料安全

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识别风险，将材料的产品安全风险定义为高、中、低三个等级。针对高风险材料，在材料引入环节，要求供应商提供产品安全检测报告。对于中低风险等级的材料，通过与供应商签署安全协议，要求供应商进行自我管理和约束，允许中兴通讯进行多种形式的安全审计。另外，公司建立了产品安全材料检测实验室，对中高风险材料进行抽检，对抽检中发现的安全问题实施闭环管理。

生产制造安全

中兴通讯制定了生产制造安全管理规范，把生产制造区域分为三个等级的安全管控区，管控生产制造过程中的安全风险，包括未经授权的硬件替换、软件植入或篡改、病毒感染等。针对不同等级的安全管控区，采取不同的安全管控措施，其中一级、二级管控区是安全风险严管区域。在这些区域设置安全管理员，负责实施区域内的安全管控和日常安全监督。

为了保障生产环境的网络安全，公司建设了生产专用网络，以防止病毒入侵或软件篡改。同时，只有授权的工程师才能使用专网。

物流货运安全

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。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。

6.2 供应链弹性

秉承安全、精准、智能、可靠、高效的 SPIRE 供应链理念，以交付有竞争力的产品和服务为目标，中兴通讯构建了预判、免疫和适应三大核心能力，通过智慧大脑实现业务监测、预警、联动、调度等功能可视化，打造安全可信的弹性供应链。

预判能力

在计划和采购阶段，分析采购需求、供方产能和采购周期等基本信息；在生产、交付和逆向阶段，关注供应弹性和关键下阶材料。结合内外部环境，前瞻洞察、平衡供需、动态调整，构建健壮智慧的供应链计划大脑，提升对需求波动的预判能力。

免疫能力

在采购环节，材料规划与产品规划同步开展，推广优选物料、管控独家供应和输出替代方案，规划资源储备。持续优化长周期物料管理和多地仓储机制，与优质供应商开展战略合作，协同上下游确保供应的连续和稳定。

在制造环节，建立产能风险扫描机制，通过布局多制造基地共享生产资源、统一调度、产能互备，保障生产连续。公司在深圳、河源、长沙、南京、西安设有五大生产基地，配合外协工厂资源，通过灵活的产能调整和弹性生产，满足产能需求。

在货运环节，公司在全球有超 5 万条运输线路，通过多重货运方案备份，保障物流交付的连续与稳定。借助数字化的货运风险地图，实时预警货运风险，监控在途风险、常见风险、塞港情况等。

适应能力

搭建数字化平台，包括供应资源风险地图、智能制造中心、货运风险地图等系统，整合核心数据，识别分析异常点，精准定位并提效改进。实现采购、制造、货运、关务各个业务全疆域可视，使业务看得见，看得清，看得准。

7 安全交付

随着产品交付给客户，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产品和维保服务交付的完整性、机密性和可用性，实现端到端的安全。

7.1 安全交付策略

中兴通讯交付领域参考 NIST CSF 安全风险管理框架、ISO 27001 等业界安全标准、最佳实践、以及客户的网络安全诉求，在全球建立了基于风险的交付安全治理体系，将一系列规范要求融入网络规划、开通、验收和运维阶段，确保交付行为安全可靠、网络设备安全运行、客户网络数据得到安全保护。

图 7 中兴通讯端到端交付安全保障

7.2 安全交付实践

中兴通讯安全交付涵盖人员管理、授权管理、软件部署、网络变更、安全核查、远程接入管理、数据保护和事件响应等模块。中兴通讯基于 AI、大数据等技术实现交付全流程指标可视化，及时识别与跟踪风险，协助客户网络安全、稳定地运行。

人员管理

中兴通讯定期对工程师进行综合安全评估、定岗定级。项目交付中，根据人员评估结果进行岗位适配，按照客户要求分配操作权限，并签署保密协议（NDA）。结合开局、运维、巡检、故障处理、安全加固等日常工作，公司对交付人员进行安全赋能，包括专题课堂、专业研讨、实战演练、技能比武等。

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、安全巡检，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，具体操作行为可通过日志进行追溯。

软件部署

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，仅授权人员才能从技术支持网站（support.zte.com.cn）下载所需版本或补丁，历史下载均有记录，且下载的软件会在升级前进行完整性检查或数字签名验证。软件部署所需的工具和软件均从指定渠道获取， 并要求接入客户网络的个人工作终端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、与业务目的有关且无信息安全风险的软件等。

网络变更

在获取客户网络变更的授权后，中兴通讯工程师在网络变更管理系统（ZXRDC）提交具体实施方案，并在方案通过产品专家评审后，在规定的时间和范围内完成变更操作。为确保网络变更后业务的稳定运行，相关人员会进行一段时间的值守，对特定指标进行观察、记录与分析。接入客户网络的个人工作终端部署了智能管控工具，能够实时拦截高危指令和非预期动作，进一步降低网络变更的风险。

安全核查

产品在研发阶段已考虑了“开箱即用”的默认安全，但随着内外部威胁的变化，产品的安全风险也会相应变化。中兴通讯基于合同要求定期进行安全核查，结合安全态势感知系统，以及客户的漏洞扫描和渗透测试结果等，对风险进行识别、评估和处置。

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，允许产品专家通过全球一张网系统（Advanced Operations Suite, AOS）和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。

数据保护

在遵循当地法律法规以及客户要求的前提下，中兴通讯执行对重要、敏感的网络数据的安全保护操作，如脱敏、加密存储与传输等。在实施 GDPR 或类似法规的国家和地区，公司与客户在合同签署阶段，签署数据处理协议和数据转移协议，明确个人数据保护条款、责任界面；合同期内，工程师按照合同条款执行各项业务操作；特殊情况下，如返修的故障板件含有个人数据，工程师会根据数据保护的合同要求，进行相应操作。

事件响应

为有效应对可能发生的网络安全事件，中兴通讯根据项目场景制定安全方案和应急响应计划，项目组定期与客户、产品团队和第三方合作伙伴进行跨团队、跨地域的联合应急演练。

中兴通讯接收到客户安全事件后，PSIRT 会立即在全球客户支持中心创建事件单并分发到对应的产品支持团队，确保各严重等级的安全事件在客户服务水平协议（SLA）约定时间内得到解决。

8 安全事件响应和漏洞管理

在日趋复杂的供应链环境中，对安全事件和漏洞的良好管理变得愈发重要。欧盟《NIS2 指令》出台重点措施以增强供应链安全，包含事件响应、漏洞处理和披露。欧盟《网络弹性法》要求数字产品制造商报告已被主动利用的漏洞。中国出台了《网络产品安全漏洞管理规定》，要求网络产品提供者履行相关安全漏洞管理义务。

安全事件响应和漏洞管理有赖于利益相关方的协同处理，设备供应商有责任和义务协助客户处置安全事件、及时消减安全漏洞。中兴通讯 PSIRT 负责响应公司产品安全事件、处置公司产品安全漏洞。中兴通讯是事件响应安全团队论坛（FIRST）成员和 CVE 编号颁发机构（CNA），发布了安全漏洞奖励计划，鼓励全球安全从业人员和机构反馈中兴通讯产品存在的安全漏洞。

8.1 安全事件响应流程

中兴通讯协助客户第一时间响应安全事件。在客户授权下，PSIRT 协助客户迅速对事件进行处置，采取必要措施控制事态发展，直到业务彻底恢复。

安全事件响应流程包括四个阶段：

1. 准备工作：制定事件响应计划并定期演练，配备工具和资源；
2. 检测分析：收集、记录和分析与事件相关的数据，确定是否发生入侵并产生后果，分析影响范围，包括受影响版本和受影响客户。如事件由安全漏洞引发，则启动安全漏洞管理流程；
3. 抑制、消除和恢复：实施缓解方案，抑制事件影响，防止继续扩散；提供解决方案，消除事件影响，恢复正常业务；
4. 事后活动：组织复盘，总结经验，持续提升事件响应能力。

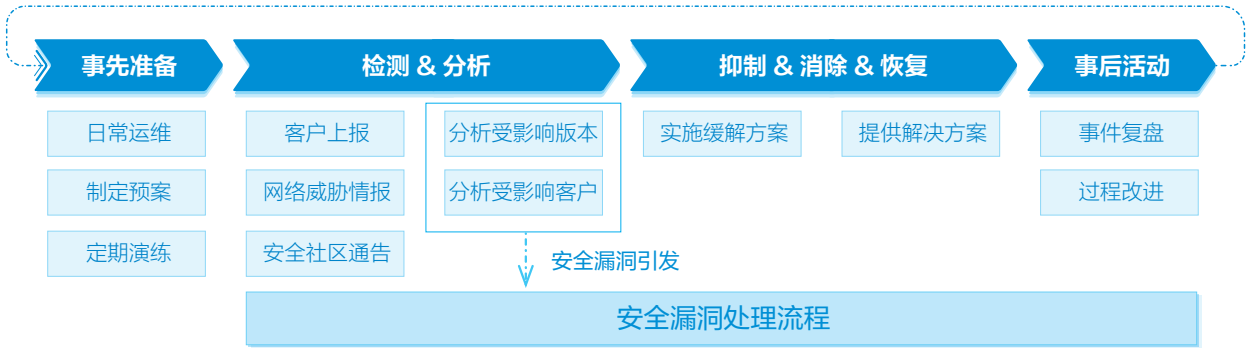

图 8 中兴通讯安全事件响应流程

8.2 安全漏洞处理流程

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进行负责任的披露。在客户实施解决方案之后，对方案的有效性进行监控，根据反馈情况进行方案迭代，实现漏洞闭环管理。

安全漏洞处理流程包括五个阶段：

1. 接收：接收来自客户、供应商、开源社区、安全团体和公司内安全测评发现的漏洞；
2. 分析验证：验证漏洞、分析影响、评估风险；
3. 开发方案：确认产品受漏洞影响后，提供缓解措施和解决方案；
4. 披露和修复：与漏洞报告方和波及客户保持沟通、实时通报进展，协助客户修复漏洞，完成漏洞协同披露；
5. 复盘：从管理、技术等维度总结改进，提升漏洞处理效率和质量。

图 9 中兴通讯安全漏洞处理流程和支撑系统

9 信息安全和隐私保护

9.1 信息安全

信息安全管理的目标是保护公司信息资产的机密性、完整性和可用性，为公司产品研发、生产、运营等关键业务提供安全的环境。中兴通讯建立了分级的、完备的和闭环的信息安全管理体系，防泄密，防入侵，一旦发生信息安全事件能快速响应，将损失降到最低，以保障公司战略目标达成和业务活动顺利进行。

图 10 中兴通讯信息安全管理体系框架

基于ISO 27001信息安全管理体系标准架构和要求，遵循业务所在地法律法规、遵从行业标准，公司通过“定、管、查”对信息分级管控、闭环管理。定，是识别管理对象，从而聚焦核心资产，实现分级管控，保障安全，兼顾效率；管，是管控信息流本身，关注信息流相关的人、事、物等要素，达到信息安全管控效果；查，是对体系符合性进行检查改进，对信息安全事件进行调查处置。

中兴通讯将生产经营活动中产生、收集和接收的信息，分为绝密、机密、内部使用、对外公开四个密级。业务活动中访问、处理的客户信息，对应至相应的密级进行分级管理，运用存储和传输加密、身份验证等技术方法，确保业务活动中运营信息和技术信息得到充分的安全保护。

2005 年，公司成为国内首个获得 ISO 27001:2005 信息安全管理体系认证的上市公司，截至 2023 年，公司总部及全球附属公司共获得 27 份 ISO 27001 认证证书。中兴通讯不断学习先进的管理理念，探索具有企业自身特点的信息安全管理模式，以应对全球数字化带来的信息安全挑战。

9.2 隐私保护

中兴通讯遵守业务所在国家和地区隐私保护法律法规，将“法律遵从、信任共建、道德履行”作为隐私保护的重要基线。中兴通讯通过隐私保护体系建设、重点场景隐私保护管控、隐私保护实践探索等方式，践行“满足法律要求、防控业务风险、赢得市场信任、共建良好生态”。

中兴通讯以风险为导向，从组织、人员、制度、技术等维度开展全面的体系建设，并在体系运行过程中，不断优化迭代，保持隐私保护体系的适配性、有效性、先进性。公司建立了场景化的业务流程合规指引，构筑了合规稽查、数据保护和业务单位三道风险防线，并针对各类高风险场景构建了管控机制，守护用户、客户及员工数据和隐私安全。公司建立了数据泄露响应流程、数据主体权利响应流程、数据跨境传输管控流程、供应商合规管控制度等数据保护合规机制。

中兴通讯遵循隐私保护设计（PbD）理念，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，使数据保护要求默认集成至产品和服务中，确保数据处理满足合法、公平、透明等原则。

中兴通讯秉持开放、透明的数据合规理念，在中兴通讯官网上线了隐私中心[9]，面向全球客户、合作伙伴、消费者等相关方展示隐私保护建设、提供隐私保护反馈窗口。

9. *https://www.zte.com.cn/china/privacy_center.html*

10

业务连续性管理

中兴通讯持续构建业务连续性管理（BCM）能力，以保障连续交付产品和提供服务能力为宗旨，运用体系化框架和方法论，构建了应急响应和复原能力，并通过了 ISO 22301 业务连续性管理体系认证。

中兴通讯产品研发的业务连续性管理面向业务解决方案和基础设施解决方案，产品设计和方案设计默认考虑设备和网络的备份方案和容灾能力；对于研发资源布局和研发云建设，定期刷新高风险点，针对独家供货、关键 IT 系统、核心实验室、病毒攻击等高风险场景开展治理。中兴通讯各地研究所具备快速部署远程办公能力，保障核心业务开展。

供应链的业务连续性管理面向采购、制造和货运业务流程，运用智能供应管理系统实现全业务的监测、预警、联动和调度，保证采购供应、生产制造和物流交付的连续性和稳定性。

交付的业务连续性管理包括工程交付及网络服务两个方面，为了保障全球客户在建及运维网络的业务，公司形成了一套从预警预防、预案演练到事件处置及复盘的管理流程。

11 开放 合作 融入

11.1 网络安全实验室

为了让客户、监管机构和利益相关方能够便捷、有效、透明地对中兴通讯产品和服务进行独立安全测评，公司在中国南京、意大利罗马和德国杜塞尔多夫设立了三个网络安全实验室，在比利时和土耳其设立了两个网络安全透明中心。

网络安全实验室是客户评估和验证中兴通讯产品、服务、过程安全性的平台。实验室能够支撑包括源代码查阅、核心文档查阅、黑盒测试、渗透测试、技术交流和分享等活动。自成立以来，实验室多次接待国内外重要客户和机构开展技术交流和安全审计。以意大利网络安全实验室为例，我们的客户借助实验室对多个产品进行了渗透测试和源代码审计，包括 5G、家庭终端和手机等产品，其中一部分是在意大利国家高校电信联盟（CNIT）[10] 的独立监督下进行的。中兴通讯还参与意大利及欧洲安全组织举办的活动，与本地安全社区共享交流，共同提升网络安全水平。

区别于网络安全实验室，网络安全透明中心在缩小规模的基础上可满足源代码查阅和文档查阅的要求，便于客户、监管机构和利益相关方检验中兴通讯产品的安全性。

11.2 测评和认证合作

中兴通讯持续对标行业安全标准，积极获取行业认证。

2022 年 6 月，中兴通讯 5G NR 和 5GC 系列产品通过了 GSMA NESAS 2.1 版本的“供应商开发和产品生命周期流程的安全评估”，成为全球首家通过 GSMA NESAS 2.1 的移动网络设备供应商。

2023 年 1 月，中兴通讯 5G NR gNodeB 产品获得由德国联邦信息安全办公室（BSI）颁发的“网络设备安全保障方案网络安全认证计划 – 德国实施”（NESAS CCS-GI）认证证书。中兴通讯作为首家获得 NESAS CCS-GI 证书的 5G 设备供应商，在认证过程中完全符合流程要求和安全规范。通过本次认证，中兴通讯既充分证明了其产品安全治理和 5G NR 产品满足德国严格的安全标准，也为德国 NESAS CCS-GI 认证的发展做出贡献。

10. 非盈利组织，由 37 所意大利公立大学参与组成。

中兴通讯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。中兴通讯还持有中国网络安全审查技术与认证中心（CCRC）信息安全风险评估一级、CCRC 信息系统安全集成服务一级、中国国家漏洞数据库（CNNVD）一级技术支撑单位等资质。同时，公司承载 OTN 全系列产品通过 CC EAL3+ 认证，数字能源通过 IEC62443 工控网络安全认证，终端通过 ePrivacy 隐私保护认证，云服务通过国家信息技术服务标准（ITSS）认证、固网终端产品通过 Wi-Fi EasyMeshTM R3 认证、公司研发云获得 SaaS 安全能力检验证书。

中兴通讯不断提升产品安全，以开放透明的态度迎接客户和机构的安全评估。

11.3 安全标准贡献

网络安全标准化是实现网络高速、安全发展的基础，是实现通信网络互操作性和开放性的前提。相较于以前的通信网络，5G 网络对网络安全提出了更高的要求。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。标准组织联合通信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，中兴通讯积极参与标准化制定工作并在多个标准组织中担任各项职务。在中国通信标准化协会（CCSA）的网络与数据安全标准技术工作委员会中，中兴通讯担任网络安全组组长，并在安全基础及产业支撑组、新兴技术和业务安全组和网络关键设备子组等工作组担任副组长，围绕信息通信网络与数据安全、融合新兴技术和业务安全，深度参与多项通信行业标准及国家标准的制定；另外，在工业互联网标准技术工作委员会中，中兴通讯担任副主席，并在包括安全工作组在内的多个工作组担任副组长，积极参与工业互联网的安全框架与管理体系、工业互联网数据相关安全要求和工业互联网安全保障平台要求等标准制定，促进工业互联网标准与产业的协调发展。同时，中兴通讯在全国信息安全标准化技术委员会 TC260 牵头的鉴别与授权、通信安全、信息安全评估、信息安全管理和大数据安全等国家标准制定中做出积极贡献。

中兴通讯广泛参与 3GPP、ITU-T、ETSI、GTI、GSMA 等国际主流的标准组织。在 3GPP 中，中兴通讯担任 3GPP RAN3 工作组主席和 CT4 工作组副主席，在 3GPP SA3 安全标准工作组中担任 5G 应用安全项目 AKMA_GBA_DTLS 的项目报告人。该项目主要面向未来物联网、5G 消息等 5G 应用业务，将进一步降低未来 5G 应用和终端 UE 之间的端到端认证和密钥获取的配置的复杂度，促进 5G 应用的商用部署。在 ITU-T 中，中兴通讯担任 FG-ML5G 及 FG-AN 网络架构组主席，在 SG17 网络安全工作组中牵头并参与多项标准的制定。此外，中兴通讯在 ETSI 产品安全标准、GTITD-LTE 技术安全标准、GSMA 安全认证相关标准的制定中也发挥了重要作用，为推动网络安全标准做出积极贡献。

附录

中兴通讯网络安全大事记

2005	中兴通讯通过 ISO 27001 信息安全管理体系认证。截至 2023 年，公司总部及全球附属公司共获得 27 份 ISO 27001 认证证书。
2011	中兴通讯 ZXR10 3900 通过信息技术安全评估通用标准 CC EAL3 级认证。
2012~2017	中兴通讯 11 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。
2014 起	中兴通讯发布企业标准《产品安全要求总则》并定期更新，确立公司级产品安全策略，提供产品安全治理的顶层要求。
2015	中兴通讯成立产品安全委员会（CSC），2019 年再次调整，由公司高层组成的 CSC 提供产品安全最高决策，安全保障的组织部署贯穿各业务管理层。
2017	中兴通讯获得 ISO 28000 供应链安全管理体系认证，覆盖 35 大类电信产品的采购、制造及物流业务。
2017	中兴通讯获得海关 AEO 贸易安全认证。
2019	中兴通讯发布《中兴通讯产品安全白皮书》，表明公司开放透明的网络安全立场。
2019	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	中兴通讯获得 ISO 22301 业务连续性管理认证。
2020~2021	中兴通讯人力资源管理和多个产品（5G NR、UME、核心网、数字技术产品、终端产品）获得 ISO 27701 隐私信息管理体系认证。

2020	中兴通讯的 5G NR 和 5GC 融合核心网系列产品通过 GSMA NESAS“供应商开发和产品生命周期流程的安全评估”。
2020	中兴通讯获得 CCRC 认证的信息安全风险评估服务一级资质。
2020 起	中兴通讯持续发布企业标准《产品安全规范 安全设计指导书》系列文档，明确公司产品安全设计应遵循的规范和技术要求。
2021	中兴通讯 5G NR、5GC 和 Flexhaul 产品高分完成 BSIMM 评估，软件成熟度全球领先。
2021	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	中兴通讯的 5G NR 和 7 个 5GC 网络设备成功通过 GSMA NESAS 网络设备产品安全评估。
2022	中兴通讯成为全球首家通过 GSMA NESAS 2.1 过程评估的移动网络设备供应商。
2022	中兴通讯获得了欧洲 ePrivacy 和美国 TRUSTe 两大国际权威隐私保护认证。
2023	中兴通讯 5G NR 产品获得由德国 BSI 颁发的 NESAS CCS-GI 认证证书。中兴通讯是首家获得该证书的 5G 设备供应商。
2023	中兴通讯承载 OTN 全系列产品通过 CC EAL3+ 认证，获得认证的产品包括 ZXONE 9700/19700 系列、ZXMP M721 系列和 ZXONE 7000 系列等 10 款主流设备。
2023	数字能源网管产品通过 IEC62443 工业互联网安全认证。

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