ZTE中兴

中兴通讯产品安全白皮书

为客户提供端到端产品和服务的安全保障

安全融入血脉 透明增进信任

中兴通讯首席安全官：**钟宏**
中兴通讯股份有限公司
2019 年 3 月

作者

本白皮书描述了中兴通讯对网络安全的原则立场、产品安全战略和实践，由许多同事共同完成。

在此，要感谢对本文档做出重要贡献的人：

曹鲲鹏、程军华、池逸飞、高瑞鑫、何英、华国红、李荣坤、刘日昇、刘岩、刘艳、龙浩、马致原、孟朱丽、聂永立、平立、宋伟强、王华刚、王琳、王玉忠、韦银星、徐国荣、杨铁建、张灿、张杰、张锐、赵善红、郑均、周继华，以及其他直接或间接对本白皮书做出贡献的人。

钟宏 中兴通讯首席安全官

目录

序言 04

执行摘要 05

中兴通讯产品安全战略 08

端到端的产品安全实践 13

基于三道防线的产品安全治理架构 14

产品安全规范体系 16

研发安全 17

研发安全流程和组织 18

概念阶段 19

计划阶段 19

开发阶段 20

测试阶段 20

发布阶段 21

第三方组件安全治理 21

持续安全交付 21

供应链安全 22

供应商及材料管理 23

生产制造及返修安全 25

仓储物流安全 26

交付安全 27

交付安全的三个阶段 28

第三方合作伙伴管理 29

信息安全 30
信息定密 31
人员安全 31
物理安全 31
IT 安全 32

个人数据保护 34
数据保护合规体系 35
数据泄露响应机制 36
数据保护方案实践 36

安全事件管理 37
产品安全事件响应机制 37
产品安全漏洞处理流程 38

业务连续性管理 40
研发过程业务连续性管理 41
供应链业务连续性管理 41
工程服务业务连续性管理 41
IT 系统业务连续性管理 41

独立安全测评 42
独立安全测评控制机制 42
独立安全测评过程 43
独立安全测评技术 43

安全审计 44

网络安全实验室和外部合作 45

展望未来，共同前进 46

附录：中兴通讯产品安全大事记 48

序言

网络空间几乎渗透到社会的方方面面，与人类的生活息息相关。网络空间是一个开放的舞台，由于网络威胁和防御的不对称性和网络空间固有的脆弱性，网络空间容易受到攻击和破坏。网络安全关系到每个依赖于这个庞大网络的系统和个人，受到世界各国政府、运营商和用户的广泛关注。

电信设备和系统是网络空间中一项关键基础设施，作为全球综合通讯解决方案提供商，中兴通讯在网络安全方面的原则和立场如下：

安全是中兴通讯产品研发和交付的最高优先级之一，中兴通讯根据公司发展战略规划，参考适用的法律法规和国际国内标准，建立健全的产品安全治理结构，培养全员安全意识，强调全流程安全。中兴通讯重视客户的安全价值，遵从网络安全的相关法律法规，保证端到端交付安全可信的产品和服务。

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，共同建立安全的网络环境，维护良好的网络空间安全秩序。

执行摘要

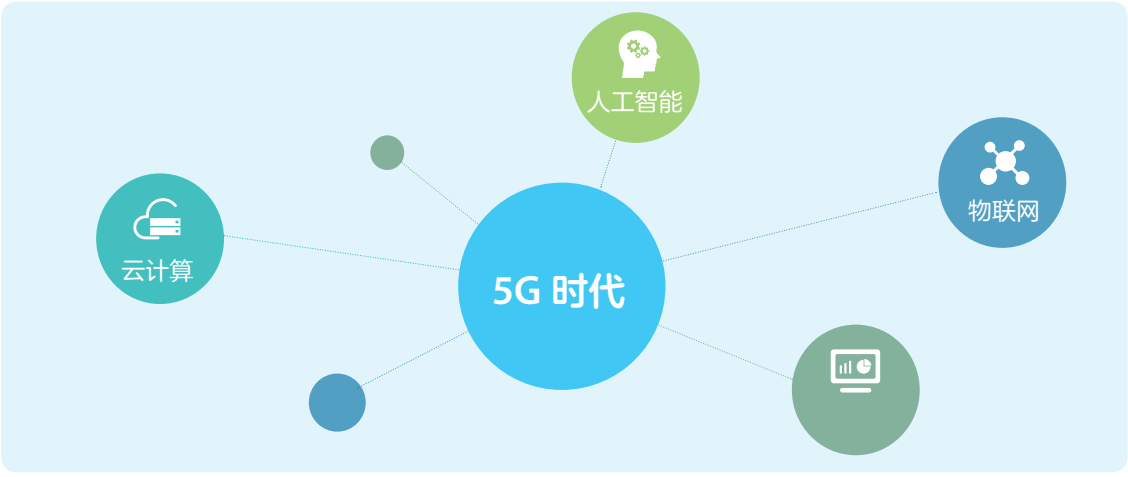
5G 时代已经开启，云计算、物联网、大数据、人工智能等技术得到越来越广泛的应用。新技术应用在带来新一轮的产业变革的同时，网络安全形势越发严峻。

中兴通讯坚持开放、透明和信任的态度，以自顶向下的方式开展产品安全治理工作。

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。新技术应用在带来新一轮的产业变革的同时，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《2018 数据泄露调查报告》[1] 深入挖掘了全球多个行业的网络安全状况，报告了在 2018 年超过 5.3 万起网络安全事件和 2216 起经证实的数据泄露；另一方面，信息系统存在大量的安全漏洞，截止 2019 年 2 月底，公开批露的 CVE 漏洞达 112364 件 [2]，严重漏洞占 13.5%，高危漏洞占 23.0%。

电信设备和系统是网络空间中一项关键基础设施，由于安全威胁和防御的不对称性和系统固有的脆弱性，电信基础设施容易受到攻击和破坏，系统面临着巨大的安全风险。各国政府和运营商对产品安全存在担忧，如：产品完整性、后门、供应链安全、个人数据保护等。

中兴通讯坚持开放、透明和信任的态度，以自顶向下的方式开展产品安全治理工作。中兴通讯构筑三道防线安全治理结构，将安全策略融入到产品生命周期的每个阶段，建立覆盖产品研发、供应链与制造、工程服务、安全事件管理和独立验证审计等领域的产品全生命周期的产品安全保障机制，通过产品安全的基线化、流程化和闭环化，实现产品和服务的端到端的安全交付。



[1] https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf

[2] https://www.cvedetails.com/

高层领导重视和承诺

中兴通讯重视客户的安全价值，遵从网络安全的相关法律法规，保证端到端交付安全可信的产品和服务。安全是中兴通讯产品研发和交付的最高优先级之一，中兴通讯根据公司发展战略规划，参考法律法规和国际国内标准，建立健全的产品安全治理结构，培养全员安全意识，强调全流程安全。

产品安全方针

中兴通讯的产品安全保障计划坚持六点方针：有规范，严执行，强监管，能追溯，全透明，可信赖。

有规范：尊重规则和规范，根据适用的法律法规和国际国内标准，制定一系列产品安全的策略、标准、流程和指导书。

严执行：各业务部门的日常工作均按照规范严格执行，通过问责制和发布“产品安全红线”加强执行的力度。

强监管：通过三道防线治理模型进行强有力的监督和管理。

能追溯：所有安全活动都做到有记录可查询，有证据可追溯，快速发现和定位问题。

全透明：公司的安全活动向客户、政府和利益相关方公开，客户可参观、代码可审查。安全问题披露透明公开，漏洞和补丁及时发布。

可信赖：通过开放透明的安全治理活动以及第三方安全认证，增进客户的信任。

三道防线治理架构

在组织架构方面，中兴通讯采用三道防线治理架构，从多角度保障产品及服务的安全性。各业务单位作为第一道防线实现产品安全性的自我管控；公司产品安全部作为第二道防线实施独立的安全测评和监督；公司内控审计部作为第三道防线评估与审计第一、第二道防线运作的有效性，同时公司接受客户和外部第三方独立机构的安全审计。

安全人才队伍建设

中兴通讯组织了多种层面的产品安全意识和专业技能培训，如高层研讨会、管理干部读书班、全员培训、安全设计培训、渗透测试培训和安全编码比赛等，推动了公司产品安全能力提升，形成了公司产品安全文化。

中兴通讯重视安全人才队伍的专业化，公司目前有 30 余位持有国际安全认证的人员，如 CISSP、CISA、CSSLP、CEH、CCIE、CISAW、C-CCSK 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。

端到端的安全交付

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。中兴通讯的安全治理覆盖研发、供应链、工程服务、事件管理和各支撑职能。对产品研发来说，包括安全需求、安全设计、安全编码、安全测试、安全交付、安全运行维护等阶段的安全控制，同时考虑第三方组件安全。对供应链来说，涉及到采购、生产、制造、仓储、运输直到交付给客户。

产品安全事件响应

中兴通讯产品安全事件响应团队（PSIRT）负责识别和分析安全事件，跟踪事件处理过程，与内部和外部相关方密切沟通，及时披露安全漏洞，以减轻安全事件带来的不利影响。作为事件响应和安全团队论坛（FIRST）成员和 CVE 编号颁发成员（CNA），中兴通讯以公开的方式与客户及相关方进行协同。

独立测评验证

在三道防线的组织架构下，独立安全测评属于第二道防线，负责对一线安全实践进行评估和监督。通过应用风险控制的原则，从多个角度审核产品的安全性。通过监督与制约机制进一步降低安全风险，对发现的问题实施闭环管理跟踪，直到问题解决，实现产品安全治理的持续改进。

安全审计

中兴通讯的安全审计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，以组织与运作、风险管理过程、控制活动、内部监督等维度开展，覆盖产品安全总体治理、研发安全、供应链安全、交付安全、安全事件响应、独立安全测评等端到端的产品安全保障全流程，实现产品安全体系的可监管、全透明管理。

第三方安全认证与合作

2005 年，中兴通讯通过 ISO 27001 信息安全管理体系认证审核，并每年持续更新，所覆盖的范围包括中兴通讯所从事的所有业务。2017 年通过 ISO 28000 供应链安全管理体系认证。通用准则（CC）认证是国际认可的产品安全认证，中兴通讯目前已有 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。

中兴通讯积极与多个第三方机构开展合作，对中兴通讯的产品进行安全测评，如源代码审计、安全设计评估和渗透测试。

中兴通讯产品安全的愿景是“安全融入血脉，透明增进信任”，目标是为客户提供可信赖的、端到端的、全生命期的安全保障。中兴通讯愿以公开和透明的方式与监管机构、客户、合作伙伴和其他利益相关方沟通与合作，共同创造良好的安全生态环境。

在本安全白皮书中，提出了中兴通讯的产品安全战略，描述了中兴通讯产品安全的愿景、使命、目标、战略和方针；介绍了中兴通讯端到端的产品安全实践，覆盖三道防线治理架构、研发安全、供应链安全、工程服务安全、信息安全、安全事件管理、业务连续性管理、独立安全测评和安全审计；最后回顾了中兴通讯在产品安全领域的里程碑事件。

中兴通讯产品安全战略

电信网络是一项关键国家基础设施，对运行在网络上的各项业务和公共服务至关重要。电信运营商、政府和用户对电信网络的安全非常重视，中兴通讯对安全也高度重视，制定了公司的产品安全战略，把安全作为公司产品研发和交付的最高优先级之一。

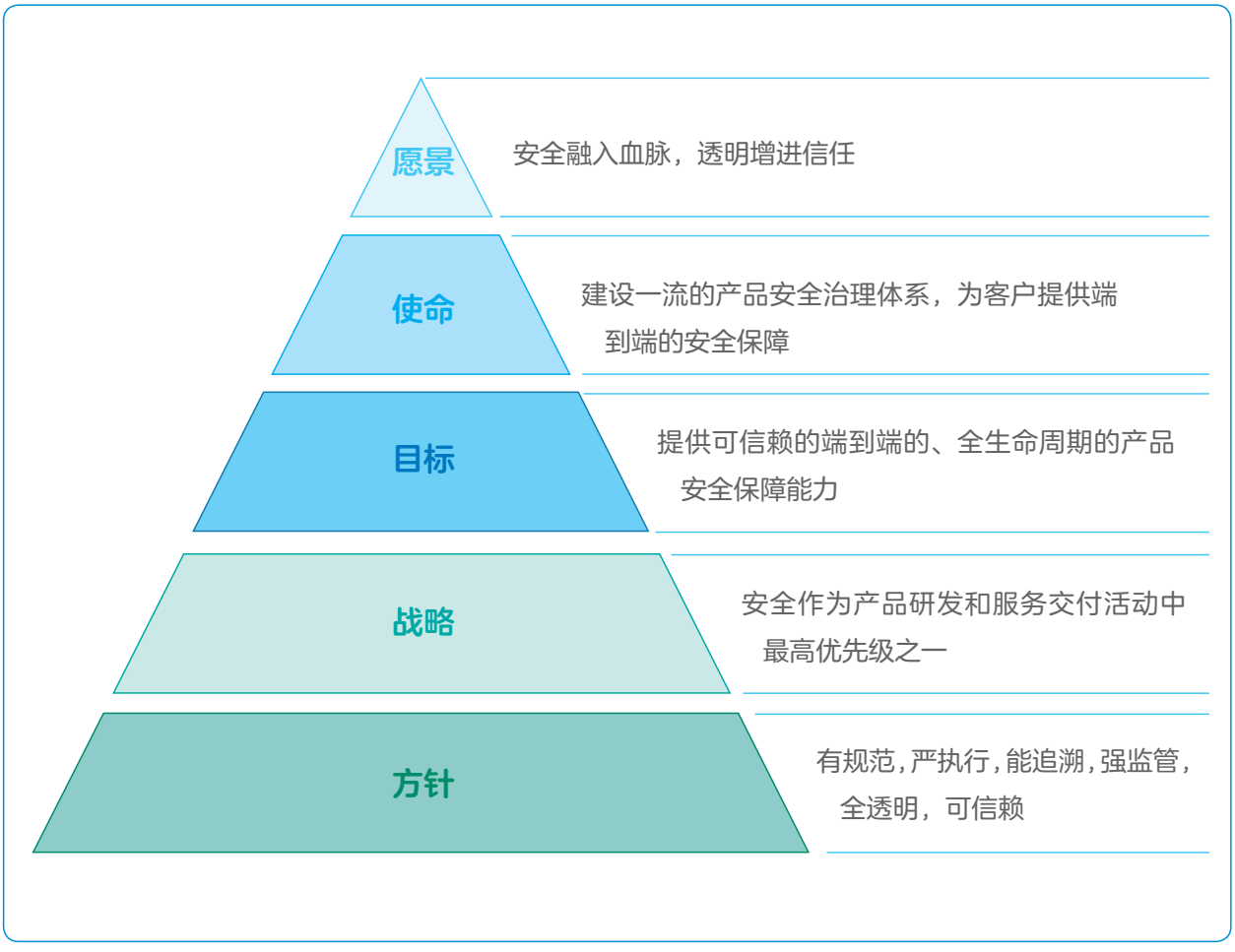


图 1 产品安全战略

愿景：安全融入血脉，透明增进信任

安全是产品和服务的一项内在属性，不是一项附加的特性，中兴通讯将安全有机融入业务、组织、流程、技术、意识和文化中。中兴通讯可以向客户呈现产品实现和过程保障的每个细节，愿意以公开透明的方式增进客户的信任，客户可以审查源代码和设计文档，可以了解实际运行的系统并进行检测，可以了解采用的安全控制措施。

使命：建设一流的产品安全治理体系，为客户提供端到端的安全保障

高级管理人员投入资源并自顶向下地从组织、人员、流程和技术等方面建设一流的产品安全治理体系，保证各项业务的安全有效开展，为客户提供端到端的安全保障。

目标：提供可信赖的端到端的、全生命周期的产品安全保障能力

遵循法律法规、安全标准和最佳实践，考虑客户的要求和期望，通过组织、流程和技术，来保护网络、设备、应用和数据等资产免受攻击、破坏或未授权的访问，实现已管理的产品安全。

建立健全的产品安全治理结构，建立起覆盖产品研发、供应链与制造、工程交付、安全事件管理和验证审计等领域的端到端、全生命周期的安全保障机制，构筑三道防线的产品安全治理结构，实现产品安全的基线化、流程化和闭环化，具备可信赖的产品安全交付能力，确保中兴通讯的产品安全可信。

树立客户对中兴通讯产品安全的信心，如：产品完整性、无后门、供应链安全、个人数据保护等。

战略：安全作为产品研发和服务交付活动中最高优先级之一

当产品安全与产品的功能要求或进度出现冲突时，优先考虑产品安全。在研发和工程服务过程中关键决策节点，当需要做出选择的时刻，我们会优先选择保障产品的安全性。

方针：有规范，严执行，强监管，能追溯，全透明，可信赖

有规范：尊重规则和规范，制定涉及每个产品，每个环节的安全策略和流程规范，而且是具体可执行的，行之有效的一套标准行为规范，形成一系列产品安全的策略、标准、流程和指导书。

严执行：各业务部门的日常工作均按照规范严格执行，通过问责制和发布“产品安全红线”加强执行的力度。

强监管：通过三道防线治理模型加强监督和管理，由监管部门进行流程审计，检查安全规范执行情况，审计结果和规范执行情况上报公司产品安全委员会。

能追溯：维护管理产品的组件和局点分布；所有安全活动都做到有运行记录；安全事件发生时能快速回溯和复盘，定位问题的根本原因。

全透明：公司的安全活动向客户、政府和利益相关方公开，客户可参观、代码可审查。安全问题披露透明公开，漏洞和补丁及时发布。公司筹建海外安全实验室，可以让客户现场审查中兴通讯产品的系统、源代码和技术文档。中兴通讯是 CVE 颁发机构，通过规范的漏洞披露策略让利益相关方知晓中兴通讯的安全漏洞处理过程。

可信赖：通过开放透明的安全治理活动以及第三方安全认证，增进客户的信任。中兴通讯与客户、第三方和监管机构紧密合作，持续开展源代码审计、安全设计评审、供应商审计等活动。

端到端的产品安全实践

中兴通讯遵循适用的法律法规要求、国际国内标准和安全最佳实践，吸收领先企业的优秀安全经验，结合公司的实际情况全方位持续改进安全实践，不断提升公司产品安全能力，向客户提供安全可信的产品。

基于三道防线的产品安全治理架构

中兴通讯建立了基于三道防线的组织架构来推进产品安全治理工作，一方面从组织机制上解决利益冲突问题，避免一线业务单位为了产品和服务的市场进度，而牺牲安全要求的风险；另一方面遵循风险控制的原则，通过业务单位的自我检查、第二道防线的独立安全测评、第三道防线的安全审计，从多个角度和多个层次保障产品的安全性。

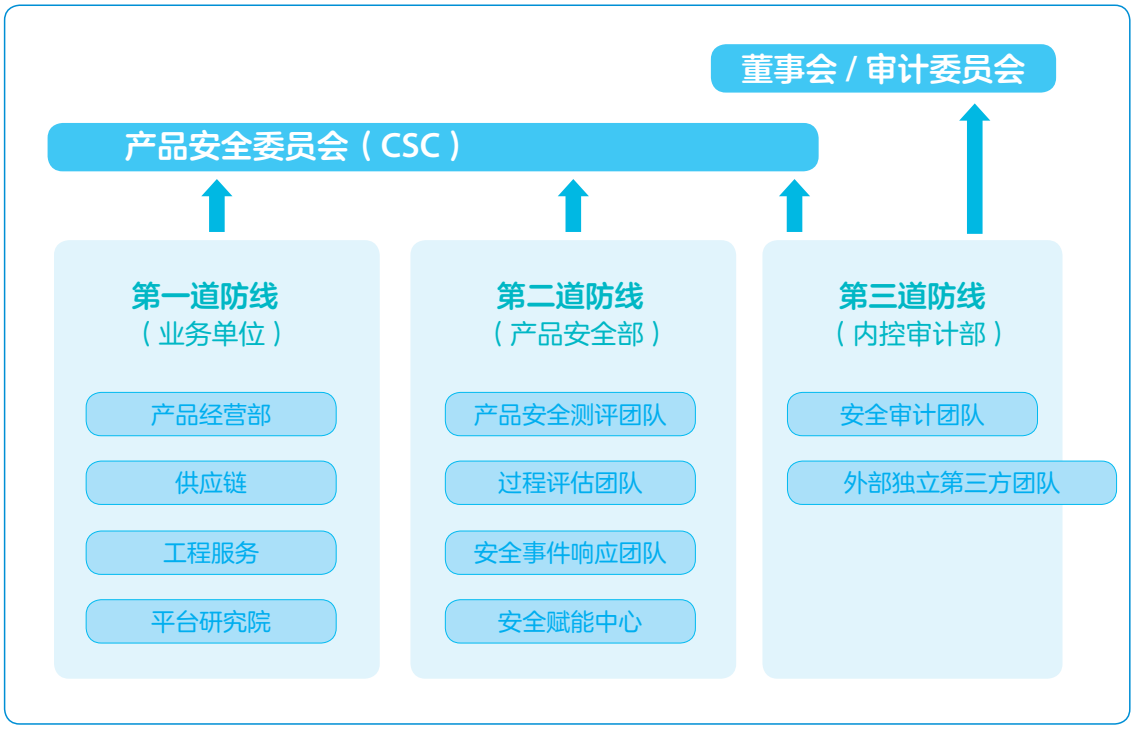


图 2 基于三道防线的产品安全治理架构

董事会 / 审计委员会

董事会授权产品安全委员会开展产品安全治理工作，董事会 / 审计委员会审核内控审计部提供的安全审计报告。

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等。

第一道防线（业务单位）

业务单位是产品安全治理的第一道防线。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。

第二道防线（产品安全部）

产品安全部是产品安全治理的第二道防线。产品安全部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、监督和评估第一道防线的工作。

第三道防线（内控审计部）

内控审计部是产品安全治理的第三道防线。内控审计部负责审计第一道防线和第二道防线的工作，包括流程执行的符合性检查和产品安全检测，向董事会 / 审计委员会汇报审计结果。内控审计部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。

产品安全治理还涉及一些其他支撑团队，如人力资源、财务、战略和投资、运营管理、公共事务、法务合规和行政物业等。

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，产品安全策略体系对产品安全治理提出了基本的要求，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

产品安全总则

该标准是公司产品安全大纲，主要内容包括产品安全的方针、目标、运作、组织、策略、流程和文件等，所有下层文件以此标准为基础。公司产品安全策略体系包括：总体治理策略、供应链安全策略、研发安全策略、交付安全策略、安全事件响应策略和安全审计策略。

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，包括从供应链到研发到交付、事件响应等一系列的安全规范和流程，如研发安全规范、供应链安全管理规范、工程服务技术交付网络安全管理规范、产品安全事件响应流程、安全编码标准等。

第三层

产品安全指导书

支撑规章和流程的文件，如安全工具使用指导书、安全基线编写指导书、安全加固指导书。

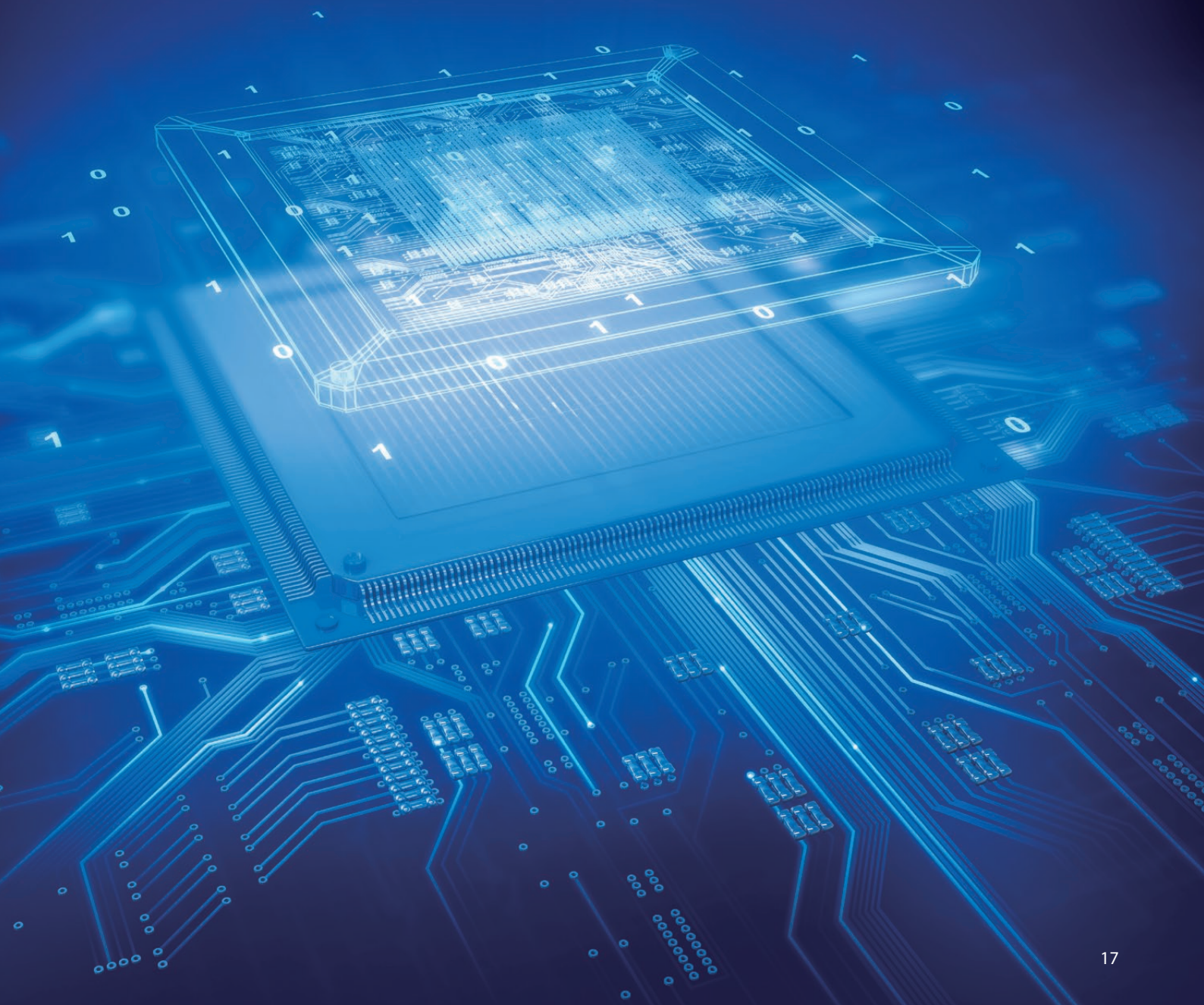
第四层

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。

研发安全

安全作为产品研发和服务交付活动中最高优先级之一，在追求高效研发的同时，我们更注重产品的安全，将“安全性”作为产品的一项基本属性融入到产品开发生命周期过程中，确保公司始终具备客户可信赖的产品安全交付能力，向客户提供安全的产品和解决方案。



研发安全流程和组织

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，为适应不同客户和市场竞争条件的要求，一直保持持续改进和演进。安全作为产品的一种基本属性，已融入到产品开发生命周期过程中。

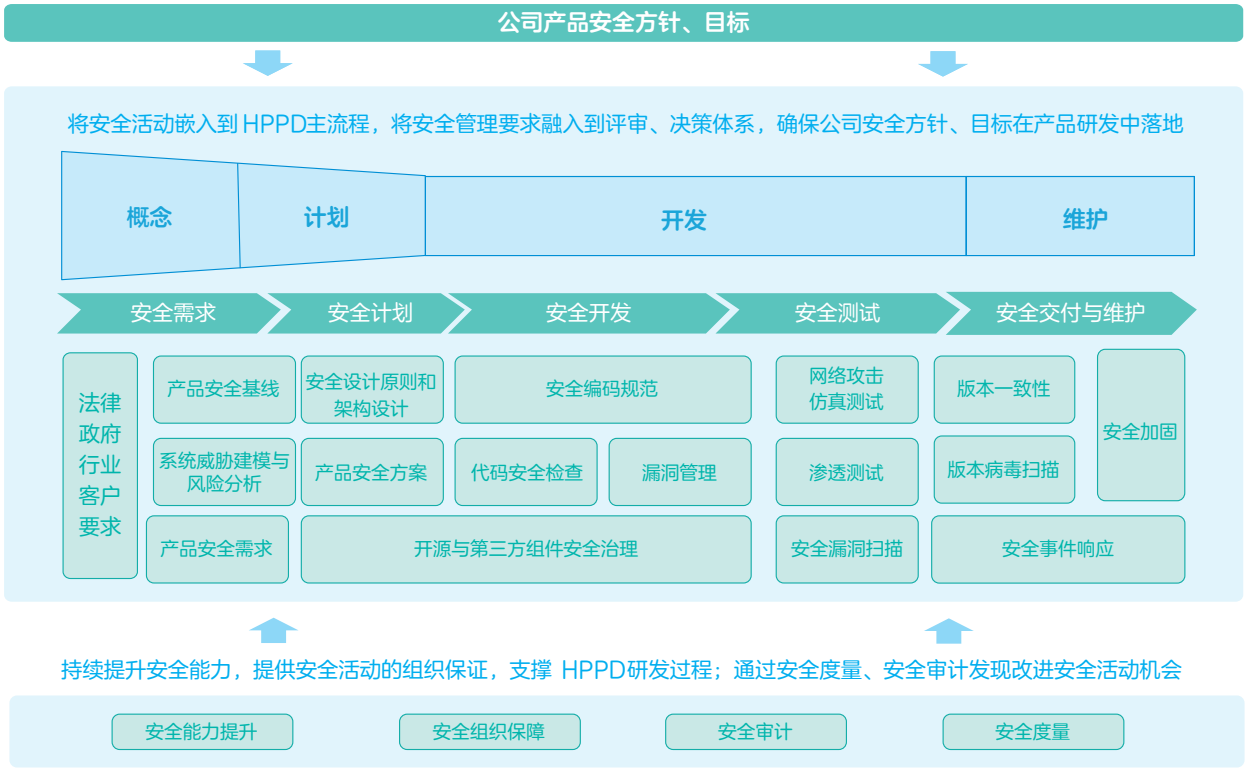


图 3 安全活动嵌入 HPPD 主流程

公司结合实际的研发活动，并参考业界安全实践模型，如 BSIMM[3]，微软 SDL[4]，在高效产品开发流程 (HPPD) 中定义了安全需求、安全计划、安全开发、安全测试、安全交付与维护等安全活动，确保安全特性有效地融入到产品中。同时，公司不断提升安全能力，为安全活动提供组织保障，从而有效支撑高效产品开发流程的运行。实施安全审计和安全度量，不断对高效产品开发流程的持续改进。

通过 HPPD 流程内嵌保证安全活动的有效落地，为向客户提供更安全的产品和解决方案，在端到端业务流程中融入安全要求，例如需求分析中的安全威胁分析，产品设计中的安全架构设计，产品开发中的安全编码及源代码安全扫描，产品测试中的安全功能测试及渗透测试，产品发布中的漏洞扫描、版本一致性保证等。

公司在产品研发安全组织保障方面，建立了以产品安全总监为核心力量的软件安全小组（SSG），在产品端到端过程中涉及的规划、研发（需求、设计、开发、测试）、供应链、交付、市场等主要团队的骨干均是通过威胁建模来理解安全需求，确保产品涉及的各领域的风险充分识别，问题得以快速解决。公司级产品安全委员会对产品安全问题重大风险、问题进行决策，授权 SSG 主管对产品安全总监进行业务指导。

[3] https://www.synopsys.com/software-integrity/software-security-services/bsimm-maturity-model.html
[4] https://www.microsoft.com/en-us/securityengineering/sdl/

概念阶段

在概念阶段，中兴通讯根据市场准入需求（法律法规及行业标准）、客户安全需求、竞争分析、行业活动、同行经验、特定信息保护、公司内部安全要求，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。

产品安全需求主要包括两部分，一是公司产品安全基线，作为最基本的安全需求强制执行；二是对产品在运营商网络或政企网络的应用场景进行评估风险，将相关的应对措施纳入安全需求。

计划阶段

在计划阶段，中兴通讯参考 ITU-T X.805、ISO 15408、3GPP 和 IETF 等安全规范和业界最佳实践，制定了产品安全设计规范。在此阶段，研发团队进一步细化安全需求，并依据产品安全设计规范进行产品的安全架构设计和特性安全设计。

分析系统的安全需求和潜在安全威胁，确定产品的安全架构和系统方案，确保系统方案满足市场和客户的安全要求。根据公司安全准入标准，由专业团队来验证供应商的关键物料的安全性，评估第三方的组件的安全性。

通过威胁建模来理解安全需求，在早期发现其他技术不能发现的问题并进行控制。参考业界最佳实践，如 ITU-T X.805，微软 STRIDE/DREAD，Synopsys ARA 等模型，建立了一套适合通讯产品的系统威胁建模方法 -SATRC[5]。

[5] SATRC: System, Asset, Threat, Risk, Control

开发阶段

在开发阶段，遵循安全编码规范要求，完成编码实现和安全文档开发，并对代码进行静态检查和自动化扫描。

安全编码和代码安全性检查

基于业界权威的安全编码规范，如 CERT（计算机安全应急响应小组）、OWASP（开放式 Web 应用程序安全项目）、CWE（通用缺陷列表）、STIG（安全技术实现指南），建立公司安全编码规范：C/C++/Java/Web 安全编码规范。同时，使用业界领先的源代码扫描工具，如：Klocwork、Coverity。对代码的质量、可靠性、安全漏洞、可维护性进行有效检测和识别，针对工具扫描出的问题采取有效的跟踪和管理措施，如 Klocwork 数据的看板化管理，随时监控缺陷遗留情况。

建立三层检查控制点机制，对代码进行三次扫描，分别是：个人构建自检；模块构建扫描；项目构建扫描，如未达成安全缺陷零遗留的目标，无法通过控制门。

测试阶段

制定安全测试规程和安全测试方案，设计并执行测试用例以验证安全功能模块，对产品进行漏洞扫描、协议健壮性扫描、渗透性测试，完成系统脆弱性分析。确定产品的安全加固实施方案，提供产品安全认证需要的证据。

发布阶段

产品确保经过多种主流杀毒软件检查无异常后发布版本。同时，从版本发布到用户部署以及运作维护过程中，进行必要的安全保护，保证版本的一致性。

使用混淆工具对软件版本进行保护，如采用重命名、字符串加密、虚拟代码插入、代码逻辑混淆等方式，使攻击者难以采用逆向工具直接获得原始代码，从而增强对设备的保护。

第三方组件安全治理

中兴通讯对需要使用的第三方组件实施全生命周期管理，从这些第三方组件的引入，直到作为产品的一部分向客户交付。将第三方组件的安全风险评估、安全测试、漏洞管理嵌入到 HPPD 流程中，确保在产品生命周期中，一旦发现安全漏洞，会对漏洞进行评估，并提供解决方案或者规避措施，传递给 PSIRT，快速解决所有与第三方组件相关问题。

中兴通讯建立组件广场，存储第三方组件，严格管控第三方组件的使用，确保开发人员只能从经认证的来源获取组件，同时集中保证第三方组件是合规的、安全的、最新的。我们将第三方组件作为配置项，纳入软件配置管理流程，确保可以追溯组件的使用。

中兴通讯加入开源社区，持续跟踪社区发布的漏洞，提交安全漏洞修复方案。积极为开源组件产品安全作出贡献。

持续安全交付

DevSecOps 持续安全交付由稳固的配置管理支撑系统和与开发流程相融合的 DevOps 工具链进行保障。

中兴通讯的配置管理系统保证了从客户的原始需求沿着流程的各个阶段进行追溯，从设计、软件编码、测试、质量保障、现网部署，以及反过来从现场发现的故障，一直追溯到最开始的源头，从客户的原始需求正向追溯到最终产品，并从最终产品逆向追溯到原始需求——覆盖所有步骤，所有流程，所有接触过该软件的人，所有部件，所有软件版本编号等。

同时，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、安全测试、漏洞扫描、版本保护等关键活动中，确保安全工具的高效使用，形成运维监控闭环。

中兴通讯对代码进行了信息安全风险识别并确定了控制举措。研发人员通过终端接入桌面云，访问研发云。代码在研发云内实现编译、单元 / 功能测试、评审，形成交付版本。并为代码和文档在桌面云、研发云之间的流动制定了响应的控制策略：如代码未经审批不能拷贝出云；桌面云通过白名单可以访问互联网，研发云不能访问互联网；个人终端可以访问互联网，不能访问研发云、IT 服务资源；参与外部社区开发，通过中转代码库；调试区进行 A 级区域管控等，有效确保代码在开发过程中安全受控。

供应链安全

信息技术是全球开放程度最高的产业，导致产业链全球分布，通讯设备提供商都不可避免的需要全球产业链上合作伙伴的支持，来自第三方的部件也可能存在安全风险，中兴通讯在供应商与材料管理、制造与返修、物流与仓储等可能出现产品安全风险的业务中采取了一系列管控措施，保障在这些业务活动中不引入、不产生、不流出安全缺陷，将自主研发设计的产品以及从第三方采购的配套材料安全地交付给客户。

中兴通讯把产品安全的要求嵌入到供应链的业务流程之中，包括：供应商及材料管理流程、制造及返修流程、物流、仓储及逆向物流流程等。

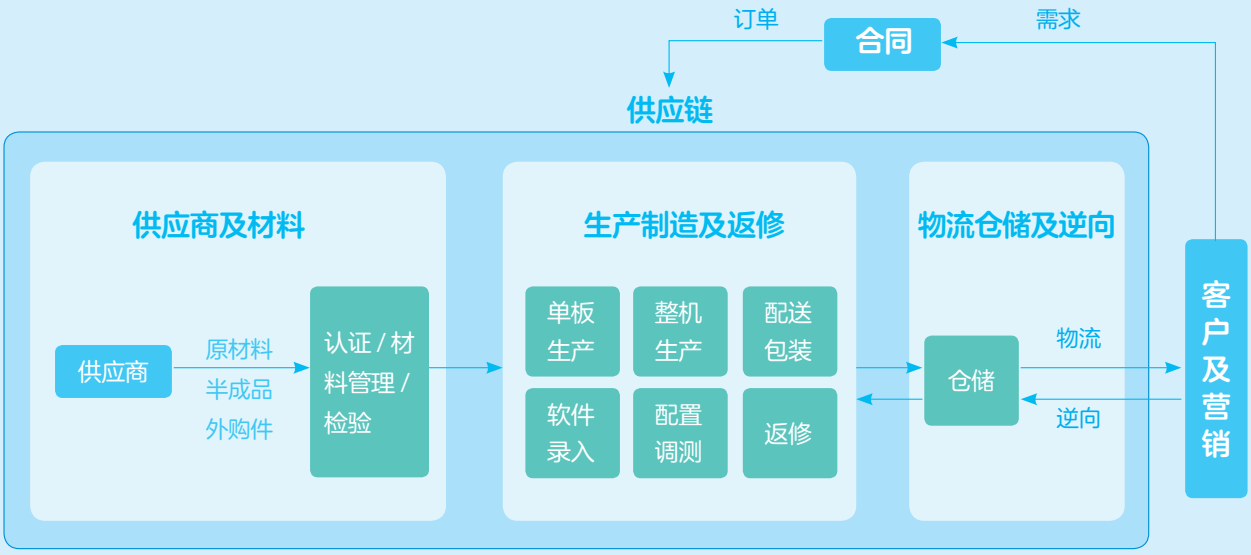


图 4 全球供应链管理流程图

供应链建立有专门的产品安全保障团队，识别供应链产品安全风险，健全并完善业务流程，制定有效的风险管控措施和安全事件响应机制，并通过持续改进的方法，保障公司产品安全管控措施落到实处，确保公司产品在供应链中的完整性、可靠性和可追溯性。

中兴通讯通过了 ISO9001 认证，加入全球电信业优质供应商联盟（QuEST Forum）并担任亚太区、大中华区联席主席。2017 年中兴通讯正式获得 ISO28000（供应链安全管理体系）和海关 AEO 贸易安全认证，供应链安全管理迈上了一个新台阶。

供应商及材料管理

中兴通讯致力于与合作伙伴建立长期稳定的合作关系，实施战略采购，不断扩展与战略合作伙伴的合作机会，形成互信、稳定、可持续的“共赢”关系。同时希望合作伙伴能够尽早地参与到产品研发和市场项目中来，共创价值。

设立了实践者社区（Communities of Practice），实践者社区提供了一个与合作伙伴全新的技术交流和产品安全交流方式，是一种正式学习与非正式学习相混合的学习环境。自 2017 年成立中兴通讯材料 COP 以来，与多家供应商一起，举办了线上、线下超过百余场的技术交流。2018 年我们还与多个合作伙伴举行过 CTO Day 活动，取得了很大成效。

中兴通讯实施战略采购，不仅仅体现在中兴通讯与单个供应商之间点对点的协同，我们希望将更多的合作伙伴以及合作伙伴的上下游联合起来，形成生态圈，通过标准、技术、产品、市场、商业模式等方面的创新与实践来发展壮大产业链，通过供应链协同规划、IT 系统对接、管理经验共享，优势互补，共同提升，形成更加紧密的战略合作关系。在 5G、物联网、大数据、人工智能等新兴行业，将与合作伙伴进行更加深入的合作。

供应商及材料管理是公司产品安全管理体系的一个重要组成部分。分布于全球各地不同行业、规模和文化的数千家供应商及合作伙伴，分工合作，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。

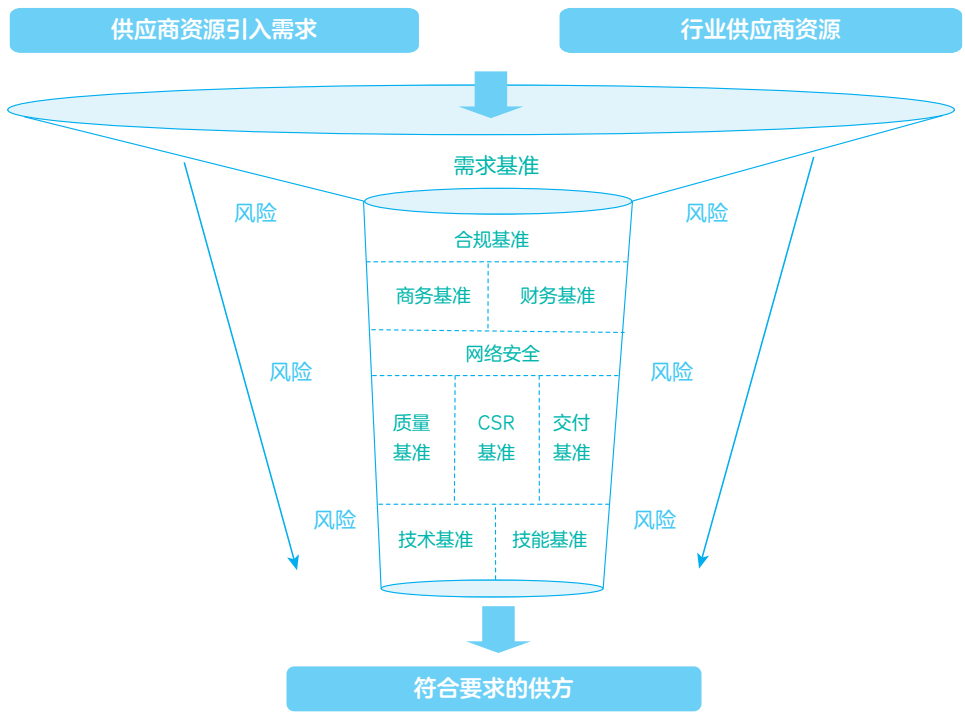


图 5 中兴通讯供应商准入机制

中兴通讯一直非常重视供应商管理制度建设，建立了一整套从寻源评估、到资质认证、再到淘汰退出的供应商全生命周期管理机制，包含产品安全管理、企业社会责任（CSR）管理、质量管理、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产品安全评估及其它诸多方面考察，通过综合评估，才能成为中兴通讯的合格供应商。

在材料管理方面，中兴通讯同样也有一整套业务管理流程。我们将材料的产品安全风险定义为高、中、低三个风险等级。高风险材料的产品安全测试在新材料引入和旧材料变更中进行。对于中低风险等级的材料，则通过与供应商签署产品安全协议的形式，要求供应商进行自我管理和约束，中兴通讯对该协议的实施情况，会组织定期或不定期的安全审计。

供应商对产品安全事件的响应是中兴通讯产品安全事件响应的重要组成部分。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与中兴通讯达成的产品安全协议，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。比如在安全测试和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进行追踪和定位，并及时提供补丁、升级、替换或召回等解决方案。

生产制造及返修安全

生产制造过程中的产品安全管理是公司产品安全管理体系的一个重要组成部分。基于供应链安全管理体系规范（ISO28000），中兴通讯建立了一套端到端的制造安全管控体系，覆盖了从来料检测、部件制造、整机组装、到成品包装和成品入库的整个过程，包括一系列流程文件、操作指导书和其它工作说明等文件，把产品安全规范的要求嵌入到制造业务流程之中。通过有组织的培训和学习，把产品安全规范的要求溶入员工的意识之中。

为了管控生产制造过程中的产品安全风险，中兴通讯建立了端到端的管理流程，以防止软件、硬件被篡改，包括未授权的硬件替换、软件植入或篡改、病毒感染等。在生产制造过程中，识别出与产品安全相关的关键生产工序，包括：产品软件版本管理、芯片写片、印制电路板装配（PCBA）最终测试、模块调测、老化测试、整机调测、包装、运输与返修等。根据产品安全风险等级，将所有产品制造与存储区域划分为三个等级的产品安全管控区域，其中产品安全一级、二级管理区是安全严管区域。在产品安全严管区域，均设置有安全管理员负责日常监管、实施区域内的安全管控措施。中兴通讯还对产品安全敏感岗位上的人员实施例行的人事背景调查，以避免因人的因素而产生的产品安全风险。软件产品安全管理流程中，为了防止制造过程中对产品软件的篡改，中兴通讯的工程师只能通过授权访问的产品数据管理系统（PDM）来归档和发布软件。

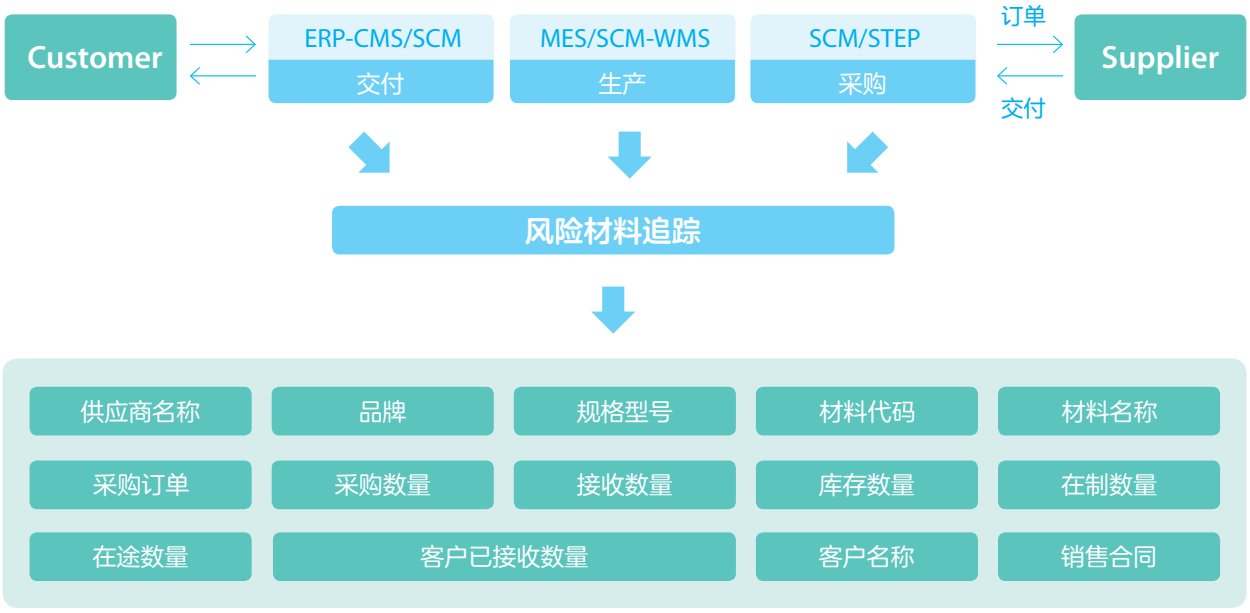


图 6 生产制造过程产品安全管理

中兴通讯采用制造执行系统 (MES)，对产品的制造过程信息进行完整的记录。根据产品条码、批次信息可以对产品的制造过程信息进行端到端的有效追溯，包括供应商的来料批次号（含序列号）均在追溯范围之内，同时配合采购的供应链（SCM）系统、交付的仓储管理系统（WMS）系统实现从材料采购到成品交付的端到端管理和追溯。通过这些管理措施，中兴通讯可以及时定位到质量问题或产品安全漏洞所涉及的整机、部件、单板或器件，及时掌控在库、在制、在途、客户已接收的数量和状态，提升安全响应的速度和效率。

返修业务中的产品安全是中兴通讯产品安全管理的重要一环。在公司产品出现故障需要送修时，通过《中兴通讯故障设备送修单》及其他方式提醒客户对敏感信息进行处理，如数据保存、删除、移除存储介质后再送修等，并在送修设备的监护权转移到中兴通讯之后，由中兴通讯负责该设备的软件、硬件产品的安全保护。

在维修过程中，中兴通讯只使用认证合格的供应商供应的物料，严禁使用来源不明的物料与器件，从物料源头上保证返修设备不会受到非法侵害；物料、返修设备在周转期间也采用相应措施，采取视频记录、网络隔离等方式，保证返修设备在维修过程中不会受到非法篡改、病毒感染以及数据泄露等。中兴通讯有专门针对维修环节进行数据清除的工艺与要求，对无法修复并替换的设备，由专业单位进行回收处理。返修设备使用售后服务管理系统（ECC-ASM）记录设备返修各环节的信息及追溯，能够直观了解到设备的处理状态与处理人，并有一整套相应的查询、记录、信息分析功能。

仓储物流安全

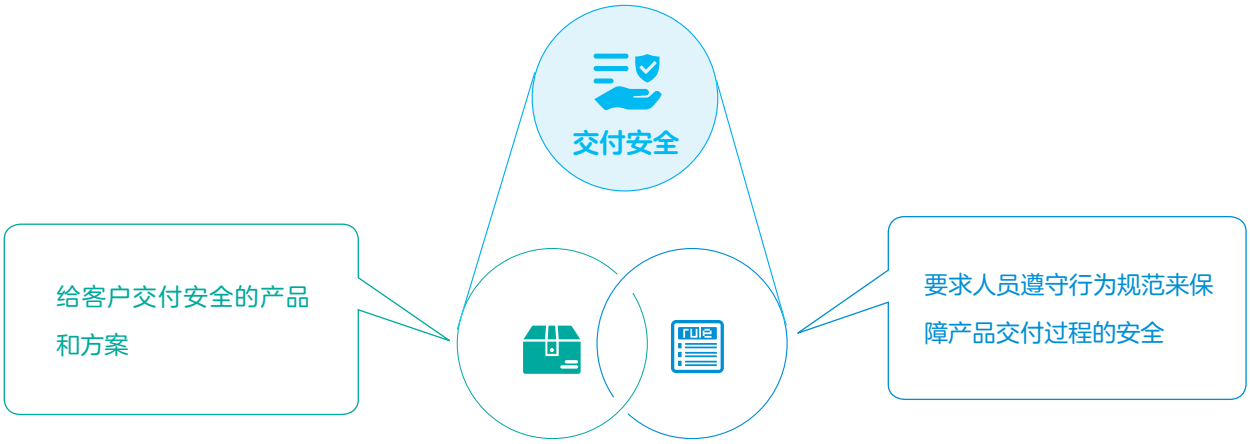
在物流仓储方面，中兴通讯依托国内六大物流中心，与全球物流服务商深入协同，逐步建设大国物流中心，优化全球供应链网络布局，策划精品货运线路，确保项目及时交付。携手全球优质物流服务商，依托物联网技术和智能平台，实现物流状态全程可视，保障客户资产的物理安全。

中兴通讯通过仓储管理系统实现在库货物全程跟踪。对物流仓储 IT 系统、监控设备和安保设施定期升级，避免物流和仓储过程中恶意代码植入、核心器件替换或被破坏。通过可视化平台实现订单信息一键查询，状态全程可视。

中兴通讯建立有完整的逆向物流管理流程，依据所在国和当地的法律法规要求策划逆向物流方案，满足客户及所在国家和地区对信息安全和隐私保护的要求。当逆向回收设备可能含有敏感数据风险时，中兴通讯会提醒并要求客户在设备返回前对数据进行清除。对于需要报废的产品，则要求报废回收商提供销毁报告，对敏感产品的报废要求有专人现场监督进行销毁。

交付安全

保护交付给客户的产品安全是基本的目标，中兴通讯通过技术手段和管理双重措施来保障交付安全，一方面是给客户交付安全的产品和方案，另一方面是要求人员遵守行为规范来保障产品交付过程的安全。



一个完整的项目交付周期涵盖新建、验收 / 移交和运维三个阶段。每个阶段均设置有关键安全检查点。根据各个环节的业务特点，在交付领域定义了一系列安全措施，减小任何操作上的不符合规范可能引入潜在的安全风险。依据一致的产品安全标准，采用可验证、可重复的安全流程、标准和方法，保证及时发现和处理安全隐患。中兴通讯根据法律法规、客户需求和安全最佳实践（如 ISO27001 标准）建立了工程服务的行为规范，保障交付的产品和服务的安全。

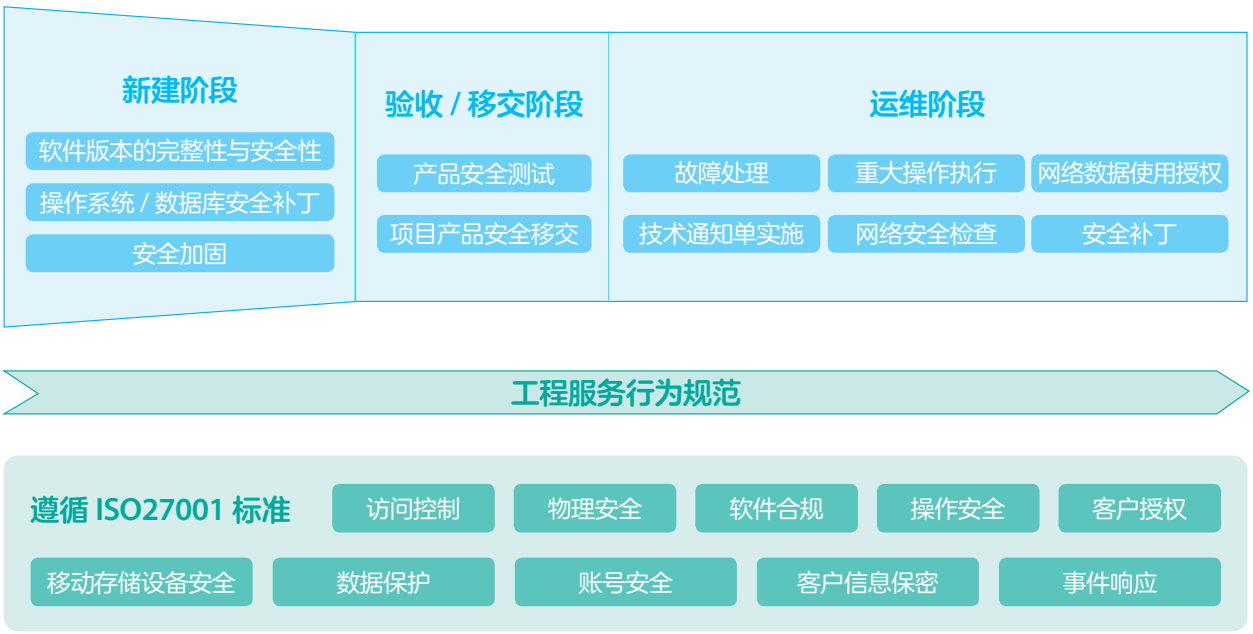


图 7 交付安全保障措施

交付安全的三个阶段

新建阶段

在项目新建阶段，为了防范配置被人为意外地修改和软件篡改，交付领域实施严格的验证措施：软件仅从指定的官方网站下载，并在版本安装前强制进行一致性检查，确保版本的完整性与安全性。

工程开通和调测期间，现场人员进行一系列动作：采取技术手段检测恶意程序、安装指定的操作系统或数据库补丁、进行安全扫描、根据配套的产品合规配置指导和安全加固指导书等完成加固配置等。

验收移交阶段

项目移交前，进行一系列安全测试（如是否清除各种临时配置等）保证产品的安全性并输出测试报告。测试报告通过客户验收后，产品方可移交。正式移交给客户的资产不仅包含具体的物理设备，还有完整的测试报告、文档资料等，并且保证系统的帐号和密码的安全性。

运维阶段

安全风险一直随着新的威胁、新的监管要求、新的攻击形式和不断发展的漏洞而变化。中兴通讯的交付人员在运维阶段持续监控不断变化的情况，定期进行安全巡检，及时进行安全漏洞的补丁升级， 保障返修件的数据安全，所有的操作都需要得到客户的许可。

第三方合作伙伴管理

在交付活动过程中，第三方合作伙伴的任何不安全行为，都会增加交付风险。交付领域从管理、能力、监控三个方面对合作伙伴进行了安全管控：

管理方面

首先根据当地法律法规和安全政策制定适合的安全制度，同时要求合作伙伴签署带有安全要求的租赁合同，从而明确对方的责任和义务。另外，对合作伙伴的背景和从事的岗位事先会分别进行调查和风险评估。

能力方面

正式入职前，合作伙伴需要签署承诺书，并通过一系列的培训进行安全意识和安全技能的提升。测评合格后，才允许进入项目组工作。

监控方面

正式进入项目组前，会对合作伙伴个人电脑进行安全审计，不合格电脑会要求其整改直至达标为止。项目期间，会按照合同要求定期对合作伙伴电脑的安全性进行检查，确保无任何恶意和未授权软件的安装。和中兴通讯解除合同、离开项目组前，会要求其电脑上清除和公司、客户和业务有关的数据，检查通过后，才允许其离开。

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。

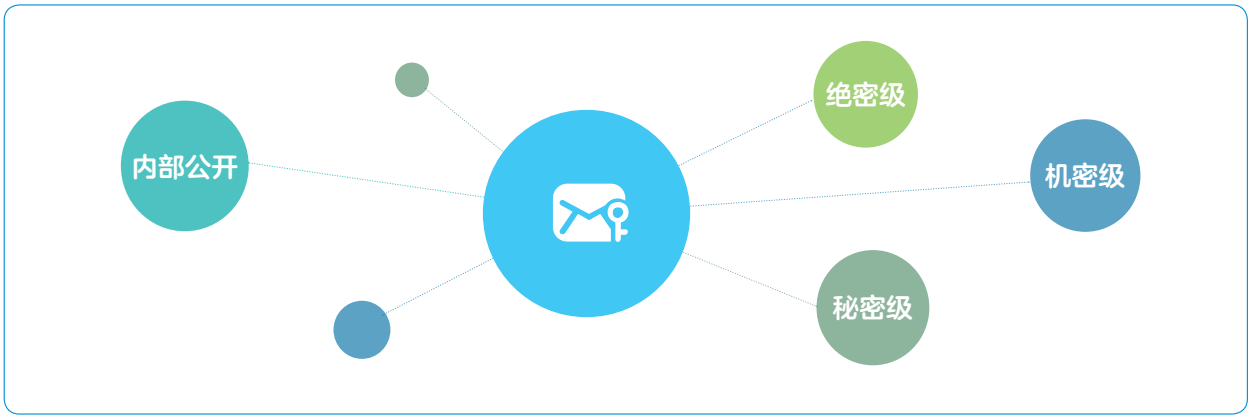
中兴通讯建立了信息安全管理体系（ISMS），定义信息安全总则、安全策略、信息分级、风险评估和安全审计等管理流程，制定了信息安全红线，通过信息安全组织执行监管、调查和处理公司信息安全的违规、侵犯公司商业秘密的行为。每年对所有员工进行安全培训和考试，提高全员的安全意识，把安全、防范信息泄漏当成工作中最重要的一个环节。建立了安全举报的多种途径，在遇到风险、漏洞和信息安全异常情况时，通过邮件、电话、公司官网等举报途径，及时对信息安全异常情况进行处理，补漏，补缺安全规则。

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 8 信息安全总体框架

信息定密

中兴通讯将公司信息根据重要程度分为四类。绝密级：公司最重要的涉密信息，信息泄漏会使公司利益遭受特别严重损害；机密级：公司重要的涉密信息，信息泄漏将会使公司利益遭受严重的损害；秘密级：是公司一般的涉密信息，信息泄漏将会使公司利益遭受损害。内部公开：不宜对公众公开，但又需要公司全员知悉的信息。根据密级的不同，我们制定了不同的管控措施。我们视客户信息为公司信息保护，在识别出的信息清单中，客户信息为公司的机密级信息和秘密级信息。



人员安全

人员安全是信息安全中的重要的一环，从产品的研发、制造到交付，这一系列端到端的活动中，公司员工的安全意识和行为起到关键做用，中兴通讯对员工在公司的整个生命周期均有管控策略。入职时，针对特定的岗位层级，会委托第三方公司进行背景调查，劳动合同中含有保密条款，告知员工其保密义务与职责，安全相关课程也嵌在了新员工入职培训的课程内。在职期间，员工签署信息安全承诺书，每年至少接受一次信息安全培训与考试，按照最小知情原则进行授权。离职时，员工签署离职信息安全声明，不带走公司任何文档。同时，视员工岗位进行脱密或履行竞业限制协议。

物理安全

中兴通讯根据区域内部门的整体涉密级别，将物理区域安全等级划分为 A 级核心涉密区域、B 级重要涉密区域、C 级一般涉密区域、D 级公共区域。员工进入公司时，需出示工卡进行身份验证。访客进入公司需由接待人员提前备案，安保人员验证访客身份后方可放行。被定义为公司核心区域的 A、B 级区域有单独的物理管控措施，例如门禁系统、安检门或配备安保人员。公司全区域 24 小时安保巡逻值守，监控全区域覆盖。如对研发调试区和安全实验室进行 A 级区域管控等，有效确保代码在开发过程中的安全。通过加强技术管控手段，在重点区域设置门禁和监控，禁止拷贝和拍照，做好信息安全的预防和稽查。

IT 安全

IT 是公司业务活动的重要支撑，承载大量的涉密信息，是安全的基础屏障。公司研发、供应链、交付等一系列活动的通过 IT 系统的技术支撑和安全保护，有日志和记录可查询，可以追溯，具有不可抵赖性。

如研发等重点安全保护领域，通过桌面云和研发云的建设和规范化使用，把研发的所有工作在云内开发、与产品相关的代码、关键文档存放在公司的云平台，非授权禁止拷贝和外发，桌面云和研发云不能访问互联网，外网访问桌面云的权限默认关闭，不同用户的桌面云间实现内存隔离和数据隔离。对于研发人员，仅能通过桌面云环境访问代码管理服务器。

公司信息管理部定期对重要办公系统相关的网络、服务器、数据库、进行审计，将整改项和整改建议提交责任单位和责任人，督促其按期整改。

资产管理

资产管理是信息安全的根基，不管是漏洞、入侵、泄密的定位、处置，均须基于资产。从信息安全角度出发，信息资产指的是一切对公司有价值的事物，包括物理区域、人员、电子 / 纸质文档、数据库、软件、硬件、终端、应用等一系列信息或信息载体。对资产进行分类，确保资产配置信息准确，责任到人，对资产的全生命周期进行管理。

公司服务器、计算机等硬件均有固定资产编号，并贴有固定资产标签，由部门的固定资产管理员负责管理和盘点，计算机等硬件资产带出办公区域，需提前进行系统备案报送相关领导，带出时由安保人员进行标签扫描、识别、确认。

身份 & 权限

IT 安全保护信息安全以最小身份授权管理为原则，如：每位员工入职时只有财务、人事、IT 等系统基本必备权限，其他特殊权限均需通过 IT 网站申请，申请时需写明理由（岗位需求）及授权期限，经过领导审批后，专人根据角色受理开通，信息管理部门定期审计员工权限情况。

对人员身份的认证，有多方面的安全保护措施，通过账号密码登录公司系统时，进行双因素认证；账号密码需设置强密码策略; 如密码输入次数错误多则锁定账户; 如设备丢失，更换绑定设备时在 IT 系统审批。

部分系统权限在一定时期有效，到期自动撤销，当员工的申请的账号权限如：虚拟专用网络（VPN）访问权限、外发邮件等权限到期或失效后，系统会自动撤销其相应权限，如需要恢复权限需要再次提交申请。当员工离职或调动岗位时，原有的相应权限也会撤销。通过 IT 系统的管控，最大程度减少可以规避的安全风险。

网络安全

中兴通讯针对基础设施网络实施相关的安全管控，如网络接入安全、远程运维安全及配置安全等。通过访问控制、安全隔离、边界保护等措施，为公司研发和生产运营等业务提供安全的网络环境。

接入公司网络的设备必须符合安全基线要求，并通过用户身份认证，接入前系统自动对终端进行多项安全检测，只有通过检测合格的终端才可接入公司网络。如：安装了公司桌面安全软件和文档安全软件，安装了安全补丁、升级防病毒软件，未安装安全高危险软件和知识产权风险软件等。

通过网络隔离将网络如研发网络和办公网络隔离，生产网络和办公网络隔离，屏蔽来自网络内部的安全威胁。

网络边界部署防火墙、入侵检测 & 防御、等自动化检测工具，在这些设备的严密监控下，来自网络外部的安全威胁大大减少，为公司研发、生产、办公创造安全的网络环境。

个人数据保护

在通讯网络和大数据、云计算等技术高速发展的背景下，越来越多的个人数据通过网络来采集、存储、传输、使用，为了保护这些重要数据的安全，全球主要国家和地区陆续颁布了一批数据保护领域的法律法规，如欧盟《通用数据保护条例》（GDPR），美国《2018加州消费者隐私法案》、中国《网络安全法》。对于中兴通讯来说，数据保护不仅仅是法律要求，更是公司合规治理和安全管理的重要一环。

一方面，中兴通讯将数据保护纳入为公司合规体系，通过聚焦核心场景、完善组织机构、引入技术措施、优化管理方法，全面推动保护个人信息，保障数据安全。另一方面，中兴通讯将数据保护视为产品安全的自我承诺，将数据保护理念融入产品设计和服务提供过程，不断满足和超越当前的全球数据保护法规要求，与全球客户、供应商及其他伙伴一起实现可持续发展。

数据保护合规体系

为了建立完备的数据保护合规体系，中兴通讯实施了风险梳理，在管理、技术、业务、流程、产品、人员等领域组织调查评审，在协议、标准、机制、工具、团队上进行提升建设，立足风险等级制定专项措施，全面合规应对。为了实现集约的数据保护实践效果，中兴通讯将欧盟 GDPR 作为整体合规的遵循基准，适度吸纳各国的属地化监管要求，最大限度地确保“一次导入，全球适用”。

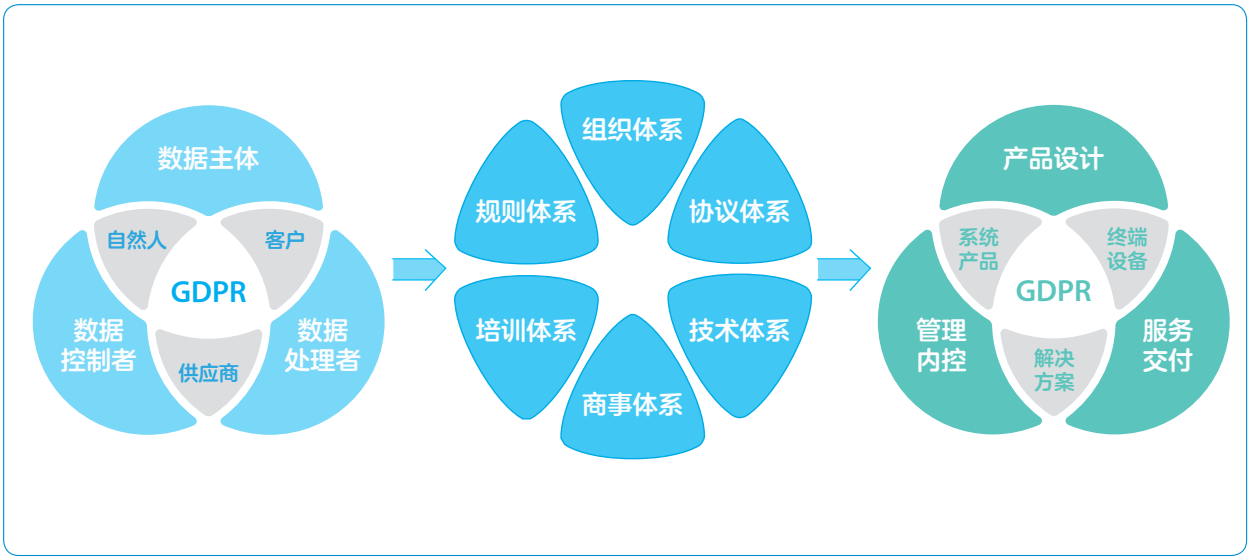


图 9 数据保护体系

中兴通讯在组织、规则、协议、培训、技术方面进行了一系列数据保护专业化建设。组织体系方面，构建了“专业团队支撑，三道防线管控，多主体内外协同运作”的组织模式。规则体系方面，中兴通讯建立了“政策、总体制度、业务指引、协议及记录”四层规则架构，帮助各部门立足各自管理场景，识别、应对业务活动中的数据保护风险。协议体系方面，统一组织、集中推动了具有法律约束力的协议签署，并将其作为数据合规的重要基础要件。培训体系方面，建立了课程开发、培训实施、效果督导的一体化实施机制，多维度促进员工数据保护合规意识和能力提升。技术体系方面，积极采用并持续寻求最佳、适用的数据保护技术措施，通过信息系统改造和专业工具嵌入，促进合规要求的落地履行。商事体系方面，依托专项合规咨询服务，实施重要展会、大型活动等商事过程中的风险防控。

通过体系化建设，中兴通讯建立了覆盖核心业务脉络的数据保护合规指引和标准规范，支撑各职能单位、各岗位员工能够理解数据保护的原则，并严格执行公司适用的规范和流程；签署了符合 GDPR 要求的数据处理协议（DPA）、标准协议条款（SCC，数据跨境转移）并辅以《通知函》、《授权函》等；嵌入了加密、匿名化、假名化等安全技术，双因素认证、权限管理、访问监测等安全措施，支撑在采集、存储、使用、传递、销毁等环节的数据保护和安全防护。

数据泄露响应机制

在整个数据保护合规体系中，数据泄露响应是最受关注的环节之一。中兴通讯建立了以多方快速协同为核心的一套个人数据泄露应急响应机制，制定了企业标准，明确了响应流程，开发了响应系统。具体运行上，依托广泛分布于各业务线和区域的数据保护经理网络，以及专家小组与数据保护官团队，在疑似事件发现或发生时快速处理和组织应对，按规则保护个人数据，减少可能损失并履行通知义务。同时，依托专业化的上报系统对整个应急响应过程进行记录，以备监管机构可能的的文件调阅和证据呈送需求。同时，中兴通讯不定期组织数据泄露应急演练，强化日常岗位责任和应急响应机制的可验证程度，最大限度地防范数据泄露的发生，科学地进行数据泄露处置。

为了确保各项政策措施的落地执行，中兴通讯建立了数据保护稽查机制和违规举报渠道。具体地，中兴通讯建立有专职合规稽查队伍，将自检审计纳入内控保障体系，实施常态稽查，促进数据保护文化建设、资源投入、流程再造、能力提升的正循环。

图 10 数据保护响应机制

数据保护方案实践

中兴通讯在技术方案上积极创新，将个人数据保护要求和产品安全需求结合推进，探索安全合规的产品体系和解决方案。

中兴通讯采用了面向产品生命周期的个人数据保护方法和实践，提高数据保护合规水平。中兴通讯遵循默认隐私设计原则，依据《通用数据保护影响评估规范》和《产品项目数据保护影响评估》，坚持在产品设计阶段就导入安全管控，将个人数据保护和安全技术处理作为产品安全的默认属性，确保个人数据处理过程满足合法、公平、透明要求。

在基于客户授权的某产品数据脱敏保护设计中，通过授权中心、安全网络、网元脱敏、安全技术等设计融入，实现数据控制者、数据处理者的良性互动，确保多方业务安全。在面向欧盟地区的客户技术问题解决和应急维护的远程接入中，基于数据跨境转移协议采用安全模式下的远程接入方案，实现客户、欧盟本地工程师、中国总部工程师的协同配合，形成自主安全驱动的数据保护实践。

安全事件管理

由于威胁、脆弱性和成本收益等因素的影响，安全风险不能被完全消除，当安全风险转变为安全事件时，需要及时、有效地响应，并与利益相关方有效合作，快速给出解决方案，以减轻安全事件的不利影响。中兴通讯秉承公开透明的原则，确保任何潜在的产品漏洞信息及时披露给客户，并提供最终解决方案。

产品安全事件响应机制

中兴通讯 PSIRT 事件响应团队负责接收、处理和公开披露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（如数据泄露）建立重大事件响应机制，确保统一协作、快速修复，迅速恢复业务。

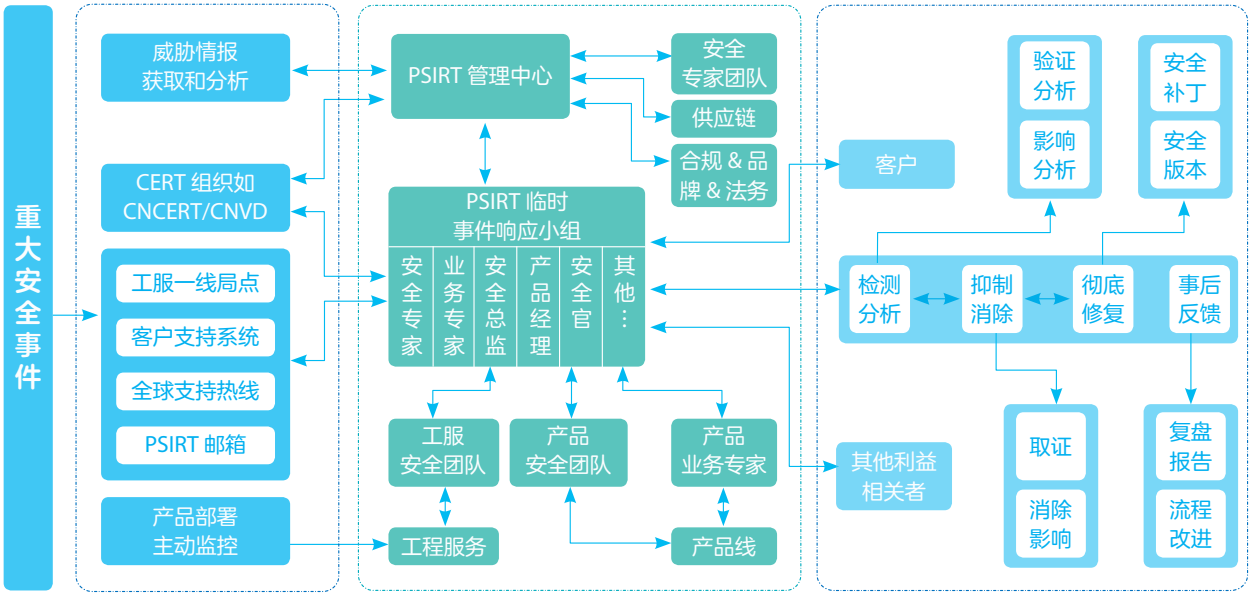


图 11 重大安全事件响应机制

对安全事件采取预防、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 迅速组建临时事件响应小组，小组成员包含安全专家、业务专家、产品安全总监、PSIRT 接口人、首席安全官等，迅速对事件进行分析，并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，为防止类似事件发生，需要进行复盘改进过程。

产品安全漏洞处理流程

中兴通讯加强与安全组织协作，对内外部发现的漏洞，公司秉承公开透明的原则，主动披露。中兴通讯作为事件响应和安全团队论坛（FIRST）成员和 CVE 编号颁发机构（CNA），公司以更加公开的方式与客户及相关方进行协同披露。对产品漏洞在CVE和公司网站上进行披露。为鼓励内外部发现中兴通讯产品的漏洞，公司设立了漏洞发现奖励计划。

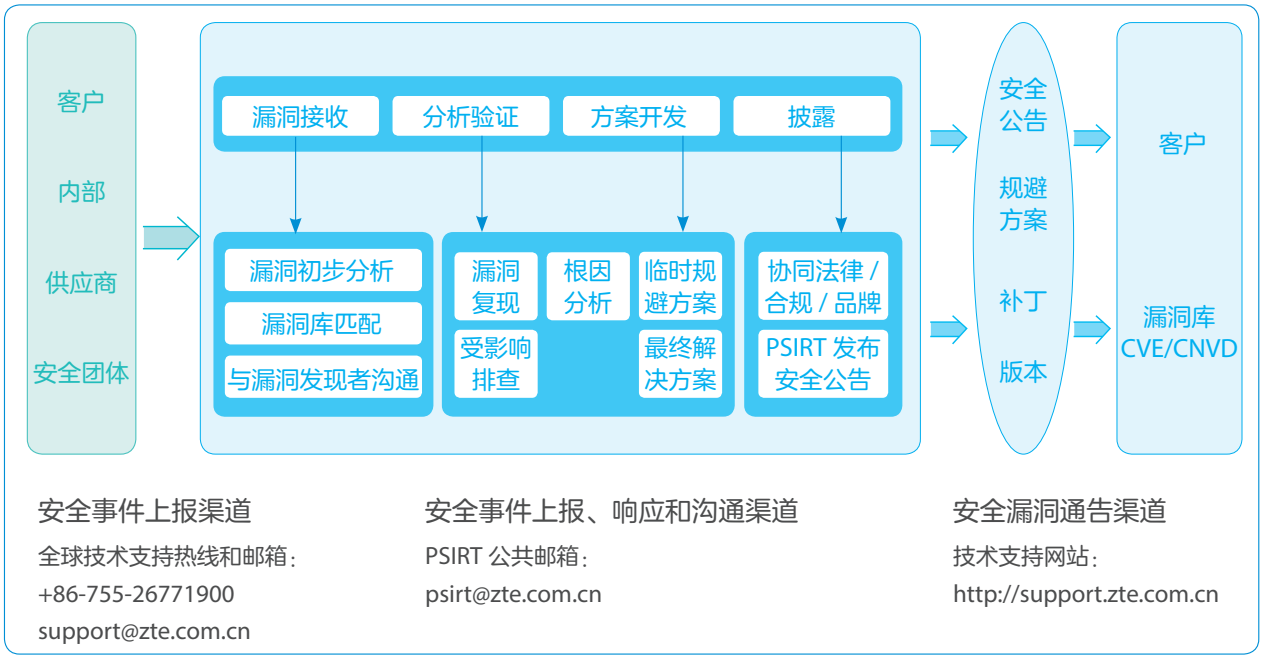


图 12 产品安全漏洞处理流程

PSIRT 漏洞处理流程包括 5 个阶段：

漏洞接收阶段

从内外部接收安全事件或安全漏洞的报告，包括客户、外部 CERT、白帽、安全研究团体，内部员工。我们鼓励负责任的披露，在公开披露之前，给供应商提供一段合理的时间去处理和解决问题。

分析验证阶段

针对每起收到的安全漏洞报告，PSIRT 团队会立即启动分析调查工作，快速完成漏洞的确认及严重级别定义。在分析和验证阶段，PSIRT 团队会与漏洞报告者保持沟通，提高漏洞分析的准确性和及时性。

方案开发阶段

PSIRT 流程与研发流程紧密承接，一旦确认漏洞存在，受影响产品团队迅速启动响应机制，调查漏洞的根本原因、进行影响产品排查工作，制定修复方案，包含临时规避方案，并对方案开发与测试，确保方案有效。对于已经披露的漏洞，需要快速完成方案开发。

披露阶段

在事件处理过程中，PSIRT 团队和漏洞报告者、产品开发团队、客户积极保持沟通，向客户透明披露问题，向客户提供规避策略以及解决方案的信息。

反馈阶段

一旦客户实施解决方案后，需要对方案的有效性或出现的问题进行监控，并根据反馈情况进行方案迭代，实行“闭环管理”，通过复盘环节，持续改进公司产品研发，确保客户的安全要求在产品的各个阶段得到覆盖，从而提高质量和安全。

业务连续性管理

业务连续性管理（BCM，Business Continuity Management），是基于面临的各类不确定风险因素以及由其所带来的脆弱性引发的思考，中兴通讯遵照 ISO22301 标准建立了业务连续性机制，组织建立并实施一套应对解决的方案，以保证组织有持续提供产品和服务的能力。

中兴通讯的 BCM 管理覆盖了产品生命周期的主业务过程（包括研发、供应链、工程服务过程），以及支撑业务过程（包括 IT 系统、财务、人事、合规等）。

中兴通讯业务连续性管理方针是：积极防范，降低风险，快速响应，持续提升企业的业务连续性管理能力，最大限度保护员工、客户、股东、供应商等相关方的利益。

业务连续性和安全事件管理是产品安全和服务的重要保障措施。事件响应流程建立快速有效的响应的能力，减缓安全事件影响，确保尽快恢复业务，并为实施业务连续性计划提供了最佳机会。业务连续性管理为安全事件管理提供了保障，在发生影响业务的安全事件时，在相应的领域启动事件响应机制，执行业务连续性计划。

研发过程业务连续性管理

在紧急情况下，中兴通讯多个研发中心都能够互相作为备份，保证业务快速恢复的能力。

针对意外事件，制定了系列的事故管理计划来针对意外事件进行紧急应对。针对第三方专利主张，研发进行专利的定期扫描，避免侵权以及交叉授权机制。针对核心人员流失风险，制定了针对关键人员的保留机制。针对主要风险还设立了 KPI 进行定期的监控以避免产生业务中断影响。

供应链业务连续性管理

中兴通讯供应链的 BCM 管理是通过作战室（Warroom）运作机制组织实施的，针对识别出的材料供应风险及时采购应对措施，针对突发性事件实施危机处理措施。

在风险应对与管控方面，中兴通讯开发了供应资源风险地图。当各类突发事件发生时，通过该地图能够迅速确定波及的供应商、材料及代码、产品，以及其影响程度，第一时间完成全面的风险评估，同时对日常的材料风险预防也可以提供有力的数据支持。

中兴通讯设在深圳、河源、长沙、南京四大生产基地的厂房环境、电力、原材料及成品库房可以互为备份。PCBA 业务在深圳、南京、河源可相互备分，而且能为长沙基地备份。

工程服务业务连续性管理

工程服务领域设计并应用了一套业务连续性策略：分为事前防控、事中应对和事后重建，三者有机互联。针对识别的灾难情景制定了基于各种业务情景的应急预案，且定期进行灾难模拟演练，保证方案的持续有效性。

为了确保客户服务业务不受中断影响，我们在中国的全球服务热线呼叫设备采用了异地备份容灾模式，海外本地的服务热线故障时可呼叫中国的全球服务热线；部分在海外的区域客户支持中心使用了“飞线技术”来进行呼叫热线的异地备份，确保在任何紧急情况下能够切换到中国进行受理。

IT 系统业务连续性管理

中兴通讯建立了三地双活数据中心：同城双活 + 异地容灾。针对核心业务系统，在深圳科技园企业数据中心（EDC）和深圳西丽 EDC，进行了双活架构的部署。同时，为应对更多事件场景，在南京 EDC 实施了容灾备份，将生产环境数据同步到异地 EDC。通过“同城双活、异地容灾”有机相结合，有效提升了核心系统连续性能力。

IT 部门每年持续对风险评估、业务影响分析进行刷新，并针对核心系统进行各种方式的恢复演练。通过对演练结果的总结分析，识别与实际需求的差距，持续进行改进。IT 服务连续性的有效管理，为公司业务的稳定连续运作提供了有力的支持和保障。

独立安全测评

在三道防线的组织架构下，独立安全测评属于第二道防线，负责对一线安全实践进行评估和监督。通过应用风险控制的原则，从多个角度审核产品的安全性。通过监督与制约机制进一步降低安全风险，对发现的问题实施闭环管理跟踪，直到问题解决，实现产品安全治理的持续改进。

独立安全测评控制机制

产品安全治理过程中，第二道防线设置目的是为避免一线安全管控机制失效，从业务中识别出风险并解决，通过第二道防线安全评估和监督以及一票否决权的运用，来降低一线安全实践未能发现或未执行到位而导致的安全风险。

为确保独立安全测评的有效运行，中兴通讯制定了独立安全测评的运作控制机制，体现了独立、威慑、全面、闭环等四个方面特点：

二线安全测评活动完全独立于一线业务，工作汇报对象为产品安全委员会，测评过程及结果不受一线业务影响，具有自主裁量权

独立

二线测评有权对问题发现直接进行结果应用，如违背公司安全红线等严重行为，二线将代表公司行使“一票否决”权，直接中止涉事单位业务活动，包括版本停发、业务暂停等，要求进行限期整改

威慑

二线测评范围覆盖一线安全过程、管控机制及最终交付物，关注治理过程与结果，具有全面监督特点

全面

二线测评对问题发现实施闭环管理跟踪，关注缺陷消除结果，并实施验证，通过验证的问题才能关闭

闭环

独立安全测评过程

中兴通讯的独立安全测评遵循规范的过程，覆盖供应链、研发、交付和事件响应各领域。

在计划阶段，以产品一线相关产品和服务项目为测评对象进行随机抽检，结合产品安全治理要求，制定具体测评计划。

在执行阶段，重点从两个角度对测评对象进行测评：

过程评估	评估各业务单位对安全治理制定的各项规范和控制点的执行过程符合度和有效性进行评估
产品评估	评估产品和系统的安全性，进行漏洞扫描，安全编码审计，协议健壮性测试等分析评估

在结果审核和上报阶段，对测评结果进行复核，向产品安全委员会汇报最终测评结果。此外，发现的产品安全漏洞提交缺陷管理系统，对问题的进一步问题分析、改进和验证进行闭环跟踪。

在产品问题和缺陷修复的验证阶段，对问题改进进行检查，必要时进行二次现场抽检。对产品安全缺陷修复进行验证，并通过缺陷管理系统进行跟踪，直至缺陷最后关闭。

独立安全测评技术

在独立安全测评过程中，采用多种测试技术手段进行评估和验证，如安全基线功能测试、安全扫描、渗透测试等，多角度对一线单位产品的安全治理的有效性进行验证。

安全基线功能测试

基于产品安全需求基线进行测试，验证基线中的安全功能在产品中的实现情况，并对安全功能的有效性进行验证。

安全扫描

采用业界专业扫描工具，对一线单位安全治理成果进行验证；包括对产品源代码进行安全编码扫描和审计，对操作系统、数据库、WEB 服务及其他第三方组件进行安全扫描，识别系统和设备中的漏洞。

渗透测试

对产品和系统进行模拟攻击测试，通过分析产品和系统实际运行场景，分析可能存在的弱点，发掘安全漏洞，并进行缺陷分析和提供改进建议。

安全审计

产品安全审计向公司管理层以及客户等利益相关方合理保证产品安全策略、规范、流程得到有效的执行，促使客户需求得到有效满足。作为产品安全治理第三道防线，安全审计通过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，促使公司加强产品安全保障体系的建设并严格执行，保证产品安全保障体系得以持续、有效的改进，实现产品安全体系的可监管、全透明管理。

对关键利益相关者，中兴通讯一直秉承开放、透明的态度，除内部审计外，依据公司章程接受外部审计。审计报告呈报董事长审批，并定期向董事会审计委员会汇报工作，审计发现的风险及时传递到管理层和董事会。

中兴通讯安全审计以组织与运作、风险管理过程、控制活动、内部监督等维度开展，覆盖产品安全治理、研发安全、供应链安全、交付安全、安全事件响应、独立安全测评等端到端产品安全保障全流程。

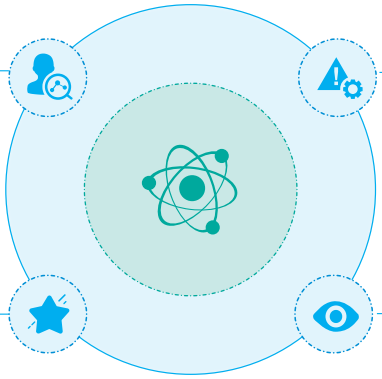
以风险为导向，贯穿整个审计流程，中兴通讯持续不断地审视公司产品安全体系的健全性和有效性，切实保障客户及其利益相关者的安全需求得以满足。

组织与运作审计

重点关注一体化运作组织、胜任能力、产品安全重大事项汇报及决策机制等。

风险管理审计

重点关注产品安全风险识别、评估、应对，以及风险预警机制、应急预案及程序、安全损失事件回溯机制的建立及执行。



控制活动有效性审计

重点关注控制点设计并嵌入业务流程，以及控制点有效执行。

内部监督审计

重点关注第一、二道防线的日常监督、专项监督机制，以及问题改进及后评估机制的建立及执行。

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

网络安全实验室和外部合作

中兴通讯不断对标安全标准和最佳实践，积极与行业组织开展合作，着力以开放透明的方式与客户和利益相关方沟通需求、增进互信，以实现抵御网络安全威胁的共同目标。

正在筹建的网络安全实验室是中兴通讯在全球范围提升透明度的重要举措，安全实验室以“1+N”模式运行，核心实验室设在中国，国内外部署多个远程接入点，借助部署在全球不同区域的地理优势，以开放产品源代码和产品文档、提供多维度安全测评服务的方式，向全球客户、监管机构和其他相关利益方提供中兴通讯产品的外部安全测评业务。

安全实验室作为中兴通讯外部审计和独立测评的物理平台，为第二道、第三道安全防线职能行使创建了一个开放、透明、安全的环境。安全实验室预设三个主要功能：

- *在安全的环境中查看和评估中兴通讯产品的源代码；*
- *提供对中兴通讯产品和服务的重要技术文档的访问；*
- *可通过手动和自动化工具对中兴通讯产品和服务进行安全测试。*

同时，中兴通讯已开始寻求与第三方的战略合作伙伴关系，获得的技术和服务将用于安全实验室建设，独立测评和安全审计。

展望未来·共同前进

中兴通讯通过多年的实践和长期以来坚持技术创新，在实践过程中不断积累经验，逐步具备了覆盖 5G 核心技术、网络安全运营和行业应用端到端的解决方案能力。5G 的大连接、低时延、高速率、广覆盖、万物互联等特性，与云计算、大数据、人工智能、虚拟现实等技术的深度融合，未来十年，移动互联网将服务于各行各业，物与物的连接将大幅增长，网络的覆盖范围更广，应用也越来越多，这也意味着我们将面临更多的安全挑战。

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。我们必须做好充份的准备，以透明、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，推动端到端的安全实践，从容应对未来的安全挑战，持续地提供安全可信的产品和服务。

表 1 缩略语和符号

缩略语或符号	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
BCM	Business Continuity Management	业务连续性管理
CC	Common Criteria	通用准则
CERT	Computer Emergency Response Team	计算机安全应急响应小组
CNA	CVE Numbering Authorities	CVE编号颁发机构
COP	Communities of Practice	实践者社区
CSA	Cloud Security Alliance	云安全联盟
CSC	Cyber Security Committee	产品安全委员会
CVE	Common Vulnerabilities & Exposures	通用漏洞披露
CWE	Common Weakness Enumeration	通用缺陷列表
EDC	Enterprise Data Center	企业数据中心
FIRST	Forum of Incident Response and Security Teams	事件响应和安全小组论坛
GDPR	General Data Protection Regulation	通用数据保护条例
HPPD	High Performance Product Development	高效产品开发
IETF	Internet Engineering Task Force	互联网工程任务组
ISO	International Organization for Standardization	国际标准化组织
ITU	International Telecommunication Union	国际电信联盟
PSIRT	Product Security Incident Response Team	产品安全事件响应小组
SATRC	S：System A：Asset T：Threat R：Risk C：Control	系统、资产、威胁、风险、控制
SSG	Software Security Group	软件安全小组
STIG	Security Technical Implementation Guide	安全技术实施指南

附录：
中兴通讯产品安全大事记

2005

中兴通讯通过 ISO27001 信息安全管理体系认证审核，所覆盖的范围包括中兴通讯所从事的所有业务。 2014 年中兴通讯升级完成 ISO27001:2013 认证。2017 年中兴通讯已通过 ISO 27001：2013 认证的所在地包括：中国、印度、美国、德国、荷兰、 英国、法国和意大利等。截至 2019 年 3 月，新增 14 家欧洲子公司顺利通过 ISO 27001:2013 审核，认证的所在地包括奥地利、希腊、西班牙、比利时等。

中兴通讯担任 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

中兴通讯成立了产品安全委员会（CSC）开展产品安全相关的工作。

中兴通讯网管产品通过通用准则 (CC) 认证，截至 2018 年底已有 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

中兴通讯成立了产品安全实验室，作为公司内独立的安全验证机构，是安全测评、安全能力开发、安全事件响应、安全知识管理和技术交流的综合平台。

2014

中兴通讯发布了产品安全要求总则和安全基线的系列标准和规范。

2015

中兴通讯加入国际安全论坛组织 FIRST（Forum of Incident Response and Security Teams），旨在提升安全事件响应能力。

2017

中兴通讯正式获得 ISO28000（供应链安全管理体系）认证，有 26 大类电信产品（含终端）的采购、制造及物流业务全部通过认证。2017 年获得了海关 AEO 贸易安全认证。

中兴通讯建立了完备的产品安全规范体系，覆盖研发、供应链、工程服务、安全事件响应和安全独立测评等领域。

中兴通讯成为 CVE 编号颁发机构 CNA（CVE Numbering Authorities），该机构提供了主动披露安全漏洞的渠道。

2018

发布了公司产品安全红线要求。

中兴通讯调整产品安全委员会，其成员由公司高级管理人员组成，安全保障的组织部署贯穿管理层。中兴通讯任命钟宏为公司首席安全官。

年筹建“1+N”的运行模式的网络安全实验室，核心实验室设在国内，国内外部署多个远程接入点。2019 年在海外建设两个安全实验室，地点分别设在比利时和意大利，在安全实验室可以开展源代码审计、安全设计审核和安全测试等。

5G 先锋