# Security Audit Model and Compliance Management Framework for Audio and Video Communication Systems

**Fei Wang**

Beijing Zhongchuang Video Technology Co., Ltd., Beijing, 100096, China

**Abstract**

Audio and video communication systems are widely used today, with complex technical architectures involving multiple links such as encoding and decoding, transmission protocols, network adaptation, and facing many security risks. This makes security auditing and compliance management key elements to ensure the stable operation of the system. Security auditing can trace system operations, detect abnormal behavior, and compliance management ensures that the system complies with laws, regulations, and industry standards. Based on this, this article proposes the research objective of constructing a systematic framework that comprehensively covers technical implementation details, security audit mechanisms, and compliance management requirements, aiming to provide solid theoretical support and practical guidance for the audio and video communication industry.

**Keywords**

audio and video communication system; security audit model; compliance management framework; distributed system; privacy protection

# 音视频通信系统的安全审计模型与合规性管理框架

王飞

北京中创视讯科技有限公司，中国·北京 100096

**摘要**

音视频通信系统在当下应用广泛，其技术架构复杂，涉及编解码、传输协议、网络适配等多环节，且面临诸多安全风险，这使得安全审计与合规性管理成为保障系统稳定运行的关键要素。安全审计可追溯系统操作、检测异常行为，合规性管理确保系统符合法律法规与行业标准。基于此，本文提出研究目标，即构建一个全面涵盖技术实现细节、安全审计机制、合规性管理要求的系统性框架，旨在为音视频通信行业提供坚实的理论支撑与切实可行的实践指导。

**关键词**

音视频通信系统；安全审计模型；合规性管理框架；分布式系统；隐私保护

## 1 引言

随着信息技术的飞速发展，音视频通信技术已从单一功能应用向全球化、分布式、智能化方向深度演进，成为教育、医疗、政企等众多领域不可或缺的核心基础设施。然而，在技术快速迭代、应用场景需求日益多样化以及安全合规要求不断提高的多重背景下，传统审计与管理模式暴露出诸多弊端，难以有效应对系统复杂性与合规性挑战。在此形势下，本研究聚焦于音视频通信系统，旨在通过构建科学合理的安全审计模型与合规性管理框架，切实提升系统可靠性、有效降低安全风险、全面保障业务合规性。为实现这一目标，研究综合运用技术分析、案例研究与行业实践等方法，创新性地提出分层审计模型与动态合规管理框架。

【作者简介】王飞（1975–），男，中国山西大同人，硕士，从事云视频与音视频通信技术及相关企业管理研究。

## 2 音视频通信系统的技术特征与安全挑战

### 2.1 技术复杂性

音视频通信系统兼具复杂技术特征与多元安全挑战。从技术复杂性来看，实时音视频链路涵盖全流程机制，采集环节需精准捕获声音图像信号，编码环节要高效压缩数据以适应网络传输，传输过程依赖稳定网络协议确保数据完整送达，解码环节将压缩数据还原，渲染环节则实现音

视频的流畅呈现。分布式系统架构下，服务发现机制能自动定位可用服务，负载均衡可合理分配资源，容灾切换保障系统在故障时快速恢复。端侧适配与多终端兼容性也是关键，需适配PC、移动端及行业专用终端等不同设备，满足多样化使用场景需求。

### 2.2 安全与合规风险

在安全与合规风险方面，数据安全威胁不容忽视。传输加密可防止数据在传输途中被窃取，端到端加密保障通信双方数据安全，静态加密则对存储数据进行保护。隐私保护面临诸多挑战，用户身份、会议数据及录制文件存在泄露风险，一旦泄露将严重侵犯用户隐私。此外，区域性合规差异给系统运营带来困难，不同地区对数据跨境、内容留存规则及行业监管要求各不相同，系统需满足各地合规标准，否则将面临法律风险与运营障碍。

## 3 安全审计模型构建

### 3.1 审计目标与原则

安全审计模型构建的首要任务是明确审计目标与遵循原则。审计目标聚焦于保障系统可靠性、数据完整性以及操作可追溯性。系统可靠性是音视频通信稳定运行的基础，确保通信过程不中断、不出现严重故障；数据完整性关乎通信内容不被篡改、丢失，保证信息的真实准确；操作可追溯性则便于在出现问题时查找原因、明确责任。

为实现这些目标，需遵循一系列原则。最小权限原则要求每个用户和系统组件仅拥有完成其任务所需的最小权限，降低因权限过度分配带来的安全风险；日志留痕原则强调对所有关键操作和事件进行详细记录，为后续审计和追溯提供依据；动态监测原则通过实时监控系统运行状态，及时发现潜在的安全问题；风险可控原则确保在审计过程中采取有效措施，将风险控制在可接受范围内，保障系统安全稳定运行。

### 3.2 分层审计架构设计

为全面、深入地进行安全审计，设计了分层审计架构，涵盖链路层、数据层和应用层。链路层审计主要针对音视频传输链路，实时监控传输质量相关指标，如卡顿率反映通信过程中出现卡顿的频率、端到端时延体现数据从发送端到接收端所需的时间、弱网恢复时间衡量系统在弱网环境下恢复正常通信的能力。通过对这些指标的监测，及时发现传输链路中的问题并采取措施解决。

数据层审计聚焦于数据的安全管理，包括加密密钥管理、访问控制和数据生命周期审计。加密密钥管理确保密钥的安全存储、分发和使用，防止密钥泄露导致数据被破解；访问控制严格限制用户对数据的访问权限，只有经过授权的用户才能访问相应数据；数据生命周期审计对数据的创建、存储、使用、共享和销毁等全过程进行审计，保证数据在各个阶段都符合安全要求。应用层审计关注用户在使用音视频通信系统时的行为，包括用户行为分析、权限分级和操作日志审计。用户行为分析通过分析用户的操作习惯和行为模式，发现异常行为；权限分级根据用户的角色和职责，为其分配不同的权限级别；操作日志审计对用户的所有操作进行记录和审查，以便在出现问题时进行追溯和调查。

### 3.3 动态审计机制

动态审计机制是安全审计模型的重要组成部分，基于QoE（体验质量）指标进行实时监测。首帧时长指用户从发起通信到看到第一帧画面的时间、接通率反映通信成功建立的比例、音质MOS（平均意见得分）用于评估音频质量。通过对这些指标的实时监测，及时了解用户的使用体验，发现影响体验的问题并加以解决。异常行为检测是动态审计的关键环节，能够及时发现非法接入、数据篡改、权限滥用等异常行为。非法接入可能导致未经授权的用户访问系统，数据篡改会破坏数据的完整性，权限滥用则可能引发安全漏洞。通过建立异常行为检测模型，对这些行为进行实时监测和预警。审计结果可视化与闭环反馈是动态审计机制的最后一步。将审计结果通过指标看板等形式直观展示，方便管理人员及时了解系统安全状况；对故障进行复盘，分析问题产生的原因和影响；根据复盘结果迭代优化方案，不断提高系统的安全性和审计效果，形成完整的审计闭环。

## 4 合规性管理框架设计

### 4.1 合规性管理目标

在全球化与数字化深度融合的背景下，音视频通信系统的合规性管理至关重要。其首要目标在于满足GDPR、等保2.0等国内外法规要求。GDPR对个人数据的保护极为严格，规定了数据处理的原则、权利和义务等；等保2.0则从安全物理环境、安全通信网络等多个层面提出了详细的安全要求。不同行业对音视频通信系统的合规标准存在显著差异。教育行业注重保护学生隐私、确保教学数据安全；医疗行业强调患者信息的保密性、医疗数据的完整性和可追溯性；政企行业则关注政务信息的安全、企业商业机密的保护。合规性管理需适配这些行业的差异化标准。通过有效的合规性管理，能够降低法律风险，避免因违反法规而面临的巨额罚款和法律诉讼；还能减少商业信誉损失，维护企业在市场中的良好形象，增强用户对系统的信任度，为系统的长期稳定发展奠定基础。

### 4.2 合规性管理要素

合规性管理涵盖多个关键要素。数据保护体系是核心要素之一，在数据传输过程中，采用SRTP、QUIC等加密技术，确保数据在传输链路中的安全性；对于静态数据，运用AES－256等高强度加密算法进行加密存储，防止数据泄露；建立密钥轮换机制，定期更换加密密钥，降低密钥被破解的风险。访问控制体系也是重要组成部分。通过OAuth2.0等身份认证技术，验证用户身份的合法性；采用RBAC模型进行授权管理，根据用户的角色分配相应的访问权限；遵循最小权限原则，确保用户仅拥有完成工作所需的最小权限，减少因权限滥用导致的安全风险。审计与留痕体系能够记录系统的操作过程和事件信息。操作日志详细记录用户的操作行为；链路追踪可追踪数据的传输路径和处理过程；合规报告生成功能能够根据审计结果生成合规

报告，为合规性评估提供依据。权限分级体系则按照管理员、普通用户、访客等不同角色划分权限边界，明确各角色的操作范围和权限级别，实现对系统访问的精细化管理。

### 4.3 动态合规管理机制

动态合规管理机制能够根据不同区域和业务场景的变化，灵活调整合规策略。在区域化合规策略配置方面，针对欧盟地区严格的数据跨境限制要求，限制数据向欧盟境外传输；遵循中国等保要求，对系统进行安全防护和等级测评。业务场景合规适配也至关重要。在医疗场景中，强调医疗数据的留存和审计，确保医疗过程的可追溯性；在直播场景中，侧重于内容分发的合规性，防止违规内容的传播。引入自动化合规检查工具，基于规则引擎进行实时合规扫描。规则引擎能够根据预设的合规规则，对系统的操作和数据进行自动检查，及时发现合规问题并发出预警。通过自动化检查，提高合规检查的效率和准确性，降低人工检查的成本和误差，确保系统始终处于合规状态。

## 5 案例分析：某政企音视频通信系统的审计与合规实践

### 5.1 系统背景与需求

政企场景下的音视频通信系统具有独特性。其特点在于对安全性要求极高，需防止信息泄露；强审计功能必不可少，以便对所有操作进行追溯；低时延保障通信的实时性；多端协同则满足不同设备接入需求。在合规方面，该系统需满足等保2.0三级标准，这是对系统安全防护能力的严格规范；数据要实现本地化存储，避免数据跨境传输带来的风险；操作日志需留存6个月，为后续审计和问题排查提供依据。

### 5.2 审计模型应用

在链路层，系统实时监测端到端时延，确保其小于200 ms，保障通信的流畅性；同时监控卡顿率，使其低于1%，减少通信中的卡顿现象。数据层采用国密SM4加密传输数据，增强数据安全性；密钥管理周期设定为7天，定期更换密钥降低泄露风险。应用层基于RBAC模型实现权限分级，不同角色拥有不同权限；审计日志全面覆盖用户登录、会议创建、文件共享等关键操作，便于追溯和审查。

### 5.3 合规性管理实践

数据保护上，录制文件存储于私有云，既保证数据安全又便于管理；支持按需删除与合规导出，满足不同场景需求。访问控制方面，通过双因素认证（短信+令牌）强化身份验证，提高用户身份识别的准确性。审计留痕环节，生成月度合规报告，内容涵盖用户行为、系统状态、安全事件等，为合规性评估提供全面依据。

### 5.4 实施效果

系统可靠性显著提升，卡顿率下降至0.8%，接通率提升至99.5%，通信质量大幅改善。合规风险有效降低，成功通过等保2.0三级认证，且未发生数据泄露事件。运营效率得到优化，审计报告生成时间从72小时缩短至2小时，提高了工作效率和决策的及时性。

## 6 结语

本研究提出“分层审计 + 动态合规”双轮驱动框架，该框架通过分层审计确保技术细节的精准把控、动态合规实现规则的灵活适配，达成技术可靠性与合规性的平衡。经实践验证其在政企场景有效，为行业提供可复制路径。展望未来 技术层面 AI 驱动的智能审计可实现异常行为预测、区块链赋能可保障审计日志不可篡改；管理层面合规性管理自动化工具链及跨区域合规策略协同机制将成趋势；但行业也面临终端生态碎片化、新兴场景如元宇宙会议合规性适配等挑战。

## 参考文献

[1] 程亮.实时音视频通信系统智能拥塞控制算法研究[D].华东师范大学,2024.

[2] 孙斐然.关于即时通信系统中的音视频处理技术的研究[J].电子技术与软件工程,2022,(22):1-5.

[3] 牛晓华,王娟,王黎明,等.基于云平台的音视频一体化通信综合业务系统设计[J].数据通信,2023,(02):1-5.

[4] 覃远超,许桂明,王梦潇,等.视频通信系统运维管理与安全应用研究[J].网络安全技术与应用,2019,(06):101-103.

[5] 杨小宝.集监控、指挥和视频会议为一体的综合通信系统的架构研究[D].西安电子科技大学,2010.