Third-Party Risk Management (TPRM) Charter

Project: StreamSafe Media Content Protection & Risk Oversight

Version: Final Combined Draft

Prepared By: TPRM Manager

Date: [Insert Date]

# 1. Purpose

This charter establishes the framework and objectives for managing third-party risk associated with vendors supporting StreamSafe Media’s media operations—specifically those involved in dubbing, content delivery networks (CDNs), and data analytics. These vendors have access to sensitive content and/or user data, and as such, pose potential risks to StreamSafe Media’s data privacy, intellectual property (IP), and business continuity.  
  
To safeguard StreamSafe Media’s intellectual property, viewer data, and streaming operations, this program emphasizes digital rights management (DRM) technologies such as encryption, watermarking, and access control, ensuring only authorized users can access, use, or share content.

# 2. Scope

This TPRM initiative covers 10 third-party vendors:  
- Dubbing: Echo Dubs, BrightVoice, Vocalcore  
- CDN: StreamServe, ContentLink, EdgePulse  
- Analytics: VizPro, DataNest, CloudQuanta, InsightEdge  
  
The charter applies to vendors who:  
- Handle or process StreamSafe Media-owned video, audio, or scripts  
- Deliver streaming content globally via CDN infrastructure  
- Analyze user or operational data for StreamSafe Media’s internal decision-making  
  
Focus areas include data privacy (GDPR, CCPA), IP protection (DRM, watermarking), and operational continuity (CDN uptime).

The charter covers the full lifecycle of vendor engagement—from onboarding and risk assessment to monitoring, remediation, and offboarding.

# 3. Objectives

- Identify and classify vendors based on inherent and residual risk.

- Evaluate vendor controls related to DRM, encryption, access control, and IP protection

- Mitigate data privacy and content leakage risks

- Ensure full compliance with SOC2,GDPR, CCPA, and ISO 27001 for vendors handling sensitive data

- Achieve 100% vendor compliance with StreamSafe Media’s security standards, including DRM protocols (e.g., Widevine, FairPlay)

- Track and monitor vendor compliance using defined KPIs and scorecards

# 4. Governance

- TPRM Manager: Oversees program execution, manages eramba and eramba configurations  
- Security Team: Reviews DRM, encryption, and access controls, and conducts vendor risk assessments  
- Legal Team: Reviews vendor contracts and SLAs, tracked in eramba’s Contract Management module  
- Privacy Team: Monitors regulatory compliance using eramba’s Compliance Management module  
- Content Operations: Helps onboard vendors by giving them the right files and instructions, and clearly explains what work they are responsible for, when it’s due, and how it should be delivered.

-Governance, Risk & Compliance (GRC): Manages SOC 2, ISO 27001, GDPR, and CCPA compliance for third-party vendors  
- Reporting: Quarterly updates to CISO and Content Operations via eramba dashboards

# 5. Key Risk Areas

- Data Privacy Risks – Handling of PII, analytics data, or user behavior metrics  
- Intellectual Property Risks – Leaks or misuse of unreleased StreamSafe Media content  
- Operational Risks – Downtime or failure of CDN and analytics services  
- Compliance Risks – Violation of contractual obligations or legal requirements

# 6. Evidence Collection and Goal Measurement

**A-Data Privacy Risks – Handling of PII, analytics data, or user behavior metrics**

* **Evidence**: Number of PII breach incidents and GDPR/CCPA compliance violations.
* **Collection Method**: Vendors submit monthly incident reports via eramba’s Compliance Management module; Privacy Team conducts quarterly compliance audits.
* **Goal Measurement**: Zero PII breaches and zero GDPR/CCPA violations indicate successful mitigation of data privacy risks and compliance with regulatory standards (Goal: Ensure full compliance with SOC 2, GDPR, CCPA, ISO 27001).

**B-Intellectual Property Risks – Leaks or misuse of unreleased StreamSafe Media content**

* **Evidence**: Number of content leakage incidents and DRM implementation status (e.g., Widevine/FairPlay).
* **Collection Method**: Security Team tracks leakage incidents in eramba’s Risk Management module; vendors provide DRM policy documentation during assessments.
* **Goal Measurement**: Zero leakage incidents and 100% vendor compliance with Widevine/FairPlay DRM protocols demonstrate effective IP protection (Goal: Achieve 100% vendor compliance with StreamSafe Media’s security standards).

**C-Operational Risks – Downtime or failure of CDN and analytics services**

* **Evidence**: CDN uptime percentages and downtime incident reports.
* **Collection Method**: CDN vendors report uptime via eramba dashboards; incident reports are logged in eramba’s Third Party module.
* **Goal Measurement**: Achieving 99.99% uptime across CDN vendors and zero downtime incidents ensures operational continuity (Goal: Mitigate operational risks).

**D-Compliance Risks – Violation of contractual obligations or legal requirements**

* **Evidence**: Number of contractual violations, legal fines, and SOC 2/ISO 27001 audit findings.
* **Collection Method**: Legal Team tracks violations in eramba’s Contract Management module; Privacy Team logs audit findings in eramba’s Compliance Management module.
* **Goal Measurement**: Zero contractual violations, zero legal fines, and 100% SOC 2/ISO 27001 compliance confirm adherence to contractual and legal requirements (Goal: Ensure full compliance with SOC 2, GDPR, CCPA, ISO 27001).

# 7. Metrics

- **Percentage of vendors with completed risk assessments (Target: 100%, tracked in eramba)**

* **Success Criterion**: All 10 vendors (Echo Dubs, BrightVoice, VocalCore, StreamServe, ContentLink, EdgePulse, VizPro, DataNest, CloudQuanta, InsightEdge) have completed risk assessments by Phase 3, with detailed risk profiles (inherent and residual) documented in eramba’s Risk Management module. This ensures the goal of identifying and classifying vendors by risk is fully met, providing a comprehensive risk baseline for mitigation.

**-Average time to remediate high-risk issues (Target: <30 days, monitored in eramba)**

* **Success Criterion**: The average time to remediate high-risk issues (e.g., non-tamper-proof logs, unclear DRM implementation) across all vendors is less than 30 days, calculated from issue identification (Phase 3 assessments) to resolution (tracked in eramba’s Third Party Risks module). For example, if Echo Dubs’s audit log issue is flagged on May 1, 2025, remediation must be completed by May 30, 2025. This demonstrates effective mitigation of data privacy, IP, and operational risks within the charter’s timeline.

**-Number of compliance violations detected (Target: 0, reported in eramba)**

* **Success Criterion**: Zero compliance violations (e.g., GDPR/CCPA breaches, SOC 2/ISO 27001 non-conformance, contractual breaches) are detected across all vendors by the end of the 6-Phase engagement, as reported in eramba’s Compliance Management module. For instance, no PII breaches (CloudQuanta), content leaks (Echo Dubs), or downtime incidents (ContentLink) occur, confirming full compliance with SOC 2, GDPR, CCPA, ISO 27001, and StreamSafe Media’s security standards.

# 8. Review and Approval

This charter will be reviewed at the end of the 6-Phase engagement and can be enhanced for long-term TPRM scalability across StreamSafe Media operations.