vStream Digital Media

Security Governance & Compliance Framework

Implementation Schedule

Document Version: 1.0
Date: 12 November 2025
Responsible Person: Andrés Pitt, CTO/DPO

Table of Contents

1. Executive Summary

vStream Digital Media operates a comprehensive security governance framework that embeds security and compliance activities into our regular business operations. This framework ensures continuous monitoring, regular assessment, and systematic improvement of our security posture.

Our security governance is built on three principles:

• Integration: Security activities are embedded into existing team meetings and workflows rather than operating as separate processes
• Automation: Where possible, security monitoring and enforcement are automated, with human oversight focused on review and decision-making
• Continuous Improvement: Regular reviews, training, and exercises ensure our security controls evolve with emerging threats and business needs

This document outlines our complete security governance schedule, from daily operations through annual strategic planning.

2. Governance Structure

vStream's security governance operates through a structured meeting cadence that ensures appropriate oversight at all levels of the organisation.

Meeting	Frequency	Duration	Participants
ShineVR Team Standup	Daily	10-20 mins	Product Manager, CTO, Developers
Management Meeting	Weekly	10-20 mins (ShineVR segment)	Senior Management
ShineVR Product Meeting	Monthly	1-2 hours	Product Team, Stakeholders
Security Review Sessions	Quarterly	2-4 hours	CTO, Technical Team
Security Workshops	Semi-Annual	Half-day	All Technical Staff
Policy & Planning Workshop	Annual	Half-day	CTO, Management

Key Roles:

Role	Security Responsibilities
Chief Technology Officer / Data Protection Officer	Overall security strategy and policy ownership; incident response coordination; compliance oversight; policy reviews and updates
Product Manager	Security review of feature releases; production deployment approval; customer security requirements
Backend Developers	Secure coding practices; code review; security testing; infrastructure-as-code development
Line Managers	Team access reviews; policy compliance monitoring; security incident reporting
All Employees	Policy compliance; incident reporting; security awareness; credential protection

3. Daily Security Operations

Security operations are monitored daily through automated systems and team communications.

3.1 Daily Team Standup

Format: 10-20 minute daily meeting

Participants: Product Manager, CTO, Developers

Activity	Owner
Automated backup verification	CTO
Security incident status update	CTO
Priority incident progress review	CTO

3.2 Automated Daily Operations

- Automated backups of all production databases and critical systems
- Continuous security monitoring via Google Cloud Security Command Centre
- Automated backup success verification
- Security alert generation and routing

4. Weekly Governance Activities

Weekly management meetings include security status reporting and review of key metrics.

4.1 Weekly Management Meeting

Format: ShineVR business segment includes security reporting (10-20 minutes total)
Participants: Senior Management

Activity	Owner
Weekly incident review and analysis	CTO
Google Cloud Security Command Centre review	CTO
Change management summary	CTO
Security metrics review	CTO

5. Monthly Compliance Reviews

Monthly product meetings include comprehensive security and compliance reviews.

5.1 Monthly ShineVR Product Meeting

Format: 1-2 hour meeting includes security review segment (15-20 minutes)
Participants: Product Team, Stakeholders

Activity	Owner
Monthly backup restoration testing results	CTO
Detailed incident analysis and trends	CTO
Change control metrics and quality review	CTO
Access exception review	CTO
Security metrics dashboard presentation	CTO
Compliance planning preview	CTO

6. Quarterly Security Assessments

Quarterly security review sessions provide focused assessment of security controls and compliance status.

6.1 Quarterly Security Review Sessions

Format: Dedicated sessions scheduled throughout each quarter
Total Time: Approximately 8-10 hours per quarter

Activity	Duration	Owner
Comprehensive access review	2-3 hours	CTO
Incident response team training	2 hours	CTO + Response Team
Incident trends analysis	1 hour	CTO
Change control audit	2 hours	CTO
Critical vendor performance reviews	1-2 hours	CTO
Vendor register review and updates	1 hour	CTO
Anti-malware recommendations update	30 minutes	CTO
Contact information accuracy testing	30 minutes	CTO
Communication channels testing	1 hour	CTO
Cloud security exception review	30 minutes	CTO

6.2 Quarterly Schedule

Week 1: Comprehensive access review session
Week 2: Incident response training and trends analysis
Week 3: Vendor reviews and anti-malware list updates
Week 4: Change control audit and communication testing

7. Semi-Annual Security Exercises

Twice annually, vStream conducts comprehensive security exercises to test incident response capabilities and assess high-risk vendor relationships.

7.1 Security Exercise Workshop

Format: Half-day workshop
Frequency: March and September
Participants: CTO, Response Team, Technical Staff

Activity	Duration
Tabletop incident response exercise	3 hours
High-risk vendor comprehensive reviews	2 hours
Lessons learned and action planning	1 hour

Workshop Format:

Morning Session:
• Scenario-based tabletop incident response exercise
• Team coordination and communication practice
• Incident response procedure validation
• Documentation and reporting review

Afternoon Session:
• High-risk vendor performance assessment
• Vendor security posture review
• Contract and SLA compliance evaluation
• Lessons learned from tabletop exercise
• Action items and improvement planning

8. Annual Security Programme

Annual activities ensure strategic security planning, comprehensive policy reviews, and organisation-wide training.

8.1 Annual Policy Review Workshop

Format: Half-day workshop
Timing: January
Owner: CTO with management input

All security policies undergo annual review:

- Information Security Policy
- Network Security Policy
- Password Policy
- Encryption Policy
- Access Management Policy
- Backup and Recovery Policy
- Change Control Policy
- Cloud Security Policy
- BYOD Policy
- Physical Security Policy
- Vendor Management Policy
- Incident Response Plan
- Media Retention and Disposal Policy

Review Process:
• Technical accuracy verification
• Alignment with current infrastructure
• Integration of lessons learned
• Regulatory requirement updates
• Version control and documentation
• Stakeholder communication

8.2 Annual Training Programme

vStream delivers comprehensive security training throughout the year in quarterly sessions.

Quarter	Training Session	Audience & Duration
Q1	Security Awareness Refresher	All Staff (2 hours) Covers: Security fundamentals, passwords, access management, incident reporting
Q2	Technical Security Training	Technical Staff (3 hours) Covers: Cloud security, encryption, backup procedures, change control
Q3	BYOD & Physical Security	All Staff (1.5 hours) Covers: Device security, BYOD compliance, physical security, data handling
Q4	Incident Response & Disaster Recovery	All Staff (2 hours) + Technical Staff (additional 2 hours) Covers: Incident response procedures, disaster recovery exercise

8.3 Other Annual Activities

Activity	Duration	Timing
Google Cloud Platform security assessment	3-4 hours	February
Line manager team access reviews	1-2 hours per manager	January
Comprehensive asset inventory audit	4-6 hours	November
Comprehensive vendor register review	3 hours	November
Annual backup and recovery exercise	4 hours	October
Comprehensive security metrics review	2 hours	Early December

9. New Employee Security Onboarding

All new employees complete comprehensive security training during their first week.

9.1 Onboarding Programme

Duration: 3-4 hours across first week

Delivery: Mix of policy review, hands-on configuration, and presentations

Day	Security Training Content
Day 1 Morning	• Information Security Policy (mandatory acknowledgement) • Password Policy and password manager setup • Multi-factor authentication enrollment • Access management overview
Day 1 Afternoon	• Physical security procedures • BYOD Policy (if applicable) • Incident reporting procedures • Emergency contacts
Days 2-3	• Technical staff: Cloud security, encryption, backup systems • Technical staff: Change control and deployment procedures • All staff: Network security basics and best practices

10. Continuous Monitoring & Response

vStream operates continuous security monitoring with automated alerting and defined response procedures.

10.1 Automated Security Monitoring

- Google Cloud Security Command Centre continuous monitoring
- ISO 27001, SOC 2, and GDPR compliance monitoring
- Backup success rate monitoring with automated alerts
- Security incident detection and alerting
- Vendor security posture monitoring
- Access control monitoring and logging

11. Annual Security Calendar

The following calendar outlines the annual schedule of dedicated security activities.

Quarter 1 (January-March)

Timing	Activity
January Week 2	Annual Policy Review Workshop (half-day)
January Week 3-4	Line manager team access reviews
February Week 1	Q1 Security Awareness Training (All Staff, 2 hours)
February Week 2	Google Cloud Platform annual assessment
March Week 1	Q1 Comprehensive Access Review
March Week 2	Q1 Incident Response Training
March Week 3	Q1 Critical Vendor Reviews
March Week 4	Semi-Annual Security Exercise Workshop (half-day)

Quarter 2 (April-June)

Timing	Activity
April Week 2	Q2 Technical Security Training (Technical Staff, 3 hours)
June Week 1	Q2 Comprehensive Access Review
June Week 2	Q2 Incident Response Training
June Week 3	Q2 Critical Vendor Reviews
June Week 4	Q2 Change Control Audit

Quarter 3 (July-September)

Timing	Activity
July Week 2	Q3 BYOD & Physical Security Training (All Staff, 1.5 hours)
September Week 1	Q3 Comprehensive Access Review
September Week 2	Q3 Incident Response Training
September Week 3	Q3 Critical Vendor Reviews
September Week 4	Semi-Annual Security Exercise Workshop (half-day)

Quarter 4 (October-December)

Timing	Activity
October Week 2	Q4 Incident Response & DR Training (All Staff, 2 hours)
October Week 3	Extended Disaster Recovery Exercise (Technical Staff, 2 hours)
November Week 1	Annual Asset Inventory Audit
November Week 2	Comprehensive Vendor Register Review
November Week 3	Q4 Comprehensive Access Review
November Week 4	Q4 Incident Response Training
December Week 1	Q4 Critical Vendor Reviews
December Week 2	Annual Security Metrics Review

Summary

vStream Digital Media's security governance framework provides comprehensive oversight through:

EMBEDDED GOVERNANCE:
• Daily security operations integrated into team standups
• Weekly security reporting in management meetings
• Monthly compliance reviews in product meetings

DEDICATED SECURITY ACTIVITIES:
• Quarterly: ~8-10 hours of focused security assessments
• Semi-Annual: Half-day security exercise workshops
• Annual: ~20 hours including policy reviews, training, and assessments

CONTINUOUS MONITORING:
• 24/7 automated security monitoring and alerting
• Defined incident response timelines
• Immediate access management procedures

TRAINING & AWARENESS:
• Comprehensive new employee onboarding (3-4 hours)
• Quarterly training sessions for all staff
• Specialised technical training for development team
• Semi-annual tabletop exercises

This framework ensures vStream maintains robust security controls, regulatory compliance, and continuous improvement while minimising disruption to business operations.

Contact Information

Data Protection Officer / Chief Technology Officer:
Andrés Pitt
Email: andres@vstream.ie
Phone: (086) 788 6570
Available 24/7 for critical security incidents

Company Address:
vStream Digital Media
37 Leeson Close
Dublin 2, D02 H344
Ireland

Website: vstream.ie