Pitch-to-Play Content Security Risk Assessment Framework

Prepared by Robinpreet Waraich

1. Project Overview

This project presents a structured Content Security Risk Assessment Framework designed to analyze and mitigate security risks across the full pitch-to-play lifecycle of a fictional Netflix original production. The framework evaluates physical, digital, and human-related risks and proposes layered mitigation strategies aligned with industry practices.

2. Pitch-to-Play Lifecycle Scope

The assessment spans Pitch & Development, Pre-Production, Production, Post-Production, and Marketing & Release. Each phase introduces unique vulnerabilities requiring tailored security controls.

3. Risk Identification and Classification

Lifecycle Phase	Key Risks	Risk Category
Pitch & Development	Script leaks, unauthorized access to creative ideas	Digital / Insider
Pre-Production	Vendor data exposure, unsecured file sharing	Digital / Vendor
Production	On-set recording, badge misuse, device theft	Physical / Human
Post-Production	Footage leaks, insider misuse, insecure transfers	Digital / Insider
Marketing & Release	Early trailer leaks, PR asset exposure	Digital / Reputational

4. Mitigation Strategies

Digital Controls: Role-based access control, least-privilege permissions, encrypted transfers, watermarking, secure collaboration tools.

Physical Controls: Credentialed access, device restrictions, secure storage, controlled screenings.

Human & Process Controls: NDAs, vendor audits, security training, incident escalation and access revocation.

5. Business and Talent Impact

Effective content security protects Netflix’s creative investment, preserves trust with talent and partners, and mitigates financial and reputational risk while enabling creative freedom.

6. Key Learnings

This project strengthened my understanding of how physical security, cybersecurity, and operational judgment intersect to protect high-value creative assets throughout their lifecycle.