GRC Case Study: Security & Privacy Risks in Rideshare Platforms (Uber & Lyft)

**Author:** Chukwuemeke Ikpeasonim

**Duration of Experience:** 6 years (35,000+ rides)

**Date Created**: May 18, 2025

**Perspective:** Independent contractor/driver for Uber and Lyft

# 1.0 Background

Rideshare platforms such as Uber and Lyft have revolutionized urban transportation. However, from the perspective of a frontline driver, these platforms expose critical weaknesses in user authentication, data protection, safety features, and incident response protocols.  
  
Having completed over 35,000 rides across various cities, I have experienced firsthand the systemic gaps that put both drivers and riders at risk. This project presents a practical risk and GRC analysis based on real-world observations, framed through the lens of governance, risk management, and compliance.  
  
As a GRC analyst transitioning from the field into cybersecurity, I believe that this project bridges real-world operational risk with strategic risk governance. It reflects both the technical and human components of security.

# 2.0 Purpose

This GRC portfolio aims to:  
\* Highlight risks related to identity verification, safety protocols, and data privacy  
\* Propose governance improvements to mitigate identified risks  
\* Map findings to compliance frameworks like NIST CSF and GDPR  
\* Simulate deliverables that demonstrate my skills in GRC documentation and reporting  
\* Provide hiring managers with clear evidence of analytical, compliance, and real-world risk awareness

# 3.0 Scope

The scope of this project includes:  
\* Risk identification and classification  
\* Policy enhancement proposal  
\* Compliance gap checklist  
\* Dashboard reporting for risk visibility  
  
This is a fictional simulation grounded in authentic experience, created for learning and career development.

# 4.0 Risk Register – Rideshare Security and Privacy Risks

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Risk ID** | **Risk Title** | **Risk Type** | **Likelihood** | **Impact** | **Risk Rating** | **Control Gap** | **Description** |
| R-01 | Fake Rider Profiles | Identity Fraud | High | High | Critical | Yes | Riders can sign up using false names/photos, increasing risk of assault or fraud |
| R-02 | GPS Spoofing or Delay | Operational | Medium | Medium | Moderate | Yes | Delayed or inaccurate GPS tracking affects fare calculation and legal disputes |
| R-03 | Inadequate Panic Button Response | Physical Safety | High | High | Critical | Yes | Panic button often fails to trigger a human follow-up or intervention |
| R-04 | App Crashes During Active Trips | Operational | Medium | High | High | Yes | Disrupts navigation, leaves no evidence of ride activity in some cases |
| R-05 | Data Exposure via Screenshots | Privacy/Data Leak | High | High | Critical | Yes | Rider screenshots show driver name, photo, license plate – risks doxxing |
| R-06 | Weak Account Recovery | Account Security | Medium | Medium | Moderate | Yes | Hijacked driver accounts via email reset scams |
| R-07 | Inadequate Rider Vetting | Compliance | High | High | Critical | Yes | No ID or biometric verification required for new riders |

# 5.0 Next Steps

As I continue to transition into a full-time GRC role, I plan to build on this project through the following actionable steps:

* **Develop a Policy Improvement Proposal:** I will create a detailed document recommending new or enhanced policies aimed at strengthening user privacy and in-ride safety.
* **Construct a Compliance Checklist:** Using the NIST Cybersecurity Framework and GDPR principles, I’ll map key requirements against observed gaps to showcase my understanding of regulatory alignment.
* **Design a Visual Risk Dashboard:** I intend to build a dashboard that represents risk severity, likelihood, and mitigation status, making the data more consumable for stakeholders.
* **Publish on GitHub and LinkedIn:** I will host this full portfolio on GitHub and share insights from the project on LinkedIn, along with a downloadable version, to boost visibility and credibility with recruiters and the GRC community.

**> Disclaimer**: This simulation is based on firsthand experience but does not disclose confidential or proprietary information. All names and incidents are anonymized.