Risk Management Plan for Sprint 7
FIA Cybersecurity App for Women

Context and Objectives

Sprint 7 focuses on improving engagement, oversight, and data integrity as we move toward an MVP test deployment. Key areas include badge progression for Participants and Helpers, stronger session tracking and linked completion rules, cleaner University Admin and Super Admin views, and clearer audit visibility through role-based logging.

This plan identifies the highest risk areas for Sprint 7 work, how we will detect issues early, and how we will respond if new risks emerge during implementation and testing.

Sprint 7 Focus Areas

- Badge tracking and rewards (planning, design, awarding, and viewing)
- Admin audit logging pages and a progress question workflow
- University Admin and Super Admin UI polish and targeted bug fixes
- Security pass through for sensitive data and secure storage practices
- Mobile WebForms optimization using mobile-only overrides
- Application Use Guide screenshot refresh and accuracy validation

Risk Identification and Assessment

Risk	Impact and Likelihood	Mitigation
Badge awarding is incorrect or inconsistent across roles	High impact; medium likelihood. Incorrect rewards reduce trust and make progress feel unreliable.	Centralize badge criteria and awarding checks, award from real tracked events, and add tests for earn, not earn, and no duplicates.
Progress and completion status becomes inconsistent when attendance is missing or sessions change	High impact; medium likelihood. Reporting and pilot reviews can be questioned if records do not match reality.	Gate completion behind validated attendance and session status, retest reschedules and late joins, and verify Admin logs reflect the same source of truth.
Admin views show confusing or incomplete audit history	Medium to high impact; medium likelihood. Admins may not be able to explain outcomes or investigate	Standardize log fields and messages, add filters for key event types and date ranges, and validate log readability

	issues.	with real scenarios.
Sensitive data is stored or logged in plaintext	High impact; low to medium likelihood. This is not acceptable for real users and blocks readiness.	Define sensitive fields, audit storage and logs, implement hashing for passwords and other sensitive values, and update all reads and writes to use hashed storage.
Mobile optimizations accidentally change desktop layouts	Medium impact; medium likelihood. Desktop polish regressions are visible and costly to fix late.	Keep all mobile changes inside media queries, scope overrides to page wrappers when needed, and compare desktop screenshots before and after merges.

Unexpected Risks and Challenges in Sprint 7

1. Cross-view progress synchronization required more retries and testing than planned.

Getting session progress to update correctly across Participant views, Helper views, Admin logs, and system logs was harder than expected because small state and timing issues can cause one area to lag behind the others.

We managed this by re-testing the same scenarios end to end, tightening the completion and attendance checks, and verifying that each write produced the expected log entries and progress updates.

2. Curating strong, session-ready cybersecurity course material took more time than expected.

We found that many resources were either too advanced, too long for a short session, or not a good fit for the FIA audience. We reduced risk by narrowing objectives, using a standard course template, and adding a quick review step before marking content ready.

Weekly Risk Reviews Summary

Week of February 23, 2026

What we review each week:

- Badge criteria clarity and awarding correctness
- Linked completion accuracy and attendance edge cases
- Admin log completeness and readability
- Security checks for plaintext storage and logging
- Mobile usability on common phone screen sizes without desktop impact

How we keep risks visible:

- Track risk items in Taiga and update the RiskManagement file in GitHub as changes land
- Use a short regression checklist before merging UI or workflow changes
- Call out any new risk signals during standups and add them as follow-up items immediately

Top Risks This Sprint

1. Progress and completion consistency across roles and logs

2. Badge awarding correctness and duplicate prevention

3. Plaintext sensitive data exposure through storage or logs

Notes for Sprint Close

- Run a final end to end walkthrough for Participant, Helper, University Admin, and Super Admin flows.
- Verify badges: earn, not earn, and locked state hints on both home screens.
- Confirm audit logs are scannable and filters work for date range and event type.
- Re-scan storage and logs to confirm sensitive fields are not present in plaintext.
- Refresh any changed screenshots in the Application Use Guide using seeded demo data.