# Agent-Based Risk Analysis and Assessment on Windows-Based Machines Using the ISO 27001 Standard

Project proposal & Statement of Work

Mehran Tajbakhsh, Project Manager

ADVISOR:

Dr. Rozhin Yasaei

Date: Feb, 15, 2026

| Revision History Table | | Template Date 2/12/2026 |
|---|---|---|
| Version | Summary of Changes | Date |
| *0.5* | *Template info removed; first draft of all sections completed* | *02/10/26* |
| *0.6* | *Add Technical Architecture and Implementation Design* | *02/14/26* |

# Contents

1. Executive Summary ..... 3

2. User/Market research ..... 4

3. Product Features ..... 5

Feature 1: Automated Context Establishment (Scope & Boundaries) ..... 5

Feature 2: Asset Identification & Classification ..... 6

Feature 3: Threat and Vulnerability Identification ..... 6

Feature 4: Identification of Existing Controls (Current Security Posture) ..... 6

Feature 5: Risk Analysis (Likelihood and Impact Assessment) ..... 7

Feature 6: Risk Evaluation (Prioritization and Decision Support) ..... 7

Feature 7: Risk Treatment Selection ..... 8

Feature 8: ISO 27001 Control Selection and Annex A Mapping ..... 8

Feature 9: Control Implementation and Action Planning ..... 8

Feature 10: Continuous Monitoring, Review, and Improvement ..... 9

Feature 11: ISO 27001 Final Deliverables and Documentation Generation ..... 9

4. Technical Architecture and Implementation Design ..... 10

5. Project Timeline & Gannt Chart ..... 11

6. Ethics ..... 12

7. Approvals ..... 14

8. Appendix ..... 15

A. Advisor Engagement ..... 15

1) Project Team Responsibilities ..... 15

2) Faculty Advisor Responsibilities ..... 15

B. Ground Rules ..... 16

# 1. Executive Summary

*The Executive Summary was written by Mehran Tajbakhsh.*

My product is an agent-based risk analysis and assessment system for Windows-based machines that automatically collect security-relevant system information and converts it into a structured, audit-ready risk report aligned with the ISO/IEC 27001 standard. Key features include automated discovery of operating system version, installed software and patch levels, running services, active configurations, and server roles, followed by mapping these findings to relevant ISO 27001 control requirements. The system will output prioritized risks, compliance gaps, and recommended mitigations, helping security teams quickly identify weaknesses and focus remediation efforts on the highest-impact issues.

This product is needed because many organizations still rely on manual or semi-manual security assessments, which are time-consuming, inconsistent, and difficult to scale across large Windows environments. These limitations increase the likelihood of missing critical vulnerabilities, misconfigurations, or outdated software, which can lead to security incidents and failed audit readiness. ISO/IEC 27001 emphasizes maintaining an effective information security management system (ISMS) with risk-based decision-making and continual improvement, but achieving this in practice requires reliable, repeatable, and evidence-based assessment processes. Our solution is unique because it combines agent-based automated evidence collection with direct mapping to ISO 27001 controls, producing results that are not only technical but also compliance-oriented, enabling organizations to reduce assessment effort while improving consistency, traceability, and audit preparedness. [1]

Development will involve designing and implementing the Windows agent, building the control-mapping and risk scoring logic, and generating a standardized reporting format suitable for security and compliance stakeholders. The project work will be completed individually, with development and testing performed in a controlled lab environment using Windows systems (server and desktop) to validate data collection accuracy and reporting outputs. By the end of the semester, the completed deliverable will include a working prototype capable of collecting system security data, mapping it to ISO 27001 requirements, and producing a structured risk report with prioritized findings and actionable mitigations.

| Team Member | Feature responsibility |
|---|---|
| Mehran Tajbakhsh | Project Manager, Developer |

*Table 1 Preliminary Subsystem Responsibilities*

[1] ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

# 2. User/Market research

The market for cybersecurity risk assessment and compliance automation is large and growing, driven by increasing regulatory requirements and the need for organizations to continuously monitor and document security controls. Governance, Risk, and Compliance (GRC) software—closely aligned with ISO/IEC 27001 risk management and audit readiness—was valued at over $21B in 2025 and is projected to reach nearly $39B by 2031, showing strong demand for tools that reduce manual compliance workload.[2] In addition, ISO 27001 adoption is increasing, with 81% of organizations reporting current or planned ISO 27001 certification in 2025, which supports the need for automated evidence collection and reporting solutions like this project.[3]
Gartner publishes the Magic Quadrant for Governance, Risk and Compliance (GRC) Tools, Assurance Leaders, which evaluates major vendors in the GRC market and helps buyers understand competitive positions and product maturity in comprehensive risk and compliance platforms. This report highlights trends such as AI and automation being key differentiators among leading GRC solutions. [4]
Recent Gartner coverage shows the GRC market is dynamic and evolving, with shifting competitive dynamics and increasing demand for integrated, automated risk and compliance capabilities. [5]
Gartner also produces Innovation Insight research on Cyber GRC tools, which specifically focuses on technologies that automate and streamline cybersecurity risk, control monitoring, and compliance workflows — directly relevant to risk assessment and compliance automation requirements like ISO 27001.

***Existing competitors**:*

- ISMS Copilot – An AI-based compliance assistant that automates policy creation, risk assessments, and audit reporting, and supports 30+ frameworks such as ISO 27001 and SOC 2. It targets information security teams seeking broad framework coverage and guided compliance workflows.
- Sprinto – A compliance automation platform focused on simplifying onboarding, tracking compliance issues in real time, and organizing audit documentation; often used by teams to streamline SOC 2 and ISO 27001 readiness with continuous compliance checks.
- Fortinet Compliance Automation – Part of the broader Fortinet security ecosystem, this tool applies AI for policy enforcement and multi-framework compliance (e.g., PCI DSS, GDPR) with risk assessment and automated remediation capabilities.
- Wiz (AI Security Posture Management) – A cloud-centric platform that simplifies compliance workflows and risk visibility across cloud assets, helping security teams assess posture and compliance continuously.
- Compliance.ai – A machine-learning-based tool that focuses on regulatory monitoring, automatically tracking changes across jurisdictions and integrating updates into internal compliance programs.

[2] Mordor Intelligence, *Governance, Risk and Compliance Software Market* (2025–2031 forecast).
[3] Secureframe, *Compliance Statistics (2025)*.
[4] Gartner, *Magic Quadrant & Critical Capabilities methodology overview*.
[5] Gartner, *Definition of GRC Tools for Assurance Leaders*.

Additional tools in the broader AI compliance ecosystem include Vanta, which automates evidence collection and continuous compliance for frameworks like ISO 27001 and SOC 2, and other AI compliance platforms such as Drata and EasyAudit focusing on SOC 2 and broader regulatory needs.

**User insights:**

Your agent-based risk analysis and ISO 27001 assessment system differentiate from these competitors in several keyways:

- Endpoint-Level Data Collection – Unlike most competitor tools that rely on agentless APIs, manual uploads, questionnaires, or cloud integrations, this product uses lightweight agents on Windows machines to automatically collect security-relevant system configuration and state data (OS version, installed software, services, roles). This yields more accurate and comprehensive technical evidence.
- Direct ISO 27001 Control Mapping – Rather than offering general compliance automation, it maps raw endpoint data directly to ISO 27001 control requirements, producing structured risk reports with prioritized findings, compliance gaps, and actionable mitigations — minimizing interpretation work for security teams.
- Technical and Compliance Focus Combined – Many competitor tools emphasize policy automation, regulatory tracking, or posture dashboards; this product combines technical security posture assessment with compliance reporting, closing the gap between security operations and audit readiness.

Together, these differentiators position your product as a specialized solution for automated endpoint data gathering and ISO 27001–aligned risk reporting, appealing to organizations that need deep technical insight and audit-ready outputs rather than just policy or documentation automation.

# 3. Product Features

## Feature 1: Automated Context Establishment (Scope & Boundaries)

This section was written by Mehran Tajbakhsh

This feature automatically establishes the risk assessment context by discovering key characteristics of a Windows-based system and generating an ISO 27001–aligned scope statement. It reduces reliance on manual scoping interviews and ensures consistency across assessments.

| Parameter | Comments: |
|---|---|
| Input | OS details, domain info, installed roles, system metadata |
| Processing | Role inference, environment classification, ISO context mapping |
| Output | Structured scope definition + human-readable ISO-style scope statement |
| User Controls | Accept, edit, or refine scope through conversation |

*Table 2: Automated Context Establishment Parameters*

This feature automatically establishes the scope and boundaries of a risk assessment by detecting key system characteristics such as OS type, domain membership, environment, and installed server roles. An LLM then translates these technical findings into clear, ISO 27001–aligned scope statements through a conversational interface that non-specialist administrators can easily review and refine. The result is a consistent, audit-ready context definition created with minimal manual effort.

## Feature 2: Asset Identification & Classification

This section was written by Mehran Tajbakhsh

This feature automatically identifies and classifies assets present on a Windows-based system by enumerating software, services, users, network exposure, and data locations. It also highlights sensitive assets and uses LLM reasoning to assign confidentiality, integrity, and availability (CIA) importance levels to support structured risk analysis.

| Parameter | Comments: |
|---|---|
| Input | Installed software, running services, open ports, user accounts, data paths |
| Processing | Asset enumeration, sensitive asset detection, CIA impact classification |
| Output | Structured asset inventory with CIA classification and sensitivity tags |
| User Controls | Review, adjust asset classifications, override CIA ratings |

*Table 3: Asset Identification & Classification Parameters*

This feature provides a comprehensive and structured inventory of system assets by automatically discovering technical components and identifying sensitive resources such as databases, certificate stores, and Active Directory objects. An LLM assists in classifying assets based on confidentiality, integrity, and availability importance, enabling consistent prioritization and reducing reliance on manual asset identification.

## Feature 3: Threat and Vulnerability Identification

This section was written by Mehran Tajbakhsh

This feature identifies potential threats, threat sources, and system vulnerabilities by analyzing discovered assets, configurations, and software versions on a Windows-based system. It combines agent-based detection with vulnerability correlation to produce a structured view of security weaknesses that could lead to risk exposure.

| Parameter | Comments: |
|---|---|
| Input | Asset inventory, software versions, system configurations, patch status |
| Processing | Threat mapping, vulnerability detection, CVE correlation, misconfiguration analysis |
| Output | List of identified threats, vulnerabilities, and weaknesses mapped to assets |
| User Controls | Review findings, suppress false positives, mark accepted risks |

*Table 4: Threat and Vulnerability Identification Parameters*

This feature maps identified assets to relevant threat categories while detecting vulnerabilities such as missing patches, insecure configurations, and unnecessary services or software. By correlating software versions with known CVE sources, the system provides actionable and up-to-date visibility into potential security weaknesses, enabling more accurate and timely risk analysis.

## Feature 4: Identification of Existing Controls (Current Security Posture)

This section was written by Mehran Tajbakhsh

This feature assesses the current security posture of a Windows-based system by detecting existing technical and administrative security controls and validating their configuration state. An LLM then maps the detected controls to relevant ISO 27001 Annex A controls and generates justification text to support compliance and audit activities.

| Parameter | Comments: |
|---|---|
| Input | Security configuration data, system policies, enabled services, protection mechanisms |
| Processing | Control detection, configuration validation, ISO Annex A mapping |
| Output | Inventory of existing controls with ISO 27001 Annex A references and justification text |
| User Controls | Review mappings, edit justification text, confirm control effectiveness |

*Table 5: Identification of Existing Controls Parameters*

This feature provides visibility into the current security posture by automatically detecting controls such as MFA, endpoint detection and response (EDR), firewalls, backups, and encryption. By mapping these controls to ISO 27001 Annex A and generating standardized justification text, the system reduces manual documentation effort and improves audit readiness.

## Feature 5: Risk Analysis (Likelihood and Impact Assessment)

This section was written by Mehran Tajbakhsh

This feature performs quantitative and qualitative risk analysis by calculating the likelihood and impact of identified threats based on system exposure, exploitability, and asset criticality. An LLM translates numeric risk scores into human-explainable reasoning and management-level risk language to support informed decision-making.

| Parameter | Comments: |
|---|---|
| Input | Threat data, vulnerability findings, asset criticality, system exposure indicators |
| Processing | Likelihood calculation, impact estimation, risk scoring |
| Output | Risk scores with qualitative explanations and management-level summaries |
| User Controls | Adjust weighting factors, review reasoning, approve risk assessments |

*Table 6: Risk Analysis Parameters*

This feature evaluates security risks by combining likelihood and impact factors derived from technical findings and asset importance. By converting calculated risk scores into clear, management-oriented explanations, the system bridges the gap between technical analysis and business decision-making.

## Feature 6: Risk Evaluation (Prioritization and Decision Support)

This section was written by Mehran Tajbakhsh

This feature evaluates analyzed risks by comparing calculated risk levels against predefined risk acceptance criteria. It automatically prioritizes risks and flags those requiring treatment, supporting consistent and defensible risk decision-making.

| Parameter | Comments: |
|---|---|
| Input | Risk scores, likelihood and impact ratings, risk acceptance thresholds |
| Processing | Risk comparison, prioritization, acceptance decision logic |
| Output | Ranked risk list with acceptance, treatment, or monitoring decisions |
| User Controls | Adjust acceptance criteria, override decisions, document approvals |

*Table 7: Risk Evaluation Parameters*

This feature enables organizations to consistently prioritize risks by evaluating them against defined acceptance criteria. By clearly identifying which risks require treatment versus acceptance, it helps decision-makers focus remediation efforts where they provide the greatest business value.

## Feature 7: Risk Treatment Selection

This section was written by Mehran Tajbakhsh

This feature supports risk treatment planning by proposing appropriate treatment options based on evaluated risk levels and organizational context. An LLM generates ISO 27001–compliant risk treatment descriptions to ensure consistency, traceability, and audit readiness.

| Parameter | Comments: |
|---|---|
| Input | Evaluated risks, risk decisions, asset criticality, organizational risk posture |
| Processing | Treatment option selection, ISO-compliant description generation |
| Output | Recommended risk treatment options with formal treatment statements |
| User Controls | Select preferred treatment option, edit descriptions, approve plans |

*Table 8: Risk Treatment Selection Parameters*

This feature helps organizations systematically decide how to address identified risks by recommending mitigation, avoidance, transfer, or acceptance options. By automatically generating ISO-compliant treatment descriptions, it reduces documentation effort and ensures alignment with ISO 27001 requirements.

## Feature 8: ISO 27001 Control Selection and Annex A Mapping

This section was written by Mehran Tajbakhsh

This feature automates the selection of relevant ISO 27001 Annex A controls based on identified risks and chosen treatment options. It also tracks applied versus excluded controls and uses LLM assistance to generate a formal Statement of Applicability (SoA).

| Parameter | Comments: |
|---|---|
| Input | Risk treatment decisions, evaluated risks, asset classifications |
| Processing | Annex A control selection, applicability tracking, SoA generation |
| Output | Selected control list with applied/excluded status and Statement of Applicability |
| User Controls | Review control selection, justify exclusions, approve SoA |

*Table 9: ISO 27001 Control Selection and Annex A Mapping Parameters*

This feature ensures systematic and consistent selection of ISO 27001 Annex A controls by aligning them with identified risks and treatment decisions. By automatically generating and maintaining the Statement of Applicability, it simplifies compliance documentation and supports audit readiness.

## Feature 9: Control Implementation and Action Planning

This section was written by Mehran Tajbakhsh

This feature supports the implementation phase by validating the status of selected security controls and assisting with action plan execution. An LLM generates structured task descriptions, remediation documentation, and draft policy text to support consistent and efficient control implementation.

| Parameter | Comments: |
|---|---|
| Input | Selected ISO 27001 controls implementation requirements, system state |
| Processing | Control status validation, action plan generation, documentation drafting |
| Output | Implementation of status reports, remediation tasks, policy and procedure drafts |
| User Controls | Review tasks, edit documentation, confirm implementation completion |

*Table 10: Control Implementation and Action Planning Parameters*

This feature bridges the gap between risk treatment decisions and operational execution by validating control implementation and generating actionable remediation plans. By automating documentation and policy drafting, it reduces manual effort while supporting consistent and auditable security improvements.

## Feature 10: Continuous Monitoring, Review, and Improvement

This section was written by Mehran Tajbakhsh

This feature enables continuous risk management by monitoring system changes, configuration drift, newly installed software, and emerging threats. When significant changes are detected, it automatically triggers risk reassessment and uses LLM assistance to summarize findings in management-friendly views and audit-ready reports.

| Parameter | Comments: |
|---|---|
| Input | System configuration changes, software inventory updates, threat intelligence signals |
| Processing | Change detection, drift analysis, reassessment triggering |
| Output | Updated risk status, management summaries, audit-ready monitoring reports |
| User Controls | Configure monitoring thresholds, review summaries, approve reassessments |

*Table 11: Continuous Monitoring, Review, and Improvement Parameters*

This feature ensures that risk assessments remain current by continuously monitoring for environmental and threat changes. By converting technical changes into management-level summaries or natural language reports, it supports ongoing compliance, informed decision-making, and continuous improvement aligned with ISO 27001.

## Feature 11: ISO 27001 Final Deliverables and Documentation Generation

This section was written by Mehran Tajbakhsh

This feature produces the standard ISO 27001 outputs by consolidating data collected throughout the risk analysis and assessment lifecycle. An LLM acts as an intelligent ISO 27001 assistant to generate structured, audit-ready documentation aligned with recognized compliance expectations.

| Parameter | Comments: |
|---|---|
| Input | Risk analysis data, asset inventory, risk decisions, control mappings, monitoring results |
| Processing | Data consolidation, ISO document structuring, narrative generation |
| Output | Complete set of ISO 27001 deliverables in audit-ready format |
| User Controls | Review documents, edit content, approve final deliverables |

*Table 12: ISO 27001 Final Deliverables and Documentation Generation Parameters*

This feature generates key ISO 27001 artifacts including the risk assessment methodology, asset inventory and classification, risk register, risk treatment plan, Statement of Applicability, and evidence of implemented controls and monitoring. By automating documentation creation through an LLM, the system reduces manual effort, improves consistency, and supports audit readiness with minimal additional work.

# 4. Technical Architecture and Implementation Design

This section defines the technical architecture, implementation strategy, and deployment model of the proposed agent-based risk analysis and assessment system designed for Windows-based enterprise environments. The architecture emphasizes privacy, scalability, and automation by leveraging locally hosted artificial intelligence components to ensure that sensitive security data remains within the organizational boundary.

Enterprise networks consist of multiple specialized Windows servers that provide essential infrastructure, security, and operational functions.

| Server Role | Purpose |
|---|---|
| Domain Controller (DC) | Authentication and Active Directory management |
| DNS Server | Name resolution for network resources |
| DHCP Server | Automatic IP address assignment |
| File Server | Centralized file storage and access control |
| Group Policy Server | Security policy and configuration enforcement |
| Certificate Authority (CA) | PKI infrastructure and certificate management |
| Application Server | Enterprise application hosting |
| Database Server | Structured data storage and management |
| WSUS Server | Patch management and update distribution |
| Backup Server | Backup and disaster recovery |
| SIEM / Monitoring Server | Security monitoring and event correlation |

*Table 1: Enterprise Server Roles Considered in the Assessment:*

The initial implementation will focus on a controlled proof-of-concept deployment consisting of one Windows Server representing enterprise infrastructure and one Windows Workstation representing an endpoint system. This phased deployment allows validation of the core system capabilities, including automated system enumeration, role identification, risk analysis, ISO 27001 control mapping, and automated report generation using AI-assisted reasoning. This approach reduces deployment complexity while enabling verification of system accuracy, reliability, and effectiveness.

During execution, the agent operates locally on each system and collects security-relevant data such as operating system version, installed software, running services, system roles, patch status, and security configuration settings. The collected data is analyzed to identify security misconfigurations, outdated or vulnerable software, missing patches, and deviations from expected role-based security baselines. The system then generates structured risk assessment reports that include identified risks, severity levels, and recommended mitigation actions.

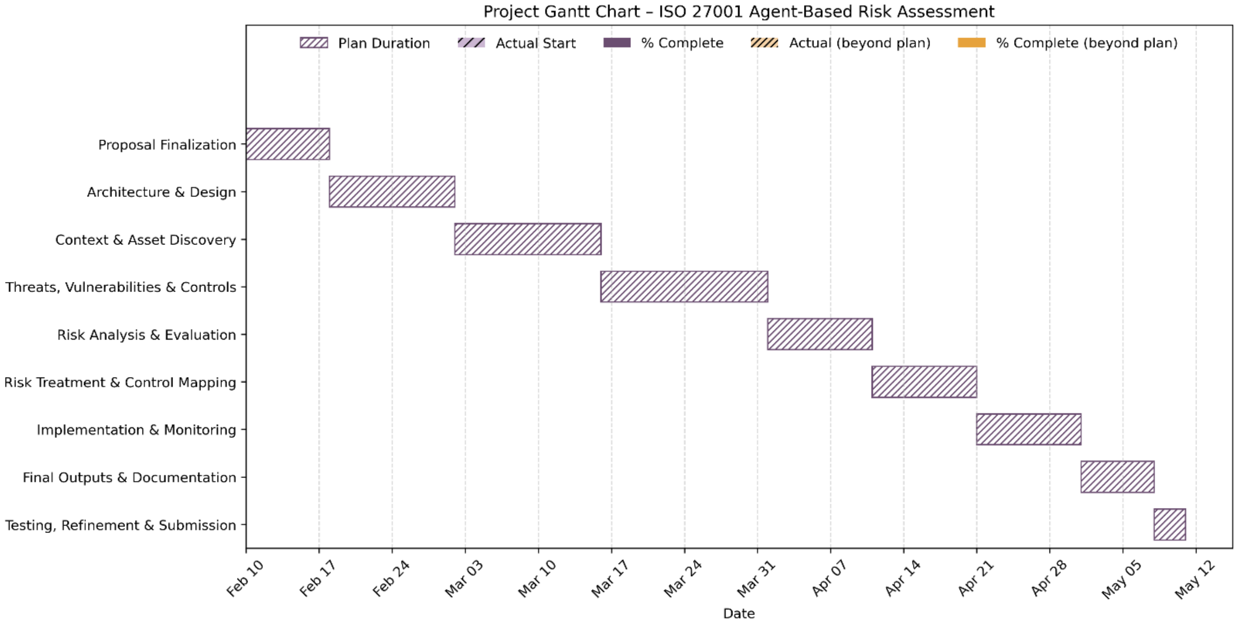
Following successful validation, architecture is designed to scale across the enterprise network. The agent-based model allows deployment across multiple servers and workstations, enabling distributed risk analysis while minimizing performance overhead. Future deployment phases will include enterprise-wide rollout, centralized aggregation of assessment results, continuous monitoring, and integration with enterprise security monitoring platforms such as SIEM systems.

To ensure privacy, security, and efficient semantic analysis, the system will use locally hosted Large Language Models (LLMs) integrated with embeddings and a vector database. ***Ollama*** will be used to host and execute the ***Llama 3*** model locally, ensuring that all sensitive enterprise data remains within the organizational environment. The LangChain Python framework will be used to orchestrate the integration between system data collection, the local LLM, embedding generation, and vector storage. System configuration data, software inventories, and security findings will be converted into vector embeddings using Ollama Embeddings and stored in a local vector database. This enables efficient semantic search, contextual reasoning, and retrieval-augmented analysis. The vector database allows the agent to compare current system states with known baselines, historical assessments, and security knowledge, improving risk detection accuracy and consistency.

## 5. Project Timeline & Gannt Chart

| Milestone | Date |
|---|---|
| | |
| Signed proposal | 02/17/26 |
| Architecture & Design | 03/01/26 |
| Context & Asset Discovery | 03/15/26 |
| Threats, Vulnerabilities & Controls | 03/31/26 |
| Risk Analysis & Evaluation | 04/10/26 |
| Risk Treatment & Control Mapping | 04/20/26 |
| Implementation & Monitoring | 04/30/26 |
| Final Outputs & Documentation | 05/07/26 |
| Poster Demo | 05/09/26 |
| Testing, Refinement & Submission | 05/10/26 |
| iShowcase | 05/10/24 |

*Table 3: Milestone Schedule*



## 6. Ethics

| # | Question | Generally | Data Breach |
|---|---|---|---|
| 1 | Could a user sell drugs or other illegal items on your platform? | N | N |
| 2 | Could a user of your platform engage in sex trafficking? | N | N |
| 3 | Could a user sell class notes or cheat on their homework on your platform? | N | N |
| 4 | Could a stalker use your project to find someone? | N | N |
| 5 | Could your app be used to spy on or track individuals? | N | N |
| 6 | Could your app/software access the camera or microphone and record things without users being aware? | N | N |
| 7 | If someone uses your platform, could they be re-traumatized or have their mental health impacted in some way? | N | N |
| 8 | Could your algorithm promote material that would traumatize or upset individuals? | N | N |
| 9 | Would your users be upset if the data you collect was given to someone else? | N | Y |
| 10 | Could a data leak potentially lead to identity theft? | N | N |
| 11 | If your site was hacked, would users of that product potentially lose their job, spouse, or family? | N | N |
| 12 | Should there be an age limitation on your product? | N | N |
| 13 | Could someone use your product to find, contact, and potentially commit elder abuse? | N | N |
| 14 | If the data on your platform was breached, could it be used to blackmail the users? | N | Y |
| 15 | Does the existence of your project imply that a particular racial group, gender, religion or other protected category is inherently bad, gross, or unwanted? | N | N |
| 16 | Could your product be used to commit hate crimes against a specific group? | N | N |

| | | | |
|---|---|---|---|
| 17 | Does the primary content of your game or algorithm focus on something considered deeply unethical? | N | N |
| 18 | Does your game or software contain race, gender, or other stereotypes? | N | N |
| 19 | Could users of your app scam other individuals? | N | N |
| 20 | Is your particular algorithm biased towards predicting correctly only for one race, gender, or other group? | N | N |
| 21 | Are the users of your project, players of your game, or those being surveyed for your data aware of how their data will be used? | N | N |
| 22 | What are the possible misinterpretations of your results? For example - would a white supremacist or misogynist be stoked about your results if they misinterpreted it? | N | N |
| 23 | Does the use or purchase of your data potentially contribute to a dangerous group or regime? | N | N |
| 24 | Could your virtual reality environment cause injury to the user? | N | N |
| 25 | Are your study participants or game players aware that their data will be collected and used? | N | N |
| 26 | Does your game or app contain addictive design elements without benefit to the user? | N | N |
| 27 | Does your survey contain an aspect of compulsion or unusually large incentive, that would command users to take it even if it was to their detriment? | N | N |
| 28 | Could your research outcomes harm an individual or entity? | N | N |

In this project, data-breach risk is mitigated by storing all collected data within an isolated system that is not accessible to external networks. Access to the data is strictly limited to authorized users, and all users with access are required to sign a Non-Disclosure Agreement (NDA). These controls ensure that sensitive information is protected from unauthorized disclosure or misuse.

# 7. Approvals

The signatures of the people below indicate an understanding of the purpose and content of this document by those signing it. By signing this document, you indicate that you approve of the proposed project outlined in this Statement of Work, the division of work, the Ground Rules and that the next steps may be taken to create a Product Specification and proceed with the project.

This document is based upon and supersedes the Agent-Based Risk Analysis and Assessment on Windows-Based Machines Using ISO 27001 Standard, Version 0.6. Deviations, (versus clarifications), from the PDR have been clearly noted. For any requirements not listed in this SOW, the PRD requirements shall remain in effect.

| Approver Name | Title | Signature | Date |
|---|---|---|---|
| Mehran Tajbakhsh | Project Manager | | |
| Rozhin Yasaei | Advisor | | |
| Greg Chism | Instructor | | |

| Section | Author | Word Count |
|---|---|---|
| *1. Executive Summary* | *Mehran Tajbakhsh* | *321* |
| *2. User\Market Research* | *Mehran Tajbakhsh* | *632* |
| *3. Product Features* | *Mehran Tajbakhsh* | *1069* |
| *4. Technical Architecture and Implementation Design* | *Mehran Tajbakhsh* | *472* |
| *5. Project Timeline & Gantt Chart* | *Mehran Tajbakhsh* | *53* |

# 8. Appendix

## A. Advisor Engagement

### 1) Project Team Responsibilities

- The Project Manager will set up and facilitate a weekly call/meeting with the Faculty Advisor. The Project Team will provide weekly status updates to the Faculty Advisor including upcoming deliverables, critical issues, and any adjustments to the Project Plan.
- Documents will be provided to the Faculty Advisor with adequate time for review and signature. The time necessary for review will be agreed with the Advisor. The minimum review time will be 3 days prior to the document due date.
- Design files will be provided to the Faculty Advisor as requested in a format agreed to with the Advisor.
- Support requirements will be clearly requested from the Faculty Advisor with the dates required and an adequate time for fulfilling the request.
- Modifications requests to the Project Plan by Faculty Advisor will be reviewed and agreed to within 1 week of the request.

### 2) Faculty Advisor Responsibilities

- The Faculty Advisor will provide knowledge and expertise to help the group stretch their skills.
- The Faculty Advisor will participate in a weekly or bi-weekly call/meeting with the Project Team to review the project status, upcoming deliverables, priorities, issues, and progress to the agreed Project Plan.
- The Faculty Advisor will provide document review, feedback and approval, rejection, approval with contingencies with adequate time for the Project Team to meet the course due dates.
- The Faculty Advisor will provide feedback on the requested support requirements from the Project Team. This includes feedback and guidance on design implementations decisions, design files, test plans, test procedures and test results.
- The Faculty Advisor shall provide technical advice and guidance to the Project Team answering inquiries approximately 1 hour per week.
- Modifications to the Project Plan by the Project Team will be resolved and documented within 1 week of the request.
- Grade the finalized project using skill-based rubric
- Attend iShowcase in May.

## B. Ground Rules

As a team and as individual team members, we agree to:

1. **Stay focused on our objectives and goals.**
   Each time the team meets, we will clearly define our objectives and desired outcomes at the beginning of the meeting. We will politely remind team members if we are getting off track.
2. **“Sidebar” any issues that are relevant but not consistent with the immediate objectives.**
   Occasionally, important matters are raised that are not relevant to the immediate goals of the meeting. To keep the group on track, but avoid losing the issue, create a “sidebar” where these topics can be listed and discussed later.
3. **Listen when others are speaking.**
   We will listen and consider others’ input before adding our own comments.
4. **All viewpoints will have an opportunity to be heard.**
   We understand that some team members may be quieter than others. We will make an effort to get each team member’s viewpoint and that no one dominates the discussion.
5. **Differences of opinion will be discussed respectfully**
   We will identify areas of agreement before assessing areas of disagreement. We will encourage each other to look beyond our own point of view. We will discuss different ideas respectfully. As a team, we will weigh the merits of different opinions and agree on a process for choosing a direction. All team members will respect and follow the decision or direction.
6. **Look for the good points in new ideas.**
   We will endeavor to explore the value in each idea as we assess and select our path forward.
7. **Focus on the future, not the past.**
   We will use our past experience to inform our decisions, but focus the discussion on the future objectives. Blame for past performance is counterproductive, we will focus on finding solutions.
8. **Agree upon specific action items and next steps.**
   At the end of each meeting and discussion, we will summarize and agree on specific next steps, action items and assignments.
9. **Accountability**
   As team members, we will each be responsible for our individual assignments and contribution to achieving the team objectives and goals. We will honor our responsibilities and not let our team members down.