RMF Tailoring & Scope Statement

1. **Purpose**
   This project exists to identify and assess the security posture of a residential home environment and to develop and demonstrate an understanding of the risk identification, assessment, and treatment. This project intends to showcase and practice my thinking and risk management, especially in the targeted steps of Categorize, Select, and Monitor, which will be discussed in detail later.

2. **Methodology**
   This project utilizes the NIST SP 800-37 Risk Management Framework (RMF) and tailors it to a small non-enterprise environment. The RMF provides context and prioritizations to support risk-related decision-making and structures the execution process.

   In enterprise environments, RMF execution typically involves separating duties across multiple roles. Due to the limited scope of this project, role responsibilities are consolidated and documented to preserve RMF intent rather than organizational structure. This project does not claim compliance with any regulatory framework or statutory requirement and is not intended to represent an auditable compliance posture.

   Household Mission & Objectives
   The residential environment supports the following primary objectives, which serve as the governing context for all risk-related decisions in this project:

   - **Support reliable remote work** by ensuring consistent access to required systems, services, and networks during working hours.
   - **Protect financial and personal information**, including banking data and personally identifiable information, from unauthorized disclosure or misuse.
   - **Enable daily communication and online activities** with minimal disruption while maintaining an acceptable security posture.
   - **Balance security controls with usability**, recognizing that excessive controls can introduce workarounds and increase overall risk.

   These objectives define acceptable trade-offs between confidentiality, availability, and integrity and inform risk tolerance, control selection, and risk acceptance decisions throughout the RMF lifecycle.

Stakeholders

The following stakeholders have an interest in the residential environment and are considered when making risk-related decisions:

- **Household members**, as primary users and owners of personal and financial information.
- **Employers**, where remote work systems access organizational data and services.
- **Financial institutions**, as external entities, are impacted by the protection of banking credentials and transactions.
- **Service providers** (e.g., internet and cloud services), which support availability and data handling.

Stakeholder identification at this stage informs impact considerations and risk tolerance. Detailed stakeholder-specific analysis is addressed within individual risk assessments as applicable.

The following is the tailored NIST SP 800-37 RMF that is used in this project:

RMF Process

1. **Prepare** | Performed to establish decision context
    - Establishing priorities (CIA emphasis)
    - Defining risk appetite and tolerance
    - Framing household missions and objectives
    - Identifying stakeholders and constraints
2. **Categorize** | Primary risk analyst responsibility
    - Asset categorization
    - Information classification
    - Impact assignment (Low / Medium / High)
3. **Select** | Primary risk analyst responsibility
    - Risk reduction aligned to tolerance
    - Control selection respecting constraints
4. **Implement** | Included to preserve lifecycle continuity
    - Controls implemented as part of risk treatment execution
    - Implementation used to validate feasibility and effectiveness
5. **Assess** | Included to validate outcomes
    - Verification of control existence
    - Confirmation of intended operation
    - Identification of residual risk
6. **Authorize** | Represented through documented risk acceptance
    - Conscious acceptance decisions
    - Awareness of residual risk
    - Ownership of consequences
7. **Monitor** | Primary risk analyst responsibility
    - Periodic reviews (6-12 months)
    - Reassessment following material changes
    - Ongoing risk posture awareness and improvement

3. **Scope Boundaries**
   This project prioritizes **Confidentiality** and **Availability**, with secondary consideration given to **Integrity**, based on household objectives and risk tolerance.

   - **Confidentiality** focuses on protecting sensitive information such as personally identifiable information (PII) and financial data. While enterprise privacy programs often require regulatory compliance, this project relies on household objectives and risk tolerance as the governing authority.
   - **Availability** addresses resilient access to systems and services required for daily operations and remote work.
   - **Integrity** is considered where unauthorized modification could materially impact financial, personal, or operational outcomes, but it is not treated as a primary driver relative to confidentiality and availability.

   Out of scope are enterprise tooling, employer-managed systems, and continuous monitoring mechanisms typically associated with large-scale environments.