Personal Risk Assessment

Author**:** Jim Kinter

Course**:** CIDM 6341

Professor: Dr. Jennex

Table of Contents

[Personal Risk Assessment 1](#_Toc211196062)

[Introduction 4](#_Toc211196063)

[Overview of Assessment 4](#_Toc211196064)

[How the inventory was conducted 4](#_Toc211196065)

[How assets were categorized 4](#_Toc211196066)

[How threats/vulnerabilities were identified 5](#_Toc211196067)

[How assets were prioritized and valued 5](#_Toc211196068)

[How systems were determined 5](#_Toc211196069)

[Representative Assessments 6](#_Toc211196070)

[Summary of Overall Risk Posture 11](#_Toc211196071)

## Introduction

The subject of this inventory and risk assessment is my personal and household assets, encompassing a multi-generational family living in a large home with extensive digital and physical assets. As Jim, a 55-year-old individual with a background in academic and professional activities, I manage a household that includes my spouse Kristie (51), children Josh (21), Ben (20), Sarah (17), and Sam (13), and in-laws Gerald (81) and Kathy (71). The household is tech-heavy, with multiple smart devices, vehicles, and equipment, reflecting a complex attack surface. The risk assessment focuses on six assets—one person (myself), one procedure (password change schedule), one data (digital tax returns), one hardware (personal laptop), one software (antivirus software), and one system (computing system)—to evaluate vulnerabilities and prioritize risk mitigation using the NIST Risk Management Framework (RMF) as outlined in NIST SP 800-37.

## Overview of Assessment

### How the inventory was conducted

The inventory was conducted systematically to ensure comprehensive coverage of assets, following NIST RMF Step 1 (Categorize). For people, I reviewed my iPhone 15 Pro Max contact list, identifying 5320 professional contacts but focusing on 12 personal/familial relationships, supplemented by social media data (LinkedIn: 3777 contacts, Facebook: 661 contacts, X: 397 followers). Hardware and networking devices, including IoT, were inventoried using Advanced IP Scanner on my Windows laptop, analyzing the NetworkScan.html output for IP addresses, MACs, and services, with manual verification for devices not detected (e.g., Calix modem, Ubiquiti radios). Software was cataloged by exporting the program list from my laptop’s control panel (60 apps) and reviewing my iPhone’s app library (187 apps). Data and physical records were collected via a room-by-room inspection of my house, checking drawers, boxes, file cabinets, and safes for items like 7 years of tax returns, with digital data cross-referenced against cloud storage, email archives, and DayOne diary entries (over 5 years). Procedures were identified using DayOne app logs. Transportation and equipment (e.g., vehicles, tools, bicycles) were physically inventoried in garages, sheds, and storage areas, excluding in-law-owned assets in the pool house.

### How assets were categorized

Assets were categorized into distinct groups—people (P), hardware (H), equipment (E), transportation (T), networking (N), IoT (I), software (S), data (D), procedures (PR), and systems (SYS)—aligned with NIST RMF’s asset identification process (NIST SP 800-37, Step 1). Each asset received a unique ID with a category prefix (e.g., P1, H1) for clear identification. Assets were assigned to systems based on functional roles, such as Identify (people), Protect (computing), or Detect (IoT), per NIST RMF. For multi-role assets (e.g., smartphones with hardware, software, and data), I assigned a primary category (hardware) and noted overlaps in descriptions to maintain relational integrity without duplication.

### How threats/vulnerabilities were identified

Threats and vulnerabilities were identified using NIST RMF Step 2 (Select) and NIST SP 800-30, focusing on the CIA triad (Confidentiality, Integrity, Availability). For each asset, I considered common threats (e.g., phishing, malware, unauthorized access) based on asset type and usage. The network scan helped identify IoT vulnerabilities (e.g., unpatched devices), while DayOne entries revealed procedural weaknesses. Physical inspections highlighted risks to hard copies, and social media/contact analysis pointed to social engineering risks. The highest-impact threat categorization was prioritized per asset (e.g., Confidentiality for personal data, Integrity for systems), following NIST SP 800-30’s risk assessment methodology.

### How assets were prioritized and valued

Assets were prioritized using the provided ratings (Vital to Facilitates), aligned with NIST RMF’s impact analysis (NIST SP 800-60). Vital assets (e.g., myself) were critical to household operations, while Critical/High assets (e.g., laptop, tax returns) could cause significant disruption if lost. Medium/Low assets (e.g., IoT devices, infrequently used apps) had lesser impact. Values were estimated based on replacement costs (hardware), financial impact (data), or operational impact (procedures/systems), with personal valuation reflecting potential income loss or legal costs, adjusted for household context and NIST SP 800-30’s risk valuation guidelines.

### How systems were determined

Systems were determined by grouping related assets based on NIST RMF functions (NIST SP 800-37, Step 1). For example, SYS1 (Personal Identity) includes people and contact lists (Identify), SYS2 (Computing) includes laptops and software (Protect), and SYS6 (IoT) includes smart devices (Detect). Each system was defined by its primary NIST RMF function, with assets linked via System IDs to reflect interdependencies, ensuring a holistic view of the household’s operational and security framework.

### Representative Assessments

Per the assignment, the following 6 assets were assessed and detailed.

#### Person Information Asset (P1: Self - Jim)

**Asset:** Self (Jim, age 55)

**CIA Asset Value:** $2,800,000

**Priority:** Vital

**Threat Categorization:** Confidentiality (High)

**Vulnerability Description:** Phishing attack leading to disclosure of personal identifiers (e.g., SSN, DOB)

**ARO:** 0.2 (Very High)

**Controls in Place:** 0.9 (Very High)

**Uncertainty:** 0.1

**Risk Value:** $33,600

**Controls Needed:** Professional liability insurance

**Action Plan ID:** AP1

**How numbers/entries were generated:** The CIA asset value of $2,800,000 was calculated using NIST RMF’s impact analysis (NIST SP 800-60), estimating income loss over 8 years ($1,800,000, based on $225,000/year), intellectual property value ($500,000 for professional contributions), and legal defense/judgment costs ($500,000) if sensitive data is disclosed. The priority is Vital, as my role is critical to household operations (NIST SP 800-30). The threat is Confidentiality (High) due to the severe impact of disclosing SSN/DOB, identified via NIST SP 800-30’s threat assessment. ARO is Very High (0.2), reflecting daily phishing attempts observed in email and social media (5320 professional contacts, 3777 LinkedIn contacts). Controls include security training and spam filters (Very High, 0.9), per NIST SP 800-53’s control selection. Uncertainty is low (0.1) due to confidence in phishing frequency and control effectiveness. Risk Value = $2,800,000 × 0.2 × (1 - 0.9) × (1 + 0.1) = $33,600, calculated per the provided formula. Professional liability insurance (AP1) is proposed to transfer risk, aligning with NIST RMF Step 4 (Implement).

#### Data Information Asset (D8: Tax Returns - Digital)

**Asset:** Tax Returns (Digital)

**CIA Asset Value:** $300,000

**Priority:** Critical

**Threat Categorization:** Confidentiality (High)

**Vulnerability Description:** Unauthorized access to financial data and SSNs

**ARO:** 0.1 (Medium)

**Controls in Place:** 0.9 (Very High)

**Uncertainty:** 0.2

**Risk Value:** $3,600

**Controls Needed:** Multi-factor authentication, access monitoring

**Action Plan ID:** AP6

**How numbers/entries were generated:** The CIA asset value of $300,000 was derived using NIST SP 800-60’s impact analysis, considering identity theft remediation for six individuals (self, spouse, four children) at $50,000 per incident, as SSNs are included. The priority is Critical, as loss could disrupt financial stability within days (NIST SP 800-30). The threat is Confidentiality (High) due to sensitive financial data and SSNs, identified via NIST SP 800-30’s threat assessment. ARO is Medium (0.1), reflecting occasional hacking attempts on personal systems. Controls include an encrypted digital vault and password protection (Very High, 0.9), per NIST SP 800-53’s control catalog. Uncertainty is 0.2 due to potential unknown vulnerabilities in cloud storage. Risk Value = $300,000 × 0.1 × (1 - 0.9) × (1 + 0.2) = $3,600, per the provided formula. Multi-factor authentication and access monitoring (AP6) are proposed to enhance security, aligning with NIST RMF Step 4 (Implement**).**

#### Procedure/Process Asset (PR2: Password Change Schedule)

**Asset:** Password Change Schedule

**CIA Asset Value:** $10,000

**Priority:** High

**Threat Categorization:** Integrity (Moderate)

**Vulnerability Description:** Weak password practices

**ARO:** 0.15 (High)

**Controls in Place:** 0.8 (High)

**Uncertainty:** 0.2

**Risk Value:** $360

**Controls Needed:** Two-factor authentication, password policy enforcement

**Action Plan ID:** AP7

**How numbers/entries were generated:** The CIA asset value of $10,000 was estimated using NIST SP 800-60, reflecting the operational impact of compromised credentials across household systems. The priority is High, as weak passwords could disrupt operations within a week (NIST SP 800-30). The threat is Integrity (Moderate) due to potential credential compromise affecting system access, identified via NIST SP 800-30. ARO is High (0.15) based on frequent password-related attacks observed in DayOne logs. Controls include monthly updates and password manager use (High, 0.8), per NIST SP 800-53. Uncertainty is 0.2 due to varying family compliance. Risk Value = $10,000 × 0.15 × (1 - 0.8) × (1 + 0.2) = $360, per the provided formula. Two-factor authentication and password policy enforcement (AP7) are proposed, aligning with NIST RMF Step 4 (Implement).

#### Hardware Asset (H1: Laptop - JIM-PERSONAL-LAPTOP)

**Asset:** Laptop (JIM-PERSONAL-LAPTOP)

**CIA Asset Value:** $2,000

**Priority:** High

**Threat Categorization:** Confidentiality (Moderate)

**Vulnerability Description:** Malware infection via phishing or unpatched software

**ARO:** 0.1 (Medium)

**Controls in Place:** 0.7 (Medium)

**Uncertainty:** 0.2

**Risk Value:** $72

**Controls Needed:** Regular patching, endpoint protection upgrades

**Action Plan ID:** AP2

**How numbers/entries were generated:** The CIA asset value of $2,000 was based on replacement cost, per NIST SP 800-60’s asset valuation. The priority is High, as loss would disrupt academic work within a week (NIST SP 800-30). The threat is Confidentiality (Moderate) due to stored sensitive data, identified via NIST SP 800-30’s threat assessment. ARO is Medium (0.1) based on phishing/malware frequency observed in email and network scans. Controls include antivirus and periodic updates (Medium, 0.7), per NIST SP 800-53. Uncertainty is 0.2 due to potential software vulnerabilities. Risk Value = $2,000 × 0.1 × (1 - 0.7) × (1 + 0.2) = $72, per the provided formula. Regular patching and endpoint protection upgrades (AP2) are proposed, aligning with NIST RMF Step 4 (Implement).

#### Software Asset (S5: Antivirus Software)

**Asset:** Antivirus Software

**CIA Asset Value:** $500

**Priority:** Medium

**Threat Categorization:** Availability (Moderate)

**Vulnerability Description:** Bypass or failure of antivirus protection

**ARO:** 0.05 (Low)

**Controls in Place:** 0.9 (Very High)

**Uncertainty:** 0.1

**Risk Value:** $2.75

**Controls Needed:** Enhanced antivirus updates, multi-factor authentication

**Action Plan ID:** AP5

**How numbers/entries were generated:** The CIA asset value of $500 was based on subscription cost and potential system impact, per NIST SP 800-60. The priority is Medium, as failure impacts systems over a month (NIST SP 800-30). The threat is Availability (Moderate) due to potential bypass affecting system protection, identified via NIST SP 800-30. ARO is Low (0.05) due to robust vendor updates. Controls include automatic updates (Very High, 0.9), per NIST SP 800-53. Uncertainty is 0.1 due to high confidence in vendor reliability. Risk Value = $500 × 0.05 × (1 - 0.9) × (1 + 0.1) = $2.75, per the provided formula. Enhanced updates and multi-factor authentication (AP5) are proposed, aligning with NIST RMF Step 4 (Implement**).**

#### System Categorization and Analysis (SYS2: Computing System)

**System:** Computing System (SYS2)

**Assets:** Laptops (H1, H4), Desktop (H3), Frequently Used Apps (S1), Infrequently Used Apps (S2), Antivirus Software (S5), Personal Documents (D1), Email Archives (D3)

**CIA Categorization:** {(Confidentiality, Moderate), (Integrity, High), (Availability, Moderate)}

**CIA Asset Value:** $25,000

**Priority:** Critical

**Threat Categorization:** Integrity (High)

**Vulnerability Description:** Unauthorized access or malware infection

**ARO:** 0.1 (Medium)

**Controls in Place:** 0.7 (Medium)

**Uncertainty:** 0.2

**Risk Value:** $900

**Controls Needed:** Firewall enhancements, intrusion detection

**Action Plan ID:** AP8

**How numbers/entries were generated:** The Computing System (SYS2) was categorized using NIST RMF Step 1 (Categorize), with assets grouped under the Protect function (NIST SP 800-37). The CIA value of $25,000 reflects combined hardware, software, and intellectual property in personal documents, per NIST SP 800-60. It’s prioritized Critical, as loss would disrupt operations within days (NIST SP 800-30). The highest impact is Integrity (High), as malware or unauthorized access could corrupt critical data or misrepresent my professional identity, identified via NIST SP 800-30. Confidentiality and Availability are Moderate, as sensitive data is limited and brief outages are tolerable. Threats include malware and unauthorized access, identified via network scans and software inventory. Controls include antivirus, updates, and access controls (Medium, 0.7), per NIST SP 800-53. ARO is Medium (0.1) due to frequent threats. Uncertainty is 0.2 due to potential gaps. Risk Value = $25,000 × 0.1 × (1 - 0.7) × (1 + 0.2) = $900, per the provided formula. Firewall enhancements and intrusion detection (AP8) are proposed, with residual risk accepted, aligning with NIST RMF Step 4 (Implement).

### Summary of Overall Risk Posture

My household’s risk posture is elevated due to a large attack surface from extensive digital connectivity (34 IoT/network devices, 247 apps), social media presence (3777 LinkedIn contacts), sensitive data (7 years of tax returns with SSNs, DayOne diary), and physical assets (8 vehicles, 29 equipment items). The multi-generational household, including less tech-savvy elderly in-laws and children, increases social engineering risks. NIST RMF-guided controls like encryption (tax returns), antivirus, and password management mitigate some risks, but vulnerabilities in IoT devices, outdated software, and scattered physical records persist. Proposed controls (e.g., MFA, intrusion detection, network monitoring) and family education, aligned with NIST RMF Step 5 (Authorize) and Step 6 (Monitor), will reduce risks, but residual risks remain due to the complex environment.

Referenced Publications: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf>

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf>