FROM LIVING ROOM TO HOSPITAL

CYBER RISK MADE SIMPLE

SkillWeed

Join the internship today and register at: academy.skillweed.com

Goal: Participants will understand:

- Asset
- Threat
- Vulnerability
- Likelihood
- Impact
- Inherent Risk
- Controls
- Residual Risk

By walking through their **own home Wi-Fi network.**

CONTENTS

PART 1:
HOME NETWORK VERSION

STEP 1 — MAP YOUR HOME NETWORK (15 MINUTES)

ASK EVERYONE:

“What devices connect to your Wi-Fi?”

Write them down:

- 📱 Phones
- 💻 Laptops
- 📺 Smart TV
- 🎮 Game console
- 🧠 Alexa / Google Home
- 🖨️ Printer
- 📡 Router
- 👶 Baby monitor
- 🏠 Cameras

DRAW SIMPLE NETWORK:

Internet → Router → Devices

ACTION:

Everyone draws their own home network map.

STEP 2 — IDENTIFY ASSETS & DATA (20 MINUTES)

Assets = What you own or use

Data = What matters inside them

EXAMPLE:

Device	What's Valuable?
Phone	Photos, banking apps
Laptop	Emails, work files
Smart TV	Login credentials
Router	Internet access
Camera	Home privacy

TEACHING MOMENT:

If someone steals or breaks this — would you care?

ACTION:

Each participant lists:

- 3 important devices
- What data matters most on each

STEP 3 — IDENTIFY THREATS & VULNERABILITIES

Threat = Something bad that could happen

Vulnerability = Weakness that allows it

EXAMPLES

Asset	Threat	Vulnerability
Wi-Fi	Neighbor hacks	Weak password
Laptop	Virus	No antivirus
Camera	Spy access	Default password
Kids tablet	Bad websites	No parental controls
Router	Takeover	Old firmware

ANALOGY:

Threat = Burglar
Vulnerability = Unlocked door

ACTION:

Pick 2 devices and list:

- 1 Threat
- 1 Vulnerability

STEP 4 — LIKELIHOOD & IMPACT (20 MINUTES)

Likelihood = How likely is it to happen?

- Low
- Medium
- High

Impact = How bad if it happens?

- Low (annoying)
- Medium (financial loss)
- High (privacy or safety risk)

EXAMPLE:

Scenario	Likelihood	Impact
Wi-Fi hacked	Medium	High
Virus on laptop	High	Medium
TV hacked	Low	Low

TEACHING MOMENT:

Risk = Probability × Damage

ACTION:

Score your two risks.

STEP 5 — INHERENT RISK VS RESIDUAL RISK (20 MINUTES)

Inherent Risk = Risk before protection

Residual Risk = Risk after protection

EXAMPLE:

Wi-Fi hacked

- Likelihood: Medium
- Impact: High
  ➡️ Inherent Risk = High

Add Controls:

- Strong password
- Firmware updates
- WPA3 encryption

Now:

- Likelihood = Low
- Impact = Medium
  ➡️ Residual Risk = Low–Medium

VISUAL:

Before lock → Door open
After lock → Door protected

ACTION:

Add at least 2 controls to reduce one risk.

STEP 6 — CONTROLS & IMPROVEMENTS (15 MINUTES)

TYPES OF CONTROLS:

- 🔐 Technical: Passwords, firewall
- 📋 Administrative: Rules, policies
- 👥 Human: Awareness

EXAMPLES:

- Change default passwords
- Enable auto updates
- Turn on router firewall
- Use guest Wi-Fi
- Teach kids safe browsing

ACTION:

Everyone commits to 1 change they will do today.

TAKEAWAY SUMMARY

Risk Assessment is simply asking:

1. What do I have?
2. What can go wrong?
3. How likely?
4. How bad?
5. What can I do about it?

PART 2:
ENTERPRISE VERSION

SKILLWEED HOSPITAL DEPLOYING EMR SYSTEM

Now we scale the SAME LOGIC.

Home Network → Hospital Network

Phone → EMR Server

Router → Firewall

Family Data → Patient Records

STEP 1 — ASSETS

Category	Examples
Systems	EMR servers
Devices	Nurses stations, tablets
Data	PHI, prescriptions
Network	Wi-Fi, VPN
People	Doctors, admins

ACTION:

Create asset inventory.

STEP 2 — THREATS & VULNERABILITIES

Asset	Threat	Vulnerability
EMR	Ransomware	Unpatched OS
Tablets	Theft	No encryption
Wi-Fi	Unauthorized access	Weak segmentation
Staff	Phishing	No training
Vendors	Breach	No due diligence

STEP 3 — LIKELIHOOD & IMPACT

Risk	Likelihood	Impact
Ransomware	High	Very High
Data breach	Medium	Very High
Downtime	Medium	High
Insider misuse	Low	High

STEP 4 — INHERENT RISK

Before controls:

- HIPAA violations
- Patient safety impact
- Regulatory fines
- Reputation loss

STEP 5 — CONTROLS

TECHNICAL

- Network segmentation
- MFA for EMR
- Encryption
- Backups
- EDR
- SIEM

ADMINISTRATIVE

- Incident response plan
- Vendor risk management
- Access policies
- Change management

HUMAN

- Phishing training
- EMR security training
- Role-based access

STEP 6 — RESIDUAL RISK

Re-score risks after controls.

Accept only risks aligned with business tolerance.

SAMPLE RISK ASSESSMENT TABLE (HOME NETWORK EXAMPLE)

Asset	Threat	Vulnerability	Likelihood (1–5)	Impact (1–5)	Inherent Risk	Controls in Place	Residual Risk	Owner	Action
Home Wi-Fi Router	Neighbor hacks Wi-Fi	Weak password	4	5	High (20)	Strong password, firmware updates	Medium (10)	Akin	Change router password
Laptop	Virus infection	No antivirus	5	4	High (20)	Antivirus installed	Medium (8)	User	Enable auto scans
Security Camera	Privacy breach	Default password	3	5	High (15)	Password changed	Low (5)	Home Admin	Enable MFA
Kids Tablet	Unsafe websites	No parental controls	4	3	Medium (12)	Parental filter enabled	Low (4)	Parent	Review screen rules
Smart TV	Account hijack	Old software	2	2	Low (4)	Auto updates enabled	Very Low (2)	Home Admin	Monthly updates

Inherent Risk Score = Likelihood × Impact
Residual Risk = Risk after controls

APPENDIX

ASSET

What you are protecting.

Examples:

- Router
- Laptop
- Phone
- Camera
- EMR Server (hospital)

👉 If this breaks or is stolen — would you care?

THREAT

What bad thing could happen.

Examples:

- Hacking
- Virus
- Data theft
- Ransomware
- Unauthorized access

👉 Who or what could cause harm?

VULNERABILITY

The weakness that allows the threat to happen.

Examples:

- Weak password
- No updates
- No encryption
- No training
- Old software

👉 What makes this easy to attack?

LIKELIHOOD (1–5)

How likely is it to happen?

Score	Meaning
1	Rare
2	Unlikely
3	Possible
4	Likely
5	Almost Certain

👉 How often could this realistically happen?

Impact (1–5)

How bad would it be if it happened?

Score	Meaning
1	Negligible
2	Minor
3	Moderate
4	Major
5	Critical

👉 Money loss? Privacy loss? Safety risk?

INHERENT RISK

Risk level BEFORE any protection exists.

Formula:

Likelihood × Impact

Risk Level:

- 🟢 Low (1–8)
- 🟡 Medium (9–15)
- 🔴 High (16–25)

👉 This shows your raw exposure.

CONTROLS IN PLACE

What protections exist today.

Examples:

- Strong passwords
- MFA
- Firewall
- Antivirus
- Training
- Backups

👉 What is already reducing the risk?

RESIDUAL RISK

Risk remaining AFTER controls.

👉 Is this risk acceptable or still too high?

OWNER

Who is responsible for this risk.

Examples:

- Parent
- IT Admin
- Security Team
- Vendor Manager

👉 Someone must own every risk.

ACTION

What must be done next.

Examples:

- Change password
- Enable updates
- Train users
- Add monitoring
- Buy security tool

👉 Risk without action is useless.

In conclusion, a risk assessment only matters when it is understood by the right people — from leadership and the board to frontline operational teams. Insight without clarity creates no impact. The sample prompts below help transform raw risk data into concise, meaningful, and actionable intelligence. Use them as needed to inspire alignment, accountability, and decisive action.

VERSION 1:
EXECUTIVE / BOARD READY

BEST FOR:

Board members, executives, investors, hospital leadership, CIO, compliance leadership.

PROMPT

You are a senior cybersecurity risk consultant preparing a management report for executive leadership.

Analyze the attached risk assessment data and generate a professional executive report that includes:

1. EXECUTIVE SUMMARY

- Overall risk posture (high / medium / low).
- Top 5 critical risks and why they matter to the business.
- Business impact (financial, operational, safety, compliance, reputation).
- Key trends or patterns observed.

2. RISK OVERVIEW

- Summary of total risks assessed.
- Distribution of inherent vs residual risk.
- Any concentration areas (systems, people, vendors, network).

3. PRIORITY RISKS

- List the top 5 risks ranked by residual risk.
- For each risk include:
    - Asset affected
    - Threat and vulnerability
    - Inherent risk level
    - Residual risk level
    - Business impact

4. REMEDIATION STRATEGY

- Recommended controls and improvements.
- Quick wins vs long-term investments.
- Risk reduction benefits.

5. ACTION PLAN

- Table with:
    - Action
    - Owner
    - Priority (High / Medium / Low)
    - Timeline
    - Expected risk reduction

6. RISK ACCEPTANCE & LEADERSHIP DECISIONS

- Identify which risks can be accepted.
- Identify which risks require funding or escalation.
- Strategic recommendations for leadership.

Write in clear executive language, concise, professional, and business-focused.

VERSION 2:
OPERATIONAL / SECURITY TEAM REPORT

BEST FOR:

IT teams, security teams, SOC, GRC teams, hospital IT leadership, program managers.

PROMPT

You are a cybersecurity risk analyst preparing an operational risk report based on the provided risk assessment data.

Generate a structured report including:

1. OVERVIEW

- Purpose of the assessment.
- Scope and systems reviewed.
- Summary of risk levels.

2. DETAILED RISK FINDINGS

- Group risks by category (network, endpoint, people, vendor, data).
- Highlight high and medium residual risks.
- Explain root causes and contributing weaknesses.

3. CONTROL EFFECTIVENESS REVIEW

- Identify controls that are strong.
- Identify control gaps or inconsistencies.
- Areas needing automation or monitoring.

4. REMEDIATION PLAN

- Recommended technical, administrative, and human controls.
- Dependencies and prerequisites.
- Estimated effort level (low / medium / high).

5. ACTION PLAN TABLE

- Risk
- Recommended Action
- Owner
- Priority
- Timeline
- Dependencies

6. METRICS & TRACKING

- KPIs to track improvement.
- Suggested review cadence.

Write in practical operational language suitable for execution teams.

VERSION 3:
TRAINING / INTERNSHIP / LEARNING REPORT

BEST FOR:

Internships, Skillweed labs, students, workshops, beginner audiences.

PROMPT

You are a cybersecurity instructor creating a simple management-style report based on a risk assessment exercise.

Using the provided risk data, generate a clear, easy-to-understand report that includes:

1. SUMMARY

- What was assessed.
- What risks were found.
- Overall risk level.

2. TOP RISKS EXPLAINED SIMPLY

- Top 3–5 risks.
- What could happen in real life.
- Why they matter.

3. WHAT WE CAN IMPROVE

- Simple security improvements.
- Behavior changes.
- Technology improvements.

4. ACTION PLAN

- Who should do what.
- What should be done first.
- What can wait.

5. LESSONS LEARNED

- Key cybersecurity concepts learned.
- How this applies to home, school, and work.

Keep language simple, friendly, and practical.


SkillWeed