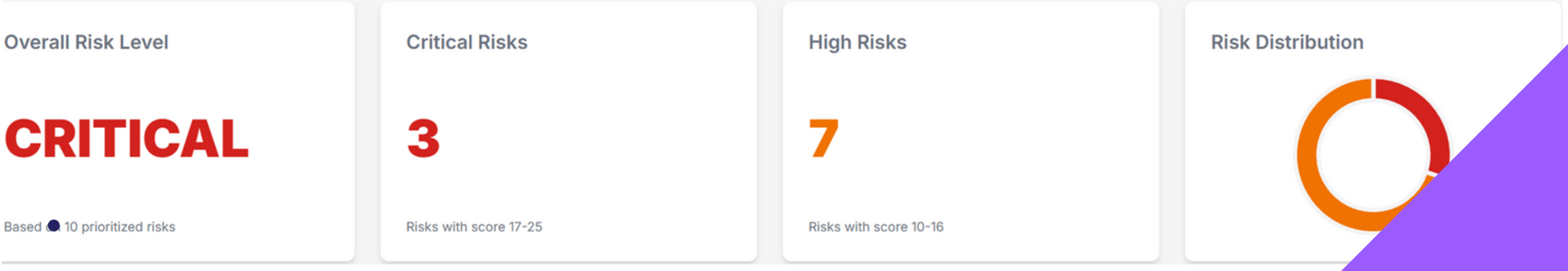
Cyber U.N.C.L.E.

BASIC
CYBER RISK ASSESSMENT
GUIDE



Overall Risk Level

CRITICAL

Based on 10 prioritized risks

Critical Risks

3

Risks with score 17-25

High Risks

7

Risks with score 10-16

Risk Distribution

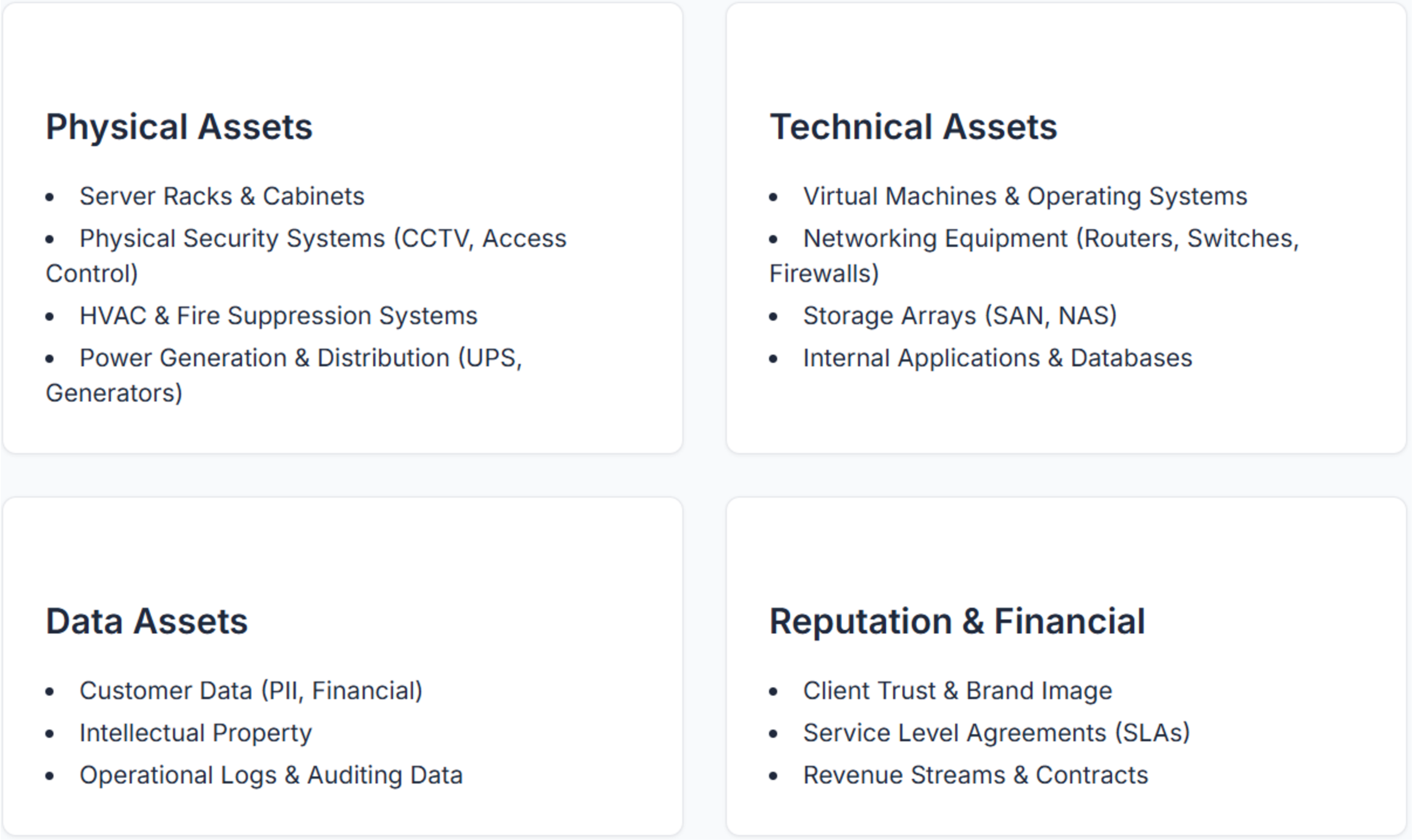
CYBER
U.N.C.L.E.

CYBER RISK ASSESSMENT GUIDE

THIS INTERACTIVE GUIDE PROVIDES A DEEP DIVE INTO EACH PHASE OF OUR SEMI-QUANTITATIVE RISK ASSESSMENT PROCESS. OUR GOAL IS TO MOVE FROM THEORY TO A PRACTICAL, ACTIONABLE METHODOLOGY THAT WILL SAFEGUARD OUR MISSION-CRITICAL DATA CENTER OPERATIONS.

1. GENERIC DATA CENTRE ASSETS:

UNDERSTANDING WHAT WE ARE PROTECTING IS THE FIRST STEP. FOR A MEDIUM-SIZED DATA CENTRE, OUR ASSETS CAN BE BROKEN DOWN INTO THE FOLLOWING KEY CATEGORIES. THESE ARE THE THINGS THAT WOULD BE IMPACTED IN A RISK SCENARIO.



Physical Assets

- Server Racks & Cabinets
- Physical Security Systems (CCTV, Access Control)
- HVAC & Fire Suppression Systems
- Power Generation & Distribution (UPS, Generators)

Technical Assets

- Virtual Machines & Operating Systems
- Networking Equipment (Routers, Switches, Firewalls)
- Storage Arrays (SAN, NAS)
- Internal Applications & Databases

Data Assets

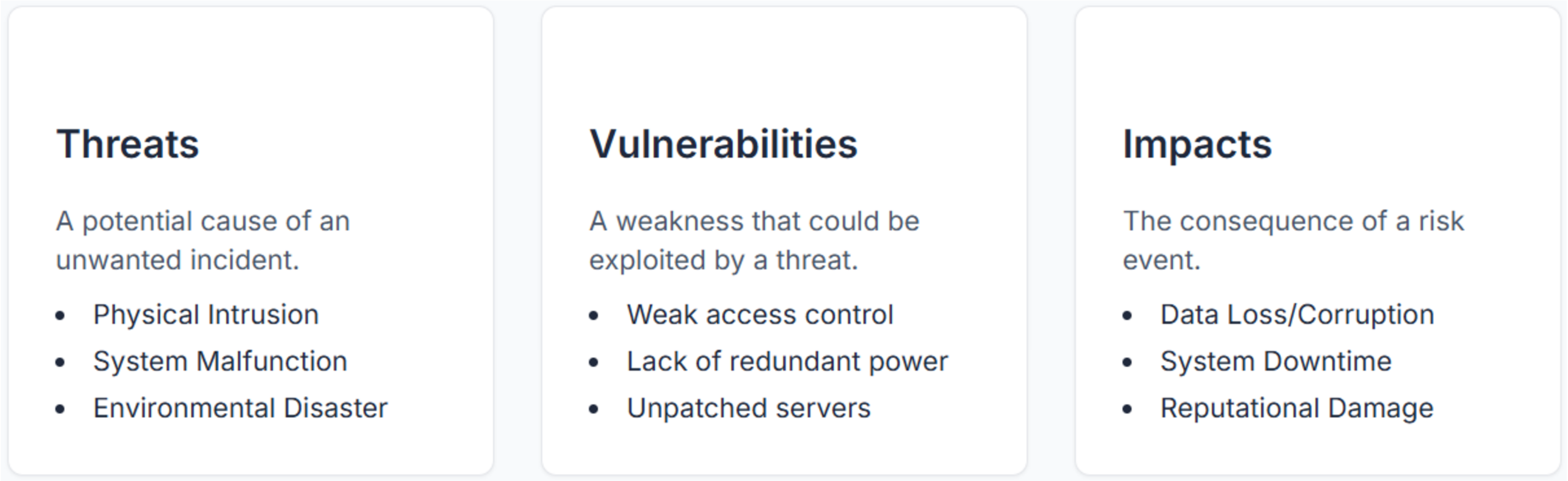
- Customer Data (PII, Financial)
- Intellectual Property
- Operational Logs & Auditing Data

Reputation & Financial

- Client Trust & Brand Image
- Service Level Agreements (SLAs)
- Revenue Streams & Contracts

2. THE RISK IDENTIFICATION PHASE

WITH OUR ASSETS IDENTIFIED, WE CAN NOW FORMULATE RISK SCENARIOS. A GOOD SCENARIO IS SPECIFIC AND DESCRIPTIVE, FOLLOWING THE PATTERN: A THREAT ACTOR EXPLOITS A VULNERABILITY ON AN ASSET TO CAUSE AN IMPACT. THE KEY IS TO BE AS PRECISE AS POSSIBLE.



Threats

A potential cause of an unwanted incident.

- Physical Intrusion
- System Malfunction
- Environmental Disaster

Vulnerabilities

A weakness that could be exploited by a threat.

- Weak access control
- Lack of redundant power
- Unpatched servers

Impacts

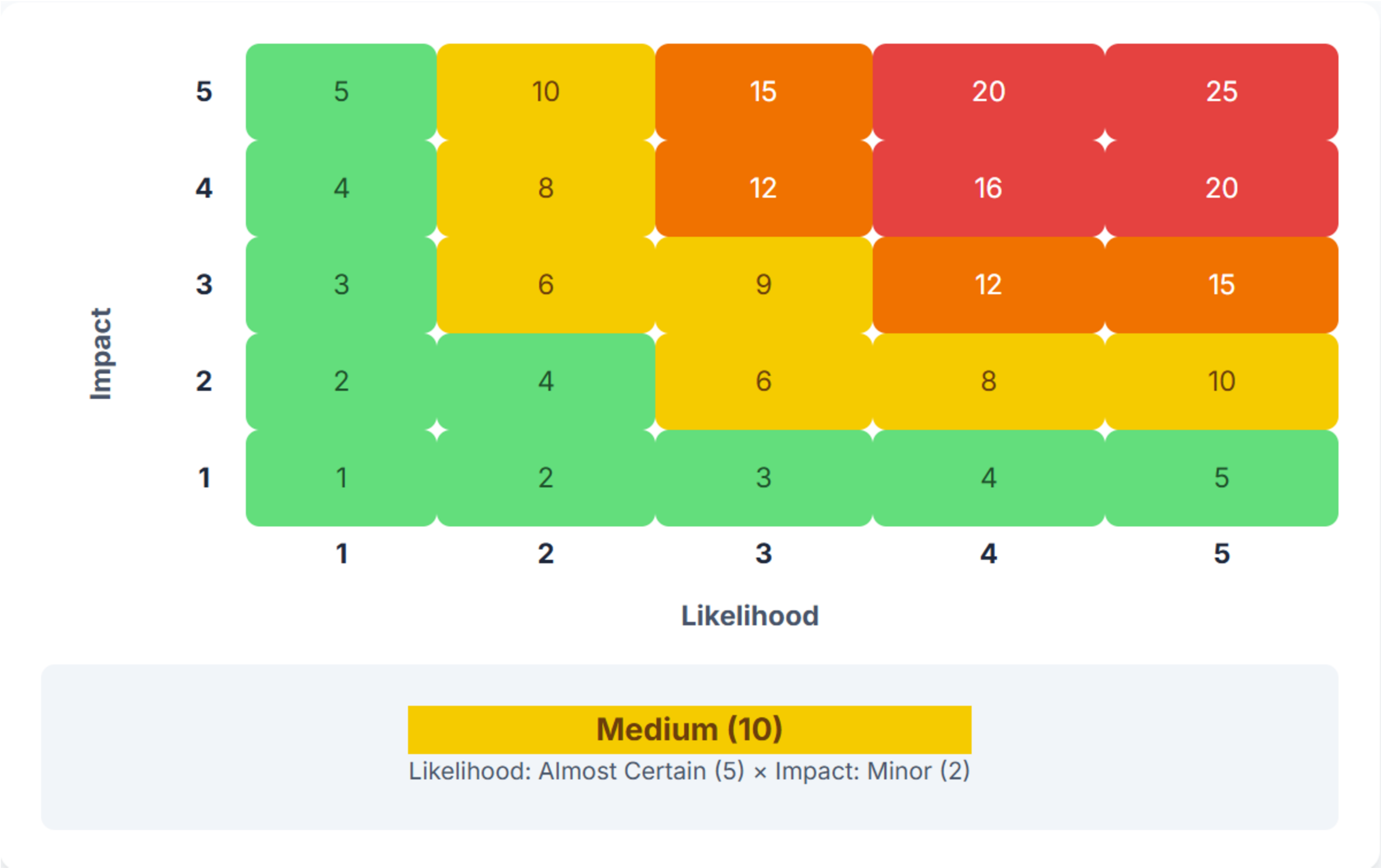
The consequence of a risk event.

- Data Loss/Corruption
- System Downtime
- Reputational Damage

CYBER
U.N.C.L.E.

3. THE SEMI-QUANTITATIVE APPROACH & RISK MATRIX

ONCE A RISK SCENARIO IS DEFINED, WE USE A 5X5 SCORING MATRIX TO DETERMINE ITS SEVERITY. THE FINAL RISK SCORE IS THE PRODUCT OF LIKELIHOOD X IMPACT. HOVER OVER ANY CELL IN THE MATRIX BELOW TO SEE ITS SCORE AND LEVEL.



Impact

	1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

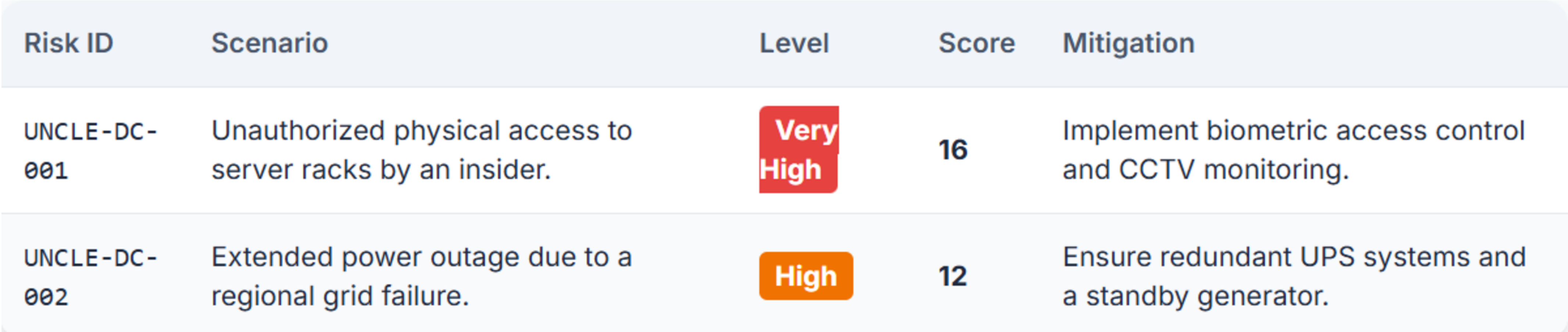
Likelihood

Medium (10)

Likelihood: Almost Certain (5) × Impact: Minor (2)

4. THE CYBER RISK REGISTER

THE RISK REGISTER IS OUR SINGLE SOURCE OF TRUTH FOR ALL RISKS. EACH ROW REPRESENTS A SINGLE RISK SCENARIO AND CONTAINS ALL THE DATA POINTS WE NEED FOR MANAGEMENT AND COMMUNICATION. THE TABLE BELOW PROVIDES A SIMPLIFIED OVERVIEW OF TWO KEY DATA CENTRE RISKS.



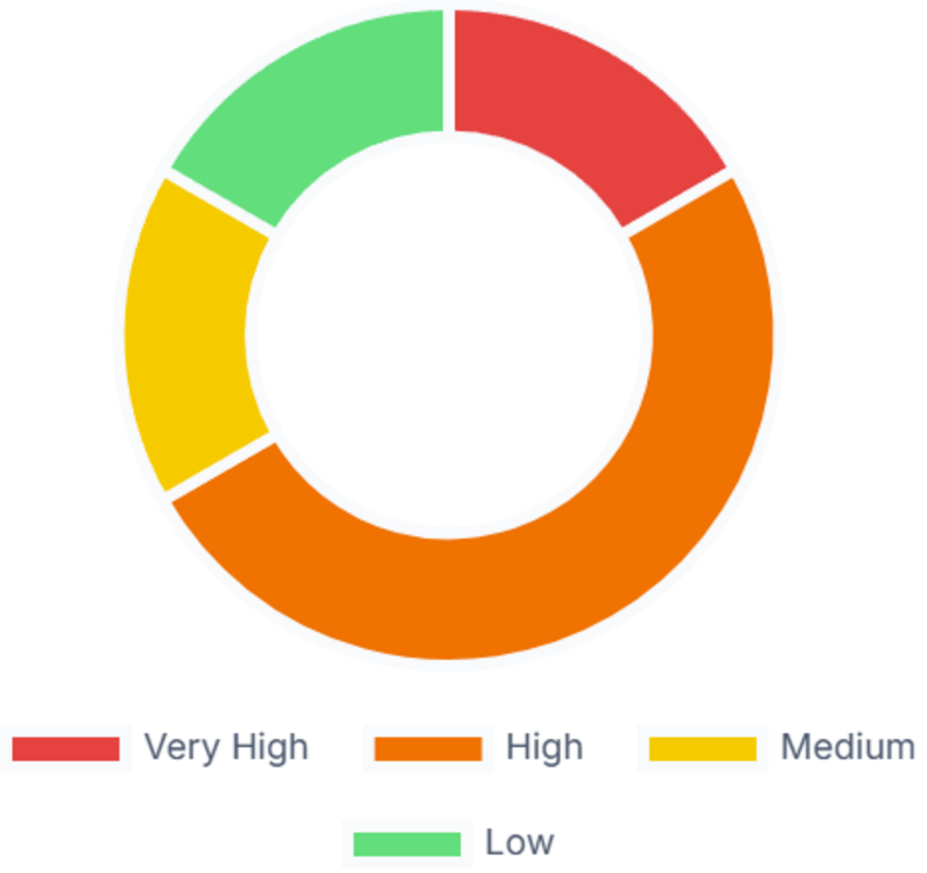
Risk ID	Scenario	Level	Score	Mitigation
UNCLE-DC-001	Unauthorized physical access to server racks by an insider.	Very High	16	Implement biometric access control and CCTV monitoring.
UNCLE-DC-002	Extended power outage due to a regional grid failure.	High	12	Ensure redundant UPS systems and a standby generator.

5. THE EXECUTIVE DASHBOARD

THE DASHBOARD TRANSLATES COMPLEX DATA FROM THE RISK REGISTER INTO STRATEGIC, HIGH-LEVEL INSIGHTS FOR LEADERSHIP. IT PROVIDES A QUICK SNAPSHOT OF OUR OVERALL RISK POSTURE AND HELPS IDENTIFY SYSTEMIC WEAKNESSES THROUGH CONTROL GAP ANALYSIS.

Risk Distribution

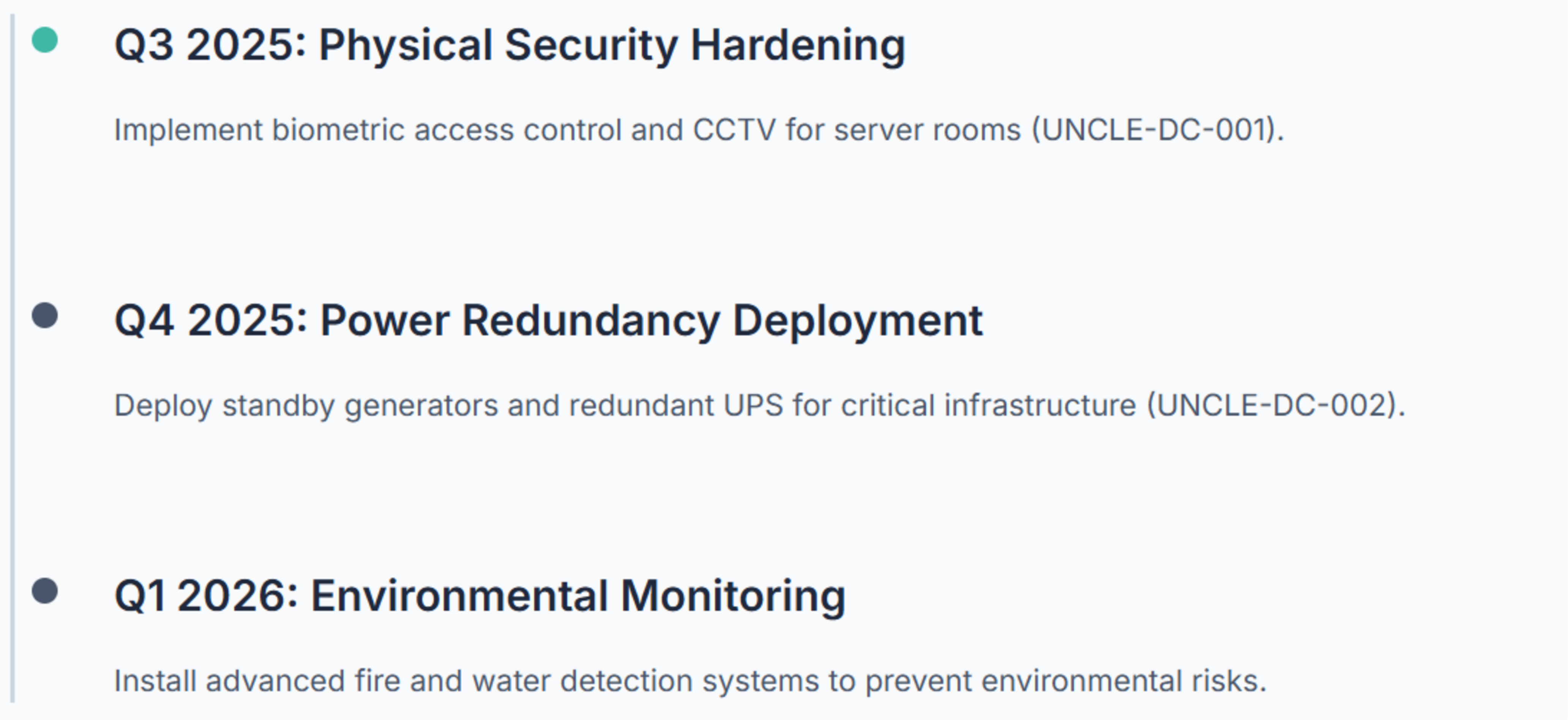
A visual breakdown of all identified risks by their severity level. This helps leadership understand where the majority of our risk lies and prioritize resources accordingly.



CYBER U.N.C.L.E.

6. THE MITIGATION ROADMAP

THE ROADMAP IS OUR VISUAL ACTION PLAN. IT'S A PRIORITIZED LIST OF PROJECTS DESIGNED TO REDUCE OUR HIGHEST RISKS, SHOWING WHAT'S PLANNED, IN PROGRESS, AND COMPLETED. THE ULTIMATE GOAL IS TO SYSTEMATICALLY LOWER RISK SCORES IN THE REGISTER.



● **Q3 2025: Physical Security Hardening**

Implement biometric access control and CCTV for server rooms (UNCLE-DC-001).

● **Q4 2025: Power Redundancy Deployment**

Deploy standby generators and redundant UPS for critical infrastructure (UNCLE-DC-002).

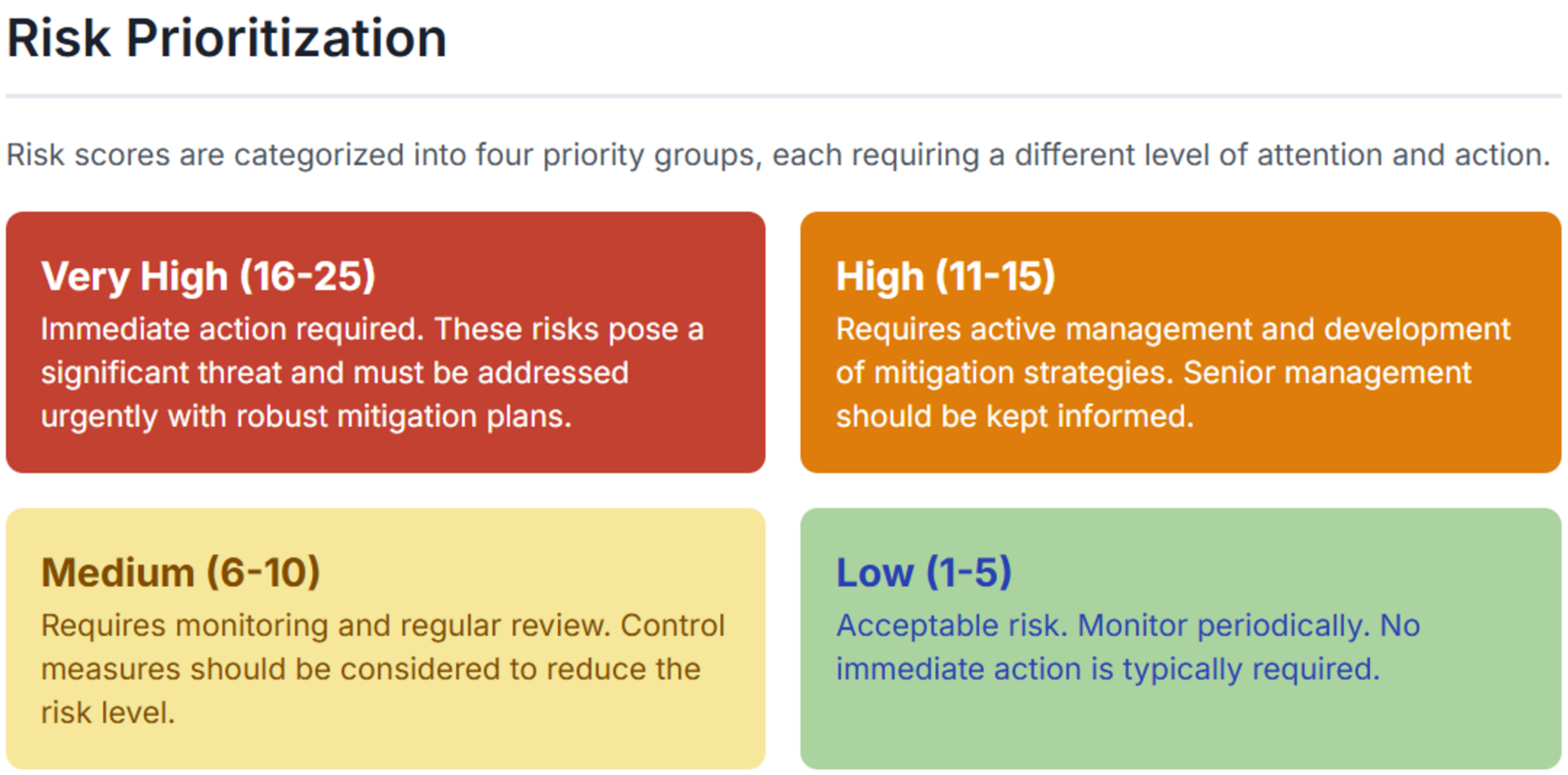
● **Q1 2026: Environmental Monitoring**

Install advanced fire and water detection systems to prevent environmental risks.

7. PRACTICAL WALKTHROUGH: AN END-TO-END EXAMPLE

LET'S FOLLOW THE PHYSICAL SECURITY RISK SCENARIO FROM BEGINNING TO END TO SEE HOW THE PROCESS WORKS IN PRACTICE.

1. RISK IDENTIFICATION: WE IDENTIFY THE RISK OF AN INSIDER GAINING UNAUTHORIZED PHYSICAL ACCESS TO A SERVER RACK DUE TO A WEAK ACCESS CONTROL SYSTEM.
2. INITIAL ASSESSMENT: WE USE THE RISK MATRIX AND SCORE THE RISK AS LIKELIHOOD: LIKELY (4) X IMPACT: MAJOR (4) = VERY HIGH (16).
3. RISK REGISTER ENTRY: WE CREATE A NEW ENTRY IN OUR CYBER RISK REGISTER, DOCUMENTING ALL THE DETAILS FOR `UNCLE-DC-001`.
4. MITIGATION PLANNING: WE DETERMINE THE BEST MITIGATION IS TO IMPLEMENT BIOMETRIC ACCESS CONTROL ON ALL SERVER ROOM DOORS AND ENHANCE CCTV MONITORING.
5. RESIDUAL RISK CALCULATION: AFTER THE CONTROLS ARE IMPLEMENTED, WE RE-ASSESS THE RISK. WE BELIEVE THE LIKELIHOOD WOULD DROP FROM A 4 TO A 1 (RARE). THE NEW RESIDUAL RISK SCORE IS 1 X 4 = 4 (LOW).
6. ROADMAP ACTION: WE ADD "IMPLEMENT BIOMETRIC ACCESS CONTROL" TO OUR MITIGATION ROADMAP AS A HIGH-PRIORITY ITEM FOR THE NEXT QUARTER.



Risk Prioritization

Risk scores are categorized into four priority groups, each requiring a different level of attention and action.

Very High (16-25)
Immediate action required. These risks pose a significant threat and must be addressed urgently with robust mitigation plans.

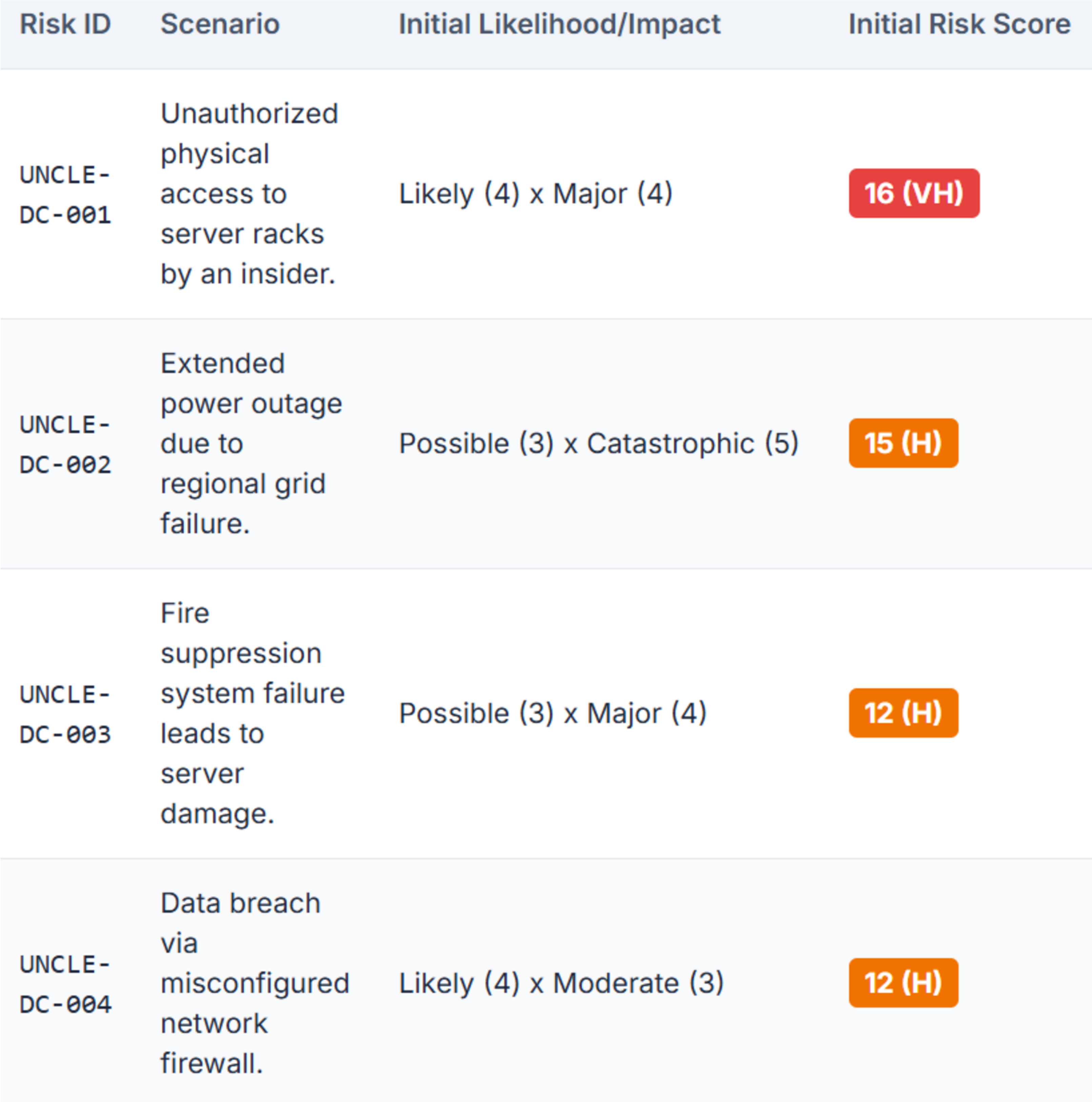
High (11-15)
Requires active management and development of mitigation strategies. Senior management should be kept informed.

Medium (6-10)
Requires monitoring and regular review. Control measures should be considered to reduce the risk level.

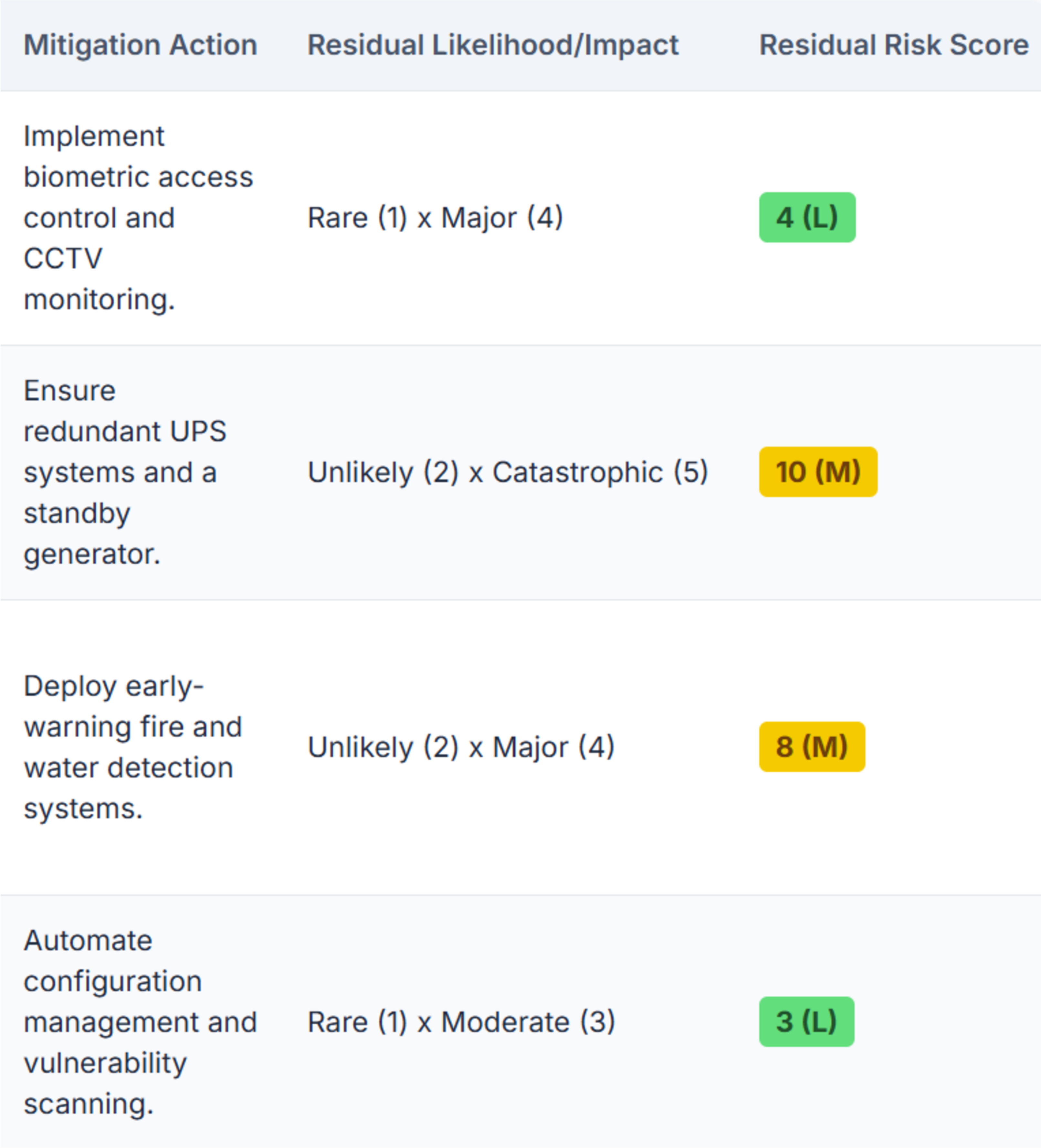
Low (1-5)
Acceptable risk. Monitor periodically. No immediate action is typically required.

8. THE ASSESSED RISK REGISTER

THIS IS A COMPREHENSIVE VIEW OF OUR RISK LANDSCAPE, DETAILING THE FULL LIFECYCLE OF A RISK FROM INITIAL ASSESSMENT TO MITIGATION AND RESIDUAL RISK CALCULATION. THIS TABLE ALLOWS US TO TRACK OUR PROGRESS IN REDUCING RISK AND PRIORITIZE OUR EFFORTS EFFECTIVELY.



Risk ID	Scenario	Initial Likelihood/Impact	Initial Risk Score
`UNCLE-DC-001`	Unauthorized physical access to server racks by an insider.	Likely (4) x Major (4)	16 (VH)
`UNCLE-DC-002`	Extended power outage due to regional grid failure.	Possible (3) x Catastrophic (5)	15 (H)
`UNCLE-DC-003`	Fire suppression system failure leads to server damage.	Possible (3) x Major (4)	12 (H)
`UNCLE-DC-004`	Data breach via misconfigured network firewall.	Likely (4) x Moderate (3)	12 (H)



Mitigation Action	Residual Likelihood/Impact	Residual Risk Score
Implement biometric access control and CCTV monitoring.	Rare (1) x Major (4)	4 (L)
Ensure redundant UPS systems and a standby generator.	Unlikely (2) x Catastrophic (5)	10 (M)
Deploy early-warning fire and water detection systems.	Unlikely (2) x Major (4)	8 (M)
Automate configuration management and vulnerability scanning.	Rare (1) x Moderate (3)	3 (L)

CYBER U.N.C.L.E.