Cybersecurity Risk Management (GRC Portfolio)

Overview: This educational project showcases a mock risk register aligned with **NIST CSF**, **ISO/IEC 27001**, and **CIS Controls**, supported by a corresponding **compliance checklist** and **governance structure** to simulate real-world GRC operations.

Step 1: Asset Overview

This document identifies potential cybersecurity risks affecting key organizational assets and outlines appropriate treatment strategies. The analysis follows risk management principles aligned with **NIST CSF**, **ISO/IEC 27001**, and **CIS Controls**, emphasizing asset protection, threat identification, and risk treatment planning.

Network Assets				
IP Address	Hardware	Software	Open ports	Business Function
10.0.0.0	Router	Linux 5.0	Port 53	DNS infrastructure
127.0.0.1	Dell Server	Apache web server	Port 443	Hosts web services
164.0.1.0	Intel CPU	MySQL Database	Port 22	Stores customer data
124.0.1.0	Cisco router	Windows Server 2019	Port 80	Manages internal apps
148.1.0.0	HP printer	Microsoft Office 365	Port 21	Handles internal print jobs
121.0.1.0	Juniper switch	Google Chrome browser	Port	Connects endpoints (RDP access)

Step 2: Identified Risks

1. **Router**	A compromised IoT device could be used to launch a DoS attack against the organization's router, causing network downtime.
2. **Dell Server**	Employees may receive phishing emails from seemingly trusted sources. Clicking on malicious links can install malware within the organization.
3. **Intel CPU**	Downloading and executing a malicious file could grant unauthorized access and lead to data theft.
4. **Cisco Router**	External attackers may compromise the router to gain control over the network.
5. **HP Printer**	Insider threats could intercept sensitive print jobs containing confidential documents.
6. **Juniper Switch**	Protocol vulnerabilities may allow malicious actors to gain unauthorized network access and inject malware.

Step 3: Risk Register

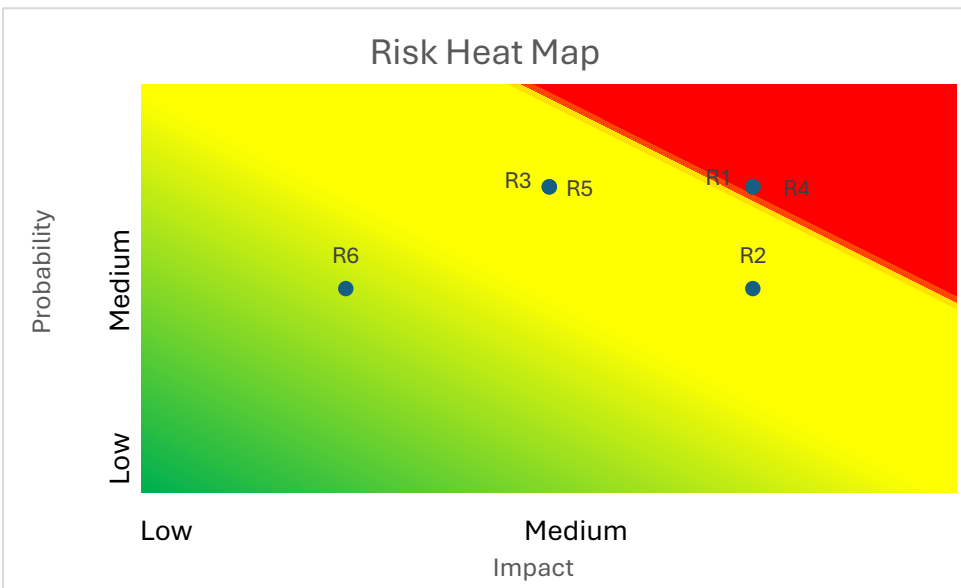
ID	Threat	Threat Source	Likelihood	Vulnerability	Impact	Treatment	Type	Residual Risk
R1	DoS Attack	Compromised IoT	High	Unpatched Software	High	Isolation	Mitigation	Medium
R2	Malware Injection	Phishing Emails	Medium	Outdated Security Configurations	Medium	Anti-Phishing Tools	Mitigation	Low
R3	Data Theft	Malware	Medium	Inadequate Security Measures	Medium	Security Best Practices	Avoidance	Low
R4	Unauthorized Access	External Hackers	High	Poor Router Access Controls	High	Security Configuration	Mitigation	Medium
R5	Print Job Interception	Insider Threats	Medium	Unrestricted Print Privileges	Medium	Access Control	Mitigation	Low
R6	Network Intrusion	Malicious Software	Medium	Protocol Vulnerabilities	Low	Access Control	Mitigation	Low

Step 4: Risk Evaluation (Impact vs Probability)

Risk ID	Impact	Probability
R1	High	High
R2	Medium	Medium
R3	Medium	Medium
R4	High	High
R5	Medium	Medium
R6	Low	Medium

Risk Factors	Impact	Probability
R1	**3**	**3**
R2	**2**	**2**
R3	**2**	**2**
R4	**3**	**3**
R5	**2**	**2**
R6	**1**	**2**

1	**Low**
2	**Medium**
3	**High**



Legend:

- **Mitigation**: Reducing the likelihood or impact of the risk.
- **Avoidance**: Eliminating the activity that leads to the risk.
- **Residual Risk**: The remaining risk after treatment is applied.
- **Control Maturity**: Evaluation of how well current security controls are implemented and maintained (Low / Moderate / High).
-

Compliance Checklist (Mapped to Risk Register)

Risk ID	Control Area	Control Objective	✓ Compliant	Notes
R1 DoS Attack via Router	Patch Management (ISO A.12.6.1, CIS Control 7)	Is router firmware and associated IoT software regularly patched and monitored?	☐ Yes ☐ No ☐ Partial	Consider patch automation or isolation policies
R2 Malware from Phishing	Email Security (ISO A.13.2.3, CIS Control 9)	Are phishing simulations and anti-malware tools deployed across the organization?	☐ Yes ☐ No ☐ Partial	Review employee awareness programs
R3 Data Theft	Endpoint Protection (ISO A.12.6, CIS Control 10)	Are endpoint security tools (DLP, AV) active and enforced?	☐ Yes ☐ No ☐ Partial	Implement USB controls if applicable

R4 Unauthorized Router Access	Access Control (ISO A.9, CIS Control 6)	Are strong authentication and admin access controls enforced on networking gear?	☐ Yes ☐ No ☐ Partial	Consider MFA and port filtering
R5 Print Job Interception	Insider Threat Monitoring (ISO A.8.2.3, CIS Control 14)	Is print access restricted and logged with role-based rules?	☐ Yes ☐ No ☐ Partial	Validate privilege reviews
R6 Network Intrusion via Protocols	Network Segmentation and Control (ISO A.13, CIS Control 12)	Are protocols hardened and unused services disabled across critical switches?	☐ Yes ☐ No ☐ Partial	Review ingress/egress filtering rules

Staff & Organizational Compliance Roles Checklist

Organizational Roles Supporting Compliance

Role/ Area	Responsibility	✓ In Place?	Notes
Compliance Officer	Oversee all compliance and GRC activity; reports to executive leadership	☐ Yes ☐ No	Confirm role exists and has a clear scope
IT Security Lead	Ensure controls (patching, encryption, access) are technically enforced	☐ Yes ☐ No	Aligning with ISO A.12, A13
HR/ Policy Manager	Maintains training logs, policy distribution, and disciplinary tracking	☐ Yes ☐ No	Include acceptable use and ethics guidelines
Audit and Legal Liaison	Prepares evidence for external/ internal audits and regulatory filings	☐ Yes ☐ No	Could be part-time or shared
Backup Personnel	Ensures continuity of coverage during staffing absences	☐ Yes ☐ No	Verify cross-training documentation
PTO Coverage	Does each key compliance function have backup coverage?	☐ Yes ☐ No	Helps ensure control continuity