Exercise on ISMS Threat profiling and Control Strength

Risk assessment score of assets: Threat Profiling & Criticality Score for ISMS Assets

Assets	Threat Type	Confidentiality (C)	Integrity (I)	Availability (A)	Justification	TIS
Server	Physical damage, unauthorized access	3	3	3	Servers store critical data; damage affects all three aspects (CIA).	3
Workstations	Malware, insider threats	3	3	2	Workstations process sensitive data; malware can alter integrity and expose confidentiality	2.66
Network Devices (Firewalls, Routers)	DoS attacks, configuration exploits	1	2	3	DoS attacks target availability; weak configurations may affect integrity.	2.0
Operating Systems	Unpatched vulnerabilities, malware	3	3	2	Exploits can expose or modify sensitive application data.	2.66
Applications	SQL Injection, unauthorized modification	3	3	2	Exploits can expose or modify sensitive application data.	2.66
VPN Systems	Credential theft, MITM attack	3	3	2	VPN breaches compromise data security and system access.	2.66

TIS : Threat Impact factor

Control Strength table:

Assets	Preventive	Detective	Corrective
Servers	Physical security, biometric access, encryption.	Security cameras, access logs.	Disaster recovery, backups.
Workstations	Endpoint protection, strict access control.	Antivirus, EDR(Endpoint detection and response), behavior monitoring	Patch management, incident response
Network Devices	Firewall rules, rate limiting, VPNs.	Traffic monitoring, IDS/IPS.	Failover systems, DDoS protection services.
Operating Systems	Regular patching, privilege control.	Vulnerability scanning, SIEM.	OS rollback, incident handling.
Applications	Input validation, WAF(Firewall).	Log analysis, SIEM(security information event management).	Database backup, remediation.
VPN Systems	MFA, IP whitelisting.	Anomaly detection, logs.	Immediate credential revocation.

Risk score table:

Assets	P	D	C	CS	TIS	VS = TIS-CS	Risk score (TIS * VS)
Servers	3	3	3	9/3 = 3	3	0	0 (Low)
Workstations	3	2	2	7/3 = 2.33	2.66	0.33	0.87 (medium)
Network Devices	3	2	1	6/3 = 2.0	2.0	0	0 (Low)
Operating Systems	3	3	2	8/3 = 2.66	2.66	0	0 (low)
Applications	2	3	2	7/3 = 2.33	2.66	0.33	0.87 (M)
VPN Systems	2	2	2	6/3 = 2	2.66	0.66	1.75 (medium-high)