

## Risk Rating Scale

Scale	Likelihood	Impact
1	Rare	Negligible
2	Unlikely	Minor
3	Possible	Moderate
4	Likely	Major
5	Almost Certain	Severe

## Risk Score = Likelihood × Impact

Range: 1 to 25

Score	Risk Level
1–5	Low
6–10	Medium
11–15	High
16–25	Critical

## Risk Register

#	Risk Description	#	Likelihood	#	Impact	#	Risk Score	T↑	Risk Level	ISO 27001 Controls
1	Unauthorized access due to weak password policy		4		4		16		Critical	A.8.2 Identity Management, A.8.3 Access Control, A.5.17 Authentication Information
2	System compromise via unpatched vulnerabilities		5		5		25		Critical	A.8.23 Technical Vulnerability Management, A.8.9 Configuration Management
3	Incomplete or missing log collection from key assets		4		3		12		High	A.8.15 Logging, A.8.16 Monitoring Activities
4	Insider exfiltration of sensitive data		3		5		15		High	A.5.12 Classification, A.8.11 Data Leakage Prevention, A.6.3 Remote Working
5	Malware infection via phishing		3		4		12		High	A.8.7 Protection Against Malware, A.6.2 Awareness and Training
6	Misconfigured firewall rules exposing internal ports		3		5		15		High	A.8.9 Configuration Management, A.8.20 Network Security
7	Unauthorized use of privileged accounts		4		4		16		Critical	A.8.2 Identity Management, A.8.3 Access Control, A.5.18 Privileged Access Rights
8	Outdated version banner reveals server type/version		2		1		2		Low	A.8.9 Configuration Management, A.8.20 Network Security, A.5.30 Threat Intelligence
9	Lack of regular backups		2		5		10		Medium	A.8.13 Backup, A.8.14 System Redundancy
10	Physical access breach to server room		2		4		8		Medium	A.7.4 Physical Access, A.7.5 Equipment Security