Risk Register Summary

Risk Scoring Methodology

Risk Score = Threat Probability × Threat Impact

Risk Value = Risk Score × Asset Value × Vulnerability Level

Probability Scale (1–5)

- **1 = Very Low** — Rare (<10% annually)
- **2 = Low** — Unlikely (10–30%)
- **3 = Medium** — Possible (30–50%)
- **4 = High** — Likely (50–75%)
- **5 = Very High** — Almost certain (>75%)

Impact Scale (1–5)

- **1 = Negligible** — Minor inconvenience (<₹10 L loss)
- **2 = Minor** — Limited impact (₹10–50 L loss, <4 h downtime)
- **3 = Moderate** — Noticeable impact (₹50 L–₹2 Cr loss, 4–12 h downtime)
- **4 = Major** — Significant impact (₹2–10 Cr loss, 12–48 h downtime, regulatory fines)
- **5 = Critical** — Catastrophic (>₹10 Cr loss, multi-day shutdown, safety/contract loss)

Asset Value (1–10)

- **1–3 = Low value** — Office equipment, non-critical systems
- **4–6 = Medium value** — Supporting systems, general data
- **7–8 = High value** — Important business systems, sensitive data
- **9–10 = Very High value** — Mission-critical systems, IP, safety systems

CIA Triad (Confidentiality, Integrity, Availability)

Scale 1–3 for each:

- 1 = Low impact
- 2 = Medium impact
- 3 = High impact (critical)

Note:

For OT/ICS, *Availability* is top priority (production continuity, safety).

For IP/design data, *Confidentiality* is top priority.

Risk Treatment Priority

Critical Risks (>150)

R001 – IT/OT Segmentation

R002 – Legacy Systems

R003 – IP Protection

High Risks (100–150)

R005 – Vendor Remote Access

R006 – USB Malware

R007 – OT Backups

R010 – OT Incident Response

R012 – OT Monitoring

R013 – Phishing

Medium Risks (70–99)

R004 – Supplier Portal

R008 – Insider Threat

R009 – Physical Security

R011 – Supply Chain Software

R014 – Environment Segregation

Low Risks (<70)

R015 – Customer Data

OT-Specific Risk Considerations

Safety Implications

R001, R002, R006, R007, R010, R014

- PLC malfunction → equipment collision, injury
- Ransomware on SCADA → emergency systems disabled
- Corrupted PLC code → machinery damage, fire/explosion risk

Production Continuity

R001, R002, R006, R007, R010, R012, R014

- Downtime cost ₹2–5 Cr/day
- OEM penalty clauses
- Single extended outage = contract termination

Intellectual Property

R003, R008, R013, R015

- CAD theft = loss of 10 + years R&D
- Competitor undercutting risk
- Loss of TISAX = automotive disqualification

Risk Treatment Recommendations Summary

Immediate (0–3 Months)

1. Implement IT/OT segmentation (R001)
2. Deploy USB port controls (R006)
3. Backup PLC & SCADA configs (R007)

4. Establish DLP for CAD/CAM files (R003)
5. Implement MFA on supplier portal (R004)

Short-Term (3–6 Months)

1. Build OT incident response plan (R010)
2. Deploy ICS intrusion detection (R012)
3. Isolate legacy systems (R002)
4. Secure vendor remote access (VPN/jump box) (R005)
5. Run anti-phishing training + email gateway (R013)

Medium-Term (6–12 Months)

1. Deploy PAM solution (R008)
2. Build OT test lab (R014)
3. Implement firmware integrity checks (R011)
4. Upgrade physical access controls (R009)
5. Encrypt customer data processes (R015)

Document Version: 1.0

Last Updated: Oct 15 2025

Next Review: Jan 15 2026

Approved By: CEO | CISO | VP Operations