CyberNova Technologies Pvt. Ltd.
ISMS Risk Assessment & Treatment Report
Prepared By: Saksham Singh — Cybersecurity Analyst
Date: 31 October 2025

Executive Summary

This Information Security Risk Assessment Report identifies, evaluates, and treats information security risks across CyberNova Technologies Pvt. Ltd. The assessment follows the ISO/IEC 27001:2022 framework ensuring confidentiality, integrity, and availability (CIA) of all assets.

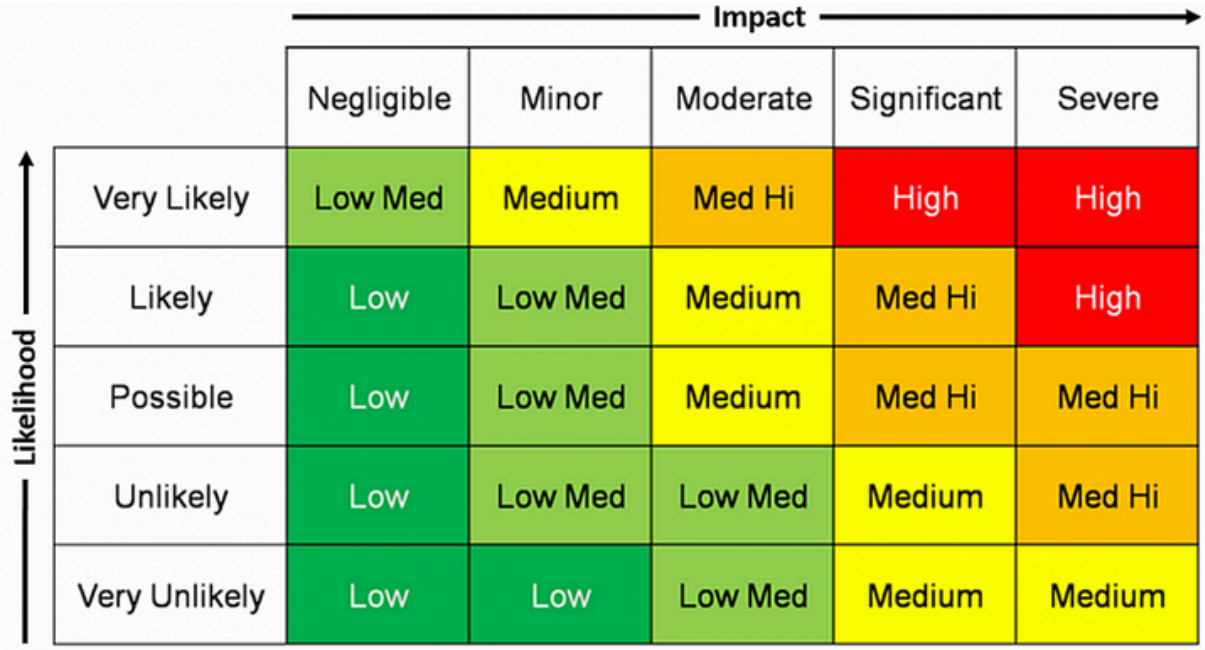
Risks are calculated as: Risk Score = Likelihood × Impact (1–25)

Low (1–5) 🟢 | Medium (6–12) 🟡 | High (13–25) 🔴

Methodology

1. **Asset Identification** – Identify all critical assets.
2. **Threat & Vulnerability Identification** – Determine possible threats.
3. **Risk Evaluation** – Assign Likelihood (1–5) & Impact (1–5).
4. **Risk Scoring** – Likelihood × Impact = Score (1–25).
5. **Risk Categorization** – Low, Medium, High.
6. **Risk Treatment** – Avoid, Reduce, Transfer, Accept.
7. **Residual Risk Evaluation** – Reassess post-treatment.

Risk Matrix



Risk Evaluation Summary

Risk Level	Count	Percentage	Interpretation
Low	0	0%	Acceptable – No immediate action
Medium	3	50%	Needs monitoring and control
High	3	50%	Immediate mitigation

📊 **Observation:**

Half of the risks fall under the High category — particularly related to data protection and encryption. These must be prioritized in mitigation planning.

Conclusion

The assessment identified High (🔴) risks in encryption, misconfiguration, and infrastructure reliability. After mitigation, risks will fall to Medium (🟡) or Low (🟢) levels, aligning with ISMS requirements.

Proposed Risk Treatment Plan

Risk ID	Risk Description	Proposed Mitigation	Responsible	Target Date	Priority
1	Data Breach – Customer Data	Implement AES encryption,	Security Team	Dec 2025	High
2	Phishing Attacks	Conduct awareness	HR Dept	Nov 2025	Medium
3	Cloud Misconfigurations	Perform IAM review & enable	Cloud Admin	Nov 2025	High
4	Laptop Theft	Enable full-disk encryption &	IT Admin	Dec 2025	Medium

Residual Risk (Post-Mitigation)

After implementing mitigation measures, risks are expected to reduce as follows:

Risk	Previous Score	New Score	New Level	Comment
Data Breach	25	9	Medium	Encryption greatly reduces
Phishing	12	6	Low	Awareness reduces
Cloud Misconfig	20	10	Medium	IAM policy reduces exposure
Laptop Theft	16	8	Medium	Encryption lowers impact

Conclusion

This assessment highlights that the organization faces moderate to high security risks, mainly around data confidentiality and misconfigurations.
Implementation of proposed controls is expected to reduce overall risk exposure to acceptable levels within the next review cycle.

Recommendations

✅ Implement data encryption for all sensitive information.
✅ Conduct security awareness training quarterly.
✅ Enforce strong IAM and change management policies.
✅ Schedule periodic vulnerability assessments.
✅ Review risk register quarterly to update residual risks.