Task: NIST 800-30 Risk Assessment for SecureTech Ltd.

Objective:

You are cybersecurity risk assessors conducting a **risk assessment** for SecureTech Ltd., a company that develops cloud-based financial software. SecureTech is concerned about security risks and wants to follow **NIST 800-30** guidelines to identify and evaluate risks.

Your task is to **assess risks**, determine their likelihood and impact, and recommend controls to mitigate them.

Scenario: SecureTech Ltd. Security Risks

SecureTech has identified **five security concerns** that could lead to data breaches, operational disruptions, or compliance failures.

1. **Access Control Risk** – Employees share login credentials for internal systems to "save time."
2. **Asset Management Risk** – No formal inventory exists for IT assets, including company-issued laptops.
3. **Incident Management Risk** – No clear process for reporting security incidents.
4. **Physical Security Risk** – Office servers are stored in an unlocked room accessible to all employees.
5. **Data Protection Risk** – Customer data is stored unencrypted in cloud storage without backups.

Task Instructions:

Step 1: Identify Risks

For each issue above, identify:

- **Threat Source** (e.g., malicious insider, hacker, accidental error)
- **Threat Event** (e.g., unauthorised access, data breach)
- **Vulnerabilities** that enable the risk

Step 2: Assess Risk Impact & Likelihood

Use the NIST **Risk Matrix** (Low, Moderate, High) to evaluate:

- **Likelihood** (How likely is the threat event to occur?)
- **Impact** (What would be the consequence if it happens?)

Risk	Threat Source	Threat Event	Vulnerability	Likelihood	Impact
Access Control Risk	Malicious insider	Unauthorized access	Weak authentication, password sharing	High	High

Step 3: Recommend Mitigation Controls

For each risk, suggest security controls that reduce likelihood or impact (based on **NIST 800-30 risk response strategies**: Accept, Avoid, Transfer, or Mitigate).