**Project Title:** Comprehensive Information Security Audit and Risk Management for Online Retailer (ChicThreads)  
**Prepared by:** Deepthi M

**Executive Summary**

ChicThreads is a small retailers’ clothing company. This Information Security Audit was conducted to identify vulnerabilities, managing customer data and processing online payments recommend improvements to strengthen cybersecurity posture. Several critical gaps were discovered, including the absence of Multi-Factor Authentication (MFA), weak backup policies, reliance on unsecured public Wi-Fi, and a lack of formal incident response plans.

**Scope**

The audit covered the following systems and operational areas:

* Company Website
* Internal IT Infrastructure (computers, servers, routers)
* Data Storage Systems
* Employee Security Practices
* Physical Office Security Measures

**Methodology**

* ISO 27001 Information Security Management System (ISMS) framework was used.
* An ISO 27001-based audit checklist guided the evaluation.
* A Cyber Risk Register was created by assigning Impact and Likelihood scores to identified risks.
* Key observations were recorded systematically during the simulated audit.

**Key Findings**

* Password policies were incomplete, lacking password expiry enforcement.
* Employees accessed company data using unsecured public Wi-Fi without VPN protection.
* No formal Incident Response Plan existed.
* Sensitive customer data was stored without encryption.
* Antivirus software was installed but outdated.
* Employees had not received any cybersecurity awareness training.
* No use of Multi-Factor Authentication (MFA) for administrative accounts.
* Physical security measures (such as CCTV and access control) were inadequate.

**Risk Register Snapshot**

| **Risk ID** | **Risk Description** | **Impact** | **Likelihood** | **Risk Score** | **Recommended Control** |
| --- | --- | --- | --- | --- | --- |
| R1 | Weak password policy | High | Medium | High | Implement strong password policies (length, complexity, expiry); Enable MFA. |
| R2 | Public Wi-Fi usage without VPN | Medium | High | High | Mandate VPN usage for remote access; Security awareness training. |
| R3 | Lack of backup policy | High | Low | Medium | Establish regular automated backup procedures; test restoration. |
| R4 | No MFA (Multi-Factor Authentication) for admin accounts | High | High | High | Implement mandatory MFA for all admin and privileged accounts. |
| R5 | Outdated antivirus software | Medium | Medium | Medium | Deploy updated antivirus and endpoint protection; schedule regular updates. |
| R6 | Sensitive data stored unencrypted | High | Medium | High | Encrypt sensitive data at rest and in transit; implement key management. |

**Recommendations**

* Enforce strong password policies, including mandatory password expiry and complexity requirements.
* Implement Multi-Factor Authentication (MFA) for all administrative and sensitive accounts.
* Mandate the use of VPNs for all remote work and public Wi-Fi connections.
* Establish, document, and regularly test a formal backup and restoration policy.
* Encrypt all sensitive customer and internal data at rest and in transit.
* Regularly update antivirus and anti-malware software.
* Conduct quarterly cybersecurity awareness training for all employees.
* Strengthen physical security with CCTV surveillance and electronic access controls.
* Develop and maintain an Incident Response Plan to effectively handle security breaches.

**Conclusion**

The Information Security Audit has revealed several critical risks that pose a significant threat to Online Retail (ChicThreads) information assets. Immediate action is recommended to address these vulnerabilities, especially concerning data protection, user authentication, and incident response capabilities. Continuous monitoring, employee training, and semi-annual audits are advised to maintain a strong cybersecurity posture over time.