Softsense Technoserve (India) Private Limited [STIPL]

Registered Under

Company Act 1956, Ministry of Corporate Affairs,

Government of India

CIN: U72900MH2012PTC236313

An ISO 9001:2015 Certified

Registered with MSME and GeM

Corporate Office

Murlidhar Complex, First Floor, Temple Bazar Rd.,

Sitabuldi, Nagpur 440012. INDIA

Registered Head Office

22A, Pande Layout, Khamla,

Nagpur 440025. INDIA

Key Cyber Security Services

1. Cyber Security Audit Services

- **Vulnerability Assessment & Penetration Testing (VAPT)**

  Supporting police or judicial bodies in solving cybercrime cases involving impersonation, harassment, fraud, hacking, ransomware, identity theft, and more. It includes security to -

  - Web Applications
  - Mobile Applications
  - Network Infrastructure
  - Cloud Environment
  - IoT/IIoT Devices

- **Internal & External Security Audit** (as per CERT-IN standards)
- **Risk Assessment & Gap Analysis** (ISO 27001, NIST, RBI-CSF, etc.)
- **Configuration Review**
  - Firewall, Router, Switch
  - Endpoint Security
  - Active Directory / Domain Controllers
- **Data Loss Prevention (DLP) Assessment**
- **Security Posture Assessment** for Core Banking & Payment Systems
- **SWIFT Environment Audit** (for BFSI)
- **Incident Response Readiness Audit**

2. Regulatory Compliance Support

- **RBI Cyber Security Framework Compliance**
- **SEBI Cybersecurity Guidelines Adherence (for brokers/DPs/AMCs)**
- **IRDAI Guidelines for Insurers**
- **ISO/IEC 27001:2022 Implementation & Internal Audit**
- **SOC 2, PCI-DSS Pre-Audit and Readiness**
- **CERT-IN Empanelled Audit Support**
- **Cyber Insurance Risk Audit Support**
- **BFSI-Specific Compliance Mapping & Reporting**

3. Corporate Cyber Security Training

- **Employee Awareness Training** (Role-Based)
  - Executive Management
  - IT Admins / DevOps / Developers
  - General Staff / Operations Team
- **Red Team & Blue Team Exercises** (Simulated Attacks & Defenses)
- **Secure Coding Practices** (for Development Teams)
- **Phishing Simulation Campaigns**
- **Cyber Hygiene & Best Practices Workshop**
- **CISO/IT Manager Enablement Programs**
- **Training as per RBI, SEBI, IRDA, and NCIIPC Guidelines**

4. Digital Forensics & Incident Response

- **Section 63(4)(c) Certificate**
  - Issuance of certificates under Section 65B of the Indian Evidence Act for the admissibility of digital evidence in court proceedings.
- **Hash Value Report**
  - Generating SHA-256/MD5 hash values to verify data integrity and authenticity of digital files and devices.
- **Account Recovery Services**
  - Assisting in recovery of hacked or compromised digital accounts, including email, social media, cloud storage, and mobile applications.
- **Digital Forensics Investigation**
  - Full-spectrum digital forensic analysis of devices, logs, storage media, networks, and systems. Useful for corporate frauds, data breaches, and financial crimes.
- **Mobile Forensics**
  - Extraction and analysis of deleted data, call logs, messages, app data, geolocation, and chat records from smartphones and tablets.
- **Testimony Services**
  - Providing detailed expert opinions, digital evidence validation, and **courtroom testimony** in cybercrime or electronic evidence-based cases.
- **Expert Witness Services**
  - Appearing in court as a **qualified digital forensic expert**, presenting findings, and answering technical cross-questions.

5. Cyber Security Consulting & Advisory

- **Cyber Risk Assessment & Mitigation Planning**
- **Policy, SOP & Cyber Governance Documentation**
- **Cyber Crisis Management Planning**
- **Third-Party Vendor Risk Assessment**
- **CIO/CISO as-a-Service** (vCISO)
- **Board-Level Cybersecurity Briefings**
- **Threat Hunting & APT Analysis**

ANNEXURE 1

Why Cybersecurity Auditing is Important for Private Sector

Introduction

In today's world, most businesses whether small startups or big factories-rely on digital tools, cloud systems, and connected networks to run smoothly. But with this convenience comes the risk of cyber threats like unauthorized access, hacking, data theft, ransomware, and system failures. This is why cybersecurity auditing is not just a technical checklist; it's a smart habit every business owner and factory manager should adopt. It helps make sure everything is running safely and securely.

Why Cybersecurity Auditing Matters for Entrepreneurs

Entrepreneurs are always busy building their brand, handling customers, and growing their business. But if cybersecurity is ignored, one small mistake can lead to a big loss. Here's how regular auditing helps:

- It keeps your important business and customer data safe from hackers.
- It shows your investors and partners that you take security seriously.
- It helps you follow the law and avoid fines or legal trouble.
- It helps spot problems in your systems before they cause damage.
- It makes sure you're ready with a backup plan if something goes wrong.

Why Cybersecurity Auditing is Crucial for Manufacturing Companies

Factories today use smart machines, automated systems, and digital supply chains. These tools are powerful but also open doors for cyberattacks. A cybersecurity audit helps by:

- Protecting your machines, control systems, smart gadgets from being hacked.
- Keeping your blueprints, designs, and formulas safe from theft.
- Making sure production doesn't stop due to a cyber incident.
- Checking that your suppliers and vendors are also following good security practices.
- Audits help detect flaws in firmware, network communication, APIs, and authentication systems before products are deployed in critical environments and prevents post-deployment issues like data breaches, operational sabotage, or device hijacking.
- Helping you follow safety and industry standards.

Common Benefits for All Businesses

No matter the size or type of business, cybersecurity audits offer clear **benefits**:

- Keeps your data and systems secure.
- Finds weak spots before attackers do.
- Helps you meet legal and industry rules.
- Builds trust with customers and investors.
- Prepares you to recover quickly after an incident.
- Keeps your business running without disruption.
- Supports your growth in a safe and secure way.

Failure to perform cybersecurity audits can expose a business to **reputational loss**, **potential defame**, **negative social and political impact**, and even **fluctuations in stock price** if the company is listed on NSE or BSE.

ANNEXURE 2

Why Cybersecurity Auditing is Important for Government Sector

Introduction

According to the **Indian Computer Emergency Response Team (CERT-In)** under the Ministry of Electronics and Information Technology (MeitY), certain categories of **government and critical digital infrastructure** are required to undergo **regular Cyber Security Audits**.

Who Needs Cyber Security Audits as per CERT-In?

As per CERT-In guidelines and directives (especially the one issued on **April 28, 2022**), the following **must undergo cybersecurity audits:**

1. All Government Organizations and Departments

- Ministries, departments, and PSUs (Public Sector Undertakings)
- State and central government websites and portals
- Any digital infrastructure handling government services or citizen data

2. Critical Information Infrastructure (CII)

Defined under the **Information Technology Act, 2000** as any infrastructure whose incapacitation may affect:

- National security
- Economy
- Public health or safety Sectors
- Power and energy
- Banking and finance
- Transportation (rail, aviation, metro, etc.)
- Telecom
- Defence and space
- Healthcare
- Smart cities and utilities

3. Entities Providing Essential Services

- Cloud service providers
- VPN service providers
- Data centers
- Cybersecurity incident response teams

Frequency of Cyber Security Audit

- **Annually (Minimum)**: Most government and public sector organizations are required to **conduct security audits at least once every year**.
- **Before Go-Live (Pre-launch Audit)**: Mandatory for any new digital service, portal, or application before it goes live.
- **Post Major Updates or Breaches**: Any significant change in software, infrastructure, or after a security incident requires a fresh audit.
- **Quarterly or Bi-Annually (Recommended for CII)**: For highly sensitive or critical systems, audits may be done more frequently depending on sector-specific policies.

Key Focus Areas of CERT-In Recommended Audits:

- Application and network vulnerability assessments
- Penetration testing
- Configuration and patch management review
- Data security and privacy compliance
- Incident detection and response capabilities
- Log retention and monitoring systems

ANNEXURE 3

Softsense & Cyber Security

- Since 2013, Softsense is partner with Information Sharing and Analysis Center (ISAC) for Cyber Security specializations including; Penetration Testing, Exploit Development, Malware Analysis, Reverse Engineering, Web Application Security, Mobile Application Security, and Digital Forensic Analysis.
- Softsense established **Nation's first Cyberange Lab** in 2018 at Nagpur. Cyberange is a smart city simulation lab based on IoT, PLC/SCADA and Simulation technology that provides hands-on labs for SCADA / IoT Security.
- Partner for **NSD** Empanelment Programs (NSD – National Security Database) and ISAC Internship Program for providing Internship in Cyber Security.
- Softsense is a recognized **Cyber Security Auditor**, successfully conducting audits for several private and public sector organizations across various industries. With a team of certified experts and hands-on experience, Softsense ensures that systems, networks, and applications meet the highest standards of security and compliance. Our audits help organizations identify vulnerabilities, strengthen cyber defenses, and align with national and international regulatory frameworks—supporting a more resilient and secure digital ecosystem.
- Softsense is involved in execution of VAPT, Boot Camps, Corporate Trainings, Forensic services, and Consultancy services to Banking, IT, Manufacturing, and Service industry since 2013.

---- END ----