CYBERSRC®
SECURITY RISK COMPLIANCE
Simplifying Cyber Risk Management..

CyberSRC® Consultancy LLP

CERT-IN GUIDELINES

WAY TO CYBERSRC SERVICES...

CYBERSRC CONSULTANCY →

CYBERSRC®
SECURITY RISK COMPLIANCE
Simplifying Cyber Risk Management..

Setting the Context

The Indian Computer Emergency Response Team has issued guidelines on 28th April, 2022 relating to information security practices, procedures, prevention, and response and reporting of cyber incidents for safe and trusted internet.

The guidelines were created after the team discovered some gaps in the analysis of breach incidents while dealing with cyber incidents and interactions with the constituency.

CERT-In (the Indian Computer Emergency Response Team) is an information technology (IT) security organization mandated by the government. The objective of CERT-In is to deal with computer security incidents, report on vulnerabilities, and promote effective IT security practices across the country. It encourages citizens in developing a better level of cyber awareness. It also improves the security of the Indian Internet domain.

CYBERSRC CONSULTANCY →

CERT-IN Guidelines

The organizations requires to:

1. To compulsorily report cybersecurity incidents, including data breaches: *within 6 hours*

2. The directions instructs concerned organization to synchronize ICT system clocks to the Network Time Protocol (NTP) Server of the National Informatics Centre (NIC) or National Physical Laboratory (NPL).

3. The organization shall designate a *Point of Contact* to interface with CERT-In as mentioned in Annexure II.

4. The organization needs to maintain logs of ICT systems: ***rolling period of 180 days.***

5. Data Centers, Virtual Private Server (VPS) providers, Cloud Service providers and Virtual Private Network Service (VPN Service) providers needs to maintain the following information *for a period of 5 years*:
   - Validated names of subscribers/customers hiring the services;
   - Period of hire including dates, IPs allotted to / being used by the members;
   - Email address and IP address and time stamp used at the time of registration / on-boarding;
   - Purpose for hiring services;
   - Validated address and contact numbers;
   - Ownership pattern of the subscribers / customers hiring services.

6. The e virtual asset service providers, virtual asset exchange providers and custodian wallet providers (as defined by Ministry of Finance from time to time) shall mandatorily maintain following information *for a period of 5 years*:
   - Maintain all information obtained as part of Know Your Customer (KYC) and
   - Records of financial transactions

CYBERSRC CONSULTANCY →

Applicability of Guidelines

Service Providers

Intermediaries

Data Centre

Government Entities

Body Corporate

Synchronization of ICT System Clocks

SUB REQUIREMENTS	CyberSRC® SERVICES
Assess the clock synchronization of all the ICT systems.	CyberSRC® vCISO Services
Synchronize the ICT system clocks with NTP server of NIC or NPL.	
Periodic reviews to ensure all the ICT systems have their clock synchronized with NIC or NPL NTP server.	

Mandatory Reporting of Cyber Incidents to CERT-IN

SUB REQUIREMENTS	CyberSRC® SERVICES
Identification of Internal cyber threats for the organization.	CyberSRC® services : Threat Hunting, Forensics
Identification of external threats for the organization. Monitoring of external incidents (data leak, phishing domain creation, source code leak, defacement of website, rogue application, credit card leak, brand abuse, social media monitoring).	SRC-TI™ Solution (External Threat Platform)
Coordinating Follow-ups with CERT-IN for any additional queries. Preparation of Incident analysis report. Coordinating with different departments for gathering required information and evidence related to the incident. Coordination with the management for reporting of incidents to CERT-IN within 6 hours.	CyberSRC® vCISO Services

Designating a Point of Contact to interface with CERT-In

SUB REQUIREMENTS	CyberSRC® SERVICES
Assisting the management in selection of Point of Contact to interface with CERT-IN. Assisting the organization in updating the information of Point of Contact to CERT-IN in the format specified in Annexure II. Coordinating with the Point of Contact for the implementation of information and direction of compliance that are received from CERT-IN. Review of the status of implementation of controls as per CERT-IN directions. Assist in sharing of responses and reports of compliance to CERT-IN on periodic basis.	CyberSRC® vCISO Services

Maintenance of Logs within Indian Jurisdiction

SUB REQUIREMENTS	CyberSRC® SERVICES
➢ Documentation of log monitoring controls as per CERT-IN direction. ➢ Assisting the management in implementing the documented controls as per the CERT-IN direction. ➢ Reviewing the status of enabling the logs for all the ICT systems for a rolling period of 180 days. ➢ Assisting the management in providing the log management report to CERT-IN when ordered or directed.	CyberSRC® vCISO Services
➢ Conducting the periodic data localization audits to ensure that the log data lies under the Indian jurisdiction.	Periodic Data Localization Audit

CYBERSRC CONSULTANCY →

Maintenance of Subscriber/Customer Details

[Data Centres, Virtual Private Server (VPS) providers, Cloud Service providers and VPN Service providers]

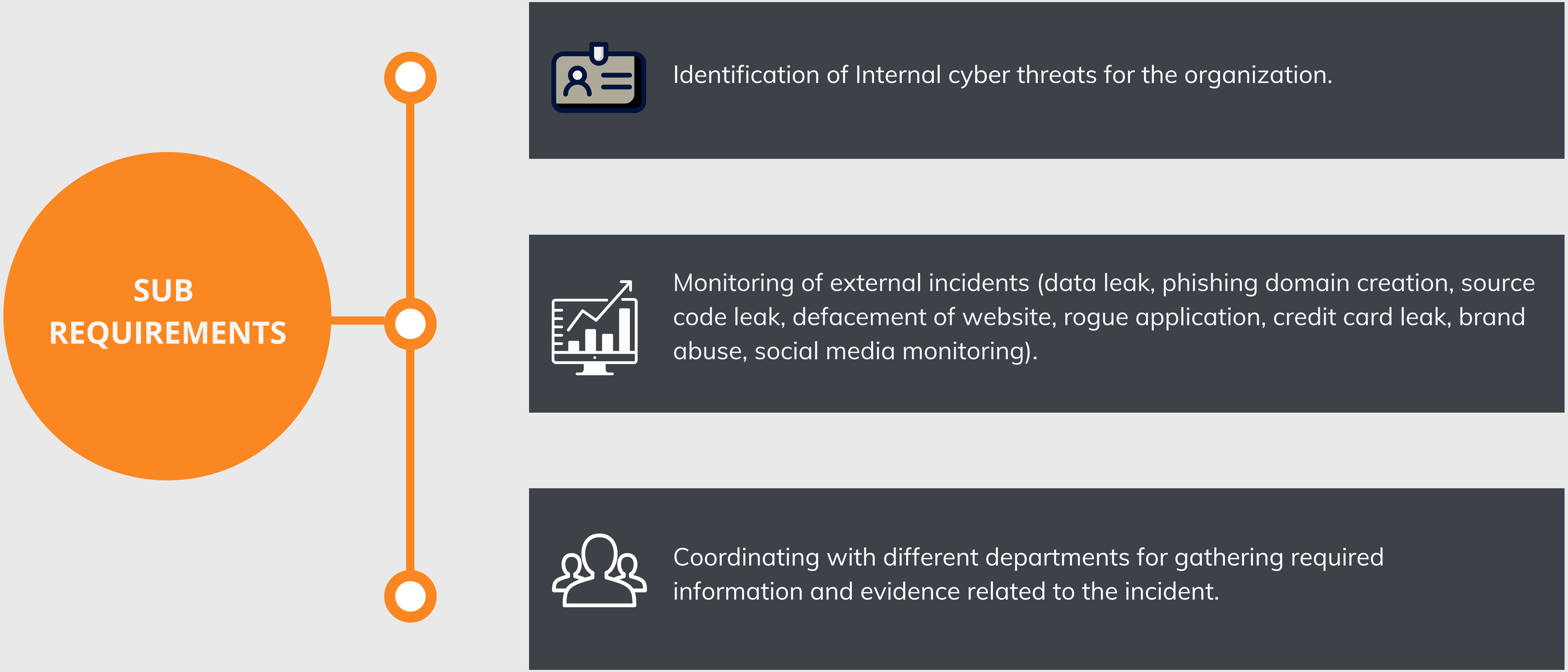
SUB REQUIREMENTS	CyberSRC® SERVICES
▶ Documentation of policies and procedures for data retention. ▶ Assisting the management in implementing the documented requirements as per the CERT-IN direction. ▶ Reviewing registering status of the following accurate information which must be maintained by the organization for a period of 5 years or longer duration as mandated by the law after any cancellation or withdrawal of the registration as the case may be: • Validated names of subscribers/customers hiring the services • Period of hire including dates • IPs allotted to / being used by the members • Email, IP address & time stamp used at time of registration / on-boarding • Purpose for hiring services • Validated address and contact numbers • Ownership pattern of the subscribers / customers hiring service	CyberSRC® vCISO Services

Information Maintenance, obtained as part of KYC

[Virtual asset service providers, virtual asset exchange providers and custodian wallet providers]

SUB REQUIREMENTS	CyberSRC® SERVICES
➤ Documentation of policies and procedures for data retention. ➤ Assisting the management in maintaining all the information obtained as part of Know Your Customer (KYC) for a period of 5 years as per the laws mandated the procedures as amended from time to time may be referred to as per Annexure III. ➤ Assisting the management in maintaining the records of financial transactions for a period of five years with accurate information. ➤ Review of the status of implementation of data retention period of KYC and financial transactions as per CERT-IN directions.	CyberSRC® vCISO Services

Incident Reporting



SUB REQUIREMENTS

Identification of Internal cyber threats for the organization.

Monitoring of external incidents (data leak, phishing domain creation, source code leak, defacement of website, rogue application, credit card leak, brand abuse, social media monitoring).

Coordinating with different departments for gathering required information and evidence related to the incident.

CYBERSRC®
SECURITY RISK COMPLIANCE
Simplifying Cyber Risk Management..

Mandatory Incident Reporting

Types of cyber security incidents mandatorily to be reported by service providers, intermediaries, data centres, body corporate and Government organisations to CERT-In are:

- Data Leak
- Fake mobile Apps
- Compromise of critical systems/ information
- Attacks through malicious mobile apps
- Targeted scanning/probing of critical networks/systems
- Data Breach
- Unauthorised access of IT systems/ data
- Identity theft, spoofing and phishing attacks
- Unauthorised access to social media accounts
- Attacks or incident affecting digital payment systems

CYBERSRC CONSULTANCY

CYBERSRC®
SECURITY RISK COMPLIANCE
Simplifying Cyber Risk Management..

Mandatory Incident Reporting

Types of cyber security incidents mandatorily to be reported by service providers, intermediaries, data centres, body corporate and Government organisations to CERT-In are:

- Attacks on application such as E-Governance, E-Commerce etc.
- Defacement of website and unauthorized changes in the website.
- Malicious activities affecting cloud computing systems/ servers/ software/ applications.
- Attacks on critical infrastructure, SCADA & operational technology systems and wireless networks.
- Attacks related to big data, block chain, virtual assets, virtual asset exchanges, custodian wallets, robotics, 3D & 4D printing and drones.
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.
- Attacks related to artificial intelligence and machine learning.
- Attack on servers such as database, mail and DNS and network devices such as routers.
- Attacks on Internet of Things (IoT) devices & associated systems, networks, software, servers.
- Malicious code attacks such as spreading of virus/ worm/ trojan/ bots/ spyware/ ransomware/ cryptominers.

CYBERSRC CONSULTANCY →

CYBERSRC®
SECURITY RISK COMPLIANCE
Simplifying Cyber Risk Management..

Why CyberSRC®?

Cost-effective and Scalable:

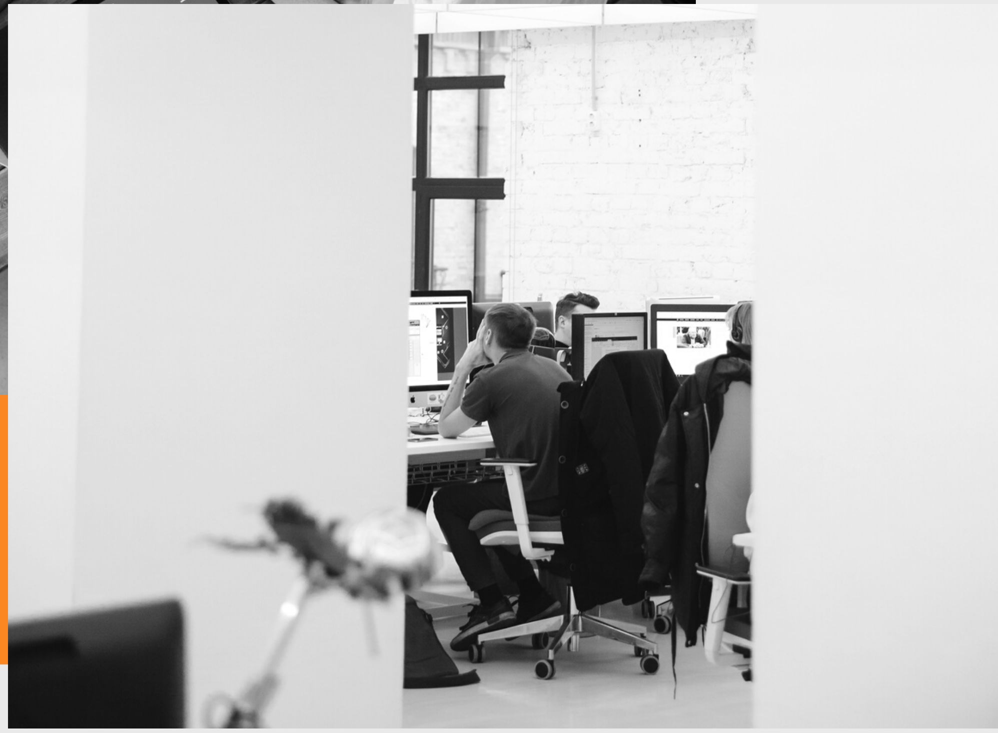
We provide a cost-effective scalable solution at a price that can be budgeted by small mid-size organizations. The pricing model is dynamic and suits your business requirements. We provide both onsite and offshore support based on the plans you select with us.

True Security Advisory:

Every client has access to our team of security and compliance experts which comprises of security leadership, technical support executives, compliance experts, and researchers.

Complete Security and Compliance Solution:

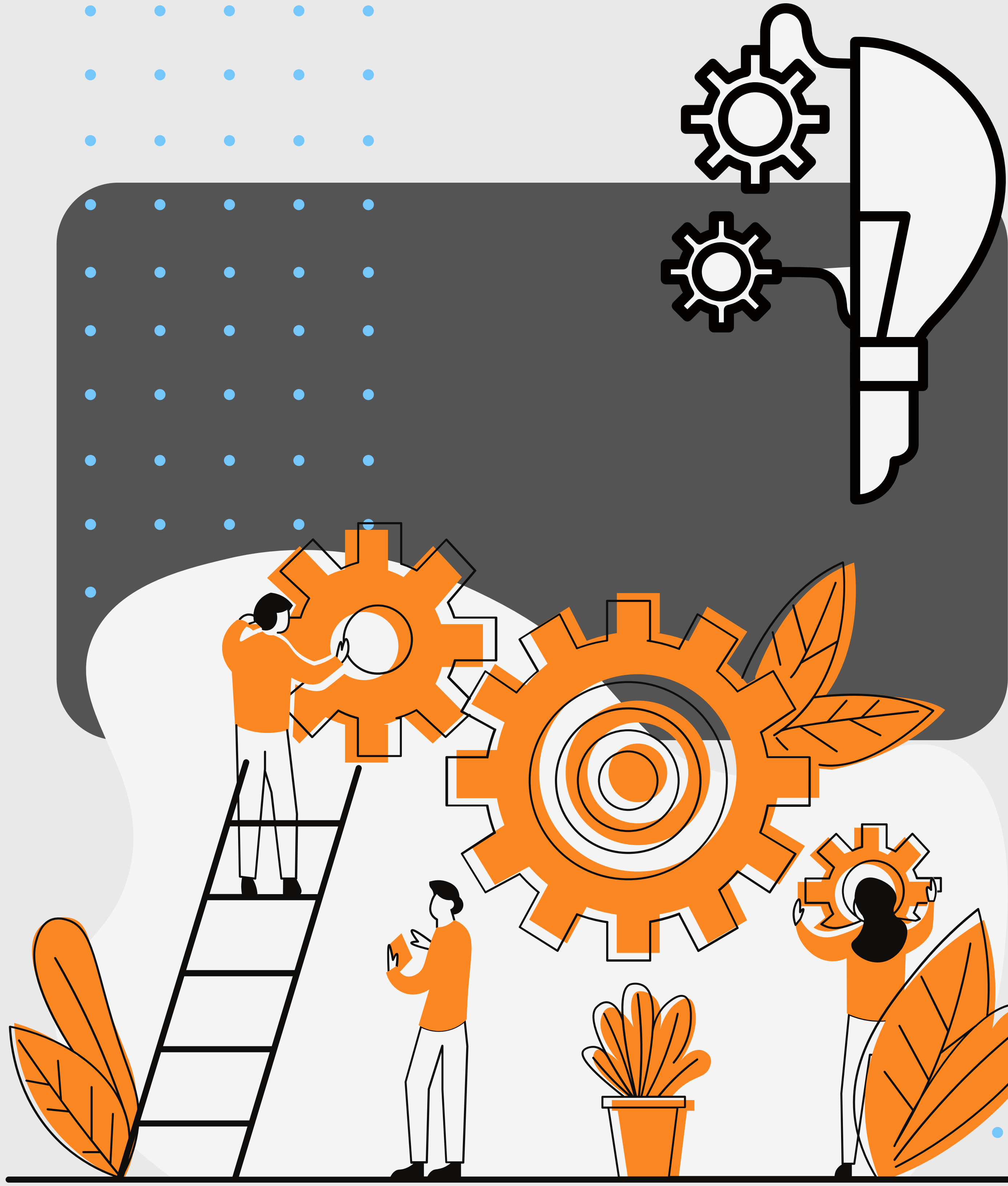
Our team has developed cybersecurity programs for multiple organizations ranging from SMEs, MSMEs & corporates. Our client ranges from manufacturing IT, BPO/KPO, insurance, BFSI, and others.



CYBERSRC CONSULTANCY →

CyberSRC® Unique Selling Point (USP)

- Transform your security profile under the convenient and cost-efficient model.
- Provide executive-level strategy, security planning, pre-assessments, annual risk assessments, and scalability according to changing business requirements.
- Provide effective solutions, vendor assessment, operations, budgets, review of security contracts of third-party vendors, and training that is tailored to your needs.
- Establish a security roadmap, align the security program with an industry framework, and support and augment your existing team.
- Provide end-to-end security and compliance solutions.
- CyberSRC® has channel partnerships with multiple vendors and provide cost-effective scalable solutions at a reasonable price.
- Our team has developed cybersecurity programs for multiple organizations ranging from SMEs, MSMEs & corporates.



CYBERSRC CONSULTANCY →

Scope of Services

- Incident Response
- Policies & Procedures
- Risk Assessment
- On-Demand Strategy & Services
- Security Awareness & Trainings
- Customer Onboarding Support
- Determine Security Framework
- Strategic Security Objectives
- Security & Compliance Expertise
- Third-party Vendor Risk Assessments
- Periodic Internal Audits
- Customized Security Solutions
- DR Drills
- Phishing Simulation Exercise

Services Offering

COMPLIANCE MANAGEMENT

- ✓ ISO 27001 ISMS
- ✓ ISO 22301 BCMS
- ✓ ISO 27701 PIMS
- ✓ National Institute of Standards and Technology (NIST)
- ✓ Health Information Trust Alliance(HITRUST)
- ✓ Control Objectives for Information and Related Technologies (COBIT)
- ✓ Centre for Internet Security (CIS)
- ✓ PCI DSS
  SOX (Applications & ITGC)

Information System Audit & Assurance

- ✓ RBI
- ✓ Payment & Settlement Systems (PSS)
- ✓ NBFC
- ✓ Co-Operative Banks
- ✓ Prepaid Payment Instruments
- ✓ SEBI
- ✓ NPCI
- ✓ AADHAAR
- ✓ ENSIGN ASP
- ✓ Security Standards (ISO, NIST, CIS & Others)

Services Offering

IT Risk Management

- ✓ SSAE 18 – SOC1/2/3
- ✓ ISAE 3402
- ✓ Third Party Security Risk Management
- ✓ IT Risk Management
- ✓ IT Strategy & Transformation
- ✓ IT Strategy review & Alignment
- ✓ IT in Merger & Acquisition
- ✓ Governance Framework Strategy and Implementation

Data Protection& Privacy

- ✓ General Data Protection Regulation (GDPR)
- ✓ California Consumer Privacy Act (CCPA)
- ✓ Brazilian General Data Protection Law (LGPD)
- ✓ Personal Information Protection and Electronic Documents Act (PIPEDA, Canada)
- ✓ Singapore Personal Data Protection Act (PDPA)
- ✓ Health Insurance Portability and Accountability Act (HIPAA)

CYBERSRC CONSULTANCY →

How can CyberSRC® help you?

CyberSRC® offers a pool of experts and experienced cybersecurity practitioners who are aware of the challenges faced by the automotive industry. The security experts will collaborate with the entities to implement strategy that is tailored to their organization's structure and culture. They will provide the structure, transparency and guidance to the organization which they require globally for the data protection compliance.

At CyberSRC®, we work with the customers to develop programs that will support them to stay focused on their business goals and provide valuable insight to enhance their security and privacy posture.

CYBERSRC CONSULTANCY

CyberSRC® Through the Years

Our history at a glance

Established in January 2018, CyberSRC® Consultancy offers the full gambit of cybersecurity services ranging from threat intelligence to general advisory services in areas pertaining to cybersecurity such as vulnerability attacks, compliance, and cybersecurity regulations, and laws.

CyberSRC® Consultancy within a short span of three years has mitigated cyber risks across a broad spectrum of clients. For instance, there are organizations that require system auditing. This involves complying with various regulations and laws.

Our Team

We are team of qualified professionals with rich experience of multiple industries such as Manufacturing, BFSI, Insurance, Healthcare, NBFCs & others.

Our consultants and auditors are industry experts and have proven track records, some of the renowned certificates that our consultants hold such as CISA, CIPM, CISSP, COBIT, CEH, CCNA, OSCP, ISO 9001 LA/LI, ISO 27001, ITIL LA/LI, PMP, to name a few. We believe in adding value to your business which is enabled through our Centre of Excellence (CoE) and, we have the end-to-end capability for Program Build–Operations Transformation.

Backed by a very diverse and dynamic team which have a combined experience of 45+ years under the belt

CYBERSRC CONSULTANCY →

CYBERSRC®
SECURITY RISK COMPLIANCE
Simplifying Cyber Risk Management..

Our Services

INFORMATION SYSTEM ASSURANCE & AUDIT

VULNERABILITY AND PENETRATION TESTING SERVICES

EXTERNAL THREAT INTELLIGENCE

RISK COMPLIANCE ADVISORY

PHISHING CAMPAIGNS/ STIMULATION

REGULATORY COMPLIANCE AUDIT (RBI, IRDA, SEBI)

PRIVACY AND DATA PROTECTION COMPLIANCE AND AUDIT

INCIDENT RESPONSE & MALWARE ANALYSIS

ISO IMPLEMENTATION & ADVISORY (ISO 27001, 9001, 27701)

Network & Cloud Security

CYBERSRC CONSULTANCY

Our Esteem Clients

INDIAN AIR FORCE BENEVOLENT ASSOCIATION
सर्वे भवन्तु सुखिनः
INDIAN ARMY
SERVICE BEFORE SELF
DELHI PUBLIC SCHOOL
न्याय सब के लिए
ACCESS TO JUSTICE FOR ALL
UZIO
Kailash
क.रा.बी.नि. ESIC
सामाजिक सुरक्षा
SOCIAL SECURITY
ARMY PUBLIC SCHOOL
TRUTH IS GOD
एनएचपीसी NHPC
NHPC Limited
(A Government of India Enterprise)
India's Premier Hydro Power Utility
truecaller
EPOCH
WE SERVE ONTIME EVERYTIME
STONEWAIN
SYSTEMS INC
GTPFINANCE
compport
DELHI POLICE
सत्यमेव जयते
Spice money
तो Life बनी
WISH FIN
Denave
Sales.Enabled
Monkeycap
Be sure when you insure
NVT
techmatrix
CONSULTING
EPIC Private Equity
Msb
SMART DOCUMENT SOLUTIONS
epsilon
carbon
Wittybrains
MSTI
Tech Mahindra
open
knowlarity
SAIKRISHNA & ASSOCIATES
ADVOCATES
EBIX
Afflatus
Think Talent™
SERVICES
Insurance
Health Life Motor
BUY BEST
Forget the rest Buy the best!
Aarca Research
ddd
Digital Divide Data
UNO MINDA
ICONIC
spice
Digital
A spiceconnect Company

Disclaimer: Some of the above clients are not our direct clients but we have provided services as part of larger engagement

CYBERSRC CONSULTANCY

CYBERSRC®
SECURITY RISK COMPLIANCE
Simplifying Cyber Risk Management..

Contact Us

WEBSITE

www.cybersrcc.com

CONTACT NUMBER

+91 8800377255

EMAIL

info@cybersrcc.com,pre-sales@cybersrcc.com

HEAD OFFICE

Unit 605, 6th floor, World Trade
Tower, Sector 16, Noida (UP) -201301, India

OTHER OFFICE

London (UK): Kemp House 152 160 City
Road, London, UK (EC1V 2NX)

CYBERSRC CONSULTANCY →