CYBERSRC®
SECURITY RISK COMPLIANCE
Simplifying Cyber Risk Management..

CyberSRC® Solution For

ISO 42001:2024 Compliance

The world's first AI management system standard

Introduction

CYBERSRC® SECURITY RISK COMPLIANCE
Simplifying Cyber Risk Management..

ISO/IEC 42001:2024 is an international standard that provides a framework for establishing, implementing, maintaining, and continually improving an Artificial Intelligence Management System (AIMS) within organizations.

It is designed for entities that develop, provide, or use AI-based products or services, ensuring responsible development and use of AI systems.

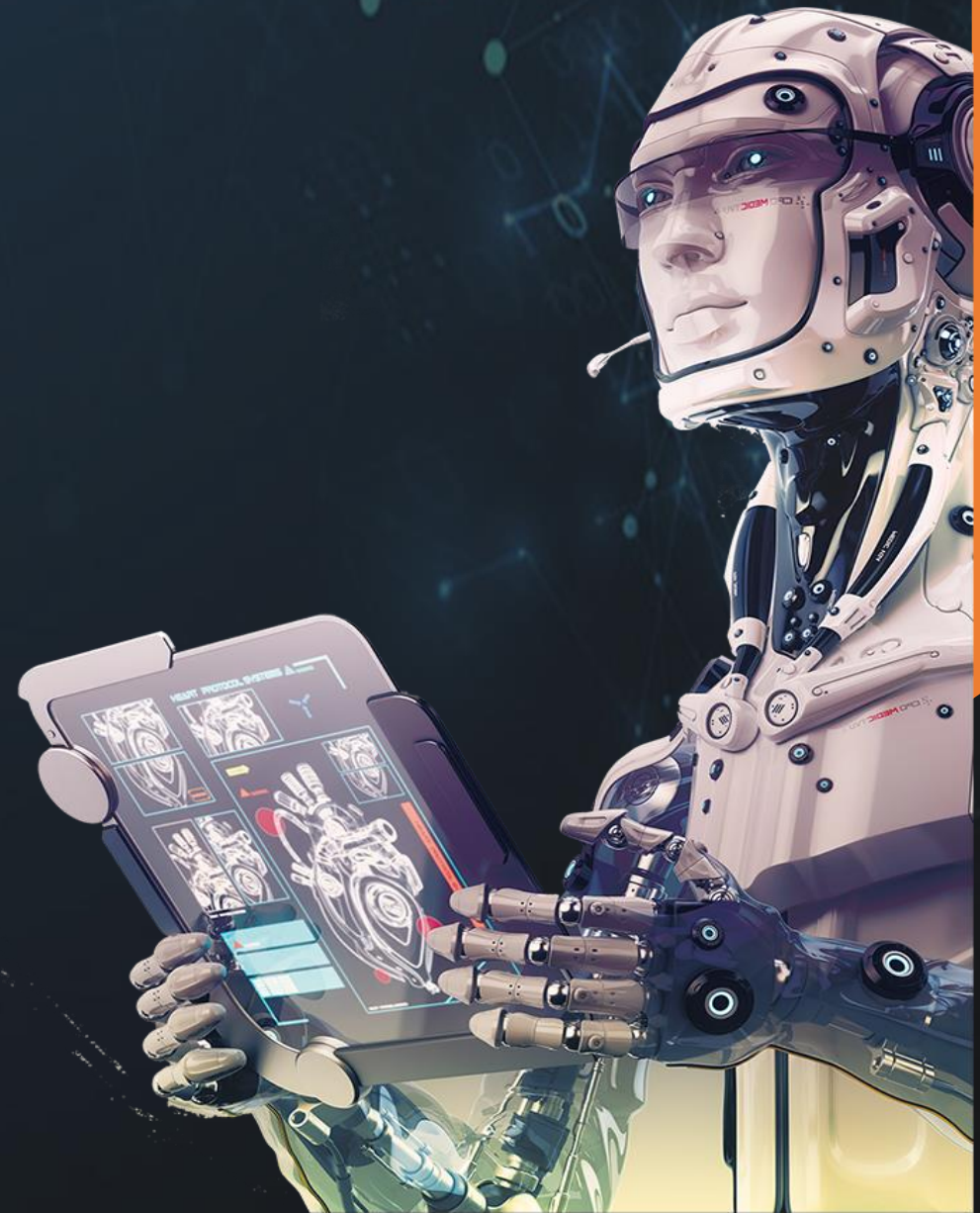
The standard addresses unique challenges posed by AI, such as ethical considerations, transparency, and continuous learning, and offers a structured way to manage risks and opportunities associated with AI.

Significance of ISO 42001

CYBERSRC®
SECURITY RISK COMPLIANCE
Simplifying Cyber Risk Management..

ISO/IEC 42001:2023 is a pivotal standard for organizations involved in the development, provision, or use of AI-based products or services. Here's why it's important and necessary:

- ✓ **First of Its Kind:** It's the world's first standard dedicated to an Artificial Intelligence Management System (AIMS), providing a structured framework for managing AI systems.
- ✓ **Addresses Unique AI Challenges:** The standard tackles the unique challenges posed by AI, including ethical considerations, transparency, and continuous learning, which are not covered by other management standards.
- ✓ **Risk Management:** It offers a systematic approach to managing the risks inherent in AI, such as biases, data privacy issues, and security threats.



CYBERSRC®
SECURITY RISK COMPLIANCE
Simplifying Cyber Risk Management..

- ✓ **Regulatory Alignment:** ISO/IEC 42001:2023 aligns with international regulatory trends, helping organizations stay compliant with evolving laws and regulations concerning AI.
- ✓ **Global Benchmark:** It sets a global benchmark for ethical, secure, and transparent AI practices, guiding organizations towards best practices in AI management.
- ✓ **Innovation and Governance Balance:** The standard balances innovation in AI with proper governance, ensuring that AI technologies are harnessed safely and effectively.
- ✓ **Sustainable Development Goals:** ISO/IEC 42001:2023 contributes to several United Nations Sustainable Development Goals, promoting a sustainable and equitable future.

Objectives

CYBERSRC®
SECURITY RISK COMPLIANCE
Simplifying Cyber Risk Management..

Responsible AI Development:

It guarantees that AI systems are created, implemented, and controlled in an accountable, transparent, safe, and responsible manner.

AddrUnique Challenges:

essing It tackles the unique challeng- es posed by AI such as ethical considerations, transparency, and the need for continuous learning in this rapidly evolving field of technology.

Balancing Innovation and Governance:

offers a structured approach to manage risks and opportunities associated with AI.

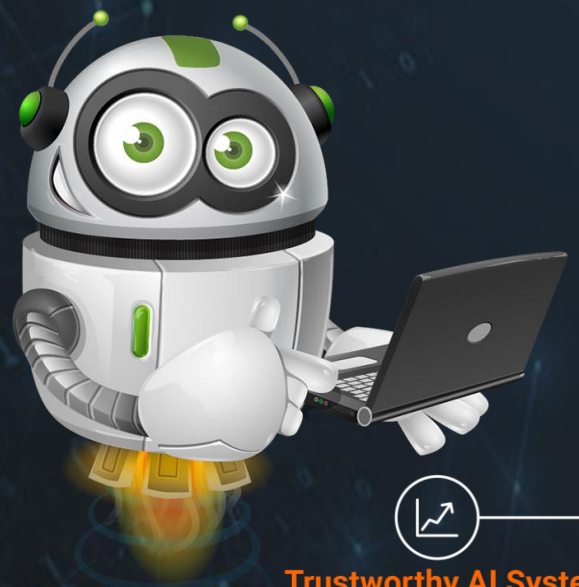
CYBERSRC®
SECURITY RISK COMPLIANCE
Simplifying Cyber Risk Management..

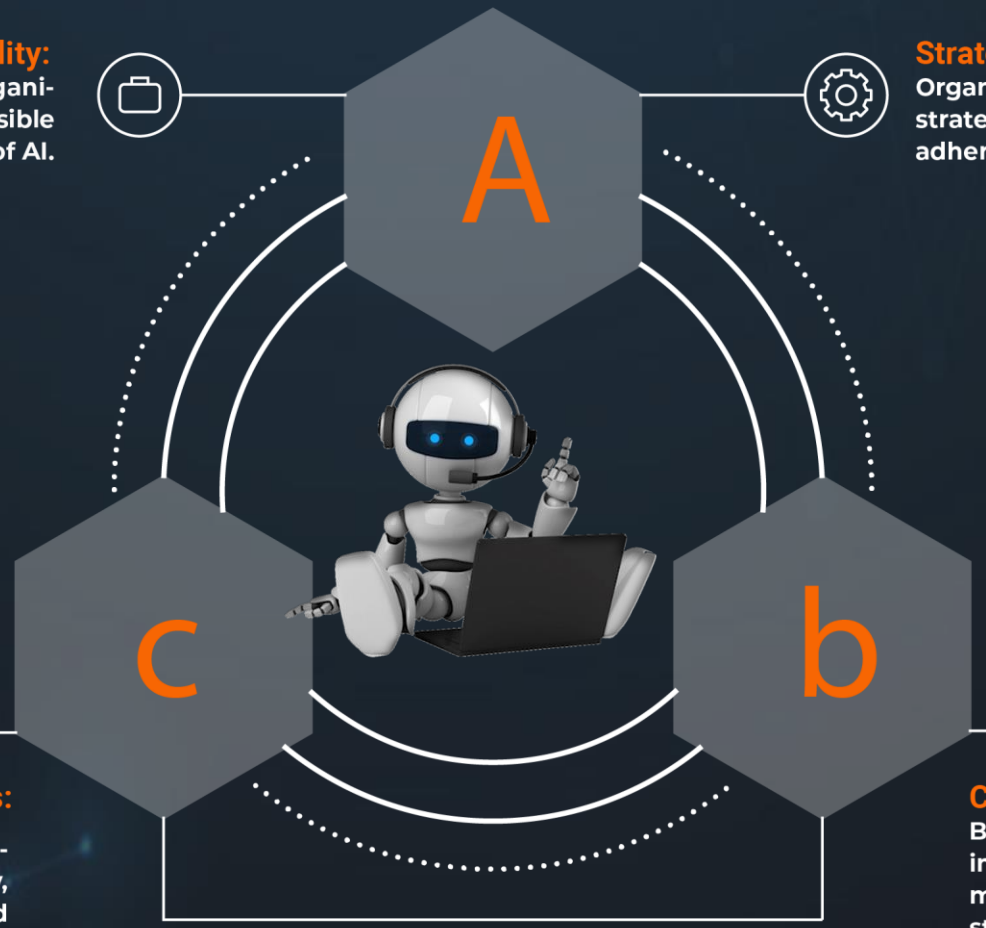
Evidence of Responsibility:

It provides verifiable proof of an organization's dedication to the responsible application of AI.

Strategic Decision-Making:

Organizations can make well-informed, strategic decisions about implementing AI by adhering to ISO 42001 standards.





Trustworthy AI Systems:

The standard promotes fairness, transparency, explainability, accountability, robust data management, safety, and reliability in AI systems

Cost Savings and Efficiency Gains:

Because of it focuses on continuous improvement and systematic risk management, AI processes are streamlined, which reduces costs and increases efficiency.

Overview of ISO 42001:2023 Controls

CYBERSRC® SECURITY RISK COMPLIANCE
Simplifying Cyber Risk Management..

- *A2 Polices Related to AI*
- *A3 Internal Organization*
- *A4 Resources for AI systems*
- *A5 Assessing impacts of AI systems*
- *A6 AI system life cycle*
- *A7 Data for AI systems*
- *A8 Information for interested parties of AI systems*
- *A9 Use of AI system*
- *A10 Third-party and customer relationships*

Our Approach & Methodology

CYBERSRC® SECURITY RISK COMPLIANCE
Simplifying Cyber Risk Management..

Implementing ISO 42001, which is the international standard for asset management, involves several key steps.

- ***Defining Scope and Objectives:*** Clearly defining the scope of the AI Management System implementation. Identification of the assets to be managed, their criticality, and the objectives which are aim to achieve through ISO 42001 compliance.
- ***Assessing Current Systems (Gap Assessment):*** Evaluating the current AI systems and management practices to identify gaps between existing processes and the standard's requirements.
- ***Documentation Support:*** Documentation of the policies, procedures and records to define the controls sufficing the requirements of ISO 42001 standard.

- ***Developing an Implementation Plan:*** Create a detailed plan that outlines the steps needed to achieve compliance with ISO 42001. This includes timelines, responsibilities, and actionable.
- ***Internal Audit:*** *Create a plan for conducting internal audit w.r.t. ISO 42001:2024 and evaluate the operating effectiveness of the implemented controls. Develop an internal audit report including observations/ findings and recommendations for the closure of the findings.*

Scope of Services

- ✓ Gap Assessment
- ✓ Documentation (Policies & Procedures)
- ✓ Implementation Advisory
- ✓ Risk Assessment and Treatment Plan
- ✓ Internal Audit and Reporting
- ✓ Security Awareness Training & Evaluation
- ✓ Third Party Risk Management
- ✓ Security Assessments & Remediation
- ✓ External Audit Support

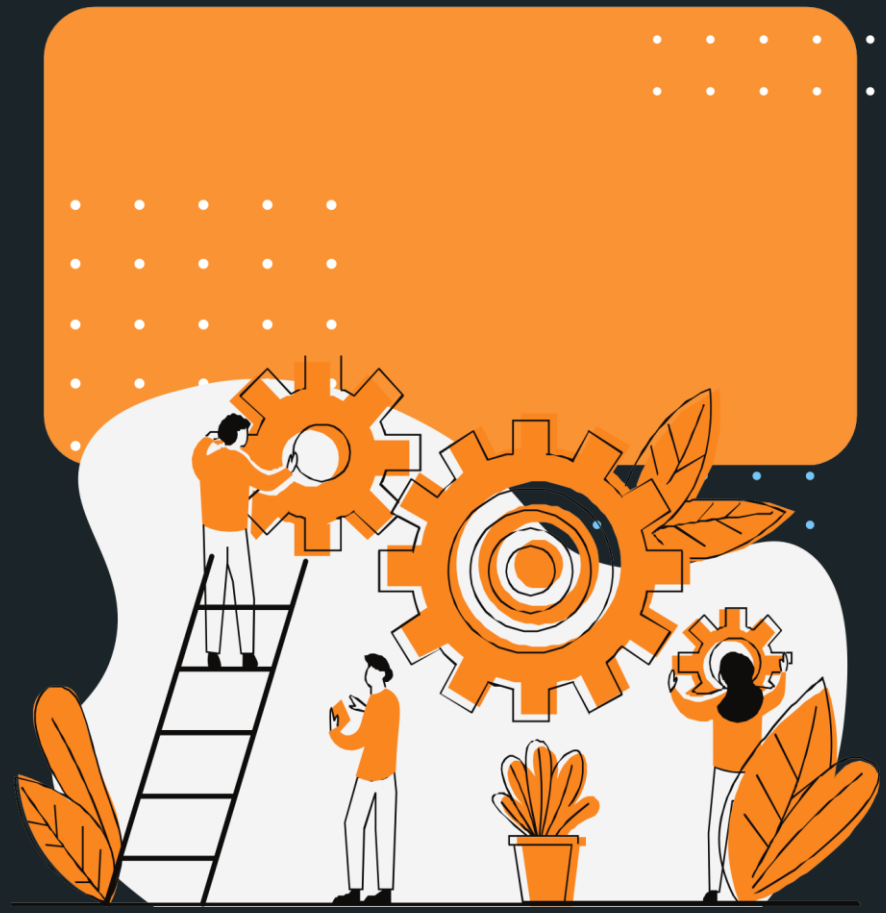
How can CyberSRC® help you?

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® Unique Selling Points (USP)

- Transform your security profile under the convenient and cost-efficient support model.
- Provide executive-level strategy, security planning, 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.
- Our pricing model is dynamic (per hour based) and suits your business requirements. We provide both onsite and offshore support based on the plans you select with us.



CyberSRC® Through the Years

Our history at a glance

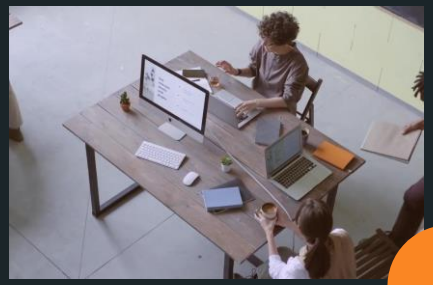
Established in January 2018, CyberSRC® Consultancy offers the full gambit of cybersecurity services ranging from threat intelligence to general advisory services in areas pertaining to cybersecurity such as vulnerability attacks, compliance, and cybersecurity regulations, and laws.

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.

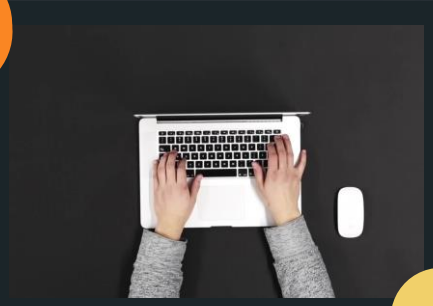
Our Team

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 35 years under the belt



Service 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)

Service 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)

Our Esteemed Clients

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

Contact Us

WEBSITE

www.cybersrcc.com

CONTACT NUMBER

0120 – 416 0448

EMAIL

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

HEAD OFFICE

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

Noida Office

Unit 1715 A, 17th floor, World Trade Tower, Tower-B, Noida- 201301, Uttar Pradesh, India

OTHER OFFICE

London (UK): 15 Castle Drive Ilford , Redbridge Ig4 5AE , London, UK.