CyberSRC® Solution for

# NIST AI RISK Management Framework



CYBERSRC CONSULTANCY

# Introduction

- Artificial intelligence (AI) has the potential to greatly improve our lives in many areas, including business, healthcare, transportation, and cybersecurity, as well as benefiting the environment and the planet as a whole. AI can drive economic growth that includes everyone and support scientific progress that makes the world a better place.

- AI technologies however, also pose risks that can negatively impact individuals, groups, organizations, communities, society, environment, and the planet.

# What is AI RMF?

- AI RMF is to offer a resource to the organizations designing, developing, deploying, or using AI systems to help manage the many risks of AI and promote trustworthy and responsible development and use of AI systems.
- AI RMF is to offer a resource to the organizations designing, developing, deploying, or using AI systems to help manage the many risks of AI and promote trustworthy and responsible development and use of AI systems.
- AI actors are defined by the Organization for Economic Co-operation and Development (OECD) as “those who play an active role in the AI system lifecycle, including organizations and individuals that deploy or operate AI”

*Flexibly Applied*

*Voluntary*

*Right Preserving*

# This Framework articulates the following characteristics of trustworthy AI and offers guidance for addressing them.

| | | | | | |
|---|---|---|---|---|---|
| Safe | Secure & Resilient | Explainable & Interpretable | Privacy-Enhanced | Fair - With Harmful Bias Managed | Accountable & Transparent |
| Valid & Reliable | | | | | |

# Why this Framework was introduced?

- As, AI systems also bring a set of risks that are not comprehensively addressed by current risk frameworks and approaches.

- Also, risks posed by AI systems are in many ways unique, such as:

  - ✓ **Changing Data:** AI learns from data, but if the data changes a lot, it can make the AI behave in unexpected ways.
  - ✓ **Complex Situations:** AI systems are often used in complicated situations, making it hard to spot and fix problems.
  - ✓ **Human and Society Influence:** AI is affected by how people behave and what's happening in society.
  - ✓ **Mix of Factors:** The risks and benefits of AI come from both technical issues and how the AI is used in real life.

# Objectives of AI RMF

- ***Responsible Development:*** We need to make sure AI is designed and used in ways that match our values and goals.

- ***Mitigating the financial and reputational damage*:** ai failures can cost an organization in every aspect of the firm, from regulatory fines to lost business all of which can be avoided if proactive risk management is instituted.

- ***Comply with Regulation*:** AI RMF aligns with fast-growing global standards and AI regulations, helping organizations stay ahead of their legal requirements.

- ***Trustworthiness:*** Managing AI risks makes AI more reliable and helps people to trust it more.

# Challenges for AI Risk Management

- *Risk Measurement*
- *Risk Tolerance*
- *Risk Prioritization*
- *Organizational Integration and Management of Risk*

# Effectiveness of the AI RMF

- Organizations and other users of the Framework are encouraged to periodically evaluate whether the AI RMF has improved their ability to manage AI risks, NIST intends to work collaboratively with others to develop metrics, methodologies, and goals for evaluating the AI RMF's effectiveness, and to broadly share results and supporting information.

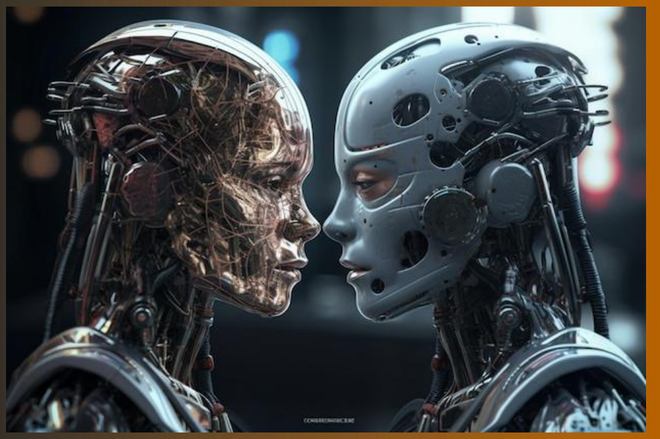
- Framework users are expected to benefit from:

  - enhanced processes for governing, mapping, measuring, and managing AI risk, and clearly documenting outcomes.

  - improved awareness of the relationships and tradeoffs among trustworthiness characteristics, socio-technical approaches, and AI risks.

  - established policies, processes, practices, and procedures.

  - strengthened engagement with interested parties and relevant AI actors.



# AI RMF Core

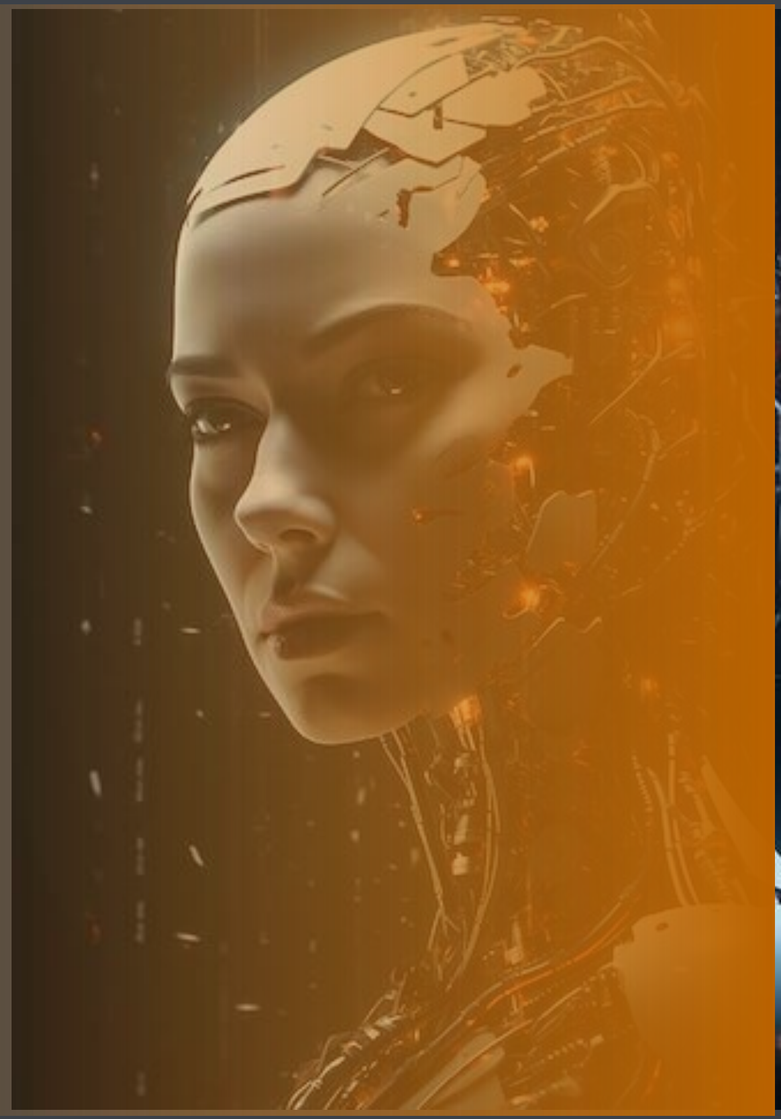
- ✓ Core is composed of four functions: ***GOVERN, MAP, MEASURE, and MANAGE***.
- ✓ Each of these high-level functions is broken down into 19 categories and 72 subcategories. Categories and subcategories are subdivided into specific actions and outcomes.

- **GOVERN :** This function involves establishing and maintaining risk management program to oversee AI systems. It includes setting policies, ensuring accountability, and promoting a culture of risk-aware decision-making.

- **MAP :** The MAP function focuses on understanding the AI system and their contexts. It enables organizations to identify potential risks and understanding the system purpose, functionality and the data it uses also recognizing stakeholders impacted by AI system.

- **MEASURE :** The MEASURE involves quantitative, qualitative, or mixed-method to monitoring and updating risk management practices as AI systems and their contexts evolve.

- **MANAGE :** The MANAGE involves implementing strategies to mitigate identified risks. This includes a developing and deploying controls, continuous

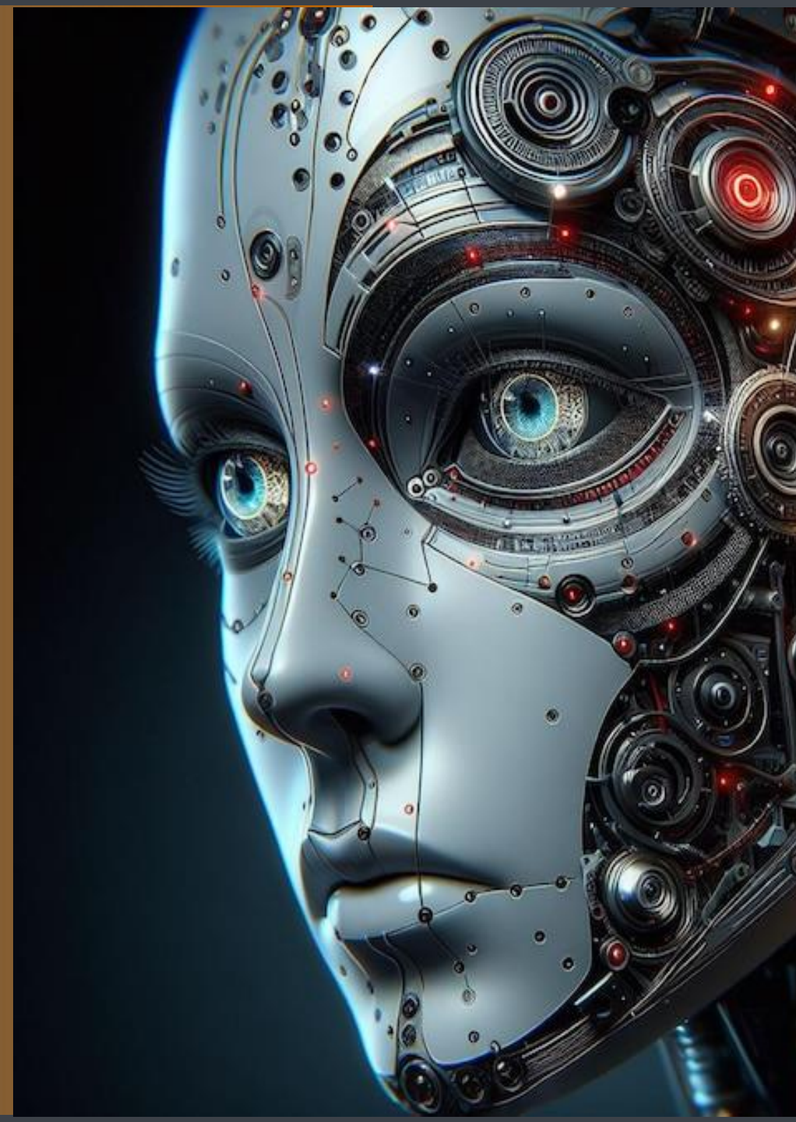


# Attributes of the AI RMF

- ✓ *Risk-based, resource-efficient, encourage innovation, voluntary- participation.*
- ✓ *consensus-Driven and Transparent Process, Inclusive contribution from all stakeholders.*
- ✓ *Uses clear and plain language that is accessible to a broad audience, including non-experts with sufficient technical depth for practitioners, also facilitates communication across various levels and sectors.*
- ✓ *Provides common language and understanding to manage AI risks with taxonomy, terminology, and definitions.*
- ✓ *Easily usable and fit well with other aspects of risk management.*

# Approach to implement RMF to within an organisation

Implementing the NIST AI RMF requires a strategic approach tailored to the specific needs and challenges of each organization. It begins with a thorough understanding of the framework and its implications for AI governance and management. The NIST AI RMF is intended to be adapted by organizations of all sizes and can be used as a template for their own AI risk management program.



### Implementing the AI RMF in Your Organization

- ✓ ***Assessment*:** Evaluate AI systems and risk management practices against the AI RMF standards.
- ✓ ***Planning*:** To address gaps and enhance AI risk management capabilities.
- ✓ ***Customization*:** Tailor the AI RMF to fit your organization's specific context, risks, and objectives.
- ✓ ***Execution*:** Implement the planned changes, including updating policies, procedures, and systems as needed.
- ✓ ***Monitoring and Review*:** Continuously monitor the effectiveness of your AI risk management practices and adjust as necessary.

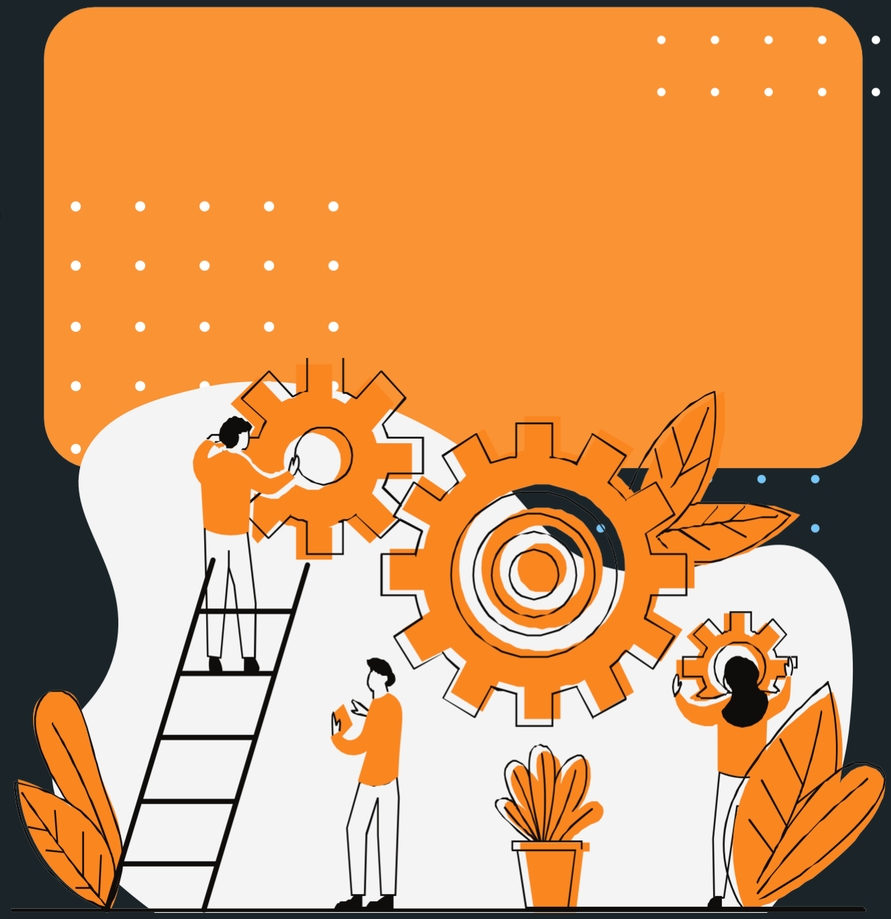
# How can CyberSRC® help you?

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

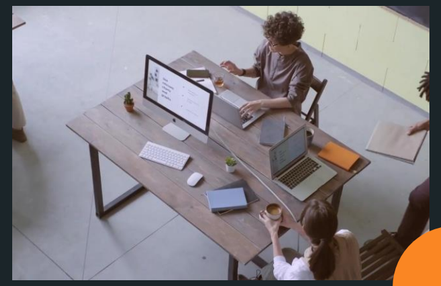
Established in January 2018, CyberSRC® Consultancy offers the full gambit of cybersecurity services ranging from threat intelligence to general advisory services in areas pertaining to cybersecurity such as vulnerability attacks, compliance, and cybersecurity regulations, and laws.

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.

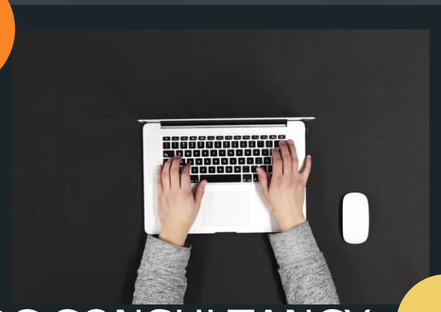
# Our Team

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*



# Services Offering

CYBERSRC SECURITY RISK COMPLIANCE
Simplifying Cyber Risk Management..

## 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

CYBERSRC SECURITY RISK COMPLIANCE
Simplifying Cyber Risk Management..

## 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.