CYBERSRC
SECURITY RISK COMPLIANCE
Simplifying Cyber Risk Management..

Simplifying Cyber Risk Management

Information & Cyber Security Implementation, Consultation & Audit Service Provider for Urban Co-operative Bank (UCB)

As per RBI's IS Guideline, Cyber Security Framework and Technology Vision 2020-2023

CYBERSRC CONSULTANCY

Setting the Context

In a race to adopt technology innovations, banks have increasedtheir exposure to cyber incidents/ attacks thereby underlining the urgent need to put in place a robust cybersecurity and resilience framework.

The Reserve Bank of India has providedguidelines on Cyber Security Frameworkvide circular DBS, CO/CSITE/BC.11/33.01.001/2015-16 dated June 2, 2016, where it has highlighted the urgent need to put in place a robust cybersecurity/ resilience framework to ensureadequate cybersecurity preparedness among banks on a continuous basis.

The RBI guidelines related to Cyber Security framework will enable banks to formalizeand adopt cybersecurity policy and cybercrisis management plan. The requirement to share information on cyber security incidents with RBI will also help structure proactive threat identification and mitigation.

Financial service companies are most vulnerable to cyber-attacks:

- The financial services industry topped the list of 26 different industries that cybercriminals most targeted.
- Financial services that remain the industry most susceptible to malicious email traffickers, as consumers are seven times more likely to be victims of an attack originating from a spoofed email with a bank brand versus one from any other industry.

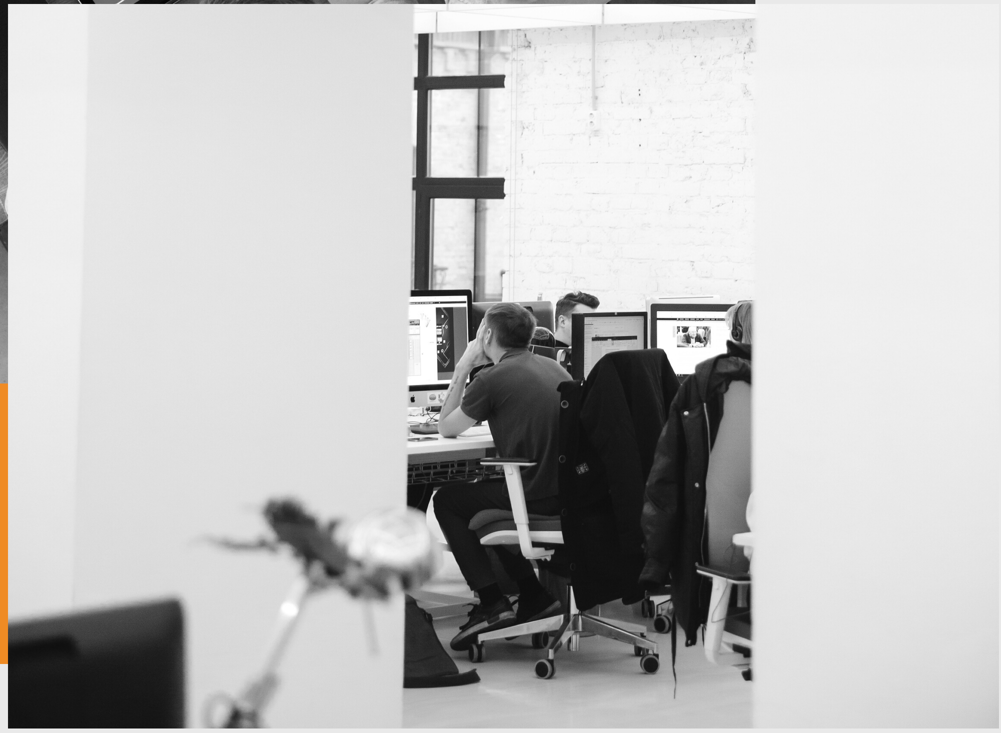
CYBERSRC CONSULTANCY →

RBI Guidelines

The Reserve Bank of India issued new guidelines in April 2011 for banks to mitigate risks of the use of information technology in banking operations. RBI guidelines are the result of Working Group recommendations on information security, electronic banking, technology risk management, and cyber fraud.
The Working Group was formed under the chairmanship of G. Gopalakrishna, the executive director of RBI in April 2020.

The guidelines highlight the following issues:

- IT Governance
- Information security
- IT operations
- IT Services Outsourcing
- Information SecurityAudit Cyber Fraud
- Business Continuity Planning
- Customer Education
- Legal issues



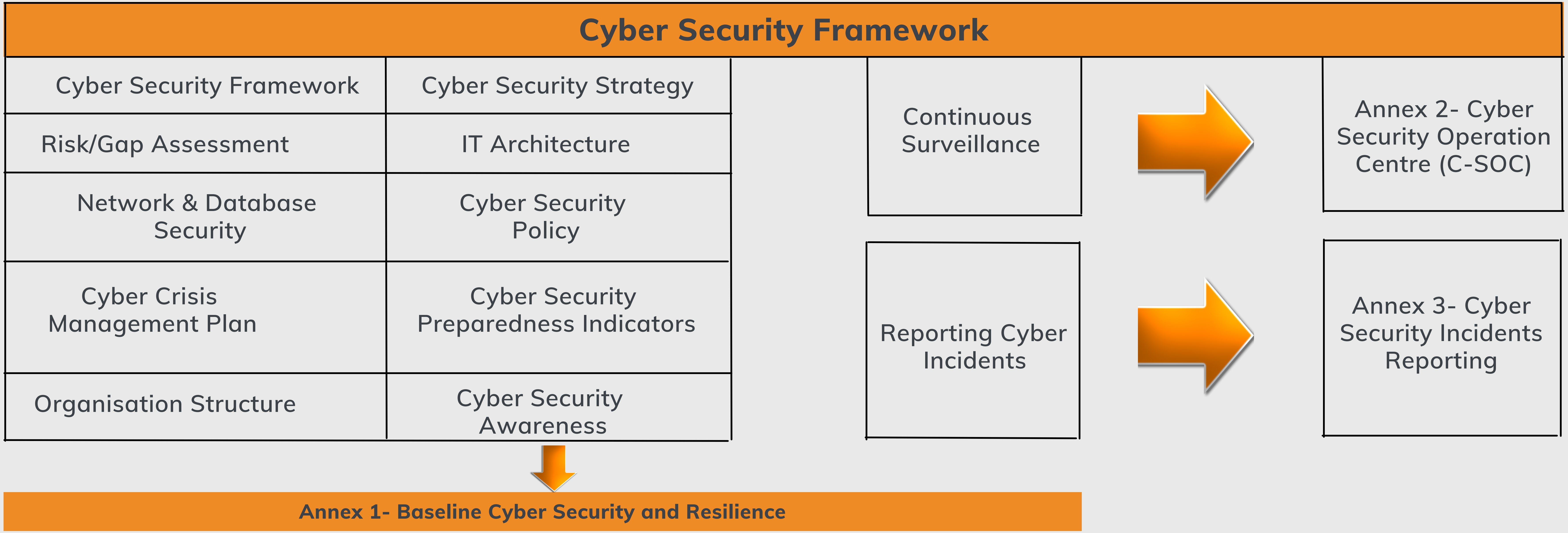
CYBERSRC CONSULTANCY

STRUCTURE OF RBI

Guidelines on Cyber Security Framework

RBI Guidelines on Cyber Security Framework focuses on the following three areas:

- Cyber Security and Resilience
- Cyber Security Operations Centre (C-SOC)
- Cyber Security Incident Reporting (CSIR)



Cyber Security Framework

Cyber Security Framework	Cyber Security Strategy
Risk/Gap Assessment	IT Architecture
Network & Database Security	Cyber Security Policy
Cyber Crisis Management Plan	Cyber Security Preparedness Indicators
Organisation Structure	Cyber Security Awareness

Continuous Surveillance → Annex 2- Cyber Security Operation Centre (C-SOC)

Reporting Cyber Incidents → Annex 3- Cyber Security Incidents Reporting

Annex 1- Baseline Cyber Security and Resilience

DETAILED REQUIREMENTS OF CYBER SECURITY

The detailed requirements for each of the Annexures of Cyber Security Framework is as follows:

Annex 1 –Baseline Cyber Security and Resilience Requirements				
Inventory Management of Business IT Assets	Preventing execution of unauthorized software	Environmental Controls	Network Management and Security	Secure Configuration
Application Security Life Cycle (ASLC)	Patch/Vulnerability & Change Management	User Access Control / Management	Authentication Framework for Customers	Secure mail and messaging systems
Vendor Risk Management	Removable Media	Advanced Real-time Threat Defence and Management	Anti-Phishing	Data Leak prevention strategy
Maintenance, Monitoring, and Analysis of Audit Logs	Audit Log settings	Threat Defence and Management Vulnerability Assessment and Penetration Test and Red Team Exercises	Incident Response & Management	Risk-based transaction monitoring
Metrics	Forensics	User / Employee/ Management Awareness	Customer Education and Awareness	

DETAILED REQUIREMENTS OF CYBER SECURITY

The detailed requirements for each of the Annexures of Cyber Security Framework is as follows:

Annex 2 –Cyber Security Operation Centre (C-SOC)		
C-SOC Functional Requirements	Governance Requirements	Integration Requirements
People Requirements	Process Requirements	Technology Requirements

Annex 3 –Cyber Security IncidentReporting (CSIR)	
Template for reporting Cyber Incidents	Cyber Security Incident Reporting (CSIR) Form

TECHNOLOGY VISION FOR UCBs 2020-2023

The Reserve Bank of India published the “Technology Vision for Cyber Security” for Urban Co-operative Banks (UCBs) 2020-2023.”

The Technology Vision Document aims at enhancing the cyber security posture of the Urban Co-operative banking sector against evolving IT and cyber threat environment. The Technology Vision Document aims at enhancing the cyber security posture of the Urban Co-operative banking sector against evolving IT and cyber threat environment.

The Technology Vision Document for cyber security for UCBs has been formalized based on inputs from various stakeholders. It envisages achieving its objective through a five-pillared strategic approach GUARD, viz., - Governance Oversight, Utile Technology Investment, Appropriate Regulation and Supervision, Robust Collaboration and Developing Necessary IT, Cyber Security skills set.

With concerted efforts and involvement of all stakeholders, the Technology Vision Document for Cyber Security for UCBs, with 12 specific actions points, aspires to:

- Involve more Board oversight over Cyber security;
- Enable UCBs to better manage and secure their IT Assets;
- Implement an offsite supervisory mechanism framework for UCBs on cybersecurity-related controls;
- Develop a forum for UCBs so that they can share best practices and discuss practical issues and challenges; and
- Implement a framework for providing awareness/ training for all the UCBs. For UCB, we understand the “Vision for Cyber Security” for UCBs- 2023.

TECHNOLOGY VISION FOR UCBs 2020-2023

we can help you in the journey of enhancing the cyber security posture of your institution (Bank) against evolving IT and cyber threat environment through a five-pillared strategic approachGUARD:

Government Oversight
Utile Technology Investment,
Appropriate Regulation and Supervision,
Robust Collaboration and
Developing Necessary IT, Cyber Security skills set

OUR CUSTOMISED UCB IS; *CYBER SECURITY SOLUTIONS*

Level	Criteria	Our Services
Level I	All UCBs	• Information Security (IS) Guidelines • Basic Cyber Security and Resilience Requirements • Baselines Cyber Security and resilience requirements- Level I • Vendor/ Outsourcing Risk Management • Assessment of Cyber Security controls • Honeypot as a Service • Network Management and security • Secure Configuration • Application Security Life Cycle (ASLC) • Change Management • Periodic Testing • User Access Control/ Management • Authentication Framework for customers • Phishing Simulation (SRC- PHaaS™) • Data Leak Prevention Strategy • Audit Logs & Incident Response Management • Assessment of Cyber Security controls • Network Management and Security • Advances Real-time Threat • Defense and Management • Risk-Based transaction monitoring • Assessment of Cyber Security controls
Level II	All UCBs, which are sub-members of Centralized Payment Systems (CPS) and satisfy at least one of the criteria given below: • offers internet banking facility to its customers (either view or transaction-based) • provides Mobile Banking facility through the application (Smartphone usage) • is a direct member of CTS/IMPS/ UPI.	
Level III	UCBs have at least one of the criteria given below: • direct members of CPS • having their own ATM • switch having SWIFT interface	
Level IV	UCBs which are members/ sub-members of CPS and satisfy at least one of the criteria given below: • having their own ATM Switch and having SWIFT interface • hosting data center or providing software support to other banks on their own or throughtheir wholly owned subsidiaries	• Arrangement for continuous surveillance- Setting up of cyber security operation Centre (C-SOC) • Participation in Cyber Drills • Forensic and Metrics • IT Strategy and Policy • IT and IS Governance Framework • Chief Information Security Officer (CISO) • Assessment of Cyber Security controls • External threat intelligence (SRC- TI™)

Our other standard BFSI offerings:

CYBERSRC SECURITY RISK COMPLIANCE
Simplifying Cyber Risk Management..

- Information System Audit
- Remediation of previous audit findings (Compliance)
- Review and preparation of IS and Cybersecurity policies.
- Vulnerability Assessment and Penetration Testing (VA/PT)
- SOC as a service.
- Business continuity
- Cyber Attack drills
- Embedded System Security Audit
- Cyber Intelligence
- Code Review and Audit
- Security Training and Staff Skill Building
- Data protection and Privacy assessments
- Virtual CISO and DPO
- ISO Certification and surveillance audit

How can CyberSRC help?

Though banks acknowledge the magnitude of the problem that cyber risks pose, this imperative is not always adequately recognized or accounted for across the enterprise.

A deeper analysis of the successes and failures of cybersecurity programs shows that banks need to develop a more comprehensive approach to cyber risk management as also suggested by RBI in their guidelines for Cyber SecurityFramework:

1 Cyber risk Strategy to be driven at the executive level as an integral part of the core company strategy

2 A dedicated cyber security management team to be established for a dynamic, intelligence-driven approach to security

3 A focused effort to be placed on automation and analytics to create internal and external risk transparency

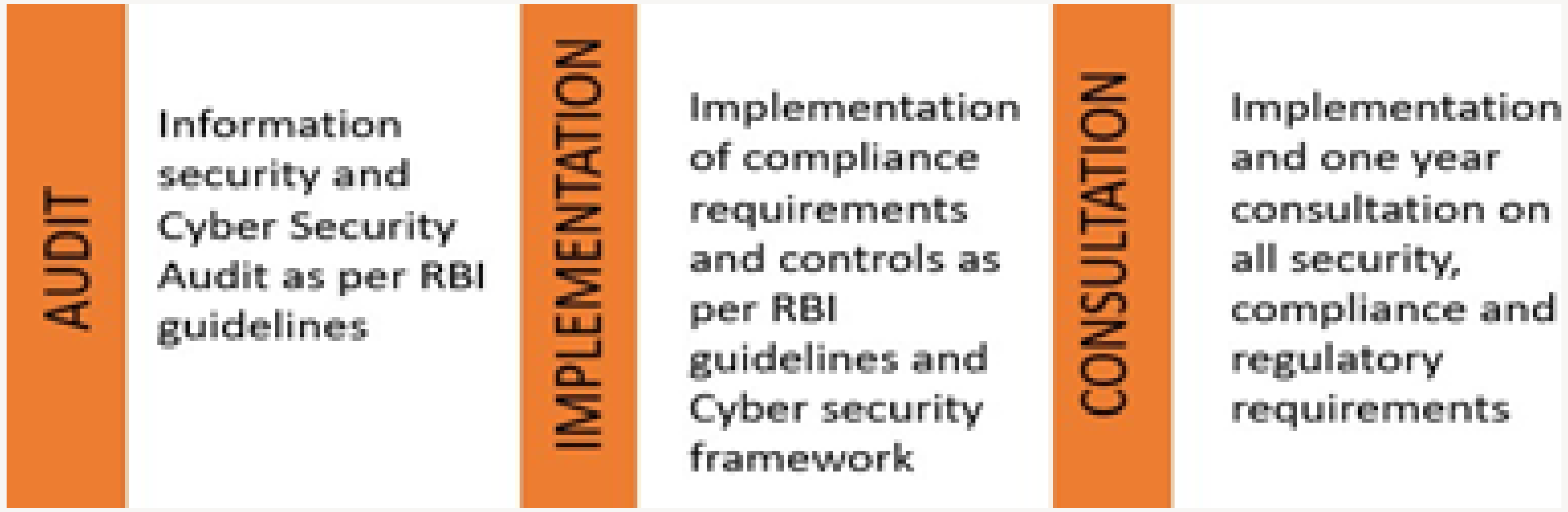
4 The "people" link in the defence chain can be strengthened as part of a cyber risk-aware culture

5 Cyber Security collaboration to be extended beyond walls to address common enemies

CYBERSRC CONSULTANCY →

MODES OF SERVICE

We provide three modes for Information and Cyber Security Services for UCBs:



AUDIT

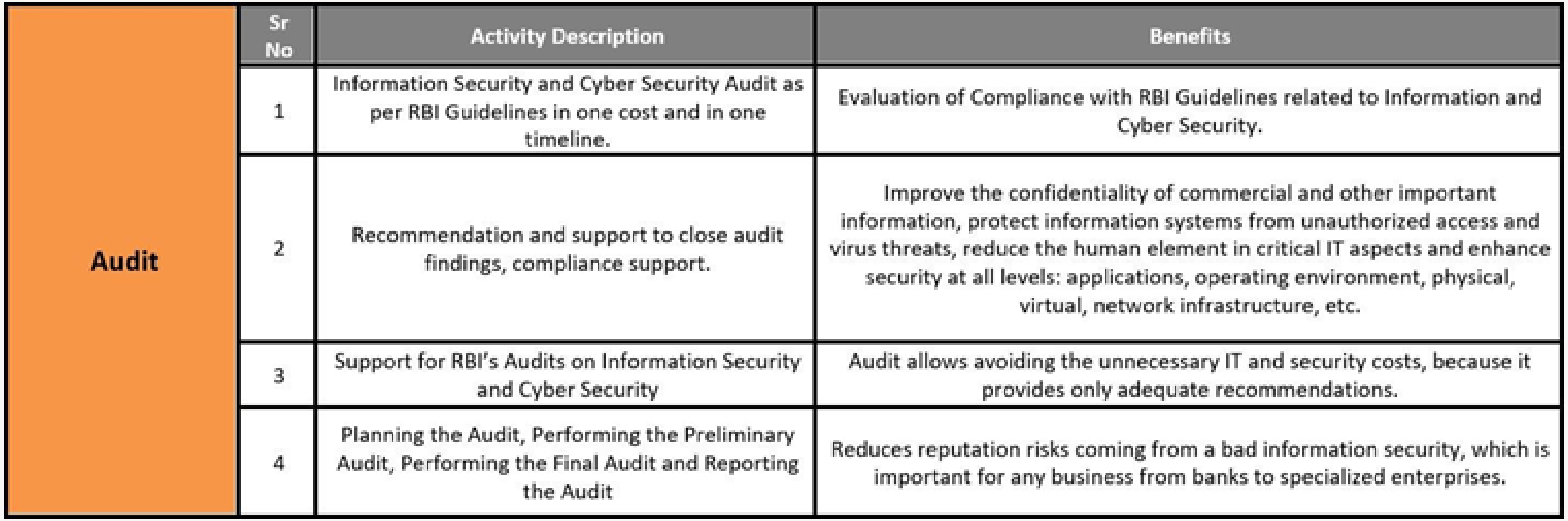
Information security and Cyber Security Audit as per RBI guidelines

IMPLEMENTATION

Implementation of compliance requirements and controls as per RBI guidelines and Cyber security framework

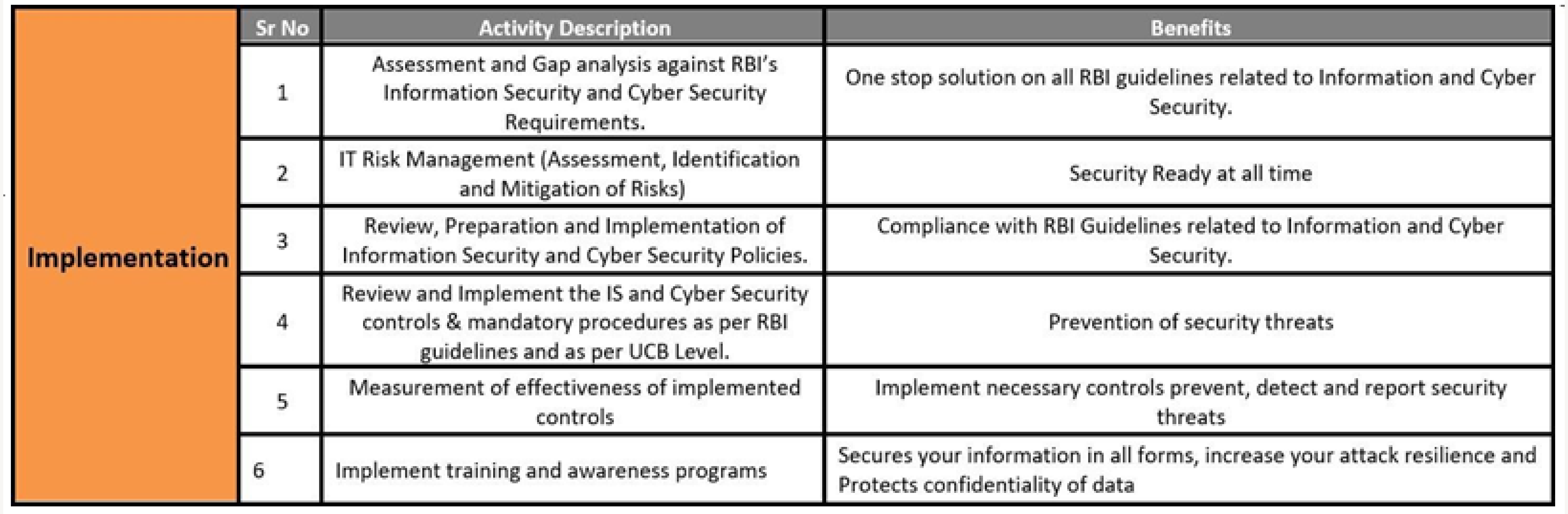
CONSULTATION

Implementation and one year consultation on all security, compliance and regulatory requirements



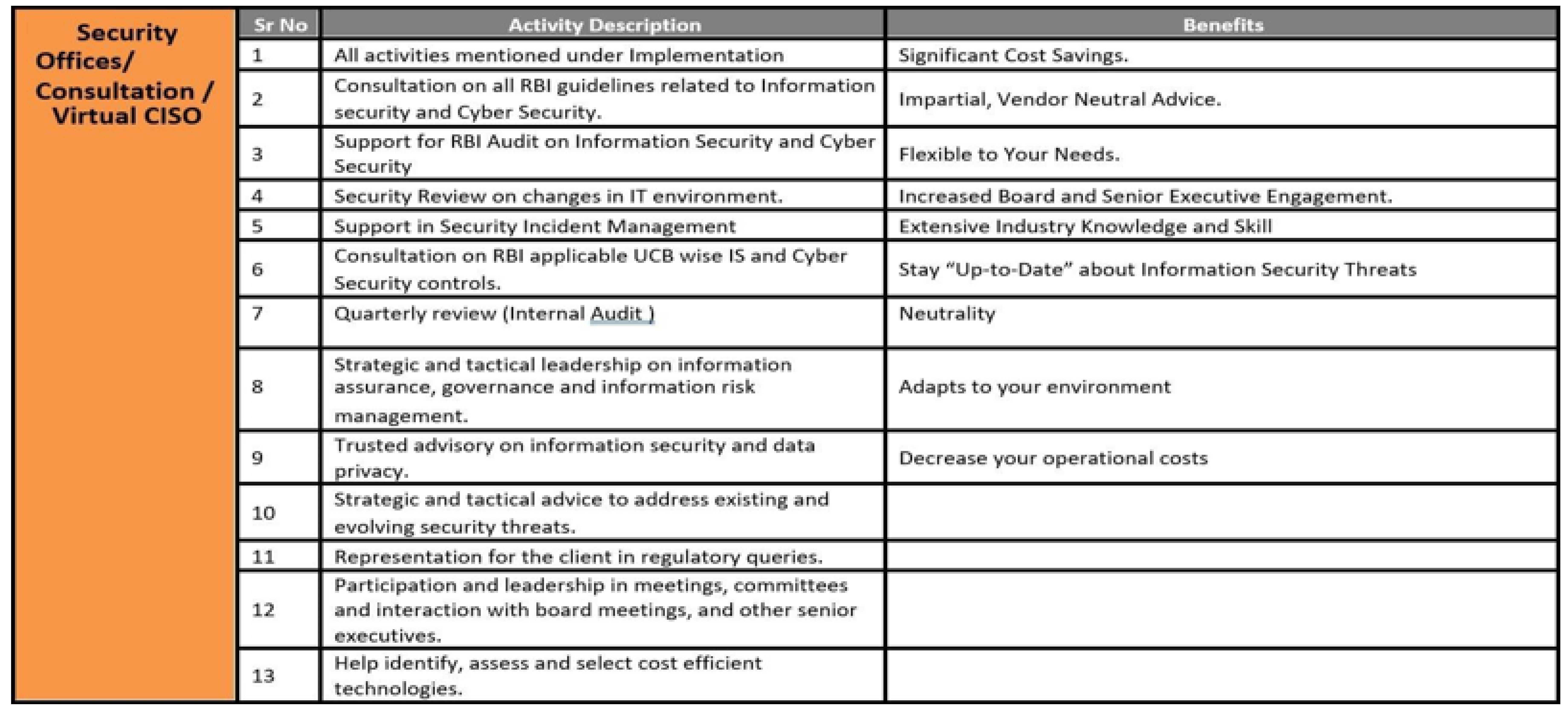
	Sr No	Activity Description	Benefits
Audit	1	Information Security and Cyber Security Audit as per RBI Guidelines in one cost and in one timeline.	Evaluation of Compliance with RBI Guidelines related to Information and Cyber Security.
	2	Recommendation and support to close audit findings, compliance support.	Improve the confidentiality of commercial and other important information, protect information systems from unauthorized access and virus threats, reduce the human element in critical IT aspects and enhance security at all levels: applications, operating environment, physical, virtual, network infrastructure, etc.
	3	Support for RBI's Audits on Information Security and Cyber Security	Audit allows avoiding the unnecessary IT and security costs, because it provides only adequate recommendations.
	4	Planning the Audit, Performing the Preliminary Audit, Performing the Final Audit and Reporting the Audit	Reduces reputation risks coming from a bad information security, which is important for any business from banks to specialized enterprises.

MODES OF SERVICE



	Sr No	Activity Description	Benefits
Implementation	1	Assessment and Gap analysis against RBI's Information Security and Cyber Security Requirements.	One stop solution on all RBI guidelines related to Information and Cyber Security.
	2	IT Risk Management (Assessment, Identification and Mitigation of Risks)	Security Ready at all time
	3	Review, Preparation and Implementation of Information Security and Cyber Security Policies.	Compliance with RBI Guidelines related to Information and Cyber Security.
	4	Review and Implement the IS and Cyber Security controls & mandatory procedures as per RBI guidelines and as per UCB Level.	Prevention of security threats
	5	Measurement of effectiveness of implemented controls	Implement necessary controls prevent, detect and report security threats
	6	Implement training and awareness programs	Secures your information in all forms, increase your attack resilience and Protects confidentiality of data

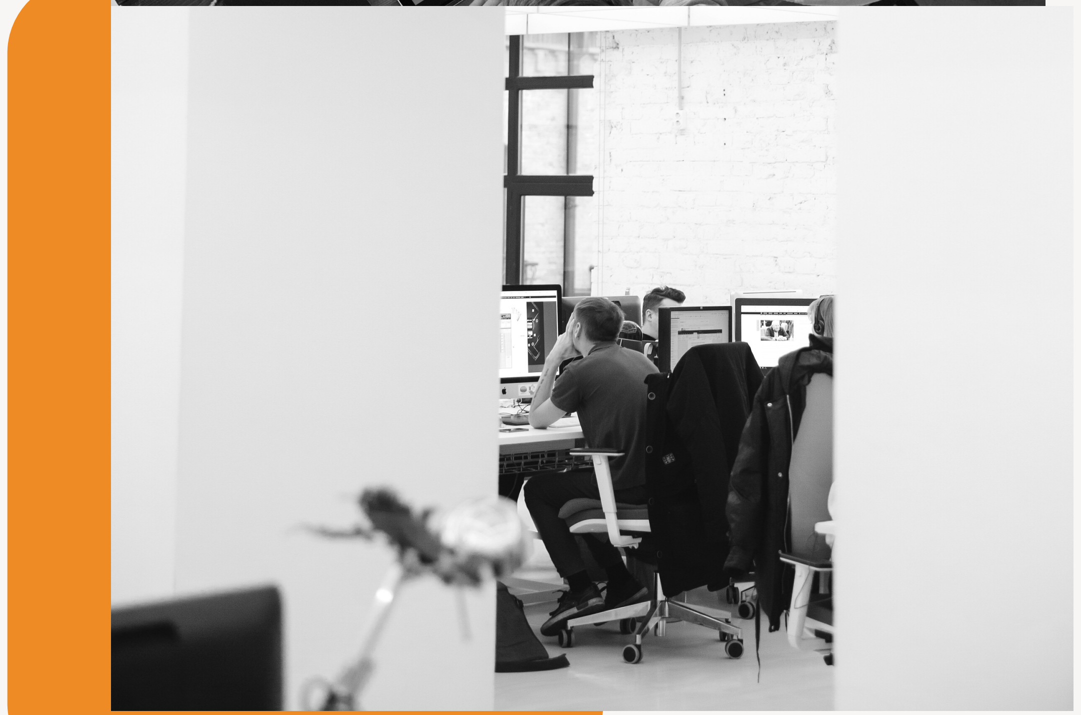
MODES OF SERVICE



	Sr No	Activity Description	Benefits
Security Offices/ Consultation / Virtual CISO	1	All activities mentioned under Implementation	Significant Cost Savings.
	2	Consultation on all RBI guidelines related to Information security and Cyber Security.	Impartial, Vendor Neutral Advice.
	3	Support for RBI Audit on Information Security and Cyber Security	Flexible to Your Needs.
	4	Security Review on changes in IT environment.	Increased Board and Senior Executive Engagement.
	5	Support in Security Incident Management	Extensive Industry Knowledge and Skill
	6	Consultation on RBI applicable UCB wise IS and Cyber Security controls.	Stay "Up-to-Date" about Information Security Threats
	7	Quarterly review (Internal Audit)	Neutrality
	8	Strategic and tactical leadership on information assurance, governance and information risk management.	Adapts to your environment
	9	Trusted advisory on information security and data privacy.	Decrease your operational costs
	10	Strategic and tactical advice to address existing and evolving security threats.	
	11	Representation for the client in regulatory queries.	
	12	Participation and leadership in meetings, committees and interaction with board meetings, and other senior executives.	
	13	Help identify, assess and select cost efficient technologies.	

INFORMATION AND CYBER SECURITY SERVICE PROVIDER

- Any company that sustains a presence in the digital world is in crucial need of modern cyber security, and CyberSRC® is here to assist. We come to you with professionals experienced in delivering the security services and latest technologies to protect against advanced security threats. Our Information and Cyber security specialists offer tailored solutions for clients nationwide.
- With our information cybersecurity consulting services, we discuss your business's requirements rather than simply
- Selling you a product or service. We believe that your required security should not interrupt your work.
- A temporary fix is not enough to withstand the ever-evolving threats in today's advancing world of technology. It takes a dedicated and knowledgeable team to stay on top of them. At CyberSRC, our experts are constantly researching and investigating new regulatory and security requirements and more to provide you with the best possible solution to a security threat.
- ·Cyber security solutions are not just for the largest enterprises, but for any organisation that possesses confidential and proprietary information. We provide cyber security solutions to customers throughout the world in the following industries: IT, Banking, Manufacturing, Energy/ Critical Infrastructure, Financial Services, Healthcare, Education, telecommunications, retail, and Government/ defence.
- ·A complete security overview available for your organisation. Review our portfolio of cyber security services or contact us today for more information.
-



The CyberSRC® Advantage

By partnering with CyberSRC®, you can leverage the following differentiators:

1. TECHNICAL ALLIANCE
2. DOMAIN EXPERIENCE
3. FOCUS ON INNOVATION
4. TECHNICAL EXPERTISE

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.

CYBERSRC CONSULTANCY →

CYBERSRC
SECURITY RISK COMPLIANCE
Simplifying Cyber Risk Management..

PARTNERING WITH A TOP CYBERSECURITY COMPANY

Cyber security companies are among the most important partner you'll work with, no matter how large or small your organisation is. As the universe of potential cyber threats continues to expand with greater speed, you need some form of cybersecurity servicesto protect every point of vulnerability within your organisation.

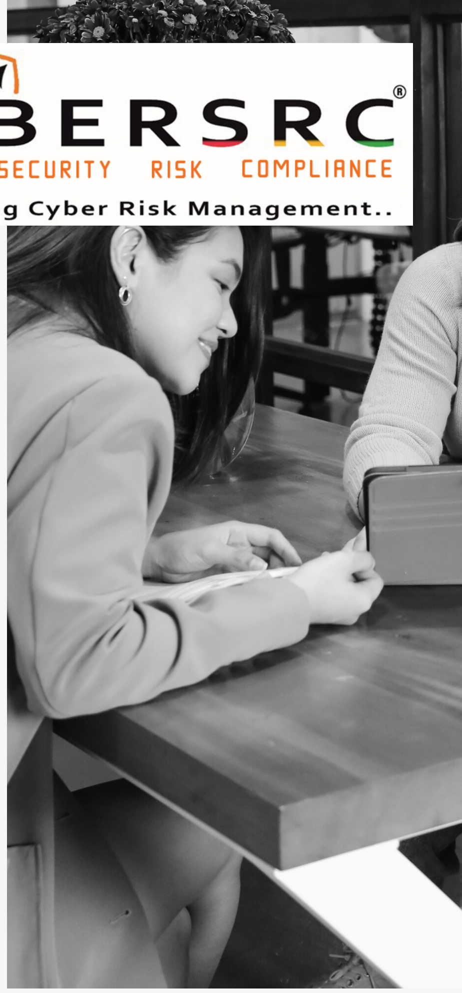
The world's top cybersecurity companies provide value and expertisein everything from security strategyand risk management to network penetration testing and securityarchitecture design.

But enterprise security management is a highly complicated tasks and partnering with and managing multiple cybersecurity companies only adds to the complexity. That's why, when evaluating cybersecurity companies and consulting firms for the most beneficial partnerrelationships, many of the leading business today turn to CyberSRC.

CYBERSRC CONSULTANCY →

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

WHAT WE DO?

Risk compliance advisory:

- IT Risk Management
- Data Privacy and Protection
- Sarbanes- Oxley Act (SOX) (ITGC, Application Controls)
- Compliance Management (HIPPA, PCI DSS, Hi- Trust and others)
- GRC Solution Consultancy (RSA Archer)
- Certification Consultancy

IT Strategy and Transformation

- IT Strategy Review and Alignment
- IT in merger and Acquisition
- governance Framework Strategy and Implementation
- Metrics and Dashboard (KPI/ KRI) Management
- Control Design and Effectiveness Review(COBIT 5, NIST 800-53, PCI DSS, ISO 27002)

Cyber Security

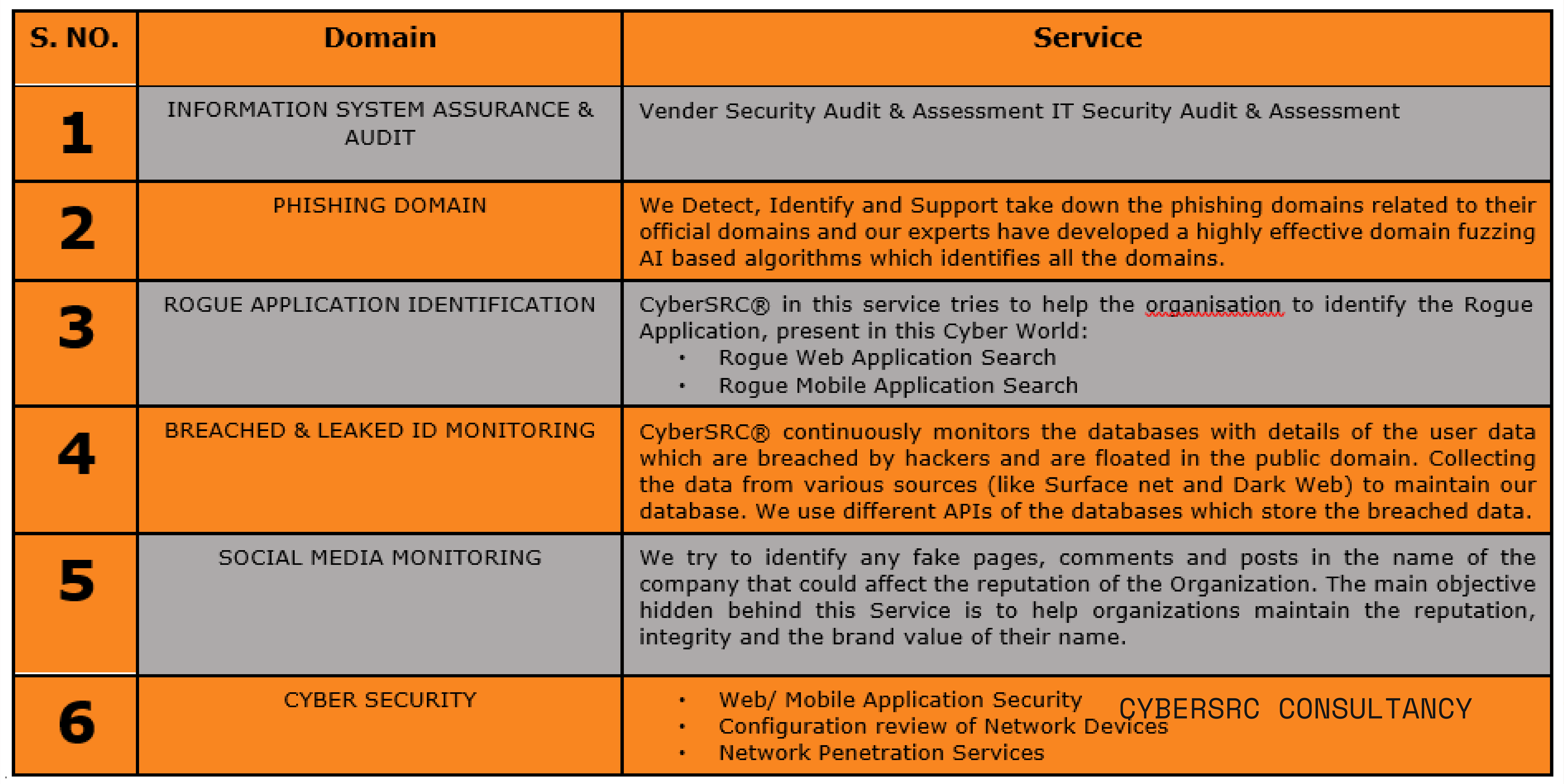
- VA/ PT (Application- IOS, Web. Android and IT infrastructure)
- Digital Security Assessment (IoT,AI/ML, BlockChain)
- IS Implementation Support

Information System and AssuranceAudit

- Information Security Audit (First and Second Party)
- IT Security Audit (First and Second Party)
- IT Security Audit and Assessment
- Network Security Testing
- Application Security Testing
- Infrastructure Security Testing
- System and Organisational control(SOC 1/2/3) reporting.
- Vendor Security Audit and assessment

CYBERSRC CONSULTANCY →

OTHER SERVICE DOMAIN



S. NO.	Domain	Service
1	INFORMATION SYSTEM ASSURANCE & AUDIT	Vender Security Audit & Assessment IT Security Audit & Assessment
2	PHISHING DOMAIN	We Detect, Identify and Support take down the phishing domains related to their official domains and our experts have developed a highly effective domain fuzzing AI based algorithms which identifies all the domains.
3	ROGUE APPLICATION IDENTIFICATION	CyberSRC® in this service tries to help the organisation to identify the Rogue Application, present in this Cyber World: • Rogue Web Application Search • Rogue Mobile Application Search
4	BREACHED & LEAKED ID MONITORING	CyberSRC® continuously monitors the databases with details of the user data which are breached by hackers and are floated in the public domain. Collecting the data from various sources (like Surface net and Dark Web) to maintain our database. We use different APIs of the databases which store the breached data.
5	SOCIAL MEDIA MONITORING	We try to identify any fake pages, comments and posts in the name of the company that could affect the reputation of the Organization. The main objective hidden behind this Service is to help organizations maintain the reputation, integrity and the brand value of their name.
6	CYBER SECURITY	• Web/ Mobile Application Security • Configuration review of Network Devices • Network Penetration Services

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

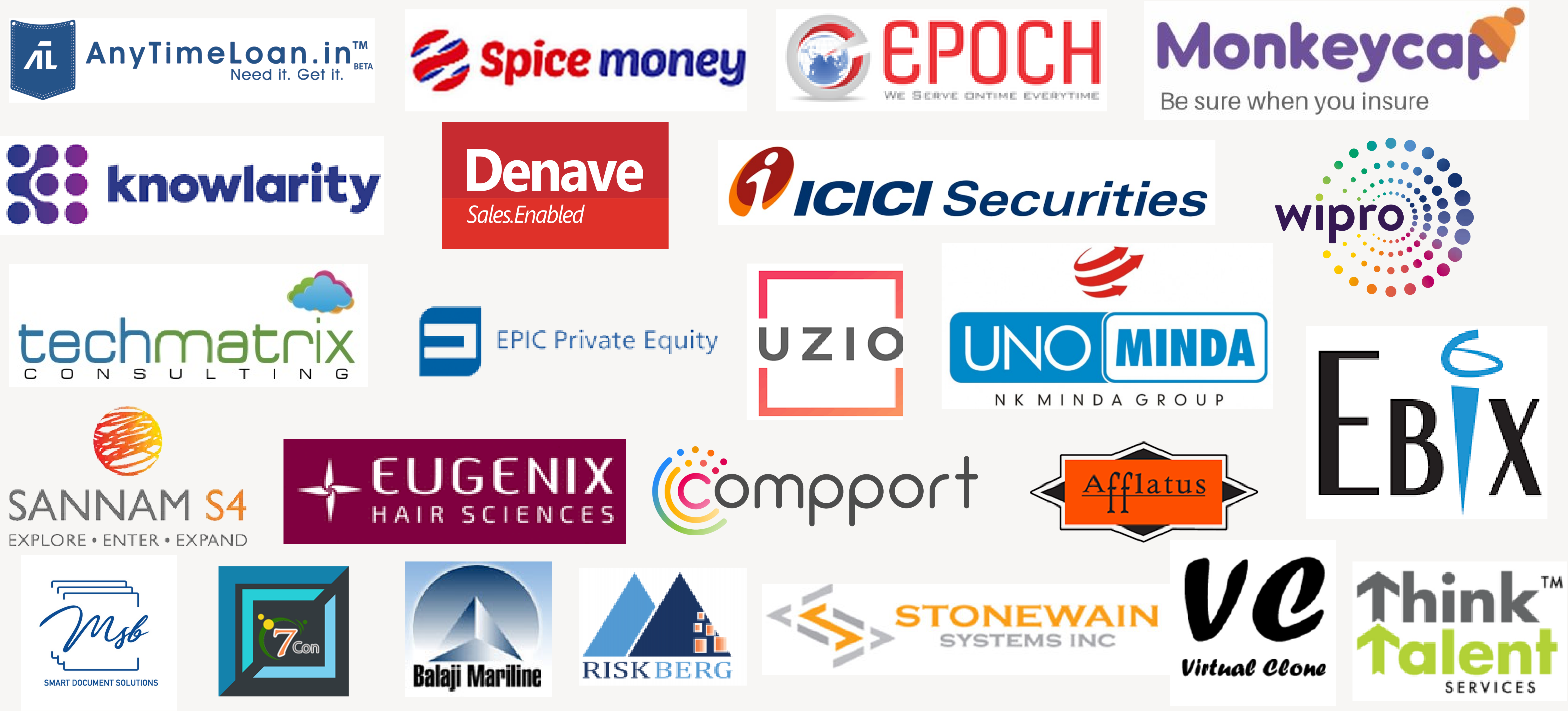
ISO IMPLEMENTATION & ADVISORY (ISO 27001, 9001, 27701)

Network & Cloud Security

CYBERSRC CONSULTANCY

CYBERSRC®
SECURITY RISK COMPLIANCE
Simplifying Cyber Risk Management..

Our Esteem Clients



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

CYBERSRC®
SECURITY RISK COMPLIANCE
Simplifying Cyber Risk Management..

Contact Us

WEBSITE

www.cybersrcc.com

EMAIL

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

CONTACT NUMBER

+91 8800377255

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)