CYBER SECURITY IN BANKING INDUSTRY

Our Perspective

BACKGROUND

Today customer expectations, technological capabilities, regulatory requirements, demographics and economics are together creating a crucial change. This leads to the need for banking institutions to get ahead of these challenges and adopt a proactive approach to security.

There is a noticeable shift in the banking industry in the way customers deal with their transactions. There is a rapid increase in the usage of digital channels such as internet banking, digital wallets, mobile banking, ATM. This leads to the increase in exposure and thereby cyber attacks which further may lead to financial and reputational losses. Banks may loose the customer confidence which can further increase the impact.

The key influencers which makes it imperative for the banks to invest in security are:

- Increase in financial data losses including card data, personal identifiable information etc.
- Unauthorized access to bank's network and systems

Key drivers for investment in Cyber Security:

- Secure sensitive customer information
- Fortify IT Processes and Systems
- Customer demands for convenience and payment security
- Adhere to regulatory requirements

OVERVIEW

With increasing risks of cyber threats, banks are facing an unprecedented challenge of data breaches and are therefore strengthening their cyber security postures. The following are the noticeable trends in banking industry from cyber security point of view:

- Financial sector faced almost three times the cyber attacks as compared to that of the other industries
- Data breaches (both internal through fraud and external through cyber criminals) leads to the exponential rise in costs
- It has been estimated that cost of implementing and managing the cyber security infrastructure will increase over 40% by 2025
- There is an increase in biometrics and tokenization as banks have begun to recognize that in addition to being a solution for payments these controls are also useful in security the sensitive data
- Customers are using biometrics for banking activities such as authentication for mobile banking, transaction at ATMs and payments
- With digital channels becoming the preference choice of customers for banking services, banks will also need to leverage advanced authentication and access control processes, without any compromise to customer experience

GLOBAL TRENDS

With the increase in the development of technologies the banking industry is evolving at an extraordinary rate. Unmanned aerial systems, the Internet of Things, Near Field of Communication (NFCs), and nearable devices are some of the technological advancements that banks will need to consider in the near future.

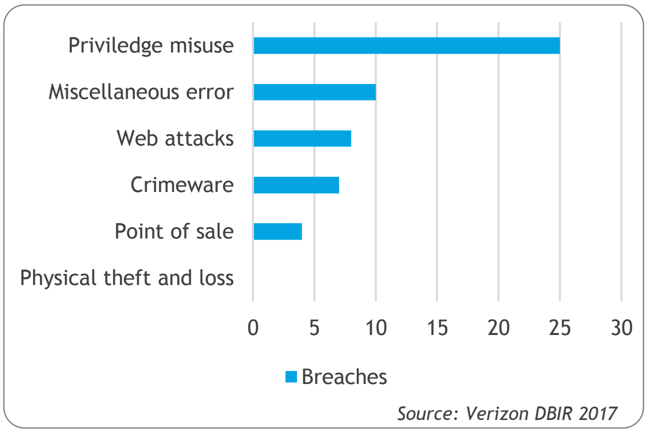
Few of the top upcoming priorities for banks could be cloud based platforms, robotic process automation and cognitive technologies. Automation will drive new efficiencies across the security lifecycle, but require the creation of control mechanisms and strong governance.

The above trends however pose their own set of challenges which are discussed in the next section.

CHALLENGES

The exponential growth of digital payments platform in India and the push towards a cashless economy has renewed focus on the need to strengthen cybersecurity posture. Few of the major challenges faced by banks include:

- **Strict compliance regulations**: Managing regulatory compliances has become enormously challenging for the banks. Over the past few years the volume of regulations has increased dramatically. Along with the larger banks, smaller ones too are required to fulfil the regulatory obligations
- **The struggle to secure customer data**: There are number of ways in which violation of privacy can take place in banking sector like stolen or loss card data, unauthorised sharing of data with third parties and loss of client's personal data due to improper security measures
- **Third party risk**: Banks need to conduct due diligence on third parties they are associated with. As per Payments card industry data security standard, third parties need to report any critical issues associated the card data environment to the bank .
- **Evolving cyber threat landscape**: The development in technologies is leading to the latest cyber threats like next generation ransomwares, web attacks etc.
- **Transaction frauds**: Fraud detection technologies should be in place with proper consideration of risks based on the business factors.
- **Secure SDLC**: Banks need to incorporate SDLC security for banking products and applications.



Source: Verizon DBIR 2017

REGULATORY PERSPECTIVE

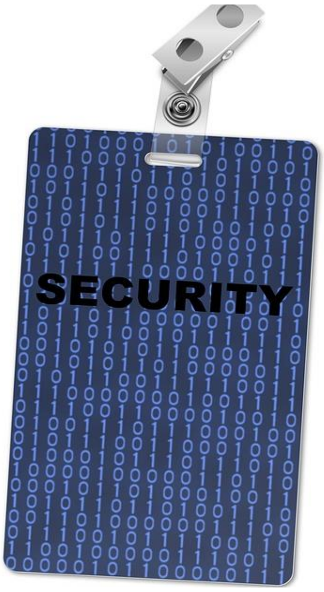
To ensure security in banking industries, the Reserve Bank of India removed a **Circular DBS.CO.ITC.BC.No.6/31.02.008/ 2010-11** dated **April 29 2011**, where all banking institutions have to comply for. Some of the key features of the regulations are:

- Cyber Security Policy to be distinct from the broader IT policy / IS Security Policy of a bank
- Arrangement for continuous surveillance
- Comprehensive network and database security
- Protection of customer information
- Cyber security preparedness indicators
- Cyber Crisis Management Plan
- IT architecture should be conducive to security
- An immediate assessment of gaps in preparedness to be reported to RBI
- Cyber security awareness among stakeholders/ Top Management/ Board

Source: www.rbi.org.in

SECURITY CONSIDERATIONS

While each bank thinks distinctively on adopting various considerations it is imperative to assume that the theme remains the same for various banking channels:



Internet Banking: Security controls like multi factor authentication, creation of strong passwords, adaptive authentication, image authentication, etc. can be considered.

Mobile Banking: It should be ensured that mobile applications are up to date and should be tested. Latest hardening standards could be implemented.

Wallet Transactions: Awareness material on Phishing, Malware attacks, vishing and social engineering, Password security etc. should be incorporated.

ATM Security: Biometrics like eye-retina, voice scan or fingerprint scan should be introduced by Banks.

UPI (Unified Payment Interface) : Banks and PSPs need to think through their security strategies, governance models and predictive controls to build a secure UPI environment that ensures a seamless user experience and at the same time balances security risks.

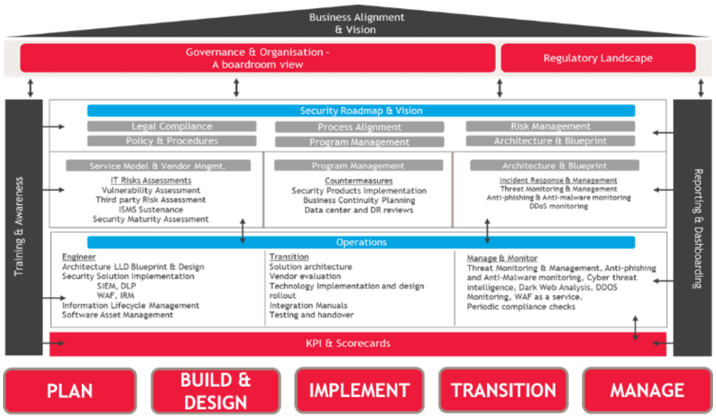
Banks must conduct regular drills, awareness programs and simulation exercises to keep their infrastructure secured.

APPROACH TO SECURITY

At BDO India, we endeavour to provide expertise driven solutions to help and assist our clients business needs are met, through a well defined risk based approach

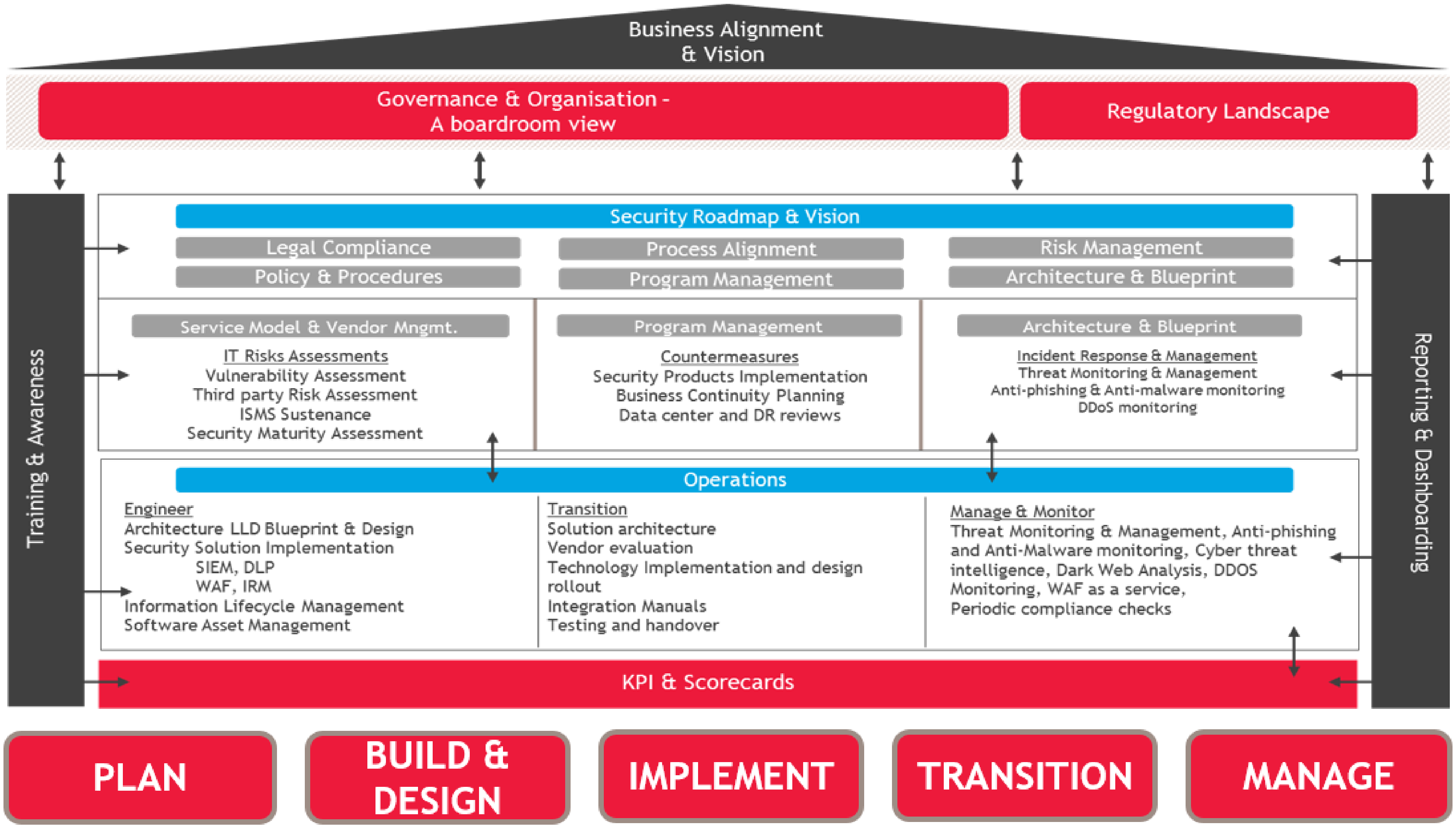
Approach to adoption can have the following phases:

- **Plan**: Discussing the scope of work, making a roadmap for the approach, formalising leadership & project SPOC and to understand the policy and procedures all can be a part of the planning phase.
- **Build & Design**: The build phase consists of requirements as a part of a systems engineering process. The main milestone of design phase would be matching the system specifications and the disposition of risk from the organisation as shown in the framework.
- **Implementation**: Gaps identified during the plan phase are implemented. Integration elements should be carefully planned.
- **Transition**: A seamless transition and handover to the operations team should be taken into consideration.
- **Manage**: This phase includes management, monitoring, and periodic reviews against security threats and frauds.


Business Alignment & Vision
Governance & Organisation - A boardroom view
Regulatory Landscape
Training & Awareness
Reporting & Dashboarding
Security Roadmap & Vision
Legal Compliance
Policy & Procedures
Process Alignment
Program Management
Risk Management
Architecture & Blueprint
Service Model & Vendor Mngmt.
IT Risks Assessments
Vulnerability Assessment
Third party Risk Assessment
ISMS Sustenance
Security Maturity Assessment
Program Management
Countermeasures
Security Products Implementation
Business Continuity Planning
Data center and DR reviews
Architecture & Blueprint
Incident Response & Management
Threat Monitoring & Management
Anti-phishing & Anti-malware monitoring
DDoS monitoring
Operations
Engineer
Architecture LLD Blueprint & Design
Security Solution Implementation
SIEM, DLP
WAF, IRM
Information Lifecycle Management
Software Asset Management
Transition
Solution architecture
Vendor evaluation
Technology Implementation and design rollout
Integration Manuals
Testing and handover
Manage & Monitor
Threat Monitoring & Management, Anti-phishing and Anti-Malware monitoring, Cyber threat intelligence, Dark Web Analysis, DDOS Monitoring, WAF as a service,
Periodic compliance checks
KPI & Scorecards
PLAN
BUILD & DESIGN
IMPLEMENT
TRANSITION
MANAGE

Detailed cyber security framework is shown on the next page

CYBERSECURITY FRAMEWORK



Business Alignment & Vision

Governance & Organisation - A boardroom view

Regulatory Landscape

Training & Awareness

Reporting & Dashboarding

Security Roadmap & Vision

Legal Compliance

Policy & Procedures

Process Alignment

Program Management

Risk Management

Architecture & Blueprint

Service Model & Vendor Mngmt.

IT Risks Assessments
Vulnerability Assessment
Third party Risk Assessment
ISMS Sustenance
Security Maturity Assessment

Program Management

Countermeasures
Security Products Implementation
Business Continuity Planning
Data center and DR reviews

Architecture & Blueprint

Incident Response & Management
Threat Monitoring & Management
Anti-phishing & Anti-malware monitoring
DDoS monitoring

Operations

Engineer
Architecture LLD Blueprint & Design
Security Solution Implementation
SIEM, DLP
WAF, IRM
Information Lifecycle Management
Software Asset Management

Transition
Solution architecture
Vendor evaluation
Technology Implementation and design rollout
Integration Manuals
Testing and handover

Manage & Monitor
Threat Monitoring & Management, Anti-phishing and Anti-Malware monitoring, Cyber threat intelligence, Dark Web Analysis, DDOS Monitoring, WAF as a service,
Periodic compliance checks

KPI & Scorecards

PLAN

BUILD & DESIGN

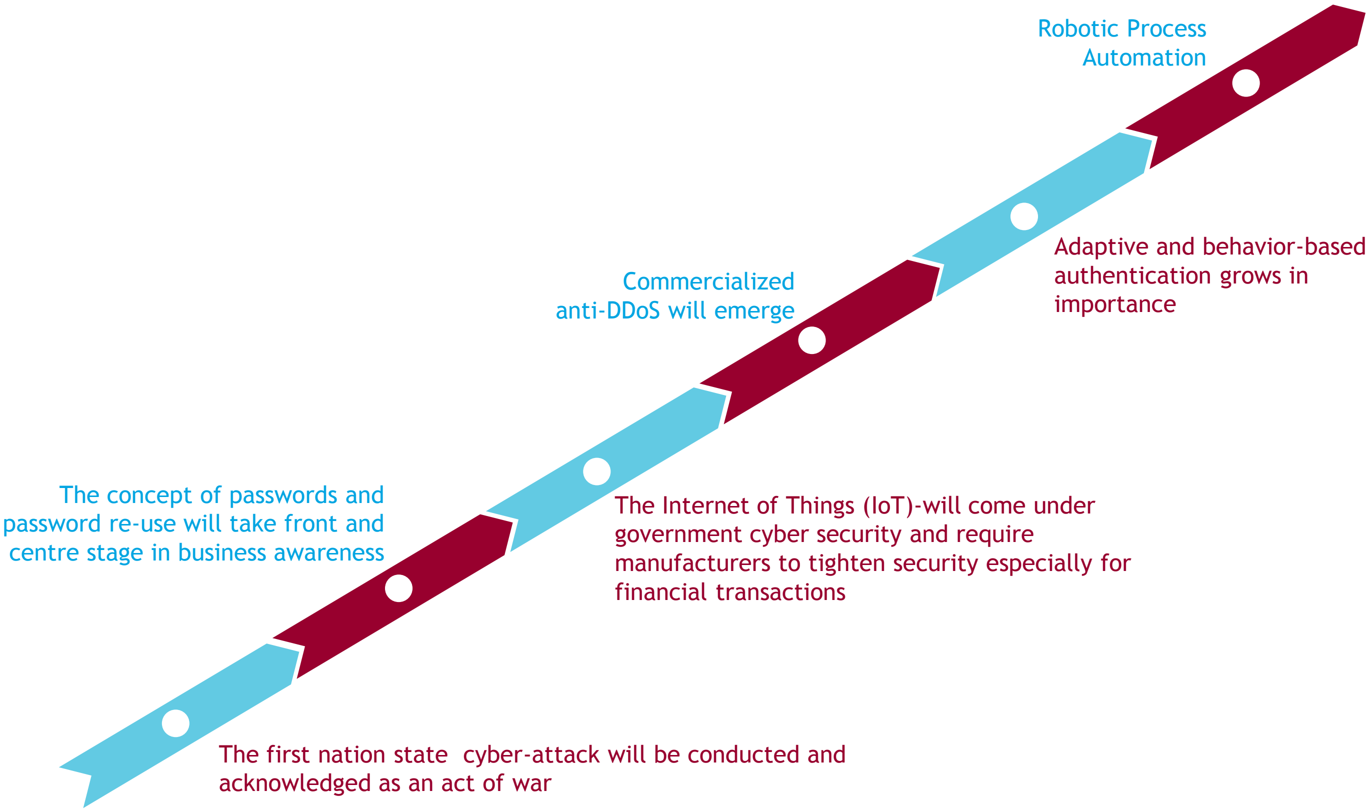
IMPLEMENT

TRANSITION

MANAGE

CYBER SECURITY TRENDS

- Blockchain is a technology that was initially developed for Bitcoin, the cryptocurrency. Blockchain could reduce banks infrastructure costs by US$ 15-20 billion per annum by 2022. Blockchain have the potential to transform how the business and the government work in vast variety of contexts.
- Banks will continue to leverage digital technologies to enhance customer experience.
- Ongoing threats related to IoT devices will force banks to tighten security layers, including patchable firmware/software, secured authentication, and controlled privilege access. Today, most IoT devices are considered throw away devices and security patches are not issued. But, new regulations will be driven by large scale attacks using IoT to amplify the attack.



The first nation state cyber-attack will be conducted and acknowledged as an act of war

The concept of passwords and password re-use will take front and centre stage in business awareness

The Internet of Things (IoT)-will come under government cyber security and require manufacturers to tighten security especially for financial transactions

Commercialized anti-DDoS will emerge

Adaptive and behavior-based authentication grows in importance

Robotic Process Automation

OUR TEAM AND EXPERIENCE

BDO India has a team of professionals with certification such as CISAs, CISSPs, Lead Auditors, OSCP and Certified Ethical Hackers. Our team has experience to conduct comprehensive technology and security assessments and conduct root cause analysis and investigation on similar attacks. BDO network has CERT and 24 x 7 security operations center with highly qualified professionals for threat and incident management.

References

Challenges faced in the banking industry: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
RBI regulatory requirements: www.rbi.org.in
Global trends in the banking industry: https://www.capgemini.com/resources/top-ten-trends-in-banking-2017
Cyber Security : https://www.beyondtrust.com/blog/ten-cyber-security-predictions-2017/
Global Trends : http://www.businessinsider.com/internet-of-things-banking-retail-mobile-trends-2016-9?IR=T

About US

The BDO Network

BDO is an international network of accounting, tax and advisory firms which perform professional services under the name of BDO. The local knowledge of network member firms combined with the international expertise and strength of the network ensures effective and efficient service delivery to clients in every country where BDO is represented.

1
Leading consolidation in the mid tier

155+
Over 1400 offices in more than 158 countries

67,700 +
Over 67,700 highly skilled partners and staff worldwide

US $7.60 bn
BDO posted global revenues of $7.6 billion in 2016

About BDO India

BDO India offers Strategic, Operational, Accounting and Tax & Regulatory advisory & assistance for both domestic and international organisations across a range of industries.

BDO India is led by more than 60 Partners & Directors with a team of over 750 professionals operating across strategic cities.

7
Key cities
60 Partners Directors
750 Staff
Delivering
exceptional client service
Direct Tax
Transaction
Indirect
Assurance
Advisory
Tax
Risk Advisory
Outsourcing

Our Services

Assurance

- Accounting Advisory
- Assurance services

Tax

- Cross Border Taxation
- Customs & International Trade
- Global Tax Services
- Goods & Services Tax (GST)
- Global Expatriate Services
- Information Exchange compliances
- Other Indirect Taxes
- Representation & Litigation Support
- Tax Advisory & Compliance
- Transaction Tax
- Transfer Pricing

Advisory

- Forensic Advisory Services
- **Risk Advisory Services**
- Transaction Advisory Services
- Business Restructuring

Business Services & Outsourcing

- Outsourcing
- Offshoring
- Revenue Cycle Management

Risk Advisory Service Portfolio

Risk Advisory team assures to be an objective source of independent findings on key aspects of operations, i.e. efficiency, effectiveness and integrity of information while ensuring compliance with regulations and protocols.

- Enterprise Risk Management
- ERP Advisory
- **IT Advisory**
- Performance Improvement Studies

IT Advisory Service Portfolio

India is going through a paradigm transformation with respect to a number of transformation themes. Our IT advisory specialists are committed to assist our clients in addressing their challenges. Largely our service capabilities are spread across three broad pillars:

- Cyber Security
- IT Assurance
- IT Performance Improvement

CONTACT US

MUMBAI

VINOD NAIR
Partner & Head
Mumbai
M: +91 98 6715 6520
E: vinodnair@bdo.in

AKSHAY GARKEL
Partner
Mumbai
M: +91 98 2020 8515
E: akshaygarkel@bdo.in

NEW DELHI-GURGAON

PRASHANT GUPTA
Partner
New Delhi-Gurgaon
M: +91 99 5888 2282
E: gprashant@bdo.in

AASHISH GUPTA
Partner
New Delhi-Gurgaon
M: +91 98 9191 4272
E: aashishgupta@bdo.in

HYDERABAD

PRASHANTH KINI
Partner
Hyderabad
M: + 91 80 0822 2879
E: prashanthkini@bdo.in

Bengaluru
Floor 6, No. 5, Prestige Khoday Tower
Raj Bhavan Road,
Bengaluru 560001, INDIA
Tel: +91 80 3041 0000

Chennai - Office 1
117/54, Floor 2, Citadel Building
Dr Radha Krishnan Salai, Mylapore
Chennai 600 004, INDIA
Tel: + 91 44 3001 0200

Chennai - Office 2
Floor 1, Tower C, Tek Meadows
No. 51, Sholinganallur
Chennai 600119, INDIA
Tel: +91 44 3001 0200

Hyderabad
Manbhum Jade Towers, II Floor
6-3-1090/A/12 & 13
Somajiguda, Hyderabad 500082, INDIA
Tel: +91 40 3024 2999

Kolkata
Floor 4, Duckback House
41, Shakespeare Sarani
Kolkata 700017, INDIA
Tel: +91 33 4600 3505

Mumbai - Office 1
The Ruby, Level 9, North West Wing
Senapati Bapat Marg, Dadar (W)
Mumbai - 400028, INDIA
Tel: +91 22 3332 1600

Mumbai - Office 2
Floor 2, Enterprise Centre
Nehru Road,
Near Domestic Airport, Vile Parle (E)
Mumbai - 400099, INDIA
Tel: +91 22 3358 9700

New Delhi - Gurgaon
The Palm Springs Plaza
Office No. 1501-08, Sector-54,
Golf Course Road,
Gurgaon-122001, INDIA
Tel: +91 124 281 9000

Pune
Floor 6, Building # 1
Cerebrum IT Park, Kalyani Nagar
Pune 411014, INDIA
Tel: +91 20 3006 4700

Note: The information contained herein has been carefully prepared, but it has been written in general terms and should be seen as broad guidance only. The information cannot be relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained therein without obtaining specific professional advice. Please contact BDO India LLP to discuss these matters in the context of your particular circumstances. BDO India LLP and each BDO member firm in India, their partners and/or directors, employees and agents do not accept or assume any liability or duty of care for any loss arising from any action taken or not taken by anyone in reliance on the information in this publication or for any decision based on it.

BDO India LLP, a limited liability partnership, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

BDO is the brand name for the international BDO network and for each of the BDO Member Firms.

Visit us at www.bdo.in