CYBER SECURITY PRACTICES AND DATA PRIVACY MEASURES

Strengthening Defences against Emerging Threats

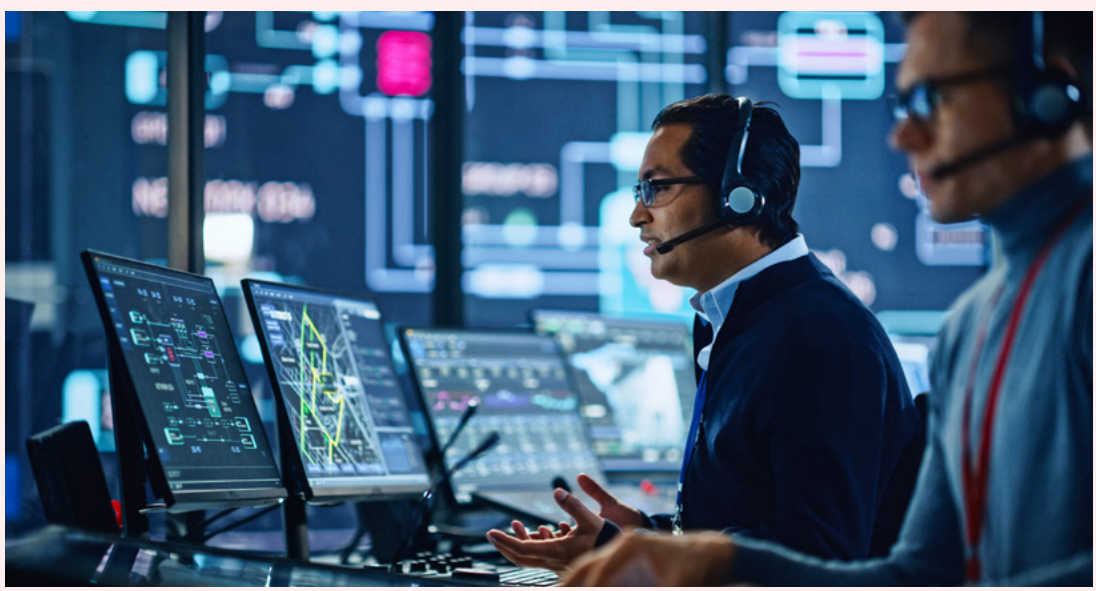
We prioritise cyber security and safeguard our customers against unauthorised access and cyber threats through robust security controls, including proactive detection and monitoring technologies. Apart from modernising our core technology stack for better performance and resilience, we are also developing new age digital platforms.

Capitals Impacted

IC

SDGs Impacted

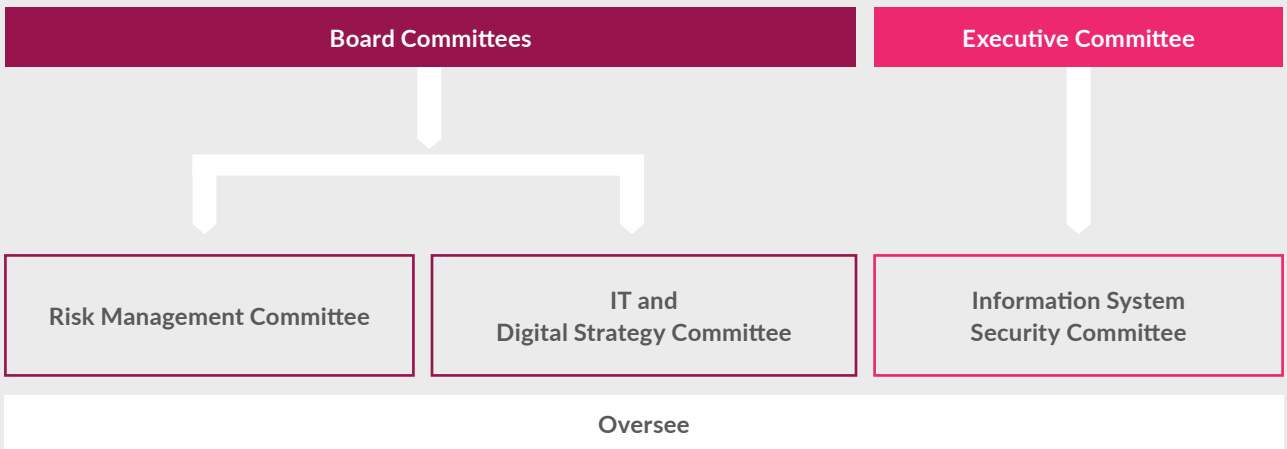
In an era of unprecedented digital transactions, cybersecurity governance and a protective architecture are essential for ensuring the safety of customer data and financial transactions. Compliant with ISO27001 and PCIDSS standards and holding a ISO27017 cloud security certification, the Bank demonstrates its commitment to stringent cybersecurity measures. To ensure adequate cyber security and customer data privacy, both of utmost importance to the Bank, we continue to deploy best-in-class technologies and resources, aligning with best practices and regulatory guidelines to reinforce customer trust across all banking channels.



Cyber Security Governance Framework

In accordance with our ***'open'*** philosophy, we have laid the groundwork for a banking franchise supported by strong corporate governance. At the executive level, our Information System Security Committee convenes quarterly to assess the threat landscape, and validate the controls implemented in the Bank to mitigate cyber risks.

Information and Cyber Security Governance Framework



Information and cyber security initiatives to assess the threat landscape and ensure that controls are commensurate with the cyber risks

The Bank has a comprehensive Information and Cyber Security Policy, and we have invested in robust technical and administrative controls to prevent, detect, and respond to suspicious activity.

We conduct pre-deployment assessments covering application security, vulnerability, penetration testing, and security architecture. Employing a defence-in-depth approach, we safeguard our critical assets and monitor digital assets 24x7 through our Security Operations Centre (SOC). Collaboration with regulatory bodies helps strengthen our cyber defence.

As part of the Bank's initiatives, we implement security best practices across digital channels such as Internet Banking, Mobile Banking, and Credit Cards, enforcing specific payment security controls such as multifactor authentication and real-time fraud monitoring. Additionally, we prioritise vendor risk management and security awareness initiatives for outsourced employees.

We deploy cyber security controls to protect our information assets from unauthorised access, hacking attempts, and data loss. Various detection and monitoring technologies enable proactive detection and response to cyber threats.

Measures for Proactive Detection of Cyber Threats

- Remote access users benefit from added security with multifactor authentication
- Robust enterprise security governance framework, ensuring compliance and monitoring across various security aspects
- Privacy by design is prioritised with Reference Architectures and SOPs covering encryption, digital rights management, and data classification
- Advanced endpoint controls and Data Leakage Prevention (DLP) safeguard against cyber-attacks
- Email protection shields against phishing attempts, particularly prevalent during the pandemic
- Continuous security monitoring and threat intelligence detect and prevent malicious activities
- Enhanced monitoring for remote users detects unauthorised access and data leaks
- Mobility security capabilities support remote work and sustainability goals
- Access controls like federated identity and network access management ensure secure data access
- The 24x7 Security Operations Center (SOC) collaborates with regulatory bodies to strengthen cyber defence
- Secure-by-design practices, including DevSecOps and application security testing, ensure the security of IT applications
- On premises infrastructure tools enforce security measures like patch management and file integrity monitoring
- Robust network security measures, including WAF and DDOS protection, fortify against cyber threats
- Cloud security measures, including encryption and compliance controls, support the Bank's cloud-first goals
- SaaS and PaaS providers undergo rigorous vetting for regulatory compliance and security standards

In today's dynamic landscape, apart from cyber security controls, future-proofing our operations through core modernisation and upgrading is also essential. This not only enhances customer satisfaction and mitigates risks but also gives us a competitive edge. At Axis Bank, we adopt a twin-engine approach, modernising our core technology stack for scalability, performance, and resilience, while simultaneously developing new-age digital platforms. We maintain agility in our core stack by regularly refreshing core applications and upgrading to the latest software. Here are some key modernisation efforts and core upgrades undertaken during the year:

Core Modernisation

In fiscal 2024, some of our core modernisation efforts were in the following areas:

- **Finacle UPI:** Transitioned elite merchant payments to a cloud-ready UPI instance
- **Financial Inclusion:** Independent entity for special focus on financial inclusion
- **Digital Transaction:** Hiving-off payment channels to a distributed network
- **Account Opening:** Fully digital account opening journey and servicing

Core Upgrades

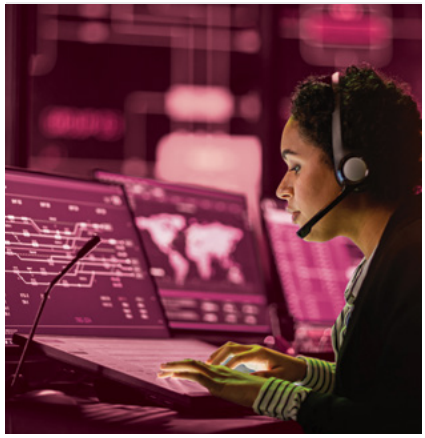
Some of the key platform upgrades completed in fiscal 2024 include Turret, Oracle EBS, and Avaya upgrade.

Additionally, the Bank has migrated from Enterprise Payments Hub (EPH) to Global Payment System (GPS); it has helped us achieve leadership in the NEFT Outward domain and improve market share.

Enterprise Architecture

The Bank is committed to enhancing its internal technology, design, and AI capabilities through a structured governance framework. As a testament to this commitment, in fiscal 2023, Axis Bank joined the Banking Industry Architecture Network (BIAN), an ecosystem comprising banks and technology providers, aimed at transforming its architecture to better serve future customers. Continuing into fiscal 2025, this initiative remains pertinent as it aligns with our vision of providing innovative and customer-centric services.

We are actively optimising our IT portfolio and guiding architectural decisions through our Enterprise Architecture practice. This practice ensures that our technology initiatives are aligned with our business objectives, thereby aiding the Bank in navigating challenges and fostering innovation efficiently.



Steps to Strengthen Enterprise Architecture in Fiscal 2024

1. Established an approved **Enterprise Data Privacy Reference Architecture** to ensure Bank's readiness towards customer privacy and data security. This is in addition to the various data at rest and data in motion encryption reference architectures.
2. Implemented an approved **API Security Guard Rails Policy** where there is differentiated treatment of public, private, and enterprise APIs with focus on cyber and data security.
3. Created Reference Architecture for **Domain Data Mesh and Data Lake House Reference Architecture** to improve data availability, faster time to market of data products, and to move towards real-time insights for use cases such as personalisation, leads, fraud detection, and mitigation. We are also working closely on projects like **NEO and SPARSH** to build the Bank's first Data Lake House to generate quick insights.
4. Pioneered the **GenAI** proof of concepts in the Bank and evangelised it through various groups, including Information security to promote adoption of GenAI services.
5. Established an **Open-Source Governance Office** to improve adoption of OSS while ensuring ongoing risk assessments of OSS frameworks, libraries, and tools.

Integrating GenAI into the Business

The Bank has embarked on integrating GenAI capabilities into its routine operations, including conversational interface, content summarisation, data analytics and visualisation, multi-modal content generation, and knowledge retrieval, among others. Notably, the Bank is among the first in the country to implement Microsoft GenAI Co-pilot. The Bank is also actively enhancing its proficiency in AI, ML, automation and data analytics, primarily targeting top-tier efficiency across robotic process automation (RPA), voice, and intelligent optical character recognition (iOCR) in retail banking operations. Throughout the year, we have consistently introduced new products, guided by our zero-based redesign approach, which has resulted in customer-centric journeys that minimise or eliminate manual data entry through automated underwriting processes.

Leadership under Cloud Architecture

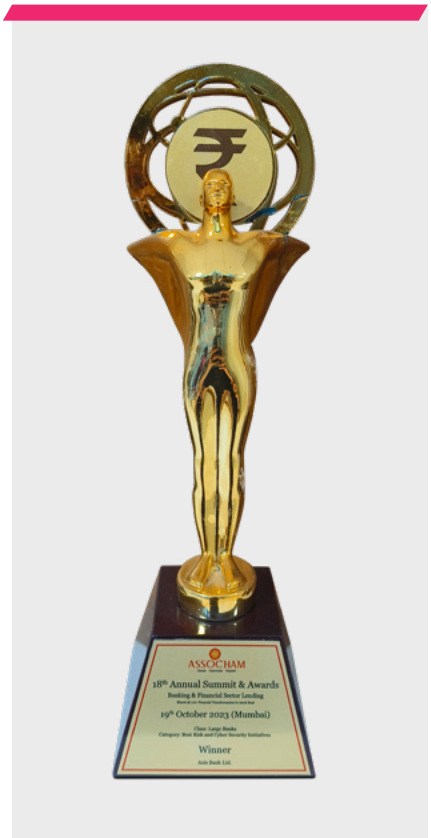
Our leadership continues with the Cloud-first, Cloud-native architecture. We are a leader among peers to have three enterprise grade landing zones and deploy 140+ critical applications on Cloud. We are the first Indian bank to be ISO certified for AWS and Azure Cloud security. We continued our journey towards next-gen initiatives such as hyper automation using Infra-as-a-Code capabilities and enhancing application observability through Cloud based SRE capabilities. In fiscal 2025, the focus will be on consolidation of key applications on Cloud, including data.

Partnerships, Ecosystem, and Integration

We are committed to our open ecosystem proposition to build dedicated partnerships using API strategy. We have adopted next-gen integration by deploying 410+ APIs on our developer portal and 3,000+ registered users across 460+ external gateway partners.

Achievements in Digital and Cyber Security space

DSCI Excellence Award for Best Security Practices in Organisation – Banking Sector for 2023



ASSOCHAM Annual Banking and Financial Sector Lending Award (Large companies)

Best Cyber Security Initiatives and Best Digital Initiatives

Infosys Finacle Innovation Awards 2023

Corporate Banking Innovation, Modern Technologies-led Innovation and Product Innovation