

One Platform to Secure, Monitor & Report - SEBI-Ready from Day One!



The Compliance Challenge in BFSI

In a rapidly digitizing economy, SEBI (Securities and Exchange Board of India) has strengthened its cybersecurity and cyber resilience framework for all regulated entities – including stock exchanges, depositories, AMCs, brokers, and investment advisers.

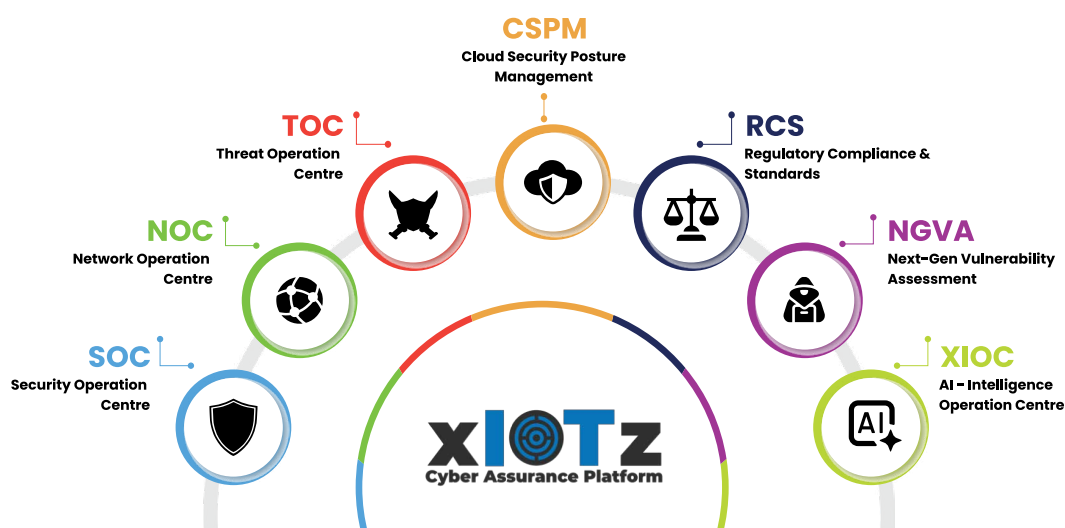
SEBI Cybersecurity Requirements:

-  Real-time threat detection and 24/7 monitoring
-  Incident response and breach reporting within 6 hours
-  Cloud Security Posture Management (CSPM)
-  System audit, vulnerability assessment, and red teaming
-  Data integrity, access control, and log retention
-  Regular cybersecurity awareness training and governance oversight

Meet Compliance with Confidence: xIoTz UCAP

xIoTz's Unified Cyber Assurance Platform (UCAP) is purpose-built to help BFSI organizations fully comply with SEBI's Cybersecurity Framework while reducing cost, complexity, and fragmentation.

-  End-to-End Visibility & Control
-  Audit-Ready Compliance Reporting



xIoTz Features addressing SEBI Cybersecurity Compliance

SEBI Cyber Security Requirement	xIoTz UCAP Feature	xIoTz UCAP Detailed Feature
Cyber Risk Management	Unified Cyber Assurance Platform (UCAP)	Provides a centralized platform for managing cyber risks, offering audit trails, real-time risk visibility, and risk mitigation strategies to comply with SEBI's requirements.
Data Classification and Retention	Log File Management	Data classification, retention policies, and secure log management ensure that sensitive data is protected and compliant with SEBI's data storage and retention guidelines.
Data Loss Prevention (DLP)	Data Loss Prevention	Detects unauthorized data access, and loss through File Integrity Monitoring and Hardening. Comprehensive monitoring of sensitive information to ensure SEBI compliance.
Access Control and Identity Management	Identity & Access Management (IAM)	Role-based access control (RBAC), Multi-Factor Authentication (MFA), user activity monitoring, and privilege escalation detection for strict access control management.
Market Systems Security & Incident Detection	User & Entity Behavior Analytics (UEBA)	Continuous monitoring of users and entities using behavioral analytics to detect anomalies, generate risk-based alerts, and provide audit-ready evidence.
Network Security	Network Detection and Response (NDR)	Network Flow Monitoring (NFM), Intrusion Detection (NIDS), Behavior Analysis (NBAD), and real-time anomaly detection provide continuous monitoring of network security.
Incident Response and Reporting	Threat Operations Center (TOC)	Automated threat detection, MITRE ATT&CK mapping, incident playbooks, & real-time alerts help identify, respond to, and report security incidents in line with SEBI requirements.

xIoTz Features addressing SEBI Cybersecurity Compliance

SEBI Cyber Security Requirement	xIoTz UCAP Feature	xIoTz UCAP Detailed Feature
Encryption of Sensitive Data	Data Protection and Encryption	AES-256 encryption & end-to-end encryption for data at rest & in transit, ensuring data confidentiality & integrity in compliance with SEBI's encryption requirements.
Business Continuity and Disaster Recovery	Business Continuity Management	System downtime management, backup automation, and disaster recovery plans ensure continuous operations and minimal disruption in case of cyber incidents.
Vulnerability and Patch Management	Next-Gen Vulnerability Assessment	Vulnerability scanners, OS patching, CVE/CWE detection, and third-party patching validation ensure constant system updates and proactive threat management.
Audit and Compliance Reporting	Compliance Reporting Dashboard	Pre-configured templates for SEBI audits, automated reporting, drill-down analytics, & real-time compliance monitoring ensure accurate documentation for regulatory audits.
Monitoring of Information Security Controls	Security Monitoring & Auditing	Audit logging, process monitoring, real-time analytics, & activity tracking ensure that security controls are constantly monitored & maintained as per SEBI guidelines.
Third-party Risk Management	Third-Party Risk Assessment	Assessments, audits, and third-party vulnerability scanning ensure that external vendors and services meet SEBI's security and compliance requirements.
Security Awareness and Training	Security Awareness & Training Module	Training platform with interactive simulations, phishing awareness, & security best practices ensures that employees are constantly trained to mitigate risks & adhere to SEBI guidelines.

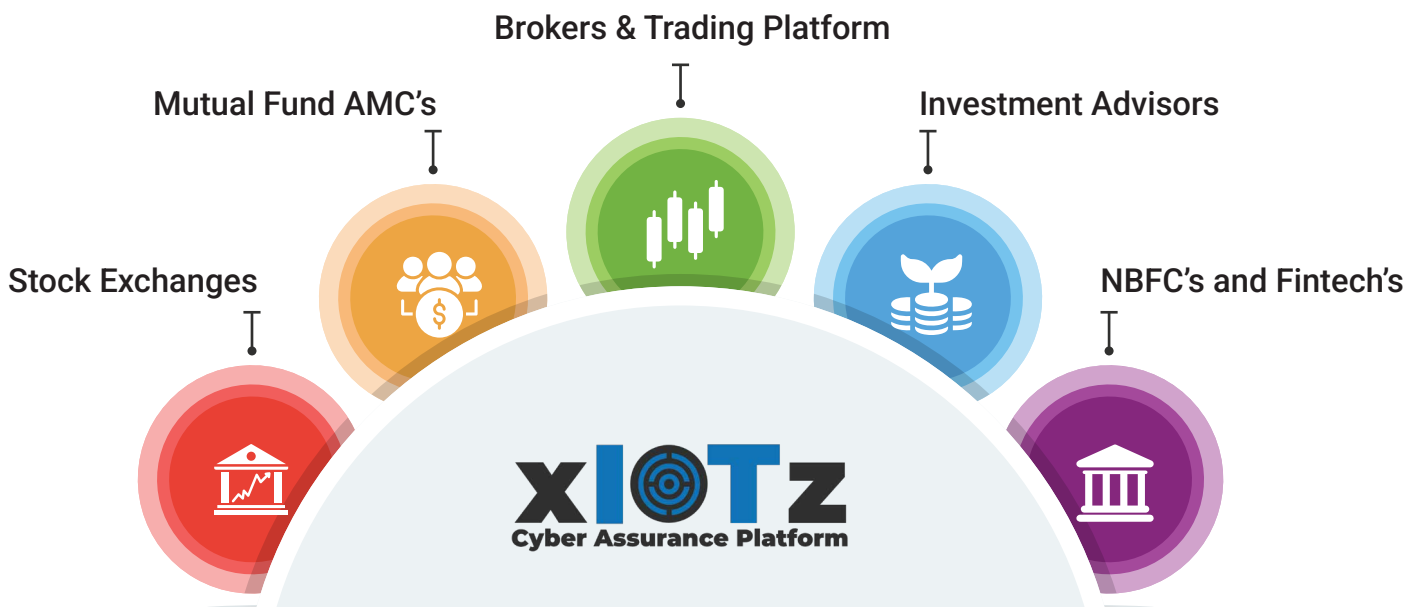
Trusted for National Security. Built for Financial Security.



xIoTz solutions power **Indian Navy-grade deployments**, ensuring our tech meets the highest standards of cyber resilience — and are now being adopted by financial institutions to proactively



Who Should Use xIoTz UCAP for SEBI Compliance?



Let's Get You SEBI-Ready!

Schedule a free compliance audit demo

 xiotz.com

 sales@xiotz.com

 +91 - 9019632210

 Bangalore, India



Non-Compliance Can Cost You Everything — Streamlined, Automated Cyber Defense for RBI Entities



Why RBI Cybersecurity Compliance Matters?

The Reserve Bank of India (RBI) has issued stringent cybersecurity mandates through its Cyber Security Framework for Banks and Master Direction for NBFCs and Financial Institutions, with emphasis on:

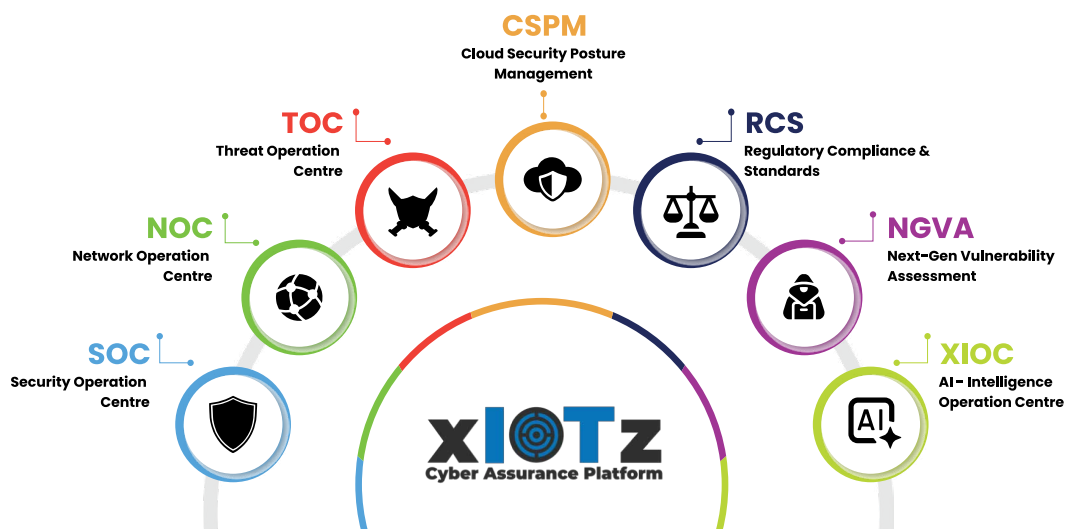
RBI Cybersecurity Requirements:

-  Risk governance and board-level oversight
-  Log retention, audit trails, and forensic readiness
-  Timely breach reporting and incident response
-  Data security, encryption, and localization
-  24x7 threat detection and monitoring
-  Vendor and third-party risk management

Meet Compliance with Confidence: xIoTz UCAP

xIoTz's Unified Cyber Assurance Platform (UCAP) is purpose-built to help BFSI organizations fully comply with SEBI's Cybersecurity Framework while reducing cost, complexity, and fragmentation.

-  End-to-End Visibility & Control
-  Audit-Ready Compliance Reporting



xIoTz Features addressing RBI Cybersecurity Compliance

RBI Cyber Security Requirement	xIoTz UCAP Feature	xIoTz UCAP Detailed Feature
Cyber Risk Governance	Unified Cyber Assurance Platform (UCAP)	Centralized platform offering real-time risk visibility, asset classification, and strategic risk mitigation aligned with RBI's enterprise risk management guidelines..
Log Management and Retention	Log File Management	Secure and tamper-proof log storage with automated retention policies (live 6 months + archived 2 years) compliant with RBI's log management requirements.
Data Loss Prevention (DLP)	Data Loss Prevention	File Integrity Monitoring, endpoint hardening, and unauthorized data access alerts protect critical banking data as per RBI norms
Access Control & Identity Governance	Identity & Access Management (IAM)	Enforces least privilege, Role-based access control (RBAC), Multi-Factor Authentication (MFA), and continuous monitoring of privileged user activity in line with RBI's guidelines for identity control.
Network Security Monitoring	Network Detection and Response (NDR)	Continuous packet analysis, anomaly detection, and network behavior monitoring to guard against internal and external threats.
Continuous Monitoring & Anomaly Detection	User & Entity Behavior Analytics (UEBA)	Continuous monitoring of users and entities using behavioral analytics to detect anomalies, generate risk-based alerts, and provide audit-ready evidence.
Incident Management & Reporting	xIoTz Automated Response (XAR)	Incident response playbooks, threat intelligence mapping, and auto-reporting mechanisms to meet RBI's breach notification SLA and lifecycle requirements

xIoTz Features addressing RBI Cybersecurity Compliance

RBI Cyber Security Requirement	xIoTz UCAP Feature	xIoTz UCAP Detailed Feature
Employee Cyber Hygiene	Security Awareness & Training Module	Regular simulation-based security training for staff, fulfilling RBI's mandate for periodic awareness programs and internal sensitization.
Third-Party Risk Control	Third-Party Risk Assessment	Continuous due diligence, onboarding risk scoring, and contract-level compliance mapping to manage risks associated with service providers.
Encryption and Data Sovereignty	Data Protection and Encryption	End-to-end AES-256 encryption for data at rest and in motion, and geo-fenced storage to support RBI's data localization mandates.
Business Continuity Planning (BCP)	Business Continuity Management	Automated backups, failover mechanisms, and crisis simulations to support RBI's BCP and disaster recovery standards.
Vulnerability and Patch Lifecycle	Next-Gen Vulnerability Assessment	OS and application-level VA/PT, third-party patch tracking, and CVE-based vulnerability detection to ensure RBI-compliant system hygiene.
Security Monitoring & Governance	Security Monitoring & Auditing	Real-time control monitoring, compliance alerting, and executive dashboards to continuously evaluate security posture.
IT Audit & Regulatory Compliance	Compliance Reporting Dashboard	Built-in RBI audit templates, configurable alerts, and automated compliance scorecards to streamline IT examinations and regulatory submissions.

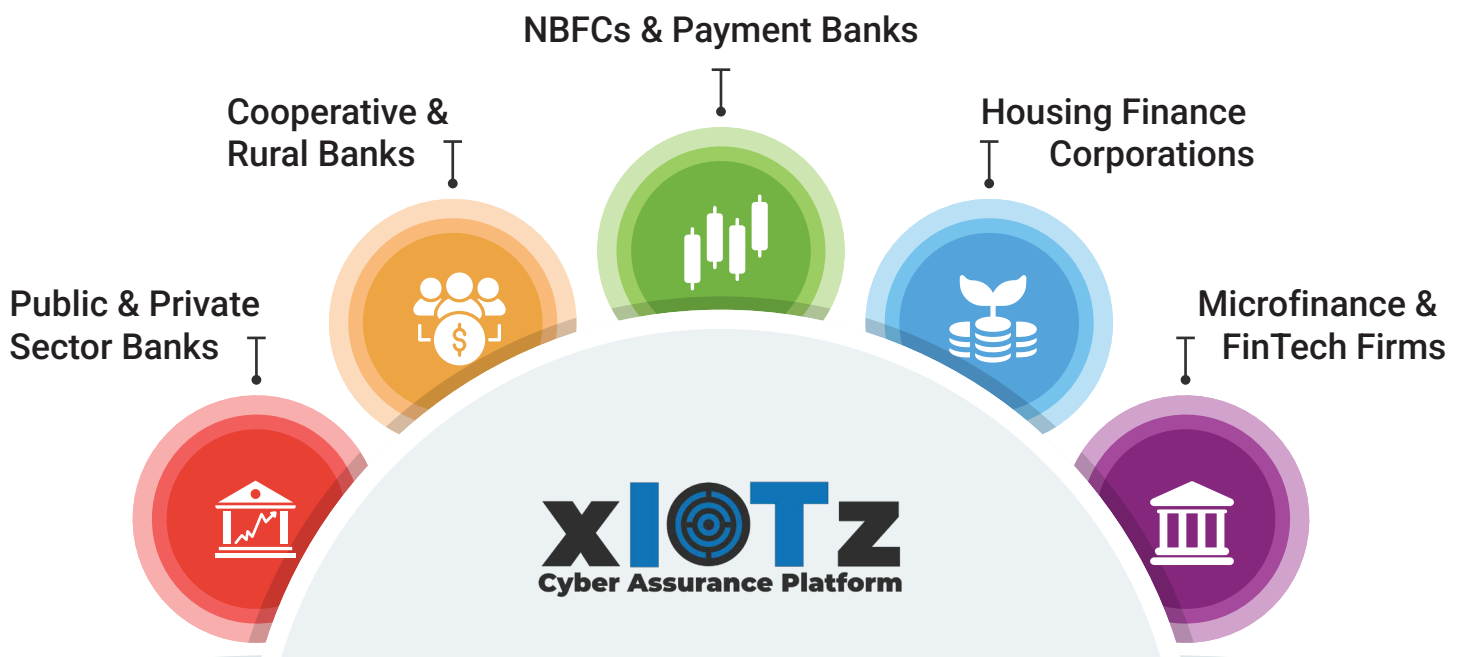
Trusted for National Security. Built for Financial Security.



xIoTz solutions power **Indian Navy-grade deployments**, ensuring our tech meets the highest standards of cyber resilience — and are now being adopted by financial institutions to proactively meet RBI mandates.



Who Should Use xIoTz UCAP for RBI Compliance?



One Breach, One Penalty, One Reputation at Risk — Stay RBI-Compliant

Schedule a free compliance audit demo

DPDP Non-Compliance Isn't a Risk — It's a Liability with Regulatory, Financial, and Operational Consequences



Why DPDP Act Compliance Matters?

India's Digital Personal Data Protection (DPDP) Act mandates organizations to protect personal data through reasonable security safeguards, accountability, and timely breach reporting. Non-compliance can lead to severe financial penalties, reputational damage, and regulatory action.

DPDP Compliance Focus Areas



Continuous monitoring to prevent unauthorized access and breaches.



Tamper-evident logs to prove lawful data handling.



Monitoring cloud misconfigurations impacting data residency.



Early detection aligned with DPDP reporting timelines.



Visibility into vendor and processor data risk.



Awareness programs to reduce human-driven data risk.

Meet Compliance with Confidence: xIoTz UCAP

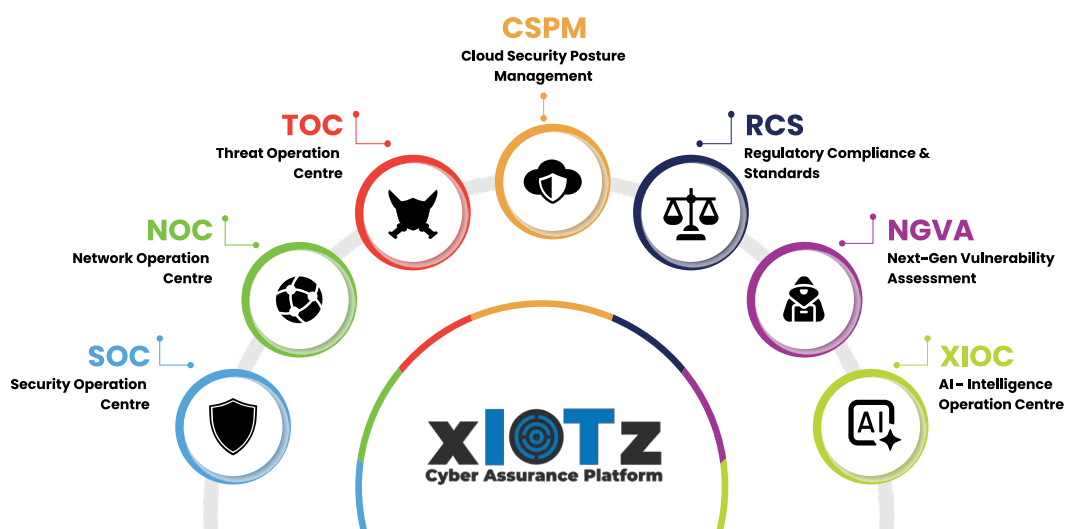
xIoTz's Unified Cyber Assurance Platform (UCAP) is purpose-built to help BFSI organizations fully comply with SEBI's Cybersecurity Framework while reducing cost, complexity, and fragmentation.



End-to-End Visibility & Control



Audit-Ready Compliance Reporting



 Incubated at SIIC, C3i Hub, IIT Kanpur	 Accelerated by NCoE, DSCI, NASSCOM	 Winner of iDEX DISC IX Indian Navy Challenge	 National Technology Award TDB, DST, MeitY	 Defence Design Technology Incubator	 Chaunauti 8.0 STPI	 National Cyber Security Framework (Cert-in)
---	---	---	--	--	---------------------------	--

xIoTz Features addressing DPDP Act Cybersecurity Compliance

DPDP Act Requirement	xIoTz UCAP Feature	xIoTz UCAP Detailed Feature
Consent Accountability & Lawful Processing	Access & Activity Monitoring	Continuous monitoring and logging of user and system access to environments handling personal data, supporting lawful processing accountability under DPDP.
Role-Based Access Governance (Oversight)	Role-Based Access Visibility	Provides visibility into role-based access usage and access events across systems to detect excessive access and policy violations (no identity provisioning or enforcement).
Reasonable Security Safeguards	SOC + TOC Security Operations	Real-time security monitoring, threat detection, & alerting to protect personal data against unauthorized access, misuse, and cyber incidents.
Vulnerability Management for Personal Data Systems	Next-Gen Vulnerability Assessment (NGVA)	OS, application, and configuration vulnerability assessment to identify weaknesses that could lead to personal data exposure.
Personal Data Breach Detection & Accountability	User & Entity Behavior Analytics (UBEA)	Continuous monitoring of users and entities using behavioral analytics to detect anomalies, generate risk-based alerts, and provide audit-ready evidence.
Encryption Safeguards (Assurance)	Encryption & Configuration Monitoring	Monitors encryption posture of data at rest and in transit by validating security configurations and control status (enforcement handled by underlying platforms).
Data Localization & Sovereignty Oversight	Cloud Security Posture Management	Detects cloud misconfigurations, region violations, and policy deviations impacting personal data residency and sovereignty requirements.

xIoTz Features addressing DPDP Act Cybersecurity Compliance

DPDP Act Requirement	xIoTz UCAP Feature	xIoTz UCAP Detailed Feature
Personal Data Breach Detection	Automated Incident Detection & Response (XAR)	Early breach detection, automated response workflows, and evidence collection to support DPDP breach reporting and regulatory timelines.
Auditability & Accountability	Security Monitoring & Auditing	Tamper-evident logs, security event trails, and centralized dashboards to demonstrate DPDP accountability and audit readiness.
Third-Party Data Processor Risk	Third-Party Risk Visibility	Continuous monitoring and risk scoring of vendors and service providers handling personal data, supporting DPDP shared responsibility.
Employee Cyber Hygiene	Security Awareness & Training Module	Ongoing awareness programs and simulations to reduce human-related risks in personal data handling.
Availability & Resilience of Personal Data	Business Continuity Monitoring	Visibility into backup status, recovery readiness, and resilience controls without owning or managing infrastructure.
Security Monitoring & Governance	Security Monitoring & Auditing	Real-time control monitoring, compliance alerting, and executive dashboards to continuously evaluate security posture.
IT Audit & Regulatory Compliance	Compliance Reporting Dashboard	Centralized compliance tracking, alerts, and evidence collation to support internal governance and regulatory submissions.

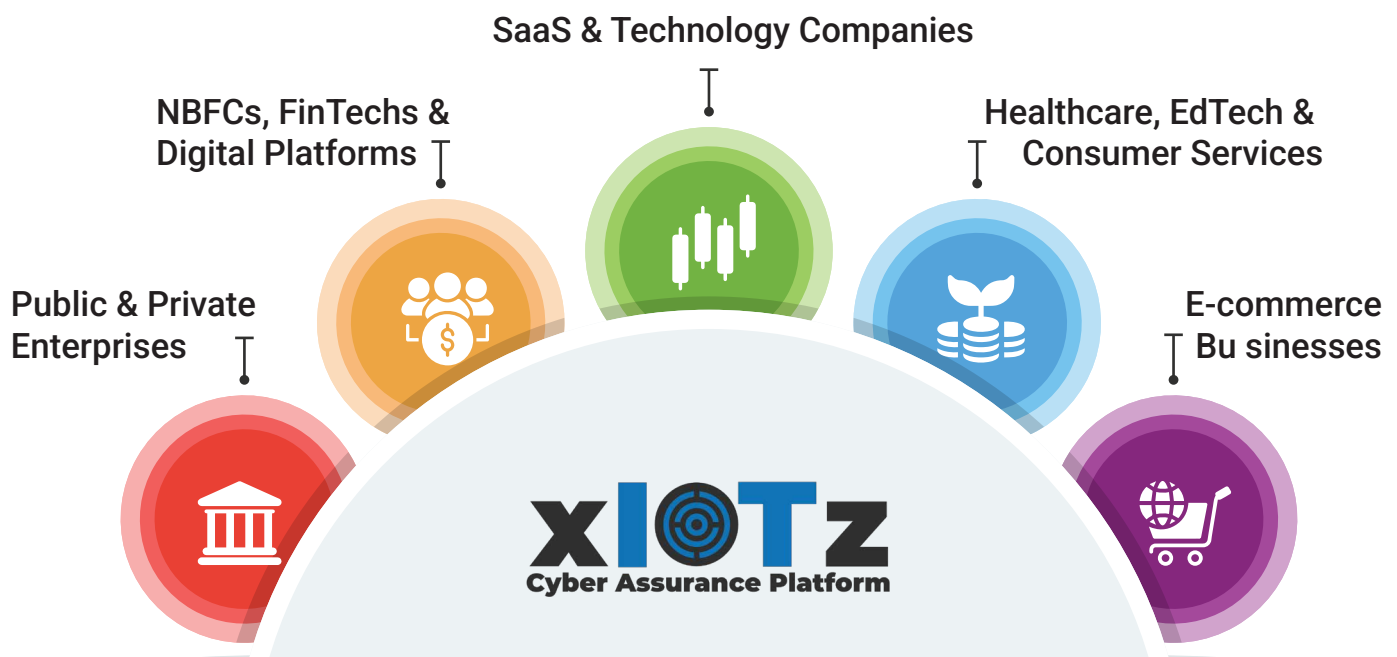
Trusted for National Security. Built for Financial Security.



xIoTz solutions power **Indian Navy-grade deployments**, ensuring our tech meets the highest standards of cyber resilience — and are now being adopted by financial institutions to proactively meet RBI mandates.



Who Should Use xIoTz UCAP for DPDP Compliance?



When Personal Data Is Compromised, Accountability Follows — Stay DPDP Compliant

Schedule a free compliance audit demo

