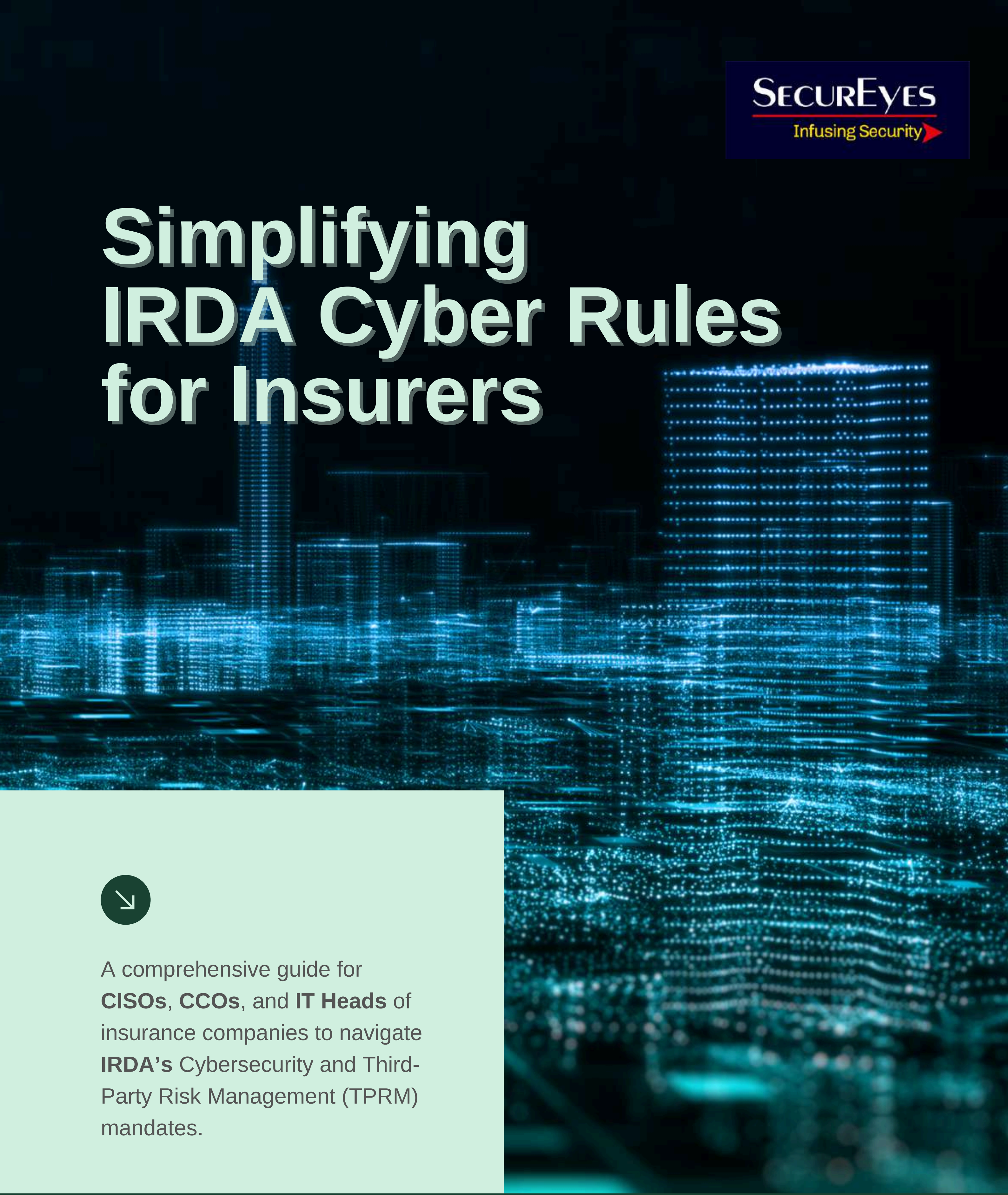


SecurEyes
Infusing Security

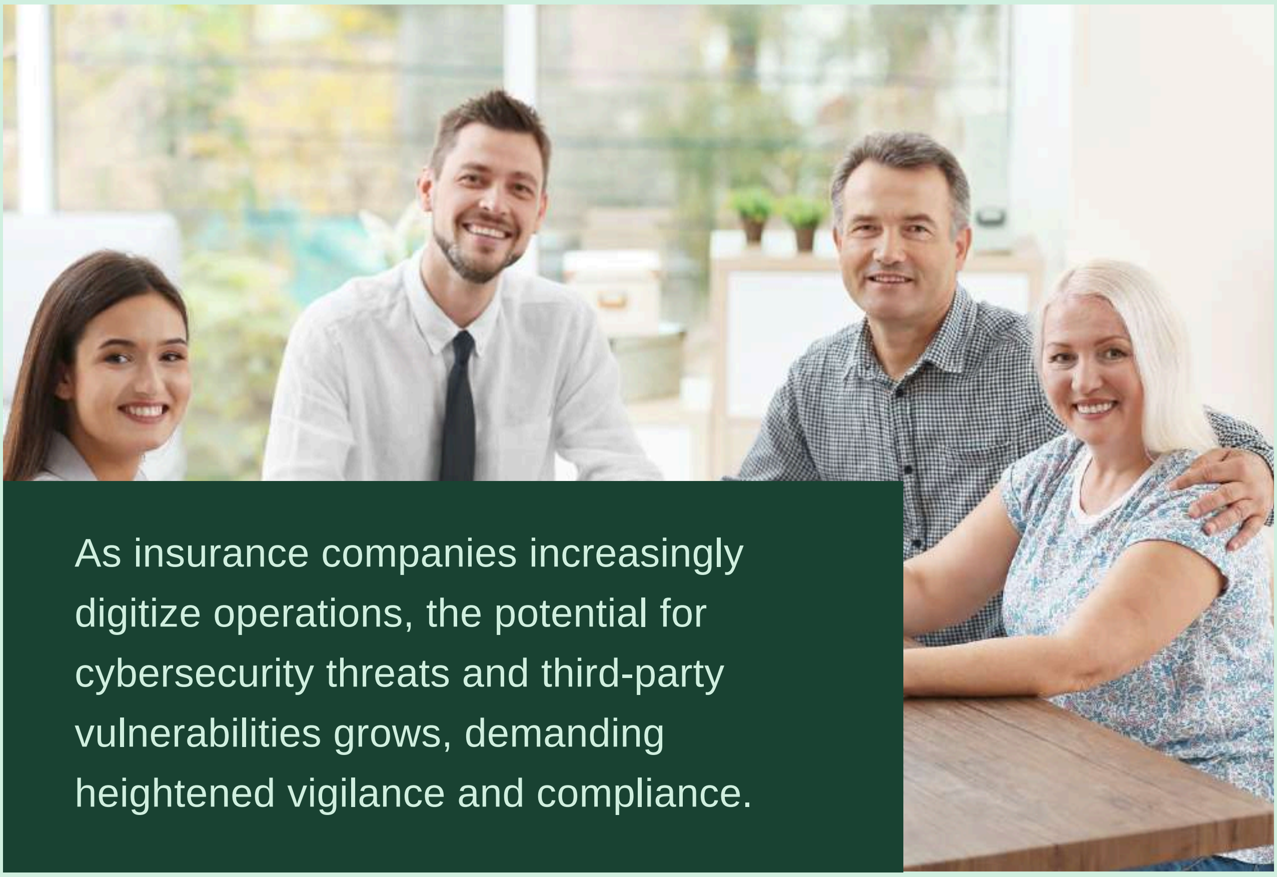
Simplifying IRDA Cyber Rules for Insurers

A comprehensive guide for **CISOs**, **CCOs**, and **IT Heads** of insurance companies to navigate **IRDA's** Cybersecurity and Third-Party Risk Management (TPRM) mandates.

www.secureyes.net

2025

Introduction

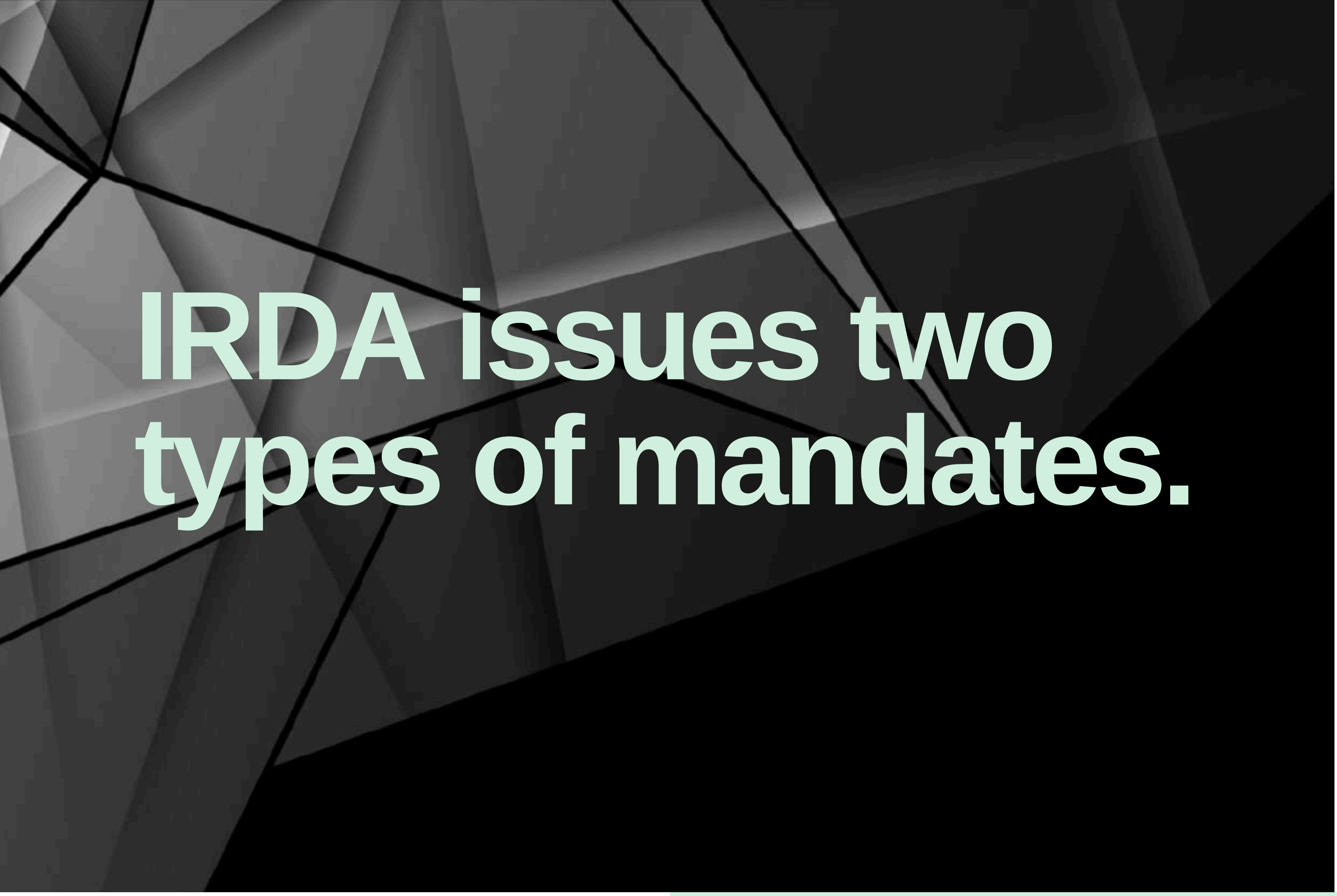


As insurance companies increasingly digitize operations, the potential for cybersecurity threats and third-party vulnerabilities grows, demanding heightened vigilance and compliance.

The Insurance Regulatory and Development Authority of India (IRDAI) has established comprehensive mandates and recommendations to ensure robust **cybersecurity** and **third-party risk management** (TPRM) practices within the insurance sector.

This guide serves as a detailed resource for **Chief Information Security Officers (CISOs), Chief Compliance Officers (CCOs), and IT Heads** to understand and implement IRDAI's requirements and recommendations, ensuring operational resilience and regulatory compliance.

- Rising Cyber Threats: The insurance sector's reliance on digital technologies exposes it to risks such as data breaches, ransomware, and fraud.
- Regulatory Accountability: The IRDAI mandates robust cybersecurity frameworks and TPRM practices to protect customer data, maintain system integrity, and prevent financial crimes.
- Operational and Reputational Impact: Non-compliance with IRDAI guidelines can lead to operational disruptions, hefty penalties, and reputational damage, impacting customer trust and business continuity.



IRDA issues two types of mandates.

01

Mandatory Mandates (Must Comply)

These refer to the processes and systems that need to be put in place to protect data and mitigate it’s misuse or destruction.

02

Recommended (Good-to-Have)

These recommend the best practices that can become a differentiator for companies, as well as a competitive advantage.

Mandatory Cybersecurity Requirements.

Information and Cyber Security Policy (ICSP)

- Develop a comprehensive ICSP to ensure the protection of critical data and assets.
- Outline responsibilities and establish goals to mitigate risks of data misuse, modification, or destruction.

Appointment of a CISO:

- Designate a CISO to oversee the cybersecurity program, enforce standards, and drive compliance.

Information Security Risk Management Committee (ISRMC):

- Form a committee comprising the CRO, CISO, and CTO to govern the ICSP and address security risks.

Security Controls Implementation:

- Deploy measures to safeguard cyberspace, reduce vulnerabilities, and mitigate cyber incidents.

Adherence to IT Act 2000 and Amendments:

- nsure compliance with legal provisions to protect customer data and prevent cybercrimes.

Mandatory Cybersecurity Requirements

Incident Reporting:

- Report cyber incidents to CERT-In within 6 hours, with copies to IRDAI and relevant authorities.

Annual Assurance Audits:

- Conduct annual independent audits to evaluate cybersecurity frameworks and submit reports within IRDAI timelines.

Data Protection Tools:

- Implement tools like Data Loss Prevention (DLP) and Digital Rights Management (DRM)

Cryptography and ICT Logs:

- Use cryptographic controls to secure data.
- Maintain ICT logs for a rolling period of 180 days within Indian jurisdiction.

DMARC Policy:

- Enforce Domain-based Message Authentication, Reporting, and Conformance to mitigate email spoofing.

Mandatory TPRM Requirements

→ **Robust AML/CFT Programs:**

- Establish Anti-Money Laundering (AML) and Combating Financing of Terrorism (CFT) programs.

→ **KYC Norms:**

- Mandate KYC for intermediaries and include these norms in contracts.

→ **Vendor Classification:**

- Define classification standards for third-party vendors based on the criticality of their operations and access levels.

→ **Periodic Assessments:**

- Assess third-party service providers for compliance with Service Level Agreements (SLAs) and competency requirements.

→ **Enhanced Due Diligence:**

- Conduct detailed assessments for high-risk entities, especially those linked to FATF-identified countries.

→ **Client Due Diligence (CDD):**

- Perform CDD as per Rule 9 of the PML Rules and ensure risk assessment exercises cover clients, geographies, products, and services.

IRDA Recommended (Good-to-Do) Practices

Cybersecurity

- Establish a Cyber Security Operations Center (C-SOC) for continuous monitoring.
- Maintain an updated software inventory.
- Conduct regular vulnerability assessments and penetration testing.
- Promote cybersecurity awareness among stakeholders.
- Develop a Cyber Crisis Management Plan (CCMP).
- Participate in information-sharing forums.

Third Party Risk Management (TPRM)

- Implement continuous monitoring and risk remediation measures for third parties.
- Develop training programs for staff and agents to prevent financial crimes.
- Use a risk-based approach for assessing third parties.

Central Banking Award 2023

ET Achievers Award 2022

Accreditations

CERT-In, NIC, ISO 9001:2015, and ISO 27001:2013 certified

250,000+

IPs covered under Penetration Testing.

10,000+

People covered under Social Engineering

30,000+

Servers reviewed

20,000+

Professionals trained

About SecurEyes

SecurEyes is a global leader in cybersecurity, empowering organizations to protect their digital assets, ensure compliance, and stay ahead of evolving threats.

With **18+** years of expertise, cutting-edge tools, and tailored consulting services, we've earned the trust of governments, regulators, and Fortune 500 companies worldwide.

Diverse Clientele

Over **700** clients across diverse industries.
Here are a few of them.

WEST ASIA & NORTH AFRICA

البنك المركزي السعودي SAMA Saudi Central Bank
الشراكات الإستراتيجية STRATEGIC PARTNERSHIPS
GIB بنك الخليج الدولي
الاتحاد ETIHAD AIRWAYS
البنك السعودي للاستثمار The Saudi Investment Bank
راس غاز RG RasGas
RAKBANK
سمة SIMAH السعودية للمعلومات الائتمانية Saudi Credit Bureau
مصرف الراجحي Al Rajhi Bank
Emirates NBD
البنك الأهلي ahlibank
تمام tamam

ASIA PACIFIC

SBI
ICICI Bank
केनरा बैंक Canara Bank
भारतीय डाक India Post
हिएलि HAL Hindustan Aeronautics Limited
bharti AXA
NIC एनआईसी National Informatics Centre
गृह मंत्रालय MINISTRY OF HOME AFFAIRS
वित्त मंत्रालय MINISTRY OF FINANCE
my GOV मेरी सरकार
MSME Ministry of MSME, Govt. of India

NORTH AMERICA

Goldman Sachs
BROCADE
EVALUESERVE
RSA SECURITY™
NTT DATA
GNAX
Walmart
UNISYS
iQUANTI

SecurEyes Infusing Security

USA: +1 361 423 1683   UAE: +971 5089 50797   IND: +91 80 4126 4078

www.secureyes.net   hello@secureyes.net