



IRDAI Mandates Incident Response Retainership

KPMG in India's Cyber Incident Response

KPMG. Make the Difference.








As per the recent IRDAI (Insurance Regulatory and Development Authority of India) circular dated 24 March 2025, all Regulated Entities, including insurance intermediaries are required to empanel Cyber Incident Response and Digital Forensics experts in advance to conduct digital forensics and root cause analysis (RCA) of cyber incident/s without any delay.

A cyber security incident is any adverse event whereby some aspect of computer system is threatened or compromised via ransomware attack, data breach, malware attacks, defacement of website, denial of service, etc. In the wake of the increasing number of cyber security incidents, IRDAI has emphasised the need to empanel external cyber incident response and digital forensics experts who are independent of other security functions to avoid any conflict of interest.

How can KPMG in India Help

KPMG in India's On-Demand Cyber Incident Response Services model is a custom-tailored service to collectively address the requirements published in IRDAI guidelines. This offering prepares clients for incident readiness and building cyber resilience that can enable effective cyber response capabilities and reducing delays.

IRDAI Guidelines	How Can KPMG in India Help
Implement a Cyber Crisis Management Plan (CCMP) for situational awareness of organization during cyber-attacks	 Enhance CCMP to incorporate procedure for cyber threat intelligence collection, analysis and consumption pre and post incident
On-board and empanel certified cyber incident response and digital forensics experts in advance	 Our Cyber Incident Retainership model offers flexible options to on-board Forensic and Incident experts anytime and anywhere
Ensure log availability and retention for a period of 180 days for all ICT infrastructure and application logs for analysis	 Help ensure availability of correct logs required for investigation during the cyber crisis
Report cyber incidents to IRDAI in the prescribed format within six hours of being noticed	 Support with incident notification to regulators within prescribed timelines
Perform incident analysis and digital forensics in the event of cyber security incident.	 Global methodologies for detailed incident investigation complemented with acceptable forensic procedures.

Reference: Circular on Cyber Incident or Crisis Preparedness.pdf, IRDAI, 24 March 2025

Our Cyber Response Email: in-fmcir@kpmg.com

Atul Gupta HOF T: +91 98100 81050 E: atulgupta@kpmg.com	Kunal Pande SSL-HOD T: +91 98926 00676 E: kpande@kpmg.com	Sony Anthony SSL-HOD T: +91 98455 65222 E: santhony@kpmg.com	Manish Tembhurkar Partner T: +91 98181 99432 E: mtembhurkar@kpmg.com
---	--	---	--

Follow us on:
[kpmg.com/in/socialmedia](https://www.kpmg.com/in/socialmedia)



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2025 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.