KPMG

KPMG in India's HITRUST assurance programme

Evolving information security demands in healthcare

Is your organisation ready?

home.kpmg/in

Healthcare service providers are increasing scrutiny on business associates in the wake of regulatory requirements, bigger penalties and ever-increasing security and privacy concerns.

Business associates refer to those entities that are involved in creating, receiving, maintaining or transmitting Protected Health Information (PHI) or Personally Identifiable Information (PII) on behalf of a healthcare service provider and include technology, business process outsourcing and platform service providers. Our HITRUST assurance programme provides organisations with a coordinated approach that helps ensure all programmes related to security and privacy are aligned, maintained and thorough to support an organisation's risk management and compliance objectives.

Healthcare companies are facing multiple challenges

- Increasing precision of computer abuse and computer crime
- Rapidly changing business, technology and regulatory environment
- Increasing scrutiny from regulators, auditors, underwriters, customers and business partners
- Gaining the assurances needed to allow organisations to safely engage with their customers and trading partners
- Inconsistent adoption of minimum controls for reliance
- Ineffective and inefficient internal compliance management processes
- Inconsistent business partner requirements and compliance expectations
- Increasing number of breaches leading to public and regulatory concerns

HITRUST

HITRUST is an alliance and it helps organisations from the healthcare sector to effectively manage data, information risk, and compliance. HITRUST provides structure, transparency, guidance and cross-references to authoritative sources. Organisations globally can be certain of their data protection compliance through the HITRUST CSF

HITRUST CSF

HITRUST CSF is a framework designed to provide organisations with a comprehensive, flexible and efficient approach to regulatory compliance and risk management. It rationalises relevant regulations and standards into a single overarching security framework.

Our HITRUST assurance programme

- Can help organisations in the healthcare sector to effectively manage information risk, data, and compliance
- Can help organisations in understanding the challenges of maintaining and assembling various programmes needed to manage information risk and compliance
- Is a risk-based approach aiming to provide guidance, structure, transparency and cross-references to authoritative sources industry frameworks (e.g. ISO27001, PCI, COBIT), international regulation (e.g. GDPR), state legislation (e.g. CCPA), federal agency rules and guidance (e.g. NIST) and federal legislation (e.g. HIPPA)

The essence of the programme is 'assess once, report many'

Applicability of our HITRUST assurance programme

Service providers already providing or intending to provide any of the following services to U.S.-based healthcare service providers.

- Provide **back-office support** such as revenue cycle management, medical coding, medical transmission, claim management
- Provide **software development**, host or support services
- Involved in **transmission of health data**
- Provide support to **U.S. healthcare federal agencies** such as CMS and FISMA
- Provide business support processes to **medical/ life Insurance providers in the U.S**
- Provide business/business support to **medical tourism.**

Our service offerings

HITRUST CSF readiness assessment

We can assist in assessing the organisations current readiness towards HITRUST CSF certification requirements and prepare organisations for the validated assessment

HITRUST certification

We can assist organisations in the process of HITRUST CSF certification by performing a HITRUST CSF validated assessment and submitting the results to HITRUST for validation and certification

SOC 2 + HITRUST report

We can assist service organisations with a SOC 2+ report that express an opinion on fairness of presentation of description and suitability of design and operating effectiveness of controls based on relevant trust service categories and HITRUST CSF

SOC 2 + HITRUST report and HITRUST certification

We can assist organizations by performing the necessary testing for expressing an opinion on the SOC 2 + HITRUST CSF assurance and submit a HITRUST CSF validated assessment and achieve HITRUST CSF certification

Did you know?

In the late 2015, HITRUST and AICPA came together to align HITRUST's common security framework (CSF) with the AICPA's SOC 2 reporting.

Aim of the collaboration was to help organisations, such as business associates, comply with regulations and obligations and streamline SOC 2 reporting requirements.

Source: New AICPA and HITRUST Report Will Help CPAs Report on Controls over Protected Health Information, AICPA, published on 17 December, 2015

Many business associates are moving ahead with preparing their organisations for the expectations that come with contractual commitments. By proactively demonstrating a serious commitment to information security, organisations can gain customer confidence and create a competitive advantage.

Our value proposition as a HITRUST external assessor

- We understand security
- We are accredited
- We have extensive experience in providing independent assurance
- We take a cross-functional approach
- We are independent and objective
- We provide quality assurance and governance
- Our methodology is in line with global practices
- We have an extensive resource pool.

Potential benefits of our HITRUST assurance programme

- Provides organisations with thorough information risk management and compliance objectives
- Helps manage cyber-related risks, provides robust controls and a consistent approach to assessment
- Reduced cost for managing data protection compliance
- Evolves according to user input and changing conditions in the standards and regulatory environment at least on an annual basis
- Rationalises relevant regulations and standards into a single overarching security framework.

KPMG in India contacts:

Akhilesh Tuteja
Partner and Head
Risk Consulting
Co-leader – Global Cyber Security
T: : +91 124 254 9191
E: atuteja@kpmg.com

Atul Gupta
Partner and Head
IT Advisory
India Cyber Security Lead
T: +91 124 336 9065
E: atulgupta@kpmg.com

Sundar Ramaswamy
Partner
IT Advisory
T: +91 9892520391
E: sr@kpmg.com

M Gururaja
Partner
IT Advisory
T: +91 9845336277
E: mgururaja@kpmg.com

home.kpmg/in

#KPMG josh

Follow us on:
home.kpmg/in/social media

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.