COMPLIANCE AND CERTIFICATIONS FOR CLOUD AND MANAGED HOSTING SERVICES: AN OVERVIEW

TABLE OF CONTENTS

For more information, visit us at www.tatacommunications.com

For more information, visit us at www.tatacommunications.com

Contact us

INTRODUCTION

Protecting customers' privacy is a top priority for firms around the world. But data privacy standards differ widely from one country to the next. In fact, according to Forrester, there are over 100 variations globally. Security professionals must protect their organisation's critical business apps and sensitive data, no matter where and how they are being hosted.

Many enterprises are moving to the cloud because of its robust capabilities, including security. To make the most of its potential, organisations still need to adjust and evolve workloads to take full advantage of the cloud platform.

As cloud adoption continues to grow, security professionals are responsible for addressing a wide range of privacy and compliance issues, as well as risks relating to:

1) Where and how the organisation stores sensitive data in the cloud

2) How the organisation secures and monitors its networks for cloud services

3) Which apps the organisation hosts or sources from the cloud

4) Which endpoints and other devices the organisation supports for cloud access.

Typical security and control issues that feature most in compliance certifications and regulations include identity federation, strong authentication, role delegation, privilege management, logging and alerting, encryption, customer key management, data discovery and disaster recovery.

TATA COMMUNICATIONS – HOSTING AND CLOUD SERVICES

Tata Communications provides managed hosting services (MHS) and managed cloud services – IZO™ Private Cloud and IZO™ Cloud Storage.

Managed hosting services (MHS) provides customers with a fully managed, end-to-end IT solution. Its range of components includes hardware, an Operating System (OS) and database, along with IT services such as platform implementation and daily proactive management. Managed hosting services give customers the leverage to reduce their capital and operational costs, along with the complex IT administration that often comes with implementation and ongoing service management. Tata Communications' Managed Hosting Services also offers improved uptime and availability thanks to 24/7/365 management and monitoring from a central Global Service Management Centre (GSMC).

IPC (IZO™ Private Cloud) is an enterprise cloud platform, offering a flexible, scalable and reliable cloud environment. Its adaptability enables end users to create the ideal combination of compute, network, security, storage and traffic management services to meet their business needs, while also being flexible enough to grow with business. The IPC service is available on two models within Tata Communications' data centres. It includes Virtual Private Cloud (VPC), Dedicated Private Cloud (DPC) and Virtual Private Data Centre (VPDC).

IZO™ Cloud Storage is based on object storage technology. It offers a flexible, scalable and reliable cloud storage environment with backed SLAs. The solution allows end users to select an appropriate combination of storage policies for availability, durability and security of data that can meet various expectations on data resiliency and retention. The service can be delivered on a dedicated or a logically separated infrastructure within Tata Communications' data centers, and it provides flexibility to support real world workloads.

Customers can choose from three levels of the IZO™ Cloud Storage service, as shown in the table below:

	Value based	Resilient	Geo-resilient
Best suited for	Infrequently accessed data	Periodically accessed data	Highly critical data
Designed for fault tolerance	Within the data centre	Within the data centre	Across data centres

We offer managed cloud services to customers from our GSMC facility in Chennai. The Tata Communications' service operations team provides 24/7/365 monitoring and support for network intrusion detection and protection devices, across a variety of platforms and technologies. The team is made up of Level 1 (L1), Level 2 (L2) and Level 3 (L3) engineers who manage the day-to-day operations of GSMC, analysing and resolving any issues.

ISO/IEC STANDARDS

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) together form the specialised system for worldwide standardisation. National bodies that are members of ISO or IEC play a part in developing international standards by appearing on technical committees set up by either organisation to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organisations, both governmental and non-governmental, also work in liaison with ISO and IEC. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

(A) ISO/IEC 20000-1:2011

What is ISO/IEC 20000-1:2011?

The ISO/IEC 20000-1:2011 is the international best practice standard for ITSM. All requirements in ISO/IEC 20000 are generic and applicable to all service providers, irrespective of the size, type or nature of the services that are delivered.

Why is ISO/IEC 20000-1:2011 required?

This standard enables organisations to benchmark the delivery of managed services, while also assessing performance levels and measuring any given SLAs. This standard of service management systems is broadly based on ITIL set processes. ISO/IEC 20000s is made up of several parts, with the first part providing requirements for ITSM. In the main, this is aimed at professionals who are responsible for initiating, implementing or maintaining ITSM, thereby providing specifications for Service management systems (SMS) in their organisation. Organisations can have their ITSM independently certified to show that they adhere to the standards of ISO/IEC 20000-1:2011. Certification enables managed services organisations to prove to clients that their IT environments will be well managed, while also enabling outsourcing organisations to assure their clients that they will receive high-quality IT services.

Is Tata Communications ISO/IEC 20000-1:2011-certified?

Tata Communications' ISO/IEC 20000-1:2011 certification reflects the fact that we have met a number of key requirements, including successful implementation of documentation and records management; a customer-first approach; and the establishment of well-defined policy, planning and implementation.

The certification covers a range of specifications, including requirements for a management system, planning and implementing of services, service delivery process, relationship processes, control processes, resolution processes, and release process.

(B) ISO/IEC 20000-9:2015

What is ISO/IEC 20000-9:2015?

ISO 20000-9:2015 is part of a series of standards relating to information technology. It provides recommendations for enterprises that are delivering cloud services on how to use ISO/IEC 20000-1:2011.

Why is ISO/IEC 20000-9:2015 required?

The guidance provided by ISO/IEC 20000-9:2015 is designed to be used by cloud service providers across various deployment models, including private, public, hybrid and community cloud. The information may well also be useful for customers who are subscribing to cloud services to host their workloads. The Standard of ISO/IEC Technical Rule 20000-9 could be implemented and certified alongside the Base Standard ISO/IEC 20000-1 for IT Service Management.

This guidance is represented as a set of 15 different scenarios that addresses the various activities taking place in the life cycle of a cloud service. Each of the scenarios listed below refers to the applicable requirements as specified by ISO/IEC 20000-1.

S01	Identify the context for service management of cloud services
S02	Establish strategy and plan for management of cloud services
S03	Provide a catalogue of cloud services
S04	Identify and manage service requirements for cloud services
S05	Design and develop a new cloud service
S06	Establish a service relationship with the cloud customer
S07	Establish a cloud service agreement
S08	Onboarding the customer
S09	Deliver and operate cloud services
S10	Monitor and report cloud services
S11	Manage resources for cloud services
S12	Check and improve the SMS and cloud services
S13	Terminate a cloud service contract
S14	Transfer a cloud service
S15	Remove a cloud service

Is Tata Communications ISO/TR 20000-9:2015-certified?

Tata Communications has achieved ISO/TR 20000-9: 2015 certification of Information Security Management System (ISMS) for the delivery of managed cloud services – IZO™ Private Cloud and IZO™ Cloud Storage by GSMC.

Tata Communications - ISO/IEC 27017: 2015 in-scope services:

IZO™ Private Cloud and IZO™ Cloud Storage	In-scope services
Compute	Cloud services, virtual services, auto scaling
Network	VPN gateway, load balancer, switches, router, WAF, firewall, NFV
Storage / backup	Block, file and ICS (object) backup Scheduled data backup and data restoration
Database	Managed Oracle, MS-SQL, DB2 or MySQL database administration
Middleware	Managed middleware service is offered on applications including JBoss, Tomcat and Apache Application maintenance
Hypervisor	VMware, Hyper-V and KVM
Load balancer	Static, dynamic, persistence : NFV-virtual appliance; physical appliance
Security	SIEM, DDoS detection and mitigation, firewall monitoring and management, WAF, UTM and network-based vUTM - SIGS, managed and monitoring IDS/IPS, OAuth

For more information, visit us at www.tatacommunications.com

(C) ISO/IEC 27001:2013

What is ISO 27001: 2013?

ISO 27001: 2013 is an international standard for information security management systems (ISMS) best practice and provides a general overview of what an organisation should do to implement information security.

The standard specifies the requirements for establishing, implementing, operating, monitoring and continually improving ISMS for any entity, irrespective of its size.

Why is ISO/IEC 27001: 2013 required?

The standard regulates part of the ISMS implementation process, stating that:

- All activities should follow the purpose and process of information security that are clearly defined and documented in policies or procedures
- Processes to verify all information security system elements through audit and reviews must be in place to ensure continuous improvement
- Any security measurements that are being used in the ISMS following risk analysis should be implemented to eliminate or reduce the level of risks to acceptable levels
- There must be security controls in place that can be used during the implementation based on specific needs.

Description	No. of controls
Context of the organisation	8
Leadership	19
Planning	39
Support	28
Operation	9
Performance evaluation	29
Improvement	16
Total management controls	**148**
Management direction for information security	2
Organisation of information security	7
Human resource security	6
Asset management	10
Access control	13
Cryptography	2
Physical and environmental security	15
Operation security	14
Communications security	7
System acquisition, development and maintenance	13
Supplier relationships	5
Information security incident management	7
Information security aspects of business continuity management	4
Compliance	8
Total operational controls	**113**
Total control points	**261**

Is Tata Communications ISO/IEC 27001: 2013-certified?

Tata Communications has achieved ISO/IEC 27001: 2013 certification of information security management system (ISMS), which covers our infrastructure, data centres and services. These standards will be valuable to customers, who can now benefit from enhanced quality and information security standards.

Tata Communications - ISO/IEC 20000-1:2011 and TCL-ISO/IEC 27001: 2013 covers a wide range of services, including:

- Data centre services
- Managed hosting services
- Managed security services
- Managed cloud services
- Cloud security services
- Security consulting services
- Storage and backup services

Managed hosting services	In-scope services
Operating system	Microsoft Windows, RHEL, OEL, Solaris, IBM-AIX, SUSE Linux, Debian Linux, Ubuntu Linux, Cent OS, Fedora
Network	VPN gateway, load balancer, switches, router
Storage / backup	Shared and dedicated models, SAN, NAS and FC / iSCSI
Database	Oracle, MS-SQL, DB2 or MySQL database administration

For more information, visit us at www.tatacommunications.com

Managed hosting services	In-scope services
Middleware	Middleware service is offered on applications including JBoss, Tomcat, Apache, WebLogic, WebSphere
Load balancer	Static, dynamic, persistent: Radware, Citrix, SLB and GSLB, mSLB and mSLB with SSL off-load
Security	SIEM, DDoS detection and mitigation, firewall monitoring and management, WAF, UTM and network-based vUTM - SIGS, managed and monitoring IDS / IPS, OAuth

IZO™ Private Cloud	In-scope services
Compute	Cloud services, virtual services, auto scaling
Network	VPN gateway, load balancer, switches, router, WAF, firewall, NFV
Storage / backup	Block, file and ICS (object) backup Scheduled data backup and data restoration
Database	Managed Oracle, MS-SQL, DB2 or MySQL database administration
Middleware	Managed middleware service is offered on applications including JBoss, Tomcat, Apache Application maintenance
Hypervisor	VMware, Hyper-V and KVM
Load balancer	Static, dynamic, persistence: NFV-virtual appliance, physical appliance
Security	SIEM, DDoS detection and mitigation, firewall monitoring and management, WAF, UTM and network based vUTM - SIGS, managed and monitoring IDS / IPS, OAuth

(D) ISO/IEC 27017:2015

What is ISO 27017: 2015?

The standard of ISO 27017:2015 stipulates guidelines for controls specific to information security that should be taken into account during the provisioning and deployment of cloud services. The standard is relevant for both cloud service providers and the service consumers.

There are two types of guidance provided:

1. Separate guidance for cloud service providers and the service consumers
2. Matching guidance for cloud service providers and the service consumers

Why is ISO/IEC 27017: 2015 required?

The standard provides supplementary recommendations to the control lists specified in ISO/IEC 27002 that address information security threats and risk considerations. Whereas ISO/IEC 27002 is intended to mitigate the risks that accompany the technical and operational features of cloud services, ISO/IEC 27017 is specific to cloud services themselves.

This control list is made up of 14 operational controls, ranging from management direction for information security, through to information security in business continuity management and compliance.

The additional list of controls include:

Description	Controls
Relationship between cloud service customer and cloud service provider	Shared roles and responsibilities within a cloud computing environment
Responsibility for assets	Removal of cloud service customer assets
Access control of cloud service customer data in shared virtual environment	Segregation in virtual computing environments Virtual machine hardening
Operational procedures and responsibilities	Administrator's operational security
Logging and monitoring	Monitoring of cloud services
Network security management	Alignment of security management for virtual and physical networks

Is Tata Communications' ISO/IEC 27017: 2015-certified?

Tata Communications has achieved ISO/IEC 27017: 2015 certification of information security management systems (ISMS) for the delivery of managed cloud services – IZO™ Private Cloud and IZO™ Cloud Storage by GSMC.

For more information, visit us at www.tatacommunications.com

Tata Communications - ISO/IEC 27017: 2015 in-scope services:

IZO™ Private Cloud and IZO™ Cloud Storage	In-scope services
Compute	Cloud services, virtual services, auto scaling
Network	VPN gateway, load balancer, switches, router, WAF, firewall, NFV
Storage / backup	Block, file and ICS (object) backup Scheduled data backup and data restoration
Database	Managed Oracle, MS-SQL, DB2 or MySQL database administration
Middleware	Managed middleware service is offered on applications including JBoss, Tomcat, Apache Application maintenance
Hypervisor	VMware, Hyper-V and KVM
Load balancer	Static, dynamic, persistence : NFV-virtual appliance; physical appliance
Security	SIEM, DDoS detection and mitigation, firewall monitoring and management, WAF, UTM and network-based vUTM - SIGS, managed and monitoring IDS / IPS, OAuth

(E) ISO/IEC 27018:2014

What is ISO 27018: 2014?

This standard is designed to be a reference for selecting PII protection controls when implementing a cloud computing ISMS based on ISO/IEC 27001, or as a guide for implementing commonly accepted PII protection controls for CSPs. This international standard is based on ISO/IEC 27002, and takes into consideration the specific risks arising from PII protection that any CSPs acting as PII processors might face.

Why is ISO/IEC 27018: 2014 required?

CSPs who process personally identifiable information (PII) under contract to their customers have to operate in a way that allows both contracting parties to adhere to the requirements of legislation that governs how PII is allowed to be processed. In other words, how it is collected, used, transferred and disposed of. This is sometimes referred to as data protection legislation.

- A cloud service provider is a 'PII processor'
- The cloud service customer can be an individual person, known as a 'PII principal'
- The customer can also be an organisation, known as a 'PII controller', processing PII relating to many PII principals

The additional list of controls include:

Description	Controls
Consent and choice	Obligation to co-operate regarding PII principals' rights
Purpose legitimacy and specification	Public cloud PII processor's purpose
	Public cloud PII processor's commercial use
Data minimisation	Secure erasure of temporary files
Use, retention and disclosure limitation	PII disclosure notification
Openness, transparency and notice	Disclosure of sub-contracted PII processing
Accountability	Notification of a data breach involving PII
	Retention period for administrative security policies and guidelines
	PII return, transfer and disposal
Information security	Confidentiality or non-disclosure agreements
	Restriction of the creation of hardcopy material
	Control and logging of data restoration
	Protecting data on storage media leaving the premises
	Use of unencrypted portable storage media and devices
	Encryption of PII transmitted over public data-transmission networks
	Secure disposal of hardcopy materials
	Unique use of user IDs
	Records of authorised users
	User ID management
	Contract measures
	Sub-contracted PII processing
	Access to data on pre-used data storage space
Privacy compliance	Geographical location of PII
	Intended destination of PII

For more information, visit us at www.tatacommunications.com

Is Tata Communications ISO/IEC 27018: 2014-certified?

Tata Communications has achieved ISO/IEC 27017: 2015 certification of information security management system (ISMS) for protection of PII (personally identifiable information) processed by GSMC for managed cloud services – IZO™ Private Cloud and IZO™ Cloud Storage.

Tata Communications - ISO/IEC 27018: 2014 in-scope services:

IZO™ Private Cloud and IZO™ Cloud Storage	In-scope services
Compute	Cloud services, virtual services, auto scaling
Network	VPN gateway, load balancer, switches, router, WAF, firewall, NFV
Storage / backup	Block, file and ICS (object) backup
Scheduled data backup and data restoration	Managed Oracle, MS-SQL, DB2 or MySQL database administration
Database	Managed Oracle, MS-SQL, DB2 or MySQL database administration
Middleware	Managed middleware service is offered on applications including JBoss, Tomcat, Apache Application maintenance
Hypervisor	VMware, Hyper-V and KVM
Load balancer	Static, dynamic, persistence: NFV-virtual appliance; physical appliance
Security	SIEM, DDoS detection and mitigation, firewall monitoring and management, WAF, UTM and network based vUTM - SIGS, managed and monitoring IDS / IPS, OAuth

SOC 1

What is SOC 1 compliance?

SOC 1 is a report on controls in a service organisation that are relevant to a user entity's internal financial reporting control. It enables the user auditor to perform risk assessment procedures, and if a type 2 report is provided, to assess the risk of material misstatement of financial statement assertions affected by the service organisation's processing.

Why is SOC 1 compliance required?

According to the American Institute of CPAs (AICPA), all service organisation reports ensure that those organisations "That operate information systems and provide information system services to other entities, build trust and confidence in their service delivery processes and controls through a report by an independent Certified Public Accountant." Customers will periodically need to comply with audit requests that come from external accounting firms, so the results of SOC testing can help those audits run more smoothly.

Is Tata Communications SOC 1-compliant?

Tata Communications is committed to SOC 1 standard for its managed hosting services.

Managed hosting services	In-scope services
Operating system	Microsoft Windows, RHEL, OEL, Solaris, IBM-AIX, SUSE Linux, Debian Linux, Ubuntu Linux, Cent OS, Fedora
Network	VPN gateway, load balancer, switches, router
Storage / backup	Shared and dedicated models, SAN, NAS and FC / iSCSI
Database	Oracle, MS-SQL, DB2 or MySQL database administration
Middleware	Middleware service is offered on applications including JBoss, Tomcat, Apache, WebLogic, WebSphere
Load Balancer	Static, dynamic, persistent: Radware, Citrix, SLB and GSLB, mSLB and mSLB with SSL off-load
Security	SIEM, DDoS detection and mitigation, firewall monitoring and management, WAF, UTM and network based vUTM - SIGS, managed and monitoring IDS / IPS, OAuth

SOC 2

What is SOC 2 compliance?

The increased awareness and adoption of cloud technology mean that organisations and CSPs are seeking to provide assurances about the management and security of sensitive data. To satisfy stakeholders' demands for effective internal controls that address touchpoints affecting information security, AICPA has developed the Service Organization Control (SOC) reporting framework. To support its risk assessments, user entities and business partners may request a SOC 2® report from the service organisation.

For more information, visit us at www.tatacommunications.com

Why is SOC 2 compliance required?

SOC 2 reports enable cloud providers to communicate details about their services and the appropriate fit of the blueprint and operating efficiency of their controls. They are particularly useful for organisations that need to demonstrate:

- How they process transactions and / or data on behalf of their customers
- How their security controls operate
- How their controls related to system availability function
- How their controls related to data privacy or confidentiality operate.

Organisations are not required to assess performance against all five Trust Services principles (TSPSs). Cloud providers may select those that best meet their reporting objectives.

Description criteria:

The description criteria are used by management when preparing the description of the service organisation's system and by the service auditor when evaluating the description.

Trust Services criteria:

The service organisation evaluates if the design and operating effectiveness of controls provides reasonable assurance that its service commitments and system requirements have been achieved, based on the Trust Services criteria relevant to the Trust Services category or the categories included within the scope of the examination.

There are five categories of Trust Services criteria:

Relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy.

Is Tata Communications SOC 2-compliant?

Tata Communications is committed to SOC 2 standards for its managed cloud services.

Managed Cloud Services: IPC (IZO™ Private Cloud) is an enterprise cloud platform, offering a flexible, scalable and reliable cloud environment. It allows end-users to create the appropriate combination of compute, network, security, storage and traffic management services that can meet business needs and have the flexibility to grow with a business.

The IPC service is available on two models within Tata Communications' data centres. It includes Virtual Private Cloud (VPC), Dedicated Private Cloud (DPC) and Virtual Private Data Centre (VPDC). MCS services are offered to customers from the GSMC facility in Chennai. The Tata Communications' Service Operations Team provides 24/7/365 monitoring and support for network intrusion detection and protection devices across a variety of platforms and technologies. The team consists of Level 1 (L1), Level 2 (L2) and Level 3 (L3) engineers who manage the day to day operations of GSMC, and analyse and resolve any issues. The Operations Engineering Team consists of competency leads, who are also referred to as technology leads.

The service organisation controls and procedures cover the objectives for:

- Information security
- Access security
- Physical security
- Facilities and equipment security
- Incident management
- Problem management
- Change management
- Backup and restoration
- Managing third party services
- Software licensing
- Managing operations
- Human resources

For more information, visit us at www.tatacommunications.com

IZO™ Private Cloud	In-scope services
Compute	Cloud services, virtual services, auto scaling
Network	VPN gateway, load balancer, switches, router, WAF, firewall, NFV
Storage / backup	Block, file and ICS (object) backup Scheduled data backup and data restoration
Database	Managed Oracle, MS-SQL, DB2 or MySQL database administration
Middleware	Managed middleware service is offered on applications including JBoss, Tomcat, Apache Application maintenance
Hypervisor	VMware, Hyper-V and KVM
Load balancer	Static, dynamic, persistence : NFV-virtual appliance; physical appliance
Security	SIEM, DDoS detection and mitigation, firewall monitoring and management, WAF, UTM and network-based vUTM - SIGS, managed and monitoring IDS / IPS, OAuth

Multi-Tier Cloud Security (MTCS) Level 3 certification

What is Multi-Tier Cloud Security?

When organisations outsource IT services to the cloud, they need enhanced controls to be in place to address any new or greater risks that might arise.

MTCS is based on the ISO 27001/02 Information Security Management System standards. The certification was prepared by the Multi-Tiered Cloud Security Working Group of the Cloud Computing Standards Coordinating Task Force. It was overseen by the Information Technology Standards Committee (ITSC).

Why does an organisation need to adopt Multi-Tier Cloud Security?

Multi-Tier Cloud Security (MTCS) is a pioneering security standard that is globally recognised, ensuring cloud security across several layers. The standard encourages the general adoption of cloud computing across various industry sectors by providing detailed security service levels of cloud service providers. With Level 1 being the basic standard and Level 3 being the most stringent, MTCS is designed for companies with regulatory compliance requirements, addressing any security risks to high impact IT systems that use cloud services.

With the generic safety controls introduced by MTCS now in place, we may well see the introduction of supplementary regulations that address security risks and threats in particular industries.

MTCS has a self-disclosure requirement. This means that providers are obliged to report on data retention, data sovereignty, data portability, liability, availability, business continuity, disaster recovery and incident management.

Is Tata Communications MTCS-certified?

Tata Communications has achieved Level 3 MTCS certification. This ensures the highest possible level of security for enterprises moving data to the cloud in Singapore, and supports the provision of IZO™ Private Cloud and VPDC cloud services using an Infrastructure as a Service (IaaS) model.

Cloud governance	• Information security management • Human resources • Risk management • Third party • Legal and compliance • Incident management • Data governance
Cloud infrastructure security	• Audit logging and monitoring • Secure configuration • Security testing and monitoring • System acquisition and development • Encryption
Cloud operations management	• Physical and environment security • Operations • Change management • Business continuity planning and disaster recovery
Cloud information security	• Cloud services administration • Cloud user access • Tenancy and customer isolation

For more information, visit us at www.tatacommunications.com

IZO™ Private Cloud	In-scope services
Compute	Cloud services, virtual services, auto scaling
Network	VPN gateway, load balancer, switches, router, WAF, direwall, NFV
Storage / backup	Block, file and ICS (object) backup Scheduled data backup and data restoration
Database	Managed Oracle, MS-SQL, DB2 or MySQL database administration
Middleware	Managed middleware service is offered on applications including JBoss, Tomcat, Apache Application maintenance
Hypervisor	VMware, Hyper-V and KVM
Load balancer	Static, dynamic, persistence : NFV-virtual appliance; physical appliance
Security	SIEM, DDoS detection and mitigation, firewall monitoring and management, WAF, UTM and network based vUTM - SIGS, managed and monitoring IDS / IPS, OAuth

Cloud Security Alliance – CSA STAR

What Is the Cloud Security Alliance?

The Cloud Security Alliance is a pioneering organisation that aims to promote and encourage the adoption of best practices to ensure a secure cloud computing environment.

Introduced by the CSA, STAR certification covers key principles of transparency, auditing and harmonisation of standards. The certification brings organisations a number of benefits, including the chance to assess their cloud technology against industry-established best practices and validate their security position.

How does the CSA help cloud security?

The Cloud Security Alliance has created the Cloud Controls Matrix (CCM) which is a baseline set of security controls to help enterprises assess the risks associated by appointing a cloud computing provider. CCM v3.0.1 is available as a free download to encourage best practice for encrypting data in storage, data in transit and key management.

Domains of the Cloud Control Matrix:

There are 16 domains identified in the CCM and Tata Communications has complied with the 133 controls of all 16 domains. They are:

Domain name	No. of Controls
Application and Interface Security; Application Security	4
Audit Assurance and Compliance; Audit Planning	3
Business Continuity Management and Operational Resilience; Business Continuity Planning	11
Change Control and Configuration Management; New Development / Acquisition	5
Data Security and Information Lifecycle Management Classification	7
Datacenter Security; Asset Management	9
Encryption and Key Management Entitlement	4
Governance and Risk Management; Baseline Requirements	11
Human Resources; Asset Returns	11
Identity and Access Management; Audit Tools Access	13
Infrastructure and Virtualisation Security; Audit Logging / Intrusion Detection	13
Interoperability and Portability; APIs	5
Mobile Security; Anti-Malware	20
Security Incident Management, E-Discovery and Cloud Forensics Contact / Authority Maintenance	5
Supply Chain Management, Transparency and Accountability Data Quality and Integrity	9
Threat and Vulnerability Management Anti-Virus / Malicious Software	3

Is Tata Communications aligned to CSA STAR?

CSA STAR Self-Assessment is open to all cloud technology players and allows them to submit self-assessment reports that record organisations' adoption of and compliance with CSA-published best practices. CSA CCM is a framework that provides organisations with structure, detail and precision relating to information security exercises that are tailormade for the cloud industry.

To show Tata Communications' compliance with CSA best practices, we have submitted the Cloud Controls Matrix (CCM). The matrix provides a controls framework, with detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains.

For more information, visit us at www.tatacommunications.com

PCI DSS

What is PCI DSS?

The Payment Card Industry Security Standards Council is a global, open body founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

The Payment Card Industry Data Security Standard (PCI DSS) ensures that organisations that accept or process payment transactions incorporate a set of operational and technical requirements in order to help protect the safety of that data. The developed framework aims to minimise payment data security breaches and fraud in any organisations that possess Cardholder Data (CHD). The standard applies to software developers and manufacturers of applications and devices used in those transactions.

How does it apply to cloud computing?

The PCI DSS provides a detailed structure of 12 requirements for securing cardholder data that is stored, processed and / or transmitted by merchants and other organisations.

Goals	Requirement	Controls
Build and maintain a secure network and systems	1. Install and maintain a firewall configuration to protect cardholder data	19
	2. Do not use vendor-supplied defaults for system passwords and other security parameters	10
Protect cardholder data	3. Protect stored cardholder data	19
	4. Encrypt transmission of cardholder data across open, public networks	3
Maintain a vulnerability management programme	5. Protect all systems against malware and regularly update anti-virus software	5
	6. Develop and maintain secure systems and applications	25
Implement strong access control measures	7. Restrict access to cardholder data on a need to know basis	8
	8. Identify and authenticate access to system components	21
	9. Restrict physical access to cardholder data	20
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data	28
	11. Regularly test security systems and processes	12
Maintain an information security policy	12. Maintain a policy that addresses information security for all personnel	34

System components include network devices (both wired and wireless), servers and applications. Virtualisation components and the subset of system components include VMs, virtual switches / routers, appliances, applications / desktops and hypervisors within PCI DSS.

Even if a cloud service provider's environment is vetted for certain PCI DSS requirements, any validation does not automatically apply to the customer environments within that cloud service.

Is Tata Communications PCI DSS-compliant?

Tata Communications is a service provider focusing on Infrastructure as Service (IaaS) where hardware and network infrastructure are assessed. We do not directly store, transmit or process any cardholder data (CHD) and sensitive authentication data (SAD). However, Tata Communications' customers may set up their own data environment which can be considered as CDE, with tools and configuration that can store, transmit or process cardholder data.

All processing, transmission, storage and protection of customers' data (including CHD) is not the responsibility of Tata Communications, as we do not have authorisation to access a customer's premises. Neither is it our responsibility to provide tools for customers to meet PCI DSS compliance .

The following services are covered under the infrastructure environment:

NTP	AV	VPN	SysLog
Monitoring	DHCP	DNS	FIM
AD	Patch management	VCenter	Proxy

HIPAA

What is HIPAA?

Healthcare is a highly regulated environment, and the nature of cloud computing infrastructure escalates concerns over privacy, security, access and compliance. In the 1990s, the U.S. Congress recognised that advances in electronic technology could erode the privacy of health information. To protect such information, the United States of America enacted the Health Insurance Portability Accountability Act of 1996 (HIPAA). It is the first comprehensive federal protection for the privacy of personal health information.

How does it affect cloud computing?

The HIPAA Privacy, Security, and Breach Notification Rules (HIPAA Rules) define crucial rules for individually identifiable health information. This information is called protected health information or PHI.

A covered entity is a health plan, a health care clearing house, or health care program that electronically transmits any health information. When this covered entity engages the services of a cloud services provider (CSP) to create, receive, maintain or transmit ePHI (such as to process and / or store ePHI) on its behalf, the CSP is a business associate under HIPAA. The covered entity (or business associate) and the CSP must enter into a HIPAA-compliant business associate agreement (BAA), and the CSP is both contractually liable for meeting the terms of the BAA and directly liable for compliance with the applicable requirements of the HIPAA Rules.

Hosting an application in compliance with HIPAA-HITECH Rules is a shared responsibility between the customer and Tata Communications. Both parties must sign a business associate agreement (BAA), which clearly defines their respective responsibilities.

What is HITECH?

Health Information Technology for Economic and Clinical Health Act (HITECH) expanded the HIPAA rules in 2009. HIPAA and HITECH together established a set of federal standards intended to protect the security and privacy of PHI. These provisions are included in what are known as the 'administrative simplification' rules. HIPAA and HITECH impose requirements related to the use and disclosure of PHI, appropriate safeguards to protect PHI, individual rights, and administrative responsibilities.

What are the HIPAA rules?

- The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity.
- The HIPAA Privacy Rule provides federal protection for personal health information held by covered entities and gives patients an array of rights with respect to that information.
- The HIPAA Breach Notification Rule requires HIPAA-covered entities and their business associates to provide notification following a breach of unsecured protected health information.

Is Tata Communications HIPAA-compliant?

The scope of HIPAA compliance includes managed hosting services offered by Tata Communications. Tata Communications' Managed Hosting Service has been assessed to be compliant with the control requirements in alignment with the HIPAA Final Omnibus Rule pertaining to the HIPAA Security Rule, HIPAA Privacy Rule and HIPAA Breach Notification Rule.

The Security Rule specifies a series of administrative, technical and physical security procedures for covered entities to use to assure confidentiality, integrity and availability.

Description	No. of controls
Administrative safeguards	24
Physical safeguards	7
Technical safeguards	8

Tata Communications-HIPAA in-scope services:

Managed hosting services (MHS)

- Managed Server
- Managed Operating System
- Managed Storage
- Managed Switch
- Managed Firewall
- Managed Backup
- Managed Load Balancer

For more information, visit us at www.tatacommunications.com

- Managed Database
- Managed Middleware
- Managed Virtualisation
- Managed Disaster Recovery (DR)

Managed Hosting Services	In-scope services
Operating system	Microsoft Windows, RHEL, OEL, Solaris, IBM-AIX, SUSE Linux, Debian Linux, Ubuntu Linux, Cent OS, Fedora
Network	VPN gateway, load balancer, switches, router
Storage / backup	Shared and dedicated models, SAN, NAS and FC / iSCSI
Database	Oracle, MS-SQL, DB2 or MySQL database administration
Middleware	Middleware service is offered on applications including JBOSS; TOMCAT; Apache; WebLogic; WebSphere
Load balancer	Static, dynamic, persistent: Radware, Citrix, SLB and GSLB, mSLB, and mSLB with SSL off-load
Security	SIEM, DDoS detection and mitigation, firewall monitoring and management, WAF, UTM and network based vUTM - SIGS, managed and monitoring IDS / IPS, OAuth

GDPR

What is GDPR?

The European Union (EU) has generally enforced stricter rules on data protection than those implemented elsewhere, but by 2018 its Data Protection Directive had become outdated. The Directive did not address the many ways in which data is now stored, collected and transferred. This led to the formation of the new EU General Data Protection Regulation (GDPR). GDPR came into effect on 25 May, 2018, with a two-fold objective. The first was to give EU residents more control over the use of their personal data. By strengthening data protection legislation and introducing stricter enforcement measures, the EU hoped to improve trust in the emerging digital economy. Secondly, the EU wanted to give businesses a simpler, more transparent legal environment to operate within.

GDPR compliance is required by all organisations who:

- Are operating in an EU country
- Process the personal data of European residents
- Have 250 employees or more
- Have fewer than 250 employees but use data-processing that affect the rights and freedoms of data subjects. This is not just on an occasional basis, and may include certain types of sensitive personal data. In effect, this means almost all organisations.

Is Tata Communications GDPR-compliant?

Tata Communications is committed to GDPR compliance across cloud services. We are also committed to helping our customers on their GDPR compliance journey by building robust privacy and security protection into our services. Our cloud and hosting solutions already have specific features and services that ensure compliance with GDPR:

- Access management
- Authentication management
- Network management
- Dashboard view of activities across resources
- Data encryption
- Data governance

Shared responsibility model:

Both the customer organisation and Tata Communications have essential roles in meeting GDPR compliance. Organisations are directly responsible for their applications and data, including data access and encryption. At the same time, partners such as Tata Communications are responsible for the underlying infrastructure, physical access control and operational security.

German Bundesdatenschutzgesetz (BDSG)

What is BDSG?

On February 1, 2017, the German federal cabinet adopted a draft data protection bill ('New BDSG') to replace the existing Federal Data Protection Act of 2003. The new BDSG is intended to adapt the current German data protection law to the EU General Data Protection Regulation ('GDPR').

The planned implementation statute aims to supplement and further define the EU General Data Protection Regulation. The new BDSG includes specific requirements that deviate from the GDPR in some respects, including the appointment of a Data Protection Officer and the processing of employees' personal data.

Is Tata Communications BDSG-compliant?

Companies operating in Germany should analyse the BDSG requirements and make sure that their German operations are fully compliant.

The scope of Tata Communications' BDSG assessment is limited to the privacy and information security requirements of IPC and ICS services and their supporting infrastructure that are applicable to a data processor. We have also assessed the controls related to physical security and the environmental safeguards of our command centres.

Control type	No. of controls
Data privacy	9
Technical and organisational control	43

IZO™ Private Cloud	In-scope services
Compute	Cloud services, virtual services, auto scaling
Network	VPN gateway, load balancer, switches, router, WAF, firewall, NFV
Storage / backup	Block, file and ICS (object) backup Scheduled data backup and data restoration
Database	Managed Oracle, MS-SQL, DB2 or MySQL database administration
Middleware	Managed middleware service is offered on applications including JBoss, Tomcat, Apache Application maintenance
Hypervisor	VMware, Hyper-V and KVM
Load balancer	Static, dynamic, persistence : NFV-virtual appliance; physical appliance
Security	SIEM, DDoS detection and mitigation, firewall monitoring and management, WAF, UTM and network based vUTM - SIGS, managed and monitoring IDS / IPS, OAuth

MeitY

What is MeitY?

Digital India envisages creating high-speed digital highways. These will usher in a new era for banking and introduce a transparent system to support e-governance, digital signatures, digital-friendly entrepreneurship and more – all aimed at encouraging inclusive growth.

To build the vital framework needed for this transformation journey, India's Ministry of Electronics and Information Technology (MeitY) has panelled a number of cloud service providers (CSPs) for Digital India initiatives using strict selection criteria.

Requirement	Criteria
Service provisioning	10
SLA management	4
Operational management	12
Data management	8
User / admin portal	3
Integration requirements	12
Data centre facilities	10
Cloud storage service	6
Virtual machine	30
Disaster recovery and business continuity	8
Security	36
Legal compliance	8
Management reporting	8
Exit management and transition	7
Backup services	10

Is Tata Communications MeitY-accredited?

Tata Communications is one of the global cloud service providers to achieve MeitY's accreditation. With this accreditation, Tata Communications can deliver cloud services in India, providing truly innovative digital services to a wider range of organisations, many of them regulated and sensitive. This accreditation also empowers us to approach central, state and local governments, as well as public sector bodies in India, to offer e-governance services as their core service proposition.

For more information, visit us at www.tatacommunications.com

The accreditation includes IZO™ Private Cloud, IZO™ Cloud Storage and Government Community Cloud.

IZO™ Private Cloud	In-scope services
Compute	Cloud services, virtual services, auto scaling
Network	VPN gateway, load balancer, switches, router, WAF, firewall, NFV
Storage / backup	Block, file and ICS (object) backup Scheduled data backup and data restoration
Database	Managed Oracle, MS-SQL, DB2 or MySQL database administration
Middleware	Managed middleware service is offered on applications including JBoss, Tomcat, Apache Application maintenance
Hypervisor	VMware, Hyper-V and KVM
Load balancer	Static, dynamic, persistence : NFV-virtual appliance; physical appliance
Security	SIEM, DDoS detection and mitigation, firewall monitoring and management, WAF, UTM and network based vUTM - SIGS, managed and monitoring IDS / IPS, OAuth

Reference and Sources

https://www.iso.org/obp/ui/#home

https://www.iso.org/obp/ui/#iso:std:iso-iec:20000:-1:ed-2:v1:en

https://www.iso.org/isoiec-27001-information-security.html

https://www.iso.org/standard/43757.html

https://www.iso.org/standard/61498.html

https://www.iso.org/standard/65671.html

https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html

https://www.ssae-16.com/soc-1/

https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html

https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/comparision-soc-1-3.pdf

https://www.imda.gov.sg/

https://www.imda.gov.sg/industry-development/infrastructure/ict-standards-and-frameworks/mtcs-certification-scheme/multi-tier-cloud-security-certified-cloud-services

https://www.imda.gov.sg/industry-development/infrastructure/ict-standards-and-frameworks/mtcs-certification-scheme

https://cloudsecurityalliance.org/

https://cloudsecurityalliance.org/star/certification/#_overview

https://www.pcisecuritystandards.org/

https://www.hhs.gov/

https://www.hhs.gov/hipaa/index.html

https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html

https://gdpr-info.eu/

https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html

http://meity.gov.in/

http://meity.gov.in/content/gi-cloud-meghraj

For more information, visit us at www.tatacommunications.com

Contact us

ABOUT TATA COMMUNICATIONS

Tata Communications Limited (CIN no: L64200MH1986PLC039266) along with its subsidiaries (Tata Communications) is a leading global provider of A New World of Communications™. With a leadership position in emerging markets, Tata Communications leverages its advanced solutions capabilities and domain expertise across its global and pan-India network to deliver managed solutions to multinational enterprises, service providers and Indian consumers.

The Tata Communications global network includes one of the most advanced and largest submarine cable networks and a Tier-1 IP network, as well as nearly 1.5 million sq. ft. of data centre and collocation space worldwide.

Tata Communications' depth and breadth of reach in emerging markets includes leadership in Indian enterprise data services and leadership in global international voice.

Tata Communications Limited is listed on the Bombay Stock Exchange and the National Stock Exchange of India.

TATA COMMUNICATIONS