NTT Global Data Centers & Cloud Infrastructure India Private Limited (NTT GDC & CI)

System and Organization Control (SOC) 2 Type 2 Report

Description of NTT GDC & CI's Hosting Services, Managed Services and certain related Information Technology General Controls relevant to the Trust Services Categories of Security, Availability, and Confidentiality

For the period 01 January 2024 through 31 December 2024

Delivery Centers located in Mumbai, Navi Mumbai, Chennai, Noida and Bengaluru.

Table of Contents

Section 1 - NTT Global Data Centers & Cloud Infrastructure India Private Limited's Management Assertion

NTT Global Data Centers & Cloud Infrastructure India Private Limited
Registered office - Lighthall 'C' Wing, Hiranandani Business Park, Saki Vihar Road, Chandivali, Andheri (East), Mumbai - 400 072. India
Tel: +91 22 4009 9099
CIN: U72900MH2005PTC153896
Website: www.services.global.ntt

NTT Global Data Centers & Cloud Infrastructure India Private Limited's Management Assertion

04 April 2025

We have prepared the accompanying *Section 3 - Description of NTT GDC & CI's Hosting Services, Managed Services and certain related Information Technology General Controls relevant to the Trust Services Categories of Security, Availability, and Confidentiality for the period 01 January 2024 to 31 December 2024* (Description) of NTT Global Data Centers & Cloud Infrastructure India Private Limited (NTT GDC & CI) (Service Organization) in accordance with the criteria for a description of a Service Organization's system set forth in the Description Criteria DC section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (Description Criteria). The Description is intended to provide report users with information about the Hosting and Managed services (System) that may be useful when assessing the risks arising from interactions with the System, particularly information about system controls that the Service Organization has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria for security, availability, and confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

The Description also indicates Complementary User Organizations Controls that are suitably designed and operating effectively are necessary along with NTT GDC & CI's controls to achieve the service commitments and system requirements. The Description presents NTT GDC & CI's controls, and the Complementary User Organizations Controls assumed in the design of NTT GDC & CI's controls.

We confirm, to the best of our knowledge and belief, that:

a. The Description presents the System that was designed and implemented throughout the period 01 January 2024 to 31 December 2024 in accordance with the Description Criteria.

b. The controls stated in the Description were suitably designed throughout the period 01 January 2024 to 31 December 2024 to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively throughout that period and if User Organizations applied the Complementary User Organization Controls assumed in the design of NTT GDC & CI's controls throughout that period.

NTT Global Data Centers & Cloud Infrastructure India Private Limited
Registered office - Lighthall 'C' Wing, Hiranandani Business Park, Saki Vihar Road, Chandivali, Andheri (East), Mumbai - 400 072. India
Tel: +91 22 4009 9099
CIN: U72900MH2005PTC153896
Website: www.services.global.ntt

c. The NTT GDC & CI controls stated in the Description operated effectively throughout the period 01 January 2024 to 31 December 2024 to provide reasonable assurance that NTT GDC & CI's service commitments and system requirements were achieved based on the applicable trust services criteria, if Complementary User Organization Controls assumed in the design of NTT GDC & CI's controls operated throughout that period.

Very truly yours,

For NTT Global Data Centers & Cloud Infrastructure India Private Limited

BAJPAI ALOK
Digitally signed by BAJPAI ALOK
Date: 2025.04.04 12:19:10 +05'30'

Alok Bajpai
Managing Director

Section 2 - Independent Service Auditor's Report

Ernst & Young Associates LLP
The Ruby, 15th Floor,
29 Senapati Bapat Marg,
Dadar (West),
Mumbai - 400 028, India

Tel: +91 22 6192 0000
Fax: +91 22 6192 1000
www.ey.com

Independent Service Auditor's Report

To the Board of Directors of NTT Global Data Centers and Cloud Infrastructure India Private Limited

Scope

We have examined NTT Global Data Centers and Cloud Infrastructure India Private Limited's (NTT GDC & CI or Service Organization) accompanying "*Section 3 - Description of NTT GDC & CI's Hosting Services, Managed Services and certain related Information Technology General Controls relevant to the Trust Services Categories of Security, Availability, and Confidentiality for the period 01 January 2024 to 31 December 2024*" (Description) in accordance with the criteria for a description of a Service Organization's system set forth in the Description Criteria DC section 200 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (Description Criteria) and the suitability of the design and operating effectiveness of controls stated in the Description throughout the period 01 January 2024 to 31 December 2024 to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria for security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA Trust Services Criteria.

The Description indicates that NTT GDC & CI's controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if Complementary User Organization Controls assumed in the design of NTT GDC & CI controls are suitably designed and operating effectively, along with related controls at the Service Organization. Our examination did not extend to such Complementary User Organization Controls, and we have not evaluated the suitability of the design or operating effectiveness of such Complementary User Organization Controls.

NTT GDC & CI responsibilities

NTT GDC & CI is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that the service commitments and system requirements

were achieved. NTT GDC & CI has provided the accompanying assertion titled, *Section 1 - NTT Global Data Centers and Cloud Infrastructure India Private Limited's Management Assertion* (Assertion) about the presentation of the Description based on the Description Criteria and suitability of the design and operating effectiveness of the controls described therein to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria. NTT GDC &CI is responsible for (1) preparing the Description and Assertion; (2) the completeness, accuracy, and method of presentation of the Description and Assertion; (3) providing the services covered by the Description; (4) selecting the trust services categories addressed by the engagement and stating the applicable trust services criteria and related controls in the Description; (5) identifying the risks that threaten the achievement of the Service Organization's service commitments and system requirements; and (6) designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve its service commitments and system requirements.

Service Auditor's responsibilities

Our responsibility is to express an opinion on the presentation of the Description and on the suitability of the design and operating effectiveness of the controls described therein achieve the service organization's service commitments and system requirements based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the Description is presented in accordance with the Description Criteria, and (2) the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the Service Organization's service commitments and system requirements were achieved based on the applicable trust services criteria throughout the period 01 January 2024 to 31 December 2024. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a Service Organization's system and the suitability of the design and operating effectiveness of controls involves:

- obtaining an understanding of the system and the Service Organization's service commitments and system requirements

- assessing the risks that the Description is not presented in accordance with the Description Criteria and that controls were not suitably designed or operating effectively based on the applicable trust services criteria
- performing procedures to obtain evidence about whether the Description is presented in accordance with the Description Criteria
- performing procedures to obtain evidence about whether controls stated in the Description were suitably designed to provide reasonable assurance that the Service Organization achieved its service commitments and system requirements based on the applicable trust services criteria
- testing the operating effectiveness of those controls to provide reasonable assurance that the Service Organization's service commitments and system requirements were achieved based on the applicable trust services criteria.
- evaluating the overall presentation of the Description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent of NTT GDC & CI and to meet our other ethical responsibilities, in accordance with the relevant ethical requirements related to our examination engagement.

Inherent limitations

The Description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to its own particular needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls at a Service Organization may not always operate effectively to provide reasonable assurance that the Service Organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any evaluation of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria, is subject to the risk that the system may change or that controls at a Service Organization may become ineffective.

Description of tests of controls

The specific controls we tested, and the nature, timing, and results of those tests are listed in the accompanying *Section 4 - Description of Criteria, Controls, Tests, and Results of Tests* (Description of Tests and Results)

Opinion

In our opinion, in all material respects:

- the Description presents the Hosting and Managed Services system that was designed and implemented throughout the period 01 January 2024 to 31 December 2024 in accordance with the Description Criteria
- the controls stated in the Description were suitably designed throughout the period 01 January 2024 to 31 December 2024, to provide reasonable assurance that NTT GDC & CI's service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively throughout that period and if User Organizations applied the complementary controls assumed in the design of NTT GDC & CI's controls throughout that period.
- the controls stated in the Description operated effectively throughout the period 01 January 2024 to 31 December 2024 to provide reasonable assurance that NTT GDC & CI's service commitments and system requirements were achieved based on the applicable trust services criteria if the Complementary User Organization Controls assumed in the design of NTT GDC & CI's controls operated effectively throughout that period.

Restricted use

This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of NTT GDC & CI, User Organizations of NTT GDC & CI's Hosting and Managed Services system during some or all of the period 01 January 2024 to 31 December 2024 and prospective User Organizations, independent auditors and practitioners providing services to such User Organizations who have sufficient knowledge and understanding of the following:

- the nature of the service provided by the Service Organization
- how the Service Organization's system interacts with User Organizations or other parties
- internal control and its limitations

- Complementary User Organization Controls and how those controls interact with the controls at the Service Organization to achieve the Service Organization's service commitments and system requirements
- User Organizations responsibilities and how they interact with related controls at the Service Organization
- the applicable trust services criteria
- the risks that may threaten the achievement of the Service Organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

For Ernst and Young Associates LLP

Anuj Gupta

Partner, India

04 April 2025

Section 3 - Description of NTT GDC & CI's Hosting Services, Managed Services and certain related Information Technology General Controls relevant to the Trust Services Categories of Security, Availability, and Confidentiality for the period 01 January 2024 to 31 December 2024

Description of Systems provided by NTT GDC & CI India Private Limited

Overview of Operations

NTT Ltd. is a leading global technology services company. Working with organizations around the world, NTT Ltd. has achieved business outcomes through 'intelligent' technology solutions. For NTT Ltd., 'intelligent' means data driven, connected, digital and secure. through Integrated Circuit Technology (ICT), stack capabilities provide unique offerings in cloud-enabling networking, hybrid cloud, data centers, digital transformation, client experience, workplace and cybersecurity. As a global ICT provider, NTT Ltd. employs more than 40,000 people in a diverse and dynamic workplace that spans 57 countries, trading in 73 countries and delivering services in over 200 countries and regions.

About NTT Global Data Centers & Cloud Infrastructure India Private Limited

NTT Global Data Centers & Cloud Infrastructure India Private Limited (NTT GDC & CI), a wholly owned subsidiary of NTT Ltd., is one of India's leading Managed Hosting and Multi-Cloud Hybrid IT solution provider serving more than 2500 enterprises globally. Headquartered in Mumbai, NTT GDC & CI also delivers Remote Infrastructure Management (RIM) services to various enterprise customers globally across Americas, Europe and Asia-Pacific region. The Company was the first in India to launch services such as Cloud Computing, Managed Security, Disaster Recovery-as-a-Service (DRaaS) and Software-Defined Storage.

Industry and Services Offerings

NTT GDC & CI has focused on building their managed services capability to manage and support mission-critical IT infrastructure for their enterprise User Organization. NTT GDC & CI services range from the basic co-location to the innovative and flexible cloud – where the User Organization can choose from Public / Private / Hybrid models based on their requirements.

There is a wide choice of services available to address specific requirements and the flexibility in the engagement models – both financial and service delivery.

NTT GDC & CI complements basic Hosting and Co-location services with a comprehensive suite of Managed and Professional services, allowing User Organizations to construct modular solutions that are tailor-made to meet specific requirements. NTT GDC & CI's services include the Information Security management for Data Center services, Cloud services, Security services, Network services and Data Resiliency services delivered through Shared, Hybrid & Dedicated delivery model for Domestic & Global User Organizations.

Scope

The scope of this report is limited to the NTT GDC & CI's controls relevant to the American Institute of Certified Public Accountants (AICPA) Trust Services Categories of Security, Availability, and Confidentiality for Hosting services and Managed Services provided to User Organization across the 18 Data Centers of NTT GDC & CI as follows:

Mumbai:

- NTT GDC & CI India Private Limited: Ground, First & Second Floor, Mehra Industrial Estate, LBS Marg, Vikhroli (W), Mumbai 400079, Maharashtra, India-BOM2.
- NTT GDC & CI India Private Limited: 1st Floor P. J. Tower, Rotunda Building, Dalal Street Fort, Mumbai 400001, Maharashtra, India-BOM3.
- NTT GDC & CI India Private Limited: Ground & Mezzanine Floor, Universal Knitting Mills Private. Limited building, Mehra Industrial Estate, LBS Marg, Vikhroli (W), Mumbai 400079, Maharashtra, India-BOM4.
- NTT GDC & CI India Private Limited: Building 4A, Universal Knitting Mills Private. Limited building Mehra Estate, LBS Marg, Vikhroli (W), Mumbai - 400079, Maharashtra, India-BOM4A.
- NTT GDC & CI India Private Limited: Lighthall 'C' Wing, Hiranandani Business Park, Saki Vihar Road, Chandivali, Mumbai 400072, Maharashtra, India-BOM5.
- NTT GDC & CI India Private Limited: Lighthall 'D' Wing, Hiranandani Business Park, Saki Vihar Road, Chandivali, Mumbai 400072, Maharashtra, India-BOM6.
- NTT GDC & CI India Private Limited: Lighthall 'E' Wing Hiranandani Business Park, Saki Vihar Rd, Chandivali, Mumbai 400072, Maharashtra, India-BOM7.
- NTT GDC & CI India Private Limited: Lighthall 'G' Wing Hiranandani Business Park, Saki Vihar Rd, Chandivali, Mumbai, Maharashtra 400072-BOM9.

Navi Mumbai:

- NTT GDC & CI India Private Limited: Plot EL-25, 'A' Wing, Village Mahape, Trans Thane Industrial Area, Mahape, Navi Mumbai – 400710, Maharashtra, India-NAV1A.
- NTT GDC & CI India Private Limited: Plot EL-25, 'B' Wing, Village Mahape, Trans Thane Industrial Area, Mahape, Navi Mumbai – 400710, Maharashtra, India-NAV1B.

Bengaluru:

- NTT GDC & CI India Private Limited: 88/A, S V R Platinum, Adjacent to KSSID Complex, Electronic City, Phase-1, Bengaluru 560100, Karnataka, India-BLR2.
- NTT GDC & CI India Private Limited: SY No. 146, Kajisonnenahalli, Bidarahalli Hobli, Whitefield-Hoskote Road, Bengaluru – 560067, Karnataka, India-BLR3.
- NTT GDC & CI India Private Limited: SY No.146, Khajisonnenahalli Village, Bidarhalli Hobli, East Taluka, Whitefield, Bengaluru, 560067, Karnataka, IndiaBLR3x.

Chennai:

- NTT GDC & CI India Private Limited: Velappanchavadi, Poonamalee high Road, No. 67, DC1 Noombal Village, Chennai 600077, Tamil Nadu, India-CNN1.
- NTT GDC & CI India Private Limited: Velappanchavadi, Poonamalee high Road, No. 67, DC1A Noombal Village, Chennai 600077, Tamil Nadu, India-CNN1A.
- NTT GDC & CI India Private Limited: Wing No 8, South Phase, Sidco Industrial Estate, MTH Road, Sai Nagar, Ambattur Industrial Estate 600077, Tamil Nadu, India-CNN2A.

Noida:

- NTT GDC & CI India Private Limited: H223, Sector 63, Noida 201301, Uttar Pradesh, India-DEL1
- NTT Global Data Centers DEL2 Pvt. Ltd: Plot No. 21, Sector Tech Zone IV, Greater Noida, Gautam Buddha Nagar, Uttar Pradesh-201306, India – DEL2A.

The report does not include any other services, locations, or Data Centers of NTT GDC & CI.

In designing its system, NTT GDC & CI has contemplated that certain complementary controls would be implemented by User Organizations to achieve the Trust Services categories of Security, Availability, and Confidentiality. The Complementary User Organization Controls are described under the section 'Complementary User Organization Controls'.

Principal Service Commitments and System Requirements

NTT GDC & CI designs its process and procedures related to the System to meet its objectives for its Hosting and Managed services. Those objectives are based on the service commitments that NTT GDC & CI makes to User Organizations, the laws and regulations that govern the provision of Hosting and Managed services, and the financial, operational, and compliance requirements that NTT GDC & CI has established for the services.

NTT GDC & CI's Security, Availability, and Confidentiality commitments if any regarding the system are included within Master Service Agreement (MSA) / Service Order Form (SOF). These commitments are standardized and include, but are not limited to, the following:

- Security principles with the fundamental designs of the System that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Use of encryption technologies to protect User Organization data both at rest and in transit.
- Periodic risk assessments
- Availability and capacity monitoring controls
- Least privileged logical access management
- Infrastructure Change management

NTT GDC & CI has defined, and documented policies and procedures related to various functions. These policies and procedures are saved on the corporate intranet and reviewed periodically.

The security, availability, and confidentiality obligations of user organizations are defined in the Master Service agreement (MSA) / Service Order Form (SOF). As a part of the MSA/ (SOF), User Organizations are instructed to report any breaches / issues / complaints to NTT GDC & CI. As a part of MSA / SOF with User Organizations, NTT GDC & CI has defined the point of contact to communicate changes / updates to NTT GDC & CI policies to User Organizations.

Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained.

In addition to these policies, standard operating procedures have been documented on how to carry out operations for providing Hosting and Managed Services.

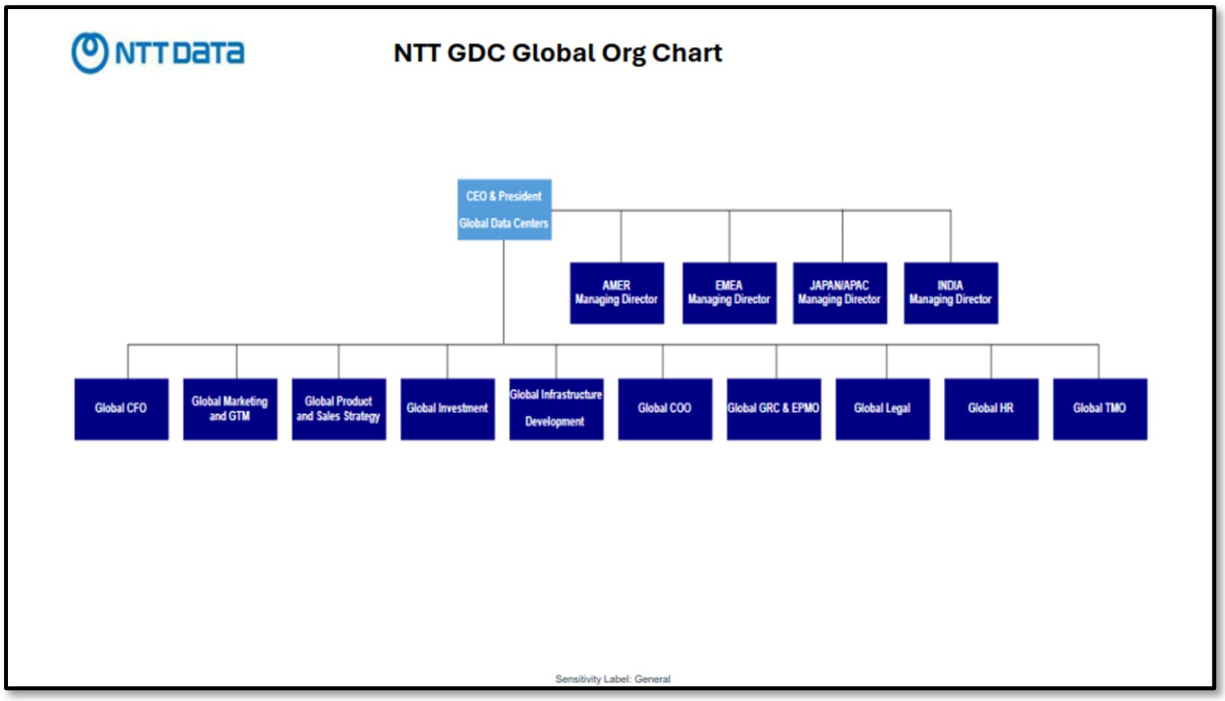
Relevant Aspects of Control Environment, Risk Assessment, and Monitoring

Control Environment

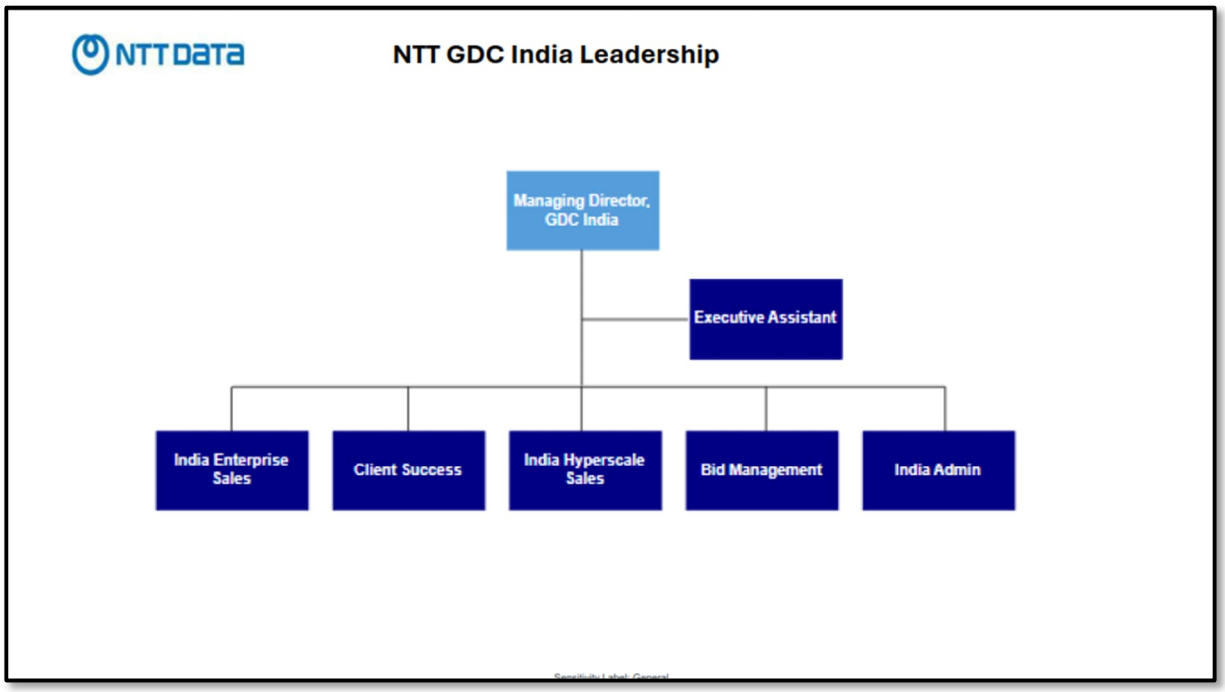
Organization Structure of NTT GDC & CI

NTT GDC & CI has defined an organizational structure which describes the line of authority and the individual roles and responsibilities to help meet its commitments and requirements related to system security, availability, and confidentiality.

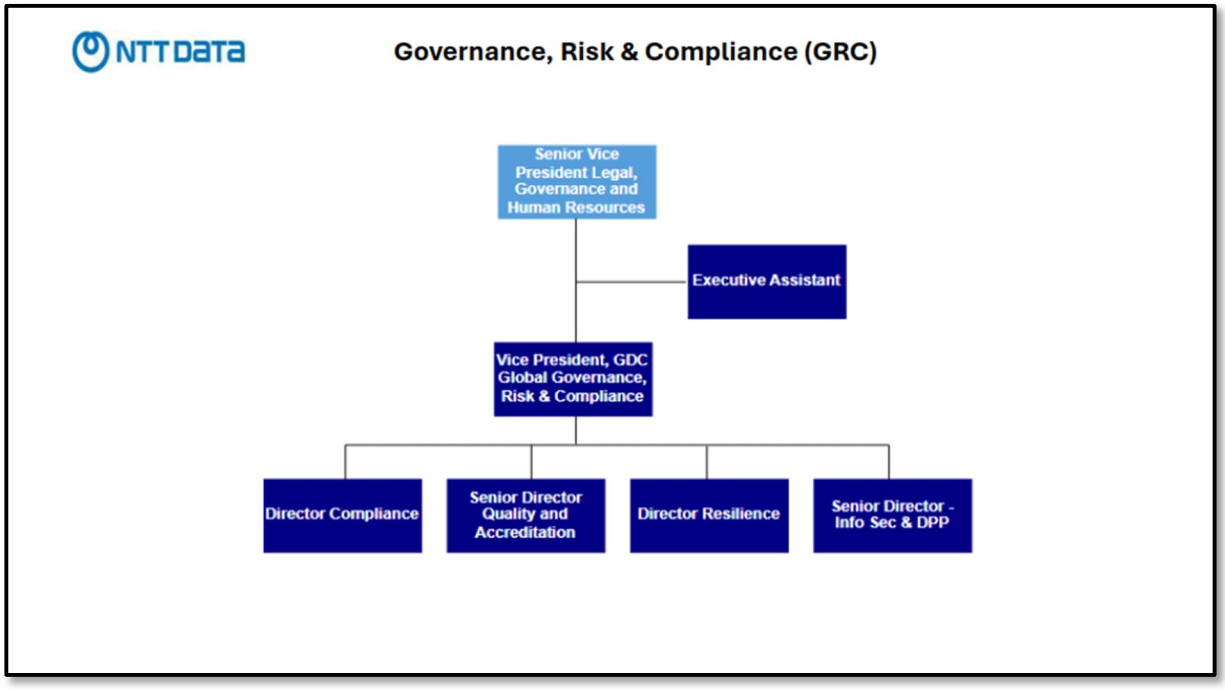
NTT GDC Global Organization Structure



GDC India: Leadership Structure



Governance, Risk and Compliance (GRC) Team Structure



Acronyms used in the chart.

Sr. No.	Acronyms	Description
1.	AMER	Americas
2.	EMEA	Europe, Middle East, and Africa
3.	APAC	Asia-Pacific
4.	COO	Chief Operating Officer
5.	CEO	Chief Executive Officer
6.	CFO	Chief Financial Officer
7.	GTM	Go-To-Market
8.	GRC	Governance, Risk & Compliance
9.	EPMO	Enterprise Program Management Office
10.	TMO	Transformation Management Office
11.	HR	Human Resources

Integrity and Ethical Values

NTT GDC & CI has laid down various policies and procedures for its employees which are available in NTT GDC & CI's intranet portal i.e., Pulse. The policies are communicated to the new hires during the Induction Training program conducted by Human Resources Team. The policies include NTT GDC & CI's Code of Conduct, Business ethics, Anti-bribery, Information Security & Privacy Policy and Disciplinary actions.

NTT GDC & CI has defined a code of conduct policy that governs standards of ethical business practice, responsibility, integrity, consequence in case of non-compliance (including disciplinary action up to termination), acceptable internet usage and resource usage. The code of conduct policy is published on corporate intranet portal 'Document Management System (DMS)' which is accessible to all NTT GDC & CI employees.

At the time of joining, new hires are required to read and acknowledge over email or physically sign the Non-Disclosure Agreement (NDA) and the Code of Conduct (COC) towards preserving the confidentiality and integrity of information within the organization.

Third-party vendors, who work at the company premises, are also required to sign an NDA to help ensure that third party contractors / vendors abide by the confidentiality requirements of NTT GDC & CI.

New hires read and acknowledge over email the Internet Usage and Acceptable Usage policy at the time of employment agreeing to maintain confidentiality and integrity of information of NTT GDC & CI's information.

Commitment to Competence

Roles and responsibilities for various positions within the organization are defined within Job descriptions to assign responsibility for security, availability and confidentiality. These job descriptions are maintained by the Human Resources Team within NTT SharePoint and are reviewed and updated when needed. Access to the NTT SharePoint is restricted to authorized members of the Human Resources team. Candidates are interviewed and assessed to evaluate qualifications against job requirements. Human Resources Team help ensure that skillsets of the candidate match with job requirements prior to their appointment and assessment records of the candidates are maintained within an Interview Assessment form or over email.

Background checks

Formalized policy and procedures exist for managing the employee screening process prior to their selection. These policies and procedures are reviewed and approved by Senior Director-Human Resource on an annual basis.

Human Resources Team is responsible for carrying out background checks for new hires with the help of third-party vendors. The third-party vendor conducts the background checks and sends the reports to Human Resources Team. In case of adverse results, the candidate may not be offered employment. Following background checks are performed:

- Verification of prior employment (for experienced employees),
- Education verification,
- Residential verification, and
- Criminal verification
- Credit Information Bureau (India) Limited (CIBIL) Check.

Risk Assessment

NTT GDC & CI has developed a Risk Assessment Matrix to help ensure applicable risks are identified, addressed, and monitored to ensure protection of information assets. Risk Assessment Matrix is approved by NTT GDC & CI Senior Management and reviewed at-least on an annual basis.

On an annual basis, NTT GDC & CI identifies the risks associated with their various functions and facilities on Yajnetra portal, an Enterprise Risk Management (ERM) portal. Based on the risks identified during the risk assessment, a Risk Assessment report is prepared for each function and facilities. Risks identified are categorized as Critical, High, Medium or Low. Based on the risk level, a Risk Treatment Plan is prepared in Yajnetra portal by GRC Team along with the respective functions where risk treatment methods and controls are identified to mitigate the risks for Critical and High Risks.

The risks arising due to inadequate infrastructure or obsolete machinery / equipment, developments in operating, regulatory, and technology environment, external factors such as cybersecurity incidents, or changes to policies and procedures are addressed during the Risk Assessment performed by the GRC Team for the Facility function.

NTT GDC & CI has developed a Vendor Relations Management policy. The identification, assessment, and management of vendor risks are carried out on an annual basis by Vendor Governance Team (part of the GRC Team), based on the documented Vendor Relations Management policy. This policy is approved by EVP – Procurement & Asset management and reviewed periodically.

Service providers, vendors or suppliers are subject to review as a part of the Supplier Risk Assessment process based on certain defined risk criteria. This review includes obtaining and evaluating information related to their management, quality system, safety and health environment, information security, business continuity management and human resources.

On an annual basis, Information Security Team conducts Information Security Risk Assessment exercises as part of ISO 27001 certification program. Risks are ranked on the basis of impact to confidentiality, integrity, and availability of information assets. Factors such as fraud, natural disasters, theft, etc. are also considered while performing risk assessment.

Monitoring

Business Continuity Management

Formalized Business Continuity Management (BCM) policy and procedure has been documented to help ensure availability commitments and requirements are met for NTT GDC & CI facilities and Data Centers. This policy is approved by CISO & VP-GRC BCMS Chief.

NTT GDC & CI Facility Team performs BCP drills for covering business disruption and continuity risks on basis of the internal BCP test calendar. Infrastructure availability, system and data availability, uninterrupted process flow and training of personnel to handle disaster are areas covered as a part of the BCP activity. A BCP test report which highlights the tests conducted and their test results is prepared post the activity. Improvement areas are also documented within the report.

For critical utilities / equipment supporting NTT GDC & CI business operations, NTT GDC & CI has built Data Center facilities which are designed to support resiliency and redundancy. The redundancy is intended to minimize the impact of common equipment failures and environmental risks.

Capacity Utilization Reporting

On a monthly basis, “Capacity Utilized Reports” are sent to the vendor and internal stakeholders by the Backup Team. The report highlights the space utilization in Commvault.

Logging and Monitoring

NTT GDC & CI uses CheckMK tool to manage the capacity of its servers including File system, memory utilization, CPU load, network devices, ports, CPU utilizations, SNMP information, etc. as a part of its system availability monitoring process. SOC Team monitors the dashboard of the CheckMK tool which shows the status of servers. Based on the thresholds defined, the dashboard reports on parameters such as disk space, memory usage, and CPU usage of the servers. In case of parameter breaches, the dashboard generates an alert, and an auto Incident is logged in the ServiceNow Tool. Based on the email alert, the ServiceNow tool notifies relevant server owners of corrective actions. The ticket then follows the Incident Management Process.

NTT GDC & CI uses Logstash and Kibana tool for log-based monitoring of Internal IT devices. Logging has been enabled for network devices, servers and firewalls etc to forward logs to ELK Stack. Log review team reviews the logs on daily basis for any exceptions/errors within the Kibana tool.

The Monitoring team shares the log review report with CISO on a daily basis. CISO reviews the log review report and communicates the exceptions noted, if any to the respective concern teams.

Internal Audit

GRC Team creates an Internal Audit calendar at the beginning of the financial year, which contains the list of audits to be carried out during the year. The audit calendar is finalized on basis of external audit schedules and inputs from other risk management functions of the company. Internal Audit is performed through the Yajnetra portal.

GRC Team carries out Internal Audit across various functions of NTT GDC & CI on a yearly basis. Based on the findings, internal control recommendations are given to the respective functions. Auditee prepares a Corrective Action Plan which is reviewed and tracked to closure by GRC Team. The Internal Audit report is shared with the respective department heads for review. The Internal Audit report covers the following aspects:

- Significant findings on internal audits during the year for the respective teams
- Internal control recommendations that need to be implemented by the respective teams.

The team prepares a "Corrective Action Plan" with details such as Root Cause of the audit findings, Corrective Actions required, Target Date & details of individuals responsible for mitigation and implementation of identified controls. GRC Team tracks the closure of the action items.

Management Review Meeting

On a Quarterly basis, a Management Review Meeting (MRM) is conducted amongst the Senior Management to discuss security incidents, their impact, root cause analysis and the respective corrective actions.

Information Security Audits

Information Security Audits are conducted by a third-party vendor on an annual basis to help ensure compliance with ISO27001: 2022, ISO 27017:2015, ISO 27018:2014, ISO 22301:2019, ISO 9001:2015, ISO 20000-1:2018, ISO 45001:2018, ISO 50001:2018, ISO 14001:2015, PCI-DSS 4.0.1 standards and MeitY empanelment for CSP. The scope of the audit spans across information security and compliance aspects of Information Technology, Data Center Facility Operations, Human Resources, Business operations and facilities and Administration functions. Observations or issues identified during the audit are graded, discussed with the auditees, and management response is sought for action plans. The implementation of action plans is tracked and assessed in the subsequent internal audit cycle. These assessments are supported with technical work programs

or pre-defined audit work steps and are coupled with vulnerability assessment scans using vulnerability assessment tools.

Vulnerability Assessment and Penetration Testing

Internal Vulnerability Assessment

On a Monthly basis, a member of the Security Operations Center (SOC) team performs vulnerability assessment using Qualys tool on various servers. Nessus tool is used for Firewalls, Network Device & Storage Device Scan which is happening on Quarterly basis by SOC Team Based on the severity of the Vulnerabilities, member of the SOC team emails the list of identified vulnerabilities to respective functional teams and functional team tracks it to closure.

External Vulnerability Assessment

An external vulnerability assessment is also performed using PCI council approved vendor, using Hackerguardian tool where IP addresses are entered. Upon completion of the assessment, the vulnerabilities identified in the generated report are notified to the respective functional teams. Closure of vulnerabilities is monitored in the subsequent quarter to check for their recurrence, if any.

Penetration Testing

On a half yearly basis, a third-party vendor conducts Penetration Testing (PT) and shares the results identified with the GRC Team. Upon completion of the assessment, the vulnerabilities rated as “Critical”, “High”, “Medium” and “Low” in the generated report are notified to the respective functional teams by the GRC Team. Closure of vulnerabilities is monitored by the GRC Team, if any.

Information and Communication

Information

Dedicated Virtual Local Area Networks (VLAN) are configured to segregate one User Organization network from the other User Organization network. NTT Active directory (AD) is used to authenticate users logging into NTT GDC & CI domain. AD is used to implement security related group policies such as password policies, account lockout policies, etc. on NTT GDC & CI domain.

NTT GDC & CI tools and applications used to support the User Organizations' business processes are described as follows:

Sr. No.	Application Name	Description
1.	ServiceNow	Third part ticketing Tool for Incident, Change, Problem, Service Request, Cloud Management, Knowledge Management, Vendor Ticketing, Store & Asset Management.
2.	Visitor Management System (VMS)	An in-house developed tool used for maintaining details of the visitors or vendors.
3.	Active Directory	Directory service for Windows domain networks
4.	TACACS	Terminal Access Controller Access Control System is an authentication protocol common to UNIX networks that allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system.
5.	HackerGuardian, Qualys Guard & Nessus	Third party tool used to conduct Vulnerability assessment externally
6.	CrowdStrike Falcon	Third-party Endpoint Detection & Response (EDR) solution used for protecting desktops, laptops, and servers against virus and malware attacks.
7.	WSUS	Windows Server Update Services used for Patch Management
8.	CyberArk	Third party tool used for privilege identity management and access to critical servers

Sr. No.	Application Name	Description
9.	Commvault	Third party backup tool that compresses, encrypts and backs up data
10.	Solus	Third party tool used to track and manage physical access of employees to the facilities and Data Centers
11.	Fusion (Ramco)/Workday	Third party HR management tool hosted in NTT GDC & CI Data Center used for HR related activities
12.	Pulse	In-house developed online portal for information publishing, information security training awareness, and assessment, Internal Training calendar, etc.
13.	FortiGate	Third party tool used for firewall and network management
14.	FortiGuard	Third Party tool used for deploying network based IPS/IDS at the external network perimeter to monitor the network traffic and prevent and detect intrusions.
15.	ELK Stack (Elastic search, Log stash and Kibana)	Third party tool used for monitoring, reviewing and analyzing activity and security logs.
16.	Yajnetra	Third-Party Automated Tool used for Risk Assessment, Internal Audit, Governance on Internal Controls & Legal Compliances.
17.	Fortinet VPN client and SafeNet Two factor authentication	Third party tools used to connect to the NTT GDC & CI network from external network.
18.	CheckMK	Third party tool to manage the capacity of its servers including File system, memory utilization, CPU load, network devices, ports, CPU utilizations, SNMP information, etc.
19.	DMS Portal	Internal Intranet Portal used for hosting policy documents available for employee access.

Sr. No.	Application Name	Description
20.	MyNTT Portal	MyNTT Portal- CRM Portal used by NTT GDC & CI Ltd. for its Customers.

Information Technology Environment

Remote Access

FortiGate VPN and SafeNet two factor authentication are used to connect to the NTT GDC & CI network from external network. This remote access is managed by Internal IT Team (part of IT Operations Team). Users enter domain credentials and SafeNet soft token passcode to access NTT GDC & CI systems.

Network

NTT GDC & CI's network is based on Wide Area Network architecture, which is highly scalable in terms of Internet bandwidth with high uptime. The Internet links provide symmetrical speed for upload and download. This provides the ability to run multiple critical application and services seamlessly. The links are under continuous monitoring for packet loss, latency and round-trip time intervals and are configured for auto-failover such that the internet traffic is routed on alternate paths in the event of path failure for maximum uptime and redundancy. Burst ability options are also available for managing heavy traffic with high-speed link as per requirement.

Personal Computers (PCs) / Laptops

Personal Computers (Desktops) / Laptops have been configured as per NTT GDC & CI guidelines. Personal Computers / Laptops are configured with software and applications depending on NTT GDC & CI Team requirements.

Uninterruptible Power Supply (UPS)

UPS and Diesel generators are used to support in the event of power failure for continuous functioning of information processing equipment. In case of UPS equipment failure, diesel generators are used to help ensure continued functioning of critical systems for a prolonged period.

Data Center

Structured cabling is done within the Data Centers. Fire suppression equipment is provided within the Data Centers. Data Centers are supported by dual power source through two different Uninterruptible Power Supply (UPS) systems and Diesel or Gas Generator Sets with redundancies wherever applicable, for continuous operation of hardware equipment in the event of a component or power failure. Temperature and humidity monitoring equipment is installed within the Data Centers.

Endpoint Detection & Response (EDR) solution

NTT GDC & CI has implemented policies and procedures for detecting and preventing virus/ malware attacks from various sources and has implemented CrowdStrike Falcon EDR solution on its workstations, laptops, and servers. CrowdStrike Falcon is a cloud-delivered solution that unifies next generation antivirus (NGAV) and provides protection against viruses and malware. CrowdStrike uses NGAV analysis to scan for vulnerabilities in real time to prevent any installation of virus or malware. Endpoint systems are encrypted using Bit locker / Trusted Platform Module (TPM) chip.

Communication

Internal Communication

Pulse portal and email is used as the primary tool for mass communication of information to employees. Email system supports dissemination of information to all, or specific categories of employees grouped by teams, designations or location. On a periodic basis, the GRC Team sends emails on Information Security updates and best practices to help ensure Information Security awareness among employees. Pulse portal is used to publish any kind of mass awareness and information to the employees.

Information Security policy and other relevant policies and procedures addressing areas related to confidentiality are published on corporate Intranet. GRC Team is responsible for developing, maintaining, and updating these policies. GRC Team reviews these policies on an 'as-needed' basis in response to the changes to technology, perceived risk, or major business change.

NTT GDC & CI uses posters, screensavers, desktop wallpapers, and newsletters for dissemination of policies, and for other awareness campaigns (such as corporate social responsibility initiatives). NTT GDC & CI uses intranet portal, Pulse, which is accessible to NTT GDC & CI employees to publish policies and procedures.

Formalized Whistle-blower Policy exists for handling sensitive incidents within NTT GDC & CI and protection of whistle blower identity. The policy is published on corporate intranet portal accessible by all employees. The Senior Management reviews and approves the policy at least annually or as needed.

External Communication

External communication by NTT GDC & CI is governed by the Corporate Communication Policy and is managed by NTT GDC & CI's Marketing and Communications function. In order to streamline external communication, key spokespersons have been nominated and authorized to interact with the media. Communication, including corporate announcements to User Organization, prospects, channel partners, alliance partners and media; major service changes, etc. are centrally drafted and released by the Marketing and Communications Team.

NTT GDC & CI has subscribed to external reporting service like Indian Computer Emergency Response Team (Cert-In) that identifies changes to applicable regulations / compliance standards relating to the services provided to User Organization.

Contributory articles or features, mass communications to external stakeholders are approved by the Marketing and Communications Team prior to publication. Service notifications, including routine updates for operational maintenance schedules,

customer notifications etc. are carried out by respective sub-functions within IT Operations Team.

Similarly, information intended for dissemination through the media or on the NTT GDC & CI website is done only after appropriate screening by the Marketing and Communications Team and relevant internal stakeholders.

Physical Security

Formalized policies and procedures exist for managing physical access to NTT GDC & CI facilities & Data Centers. These policies and procedures are reviewed and approved by Senior Director-Facilities, Securities & Administration on an annual basis. The policies define rules for granting, monitoring and removal of physical access to NTT GDC & CI infrastructure.

Access to NTT GDC & CI facilities & Data Centers

Physical Security at NTT GDC & CI begins from the perimeter of NTT GDC & CI facilities. Security guards are stationed at entry and exit points and work in shifts to monitor the physical access to NTT GDC & CI facilities & Data Centers. A shift register is maintained to record the work shifts of the security guards.

Closed Circuit Television (CCTV) surveillance equipment is used by the security guard to monitor the entry and exit points at NTT GDC & CI facilities & Data Centers. CCTV logs are retained by Administration team for a period of 90 days. Proximity based access control systems are installed at entry and exit points to restrict unauthorized entry into NTT GDC & CI facilities. Additionally, parking spaces are maintained at a safe distance from the Data Centers and vehicles entering the facility are scanned. The access control system is monitored by the Building Management System (BMS) Team.

Access to Data Center Server Hall is controlled by proximity card-based access control system. Electronic devices are deposited at the security desk before entering the Data Center. The below table lists the systems present at different Data Centers:

Functionality and safeguards	Noida-DEL1, DEL2A	Vikhroli-BOM2, BOM4 &BOM4A,	Chandivali-BOM5, BOM6, BOM7, BOM9	Chennai-CNN1, CNN1A & CNN2A	Bengaluru BLR-2, BLR 3 & BLR-3x	BOM3	NAV1-A & NAV1-B
Biometric verification (palm reader)	Y	Y	Y	Y	Y	Y	Y
Mantrap	N	N	Y	N	Y	N	Y
Turnstiles Check points	N	N	Y	Y	Y	Y	Y
Bag Scanner	Y	Y	Y	Y	Y	Y	Y
Metal Detector	Y	Y	Y	Y	Y	Y	Y
Frisking	Y	Y	Y	Y	Y	Y	Y

Physical Access Creation

When a new hire joins, Human Resources Team sends an email to Physical Security Team with a copy to new hire's reporting manager for physical access creation for a new hire. Based on the authorized request, Physical Security Team grants default access to common area to the new hires.

Access to Data Centers is restricted to authorized personnel from Facilities Operations, IT Operations and Global Service Desk, Service Account Management and Product Engineering & Innovation teams only.

Physical Access Revocation

On the last working day of the resigned employee, Human Resources Team sends an email to Physical Security Team for deactivating the physical access to NTT GDC & CI facilities and Data Centers. Physical Security Team signs off the completed Handover checklist and confirms to Human Resources Team on Ramco Fusion / Workday tool post deactivation of the access associated with the card.

Visitor Access policy

NTT GDC & CI has different color-coded access belt defined for employees, User Organization personnel, vendors/sub-contractors and visitors. Visitors are required to fill a Data Center visit form and are escorted by NTT GDC & CI representative inside the NTT GDC & CI facilities and Data Centers. Security guards at the reception are responsible to help ensure that the details of the visitors or vendors such as name of visitor or vendor, organization name, contact details, contact person, IT equipment details, entry & exit time are recorded within the Visitor Management System (VMS) maintained at the reception for permitting entry to NTT GDC & CI facilities. The Government ID / Company Photo ID and Mobile number via OTP authentication is verified at the reception prior to giving entry to the visitor.

Material Movement

Security checks are performed prior to material entry into NTT GDC & CI facilities. Physical inspection of material is performed by the Security guard before the material enters the NTT GDC & CI facility. Details such as vehicle license, challan/invoice and paperwork are checked before allowing the material into the facility.

Material movement is recorded in the Material Movement Register / Physical Challan copies. Outward material movement is approved by authorized personnel from User Organization or Facilities Team.

Access reconciliation

Access given to employees is valid for a maximum period of six months. Access given to employees are renewed on a half-yearly basis. Physical Security Team emails the list of active employees having access to NTT GDC & CI facilities from the Solus tool to Human Resources Team. Human Resources Team extracts the list of resigned employees and active employees from the Ramco Fusion tool and compares it with active users within the Solus tool. Human Resources Team emails the discrepancies to Physical Security Team for revocation of inappropriate access. Physical Security Team takes the necessary corrective actions.

Environmental Safeguards

Environmental controls at NTT GDC & CI include installation of smoke detectors, fire extinguishers, temperature & humidity monitoring, and power backup in all NTT GDC & CI facilities at in scope locations in India.

Fire Detection and Prevention

Smoke detectors and hand-held fire extinguishers are installed within the Data Center at strategic points. Fire detection and suppression units such as fire alarm, Novec 1230, smoke detectors and water sprinklers are installed at various locations within the Data Center. Servers within the Data Center Server halls are placed on raised floors. Water leak detection system is installed to detect water leakage. Rodent system is installed to avoid rats (9.1). On a half yearly basis, fire drills are carried out at the NTT GDC & CI facilities in scope (9.2).

Power Backup

Data Centers are supported by UPS and Diesel Generators for continuous operation of information processing equipment in the event of power failure. Diesel generators with fuel backup are used to help ensure continued functioning of systems in case of power failure for a prolonged period.

Temperature & Humidity Monitoring

Air-conditioners are installed at the Data Centers to maintain and control temperature and humidity conditions. Automatic temperature and humidity monitoring tool is configured to generate alerts when the reading goes beyond the set threshold value. Facilities Team monitors the temperature and humidity monitoring tool. Every two to four hours, a security guard visits the Data Centers to help ensure that the temperature and humidity conditions are maintained in the system.

Equipment Maintenance

For the Data Centers, NTT GDC & CI has documented a preventive maintenance calendar maintaining the list of critical equipment's important for maintaining business continuity. Critical equipment's such as UPS, power generators, smoke detectors, fire extinguishers, power supply, access control, humidity monitoring and temperature monitoring are serviced as per the preventive calendar. This activity is performed to maintain the continued operability of the equipment.

Information Security – Policies, Training and Awareness

NTT GDC & CI has developed an organization wide Information Security Policy to implement confidentiality, integrity, and availability of NTT GDC & CI information assets. The Information Security Policy is reviewed and approved by Senior Management of NTT GDC & CI on an annual basis.

Information regarding the design and operation of the system and its boundaries are defined within Information Security policy and related policies to help address security, availability, and confidentiality commitments. These policies and procedures are communicated to internal users by publishing them on corporate Intranet.

NTT GDC & CI has an independent Information Security Team headed by Chief Information Security Officer (CISO). The roles and responsibilities of CISO and Information Security Team are defined and documented in Information Security Policy.

Formalized Whistle-blower Policy exists for handling sensitive incidents within NTT GDC & CI and protection of whistle blower identity. The policy is published on corporate intranet portal accessible by all employees. The Senior Management reviews and approves the policy at least annually or as needed.

At the time of joining, new hires are required to read and sign over email or physically sign the Non-Disclosure Agreement (NDA) and Code of Conduct policy, Internet Usage and Acceptable Usage policy over at the time of joining, towards preserving the confidentiality and integrity of information within the organization.

New hires are made aware about their responsibility to report security, availability, and confidentiality incidents through a session on Information Security policy during the Induction program.

Third-party vendors, who work at the company premises, are also required to sign an NDA to help ensure that third party contractors / vendors abide by the confidentiality requirements of NTT GDC & CI.

On an annual basis, all employees undergo Information Security refresher awareness training program which includes information security practices and their obligations towards security, availability, and confidentiality principles at NTT GDC & CI.

Information regarding the design and operation related to job responsibilities of the operations team is communicated to the employees through periodic domain knowledge trainings conducted for them.

On a monthly basis, the GRC Team sends emails on Information Security updates and best practices to help ensure Information Security awareness among employees.

NTT GDC & CI has published all relevant policies and procedures on intranet. Any updates to the policies and procedures are updated on the intranet.

Major updates or changes to NTT GDC & CI's policies related to system security, availability, or confidentiality are communicated to employees through emails sent by GRC Team in case of any changes to policies.

Logical Access

Formalized policies and procedures exist for managing logical access to IT infrastructure of NTT GDC & CI, to restrict inappropriate and unauthorized access. These policies and procedures are reviewed and approved by Senior Director & CISO - GRC on an annual basis.

User account creation in AD

When a new hire joins, Human Resources team sends an email to Internal IT Team with a copy to new hires reporting manager for domain account and remote access creation. Based on the authorized request from the Human Resources team, Internal IT Team creates the NTT GDC & CI domain account and grants access to the new hire.

Authentication

NTT AD is used to authenticate users' login into NTT GDC & CI domain.

Privilege Identity Management (CyberArk tool)

Privilege Access Creation:

NTT GDC & CI uses CyberArk Tool for privilege identity management. The CyberArk Tool is used to manage access to database, application servers and network devices such as switches, routers, and firewall. Access to database and application servers and firewall and other network devices (switches and routers) through CyberArk Tool is provided based on approval from the Department Team Leads over ServiceNow ticket / email. The approval is then sent to the IT Team for adding the user to defined security groups on domain controller.

Privilege Access Revocation:

CyberArk Tool uses the NTT AD for authentication. Access to database / application servers and network devices such as switches, routers, and firewall through CyberArk Tool is automatically disabled when AD access gets disabled.

Administrative access to network devices and perimeter firewalls through CyberArk tool is restricted to authorized personnel from Network and SOC teams and Product Engineering and Innovation Team.

User account revocation from AD

On the last working day of the resigned employee, Human Resources Team sends an email to Internal IT Team for disabling the user account in NTT AD and resetting Lightweight Directory Access Protocol (LDAP) password of the user. The Internal IT Team disables the user account on the last working day, resets the LDAP Password

for the resigned employee and signs off the completed Handover checklist on Ramco Fusion.

User Organization Onboarding and Offboarding

Server Commissioning

User Organizations are provided access to their servers through Implementation Request (IR) which is raised in ServiceNow tool at the time of server installation.

Service Decommissioning

On decommissioning of User Organization's services, a confirmation email is sent to the User Organization indicating discontinuation of their services.

Access reconciliation for AD accounts

On a quarterly basis, Human Resources Team extracts a list of resigned employees from Workday Tool and sends it to GRC Team for access reconciliation. GRC Team compares the list of resigned employees with the active users within the AD and sends the results of this comparison to Internal IT Team. Basis the results received from GRC Team; Internal IT Team takes corrective action in case of any discrepancies.

Access review for PIM (CyberArk tool)

On a quarterly basis, PIM Team (part of IT Operations Team) sends the active user list from CyberArk Tool to all the Tower Leads from IT Operations Team for review. The Tower Leads verify the appropriateness of the access and confirm to PIM Team. In case of discrepancies, Team Leads raise a ServiceNow ticket and corrective actions are taken by IT Support Team.

Administrative privileges

Administrative privileges on NTT AD are restricted to authorized personnel of NTT GDC & CI's Microsoft Team (part of NTT GDC & CI Internal IT Team).

Password Policy

Formal password policy has been defined and established for access to domain, network devices and servers. There are separate domain controllers for servers and workstations/network devices. Passwords are controlled through group policy settings which include password expiry, password length, password history, and password complexity requirements.

User accounts are locked after a limited number of unsuccessful logons. Unattended desktops and laptops are locked within a stipulated time of inactivity.

Guest account and anonymous logins are disabled on domain controller. Default administrator accounts on servers are renamed / disabled for security purposes.

Remote access

Remote access to NTT GDC & CI systems is provided through FortiGate VPN. VPN credentials and Two factor authentication via SafeNet tool is used to establish connection with NTT GDC & CI systems from both internal and external network.

Data Backup and Data Disposal Controls

Data Backup

Formalized process and policy document exist for Backup and Restoration to assist in the continuity of business operations by maintaining backup. This process is reviewed and approved by Senior Director GRC & CISO on an annual basis.

Data backup process

Backup Team (Part of IT Operations Team) is responsible for taking backup of NTT GDC & CI servers using Commvault Tool. Daily incremental and/or weekly full backup is scheduled using Commvault Tool as agreed with respective server owners. Backup Team is notified with backup status post completion of the backup and in case of backup failure, an incident ticket is automatically raised in ServiceNow Tool. Based on the ticket raised, Backup Team takes corrective actions.

On a monthly basis, “Capacity Utilized Reports” are sent to internal stakeholders. The report highlights the space utilization in the backup tool.

Backup Encryption

Automatic backup is configured on Commvault. The backup is encrypted using in-built encryption within Commvault.

Backup Restoration

Backup Team raises a ticket in ServiceNow Tool to perform restoration of data on NTT GDC & CI servers based on User Organization request. A Backup Team member performs the data restoration activity and updates the resolution in the ticket post successful completion of the restoration.

Asset Disposal Policy

NTT GDC & CI has a formal asset classification and disposal policy stating procedures for secure disposal of assets. The Policy is approved by Senior Management of NTT GDC & CI and available on the intranet portal for employee access.

User Organization’s Service Decommissioning

On decommissioning of User Organization’s service, a confirmation email is sent to the User Organization indicating discontinuation of their services.

Secure Disposal

All assets (laptops / desktops / servers, etc.) are disposed off using secure sanitization methods prior to removal of these assets from NTT GDC & CI environment.

Network Security

NTT GDC & CI has developed an organization wide Information Security Policy to implement confidentiality, integrity, and availability of NTT GDC & CI information assets. The Information Security Policy is reviewed and approved by Senior Director & CISO - GRC on an annual basis.

A formal hardening policy exists for NTT GDC & CI servers and network devices. The hardening policy is approved by senior management and is available on intranet portal accessible to all employees.

NTT GDC & CI has an independent Information Security Team headed by Chief Information Security Officer (CISO). The roles and responsibilities of CISO and Information Security Team are defined and documented in Information Security Policy.

Network Redundancy

For critical utilities / equipment supporting NTT GDC & CI business operations, NTT GDC & CI has built NTT GDC & CI Data Center facilities which are designed to support resiliency and redundancy. The redundancy is intended to minimize the impact of common equipment failures and environmental risks.

Firewall

NTT GDC & CI has implemented firewall on the Internet gateway to protect against security, availability, and confidentiality threats from sources outside the NTT GDC & CI network perimeter boundaries. Rules are configured on FortiGate firewall, to regulate traffic in and out of NTT GDC & CI network. Rules are enforced on firewall to 'deny all' accesses to NTT GDC & CI network with access enabled for specific services as per business requirements.

URL filtering has been enabled within the firewall to regulate internet usage.

IPS / IDS

NTT GDC & CI has deployed network-based Intrusion Prevention System/Intrusion Detection System (IPS/IDS) at the external network perimeter to monitor the network traffic and prevent and detect intrusions into their network. NTT GDC & CI uses FortiGuard Tool to manage IPS/IDS. The IPS/IDS is updated by NTT GDC & CI with signatures received from the vendor as and when they are released.

Logging and monitoring

NTT GDC & CI uses CheckMK tool to manage the capacity of its servers including File system, memory utilization, CPU load, network devices, ports, CPU utilizations, SNMP information, etc. as a part of its system availability monitoring process. SOC

Team monitors the dashboard of the CheckMK tool which shows the status of servers. Based on the thresholds defined, the dashboard reports on parameters such as disk space, memory usage, and CPU usage of the servers. In case of parameter breaches, the dashboard generates an alert, and an auto Incident is logged in the ServiceNow Tool. Based on the email alert, the ServiceNow tool notifies relevant server owners of corrective actions. The ticket then follows the Incident Management Process.

NTT GDC & CI uses Logstash and Kibana tool for log-based monitoring of Internal IT devices. Logging has been enabled for network devices, servers and firewalls etc to forward logs to ELK Stack. Log review team reviews the logs on daily basis for any exceptions/errors within the Kibana tool.

The team shares the log review report with CISO on a daily basis. CISO reviews the log review report and communicates the exceptions noted, if any to the respective concern teams

Vulnerability Assessment & Penetration Testing

Internal Vulnerability Assessment

On a monthly basis, a member of the Security Operations Center (SOC) team performs vulnerability assessment using Qualys tool on various servers, Nessus tool is used for Firewalls, Network Device & Storage Device Scan which is happening on Quarterly basis by SOC Team. Based on the severity of the Vulnerabilities, member of the SOC team emails the list of identified vulnerabilities to respective functional teams and functional team tracks it to closure.

External Vulnerability Assessment

An external vulnerability assessment is also performed using PCI council-approved-vendor using Hackerguardian tool, where IP addresses are entered. Upon completion of the assessment, the vulnerabilities identified in the generated report are notified to the respective functional teams. Closure of vulnerabilities is monitored in the subsequent quarter to check for their recurrence, if any.

Penetration Testing

On a half yearly basis, a third-party vendor conducts Penetration Testing (PT) and shares the results identified with GRC Team Upon completion of the assessment, the vulnerabilities rated as “Critical”, “High”, “Medium” and “Low” in the generated report are notified to the respective functional teams by the GRC Team. Closure of vulnerabilities is monitored by the GRC Team, if any.

Data Security

Removable media devices, such as Universal Serial Bus (USB) mass storage devices are disabled on the end-user workstations through the AD group policies.

Users are not granted administrative privileges on local workstations and cannot install software / applications on local workstations.

Endpoint systems are encrypted using Bit locker /Trusted Platform Module (TPM) chip.

Dedicated Virtual Local Area Networks (VLAN) are configured to segregate one User Organization network from the other User Organization network.

Email Encryption

Email communications are transmitted over the Internet using Transport Layer Security (TLS) encryption protocol using in-built feature of Microsoft Outlook.

Network Encryption

NTT GDC & CI has enabled data encryption on MyNTT portal using Secured Socket Layer (SSL) using Advanced Encryption Standard (AES) 128-bit encryption.

Endpoint Protection Solution

NTT GDC & CI has implemented CrowdStrike Falcon EDR solution on its workstations, laptops, and servers. CrowdStrike is a cloud-delivered solution that unifies next generation antivirus (NGAV) and provides protection against viruses and malware. CrowdStrike uses NGAV analysis to scan for vulnerabilities in real time to prevent any installation of virus or malware. CrowdStrike being a next generation antivirus solution works on behavioural analysis using MITRE ATT&CK framework which is an inbuilt functionality.

Information Security Awareness

New hires are made aware about information security policies during induction training program which include elements of information security, confidentiality, integrity, and availability of data. An attendance record is maintained post the induction training. Additionally, on a periodic basis GRC Team uploads sends mailers to notify all employees on latest Information Security awareness guidelines covering topics such as antivirus malware security and social engineering.

On an annual basis, all employees undergo Information Security refresher awareness training program which includes information security practices and their obligations towards security, availability, and confidentiality principles at NTT GDC & CI.

Incident Management

Formalized policies and procedures exist for managing security, availability, and confidentiality related incidents within the organization. These policies and procedures are reviewed and approved by Operation LT team on an annual basis.

Incident Logging and Assignment

NTT GDC & CI service desk has implemented ServiceNow Tool to manage all the types of incidents / service request requested by User Organizations. User organizations can request incidents in the following ways:

- Email: Based on an email from the user with the issues mentioned in a format defined by NTT GDC & CI service desk, an incident ticket is automatically generated in ServiceNow Tool. If the email is not in the specific format, the user should mention their Customer ID and PIN to log an incident ticket in ServiceNow Tool.
- Phone Calls: The user can also raise their issues with NTT GDC & CI service desk via phone calls. Customer ID and PIN is required to log such kind of issues. NTT GDC & CI Service Desk Team raises a request on behalf of the user in ServiceNow Tool.
- Proactive ticket: Tickets can be generated by members of NTT GDC & CI service desk. Also, tickets can also be generated automatically basis the alerts received from the monitoring tools.

In addition, NTT GDC & CI users can generate a ticket with service desk on ServiceNow portal via email or phone calls. In this case, Customer ID and PIN are not required.

The Service desk personnel analyse the issue and create an Incident in ServiceNow Tool where required. The Incident is prioritized as S1, S2, S3 or S4. Based on the classification and categorization of incidents, the NTT GDC & CI Service Desk assigns the incidents to the respective functional teams.

Incident Analysis and Resolution

For Incident tickets with severity S1, a workaround resolution is provided within an incident ticket in line with the defined Service Level Agreement (SLA). A problem ticket is created for all S1 category incidents and Root Cause Analysis (RCA) is performed. The RCA is reviewed and approved by a member of incident management team and the problem ticket is marked as resolved.

For incident tickets with severity S2, S3 and S4, resolution is given based on the defined SLAs and comments are documented within the incident ticket. The SLAs

are defined in the Master Service Agreement (MSA) signed with the user organization.

Security Incident Management

Formalized policies and procedures exist for managing the information security incidents logged by User Organizations' or NTT GDC & CI employees.

Physical security incidents are logged within ServiceNow ticketing tool. A Root Cause Analysis (RCA) is performed for the incidents and the action taken is documented within the ServiceNow ticket. Administration Head reviews and approves the RCA and actions taken within the ServiceNow ticketing tool. Based on approval, a member of the Administration team marks the ticket as resolved. The incidents are categorized based on their severity as below:

- Critical: May cause system extended outage, impact user Organizations or have legal implications.
- High: May cause considerable system outage
- Medium: May affect a few systems or processes
- Low: May have a minor impact

On a monthly basis, IT Operations Team prepares a Management Information System (MIS) report which details the list of incidents which are open / closed, and key activities performed during the month. This report is shared with the IT Operations Head.

On a Quarterly basis, a Management Review Meeting (MRM) is conducted amongst the Senior Management to discuss security incidents, their impact, root cause analysis and the respective corrective actions.

Problem Management

Formalized policies and procedures exist for managing Problems within the organization. These policies and procedures are reviewed and approved by MS Operations Director on an annual basis. The objective of problem management is to prevent incidents from happening and to minimize their recurrence.

Problem Initiation

A Problem is raised in the following cases:

- To perform RCA for an S1 Incident ticket
- To perform RCA for a repetitive Incident
- To perform RCA for Failed Change Requests
- Proactive problem ticket - as a pre-emptive measure to tackle observed issues.

Problem Analysis and Resolution

Problem Management Team assigns the Problem ticket to the concerned functional team such as Network, Database, and Backup. An Interim RCA is created for S1 Problem tickets and Reactive Problem tickets and communicated to the respective stakeholders and User Organization.

Problem Closure

Upon successful completion of the final resolution, the problem ticket is closed in one of the following ways:

- The final RCA is shared with the User Organization, wherever required, and the Problem ticket is closed by the functional teams.
- Request is sent to Change Management Team which follows Change Management Process to close the problem ticket (Refer Change Management Controls)

The User Organizations and stakeholders receive an automated notification whenever the Interim or Final RCA is closed.

On a monthly basis, Operations Team prepares a Management Information System (MIS) report which details the list of problems which are open / closed, and key activities performed during the month. This report is shared with the IT Operations Head.

Change Management

Change Management is performed for changes related to NTT GDC & CI owned infrastructure. Formalized policies and procedures exist for managing infrastructure changes in NTT GDC & CI. These policies and procedures are reviewed and approved by Senior MS Operations Director on an annual basis.

Change Management process includes change initiation, change authorization Change Advisory Board review, testing, and post implementation review and closure.

Change initiation.

Based on inputs from NTT GDC & CI employees or User Organization or third-party vendors, change requests are raised in ServiceNow Tool by the NTT GDC & CI Change Management Team. A change is raised in the following cases:

- Infrastructure or configuration change required as a result of an Incident/Problem ticket.
- Planned infrastructure or configuration changes.
- Routine/Periodic changes such as maintenance activities
- Changes that are initiated by the vendor.
- Emergency Changes

Change authorization.

The Change Requestor logs the Change Request (CR) in ServiceNow Tool with details such as severity, description, location and change type. Team Leader (TL) approves the CR in ServiceNow, and the Change Requestor receives an automatic notification of change approval from ServiceNow Tool.

Change is categorized into the below types depending on the risk involved for the change:

- Pre-approved change - Change to a service or infrastructure for which the approach has been pre-authorized by Change management Team that has an accepted procedure. The risk is low for such changes. These changes include periodic maintenance activities and patch management. They are pre-defined in the ServiceNow Tool and do not need a Change Advisory Board (CAB) approval.
- Planned change - A Planned Change to a service or infrastructure for which the risk is to be assessed and which goes through the Change Advisory Board (CAB) for approval. There is impact/risk to the current environment in such cases.
- Emergency change - An Emergency change is introduced usually in order to handle an error within the environment which requires urgent rectification. The Emergency change is approved by the Emergency Change Advisory Board (ECAB).

- Retrospective change - A Retrospective change is implemented first and later they are raised in ServiceNow Tool. Retrospective changes shall fulfil the same criteria as an emergency change. They are essentially the same as emergency changes with the only difference being that the change is raised after the event.

Change Advisory Board Review

The Change Manager (CM) initiates CAB Change Advisory Board) review. Changes planned for the week are approved in the weekly CAB / ECAB review meeting.

Change Testing

Testing is performed, wherever applicable and test results are documented in ServiceNow Tool. The change is implemented post successful testing.

Post implementation review and closure

A designated independent team member, the Change Auditor, reviews the implementation report and resolves the CR in ServiceNow Tool. The CR is closed automatically within 48 hours once the CA has resolved the ticket.

On a monthly basis, IT Operations Team prepares a Management Information System (MIS) report which details the list of changes which are open / closed, and key activities performed during the month. This report is shared with the IT Operations Head.

Complementary User Organizations Controls

This section describes controls that are the responsibility of the User Organizations to complement the controls at NTT GDC & CI. The following user control considerations should not be regarded as a comprehensive list of all controls that should be deployed by User Organizations. There may be additional controls that would be appropriate for User Organizations which are not identified in this report.

Sr. No.	Complementary User Organizations Controls	Trust Criteria Number
1	User Organizations should ensure that physical access to User Organization's work areas and server halls within NTT GDC & CI facilities is restricted to authorized personnel.	CC6.4
2	User Organizations are responsible for ensuring that access to their IT systems is authenticated, authorized, modified, removed and administered based on roles and responsibilities.	CC6.2
3	User Organizations are responsible for reviewing the access to User Organizations network and systems periodically to ensure it is commensurate with the job responsibilities.	CC6.2
4	User Organizations are responsible for ensuring that logical access security measures have been implemented to protect their systems against external threats.	CC6
5	User Organizations are responsible for ensuring that the transmission, movement, and removal of information from their systems is restricted to authorized users.	CC6
6	User Organizations are responsible for defining formalized policies and procedures for managing the Information Security incidents	CC7
7	User Organizations are responsible for communicating security incidents applicable to NTT GDC & CI on a timely basis	CC7
8	User Organizations are responsible for communicating changes to infrastructure	CC8
9	Where User Organizations are responsible for data backup, they define the backup frequency and retention period of the data	A1.2 A1.3

Sr. No.	Complementary User Organizations Controls	Trust Criteria Number
10	User Organizations are responsible for communicating back up restoration requests to NTT GDC & CI on a timely basis.	A1.1 A1.2 A1.3

Section 4 - Description of Criteria, Controls, Tests, and Results of Tests

Description of Criteria, Controls, Tests, and Results of Tests

The Trust Services Criteria, and the controls that meet the criteria are listed in the accompanying section “Description of Criteria, Controls, Tests, and Results of Tests”.

On the pages that follow, the applicable Trust Services Criteria and the controls to meet the criteria have been specified by and are the responsibility of NTT GDC & CI. The testing performed by Ernst and Young Associates LLP and the results of tests are the responsibility of the service auditor.

In planning the nature, timing and extent of its testing of the controls specified by NTT GDC & CI, Ernst and Young Associates LLP considered the aspects of NTT GDC & CI’s control environment, risk assessment processes, information and communication and management monitoring procedures and performed such procedures as Ernst and Young Associates LLP considered necessary in the circumstances.

Procedures for Assessing Completeness and Accuracy of Information Provided by the Entity (IPE)

For test of controls requiring the use of IPE (e.g. Controls requiring system generated populations for sample based testing) or for test of controls requiring management’s use of IPE in the execution of the controls (e.g. periodic reviews), Ernst and Young Associates LLP performed a combination of one or more of the following procedures wherever possible based on the nature of the IPE to address the completeness, accuracy and data integrity of the data or reports used: (1) inspected the source of IPE; (2) inspected the query, script or parameters used to generate the IPE; (3) observed the reconciliation of the data between IPE and the source; (4) inspected the IPE for anomalous gaps in sequence or timing to determine the data is complete and accurate and maintains its integrity; and/or (5) inspected management procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

Criteria and Controls

The criteria for the Security, Availability, and Confidentiality categories are organized into (a) the criteria that are applicable to all three categories (common criteria) and (b) criteria applicable only to a single category. The common criteria constitute the complete set of criteria for the Security Category. For the Categories of Availability, and Confidentiality a complete set of criteria is comprised of all the common criteria and all the criteria applicable to the Categories being reported on.

Criteria	Supporting Control Activity	Criteria Description
CC1.0 - Common Criteria Related to Control Environment		
CC1.1	1,2,3,4,5,6	The entity demonstrates a commitment to integrity and ethical values.
CC1.2	7	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
CC1.3	8,9,10,11,12	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
CC1.4	3,4,5,13,14,15 , 16	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
CC1.5	8,9,10,11,17	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Criteria	Supporting Control Activity	Criteria Description
CC2.0 - Common Criteria Related to Communication and Information		
CC2.1	11,12,17	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
CC2.2	1,4, 5, 6,7,10, 11,15,16,17, 18,19,20,21, 108	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
CC2.3	12,22,23,24, 25,26	The entity communicates with external parties regarding matters affecting the functioning of internal control.

Criteria	Supporting Control Activity	Criteria Description
CC3.0 - Common Criteria Related to Risk Assessment		
CC3.1	27,28,29	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
CC3.2	30,31,32, 33,34,35	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
CC3.3	7,26,30,31, 32,33,34,35	The entity considers the potential for fraud in assessing risks to the achievement of objectives.
CC3.4	7,32	The entity identifies and assesses changes that could significantly impact the system of internal control.

Criteria	Supporting Control Activity	Criteria Description
CC4.0 - Common Criteria Related to Monitoring Activities		
CC4.1	7,18,25,26, 31,32,34,35, 108	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
CC4.2	7,18,25,26, 31,32,34,35, 108	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Criteria	Supporting Control Activity	Criteria Description
CC5.0 - Common Criteria Related to Control Activities		
CC5.1	7,26,27,29, 30,31,32	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
CC5.2	7,26,27,29, 30,31,32	The entity also selects and develops general control activities over technology to support the achievement of objectives.
CC5.3	7,9,10,11, 36,37,38,39, 40,41	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

Criteria	Supporting Control Activity	Criteria Description
CC6.0 - Common Criteria Related to Logical and Physical Access		
CC6.1	37,42,43,44, 45,46,47,48, 49,50,51,52, 53,54,55,56	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
CC6.2	57,58,59,60, 61,62,63,64, 65	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
CC6.3	57,58,59,60, 61,62,63,64, 65	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

Criteria	Supporting Control Activity	Criteria Description
CC6.0 - Common Criteria Related to Logical and Physical Access		
CC6.4	36,66,67,68, 69,70,71,72, 73,74,75,76	The entity restricts physical access to facilities and protected information assets (for example, Data Center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.
CC6.5	63,77,78	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.
CC6.6	34,35,43,45, 51,52,53,54, 79,80,81,82, 83,84	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
CC6.7	51,52,53,54, 85	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.
CC6.8	56,80,86	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

Criteria	Supporting Control Activity	Criteria Description
CC7.0 - Common Criteria Related to System Operations		
CC7.1	18,34,35,38, 80,84,87,88 89,90,91,92, 108	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.

Criteria	Supporting Control Activity	Criteria Description
CC7.0 - Common Criteria Related to System Operations		
CC7.2	18,34,35,38, 80,84,87,88 89,90,91,92, 108	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.
CC7.3	18,34,35,38, 80,84,87,88 89,90,91,92, 108	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.
CC7.4	18,34,35,38, 80,84,87,88 89,90,91,92, 108	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.
CC7.5	18,34,35,38, 80,84,87,88 89,90,91,92, 108	The entity identifies, develops, and implements activities to recover from identified security incidents.

Criteria	Supporting Control Activity	Criteria Description
CC8.0 - Common Criteria Related to Change Management		
CC8.1	40,93,94,95, 96	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

Criteria	Supporting Control Activity	Criteria Description
CC9.0 - Common Criteria Related to Risk Mitigation		
CC9.1	26,27,29	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
CC9.2	12,26,32	The entity assesses and manages risks associated with vendors and business partners.

Criteria	Supporting Control Activity	Criteria Description
A1.0 - Additional Criteria Related to Availability		
A1.1	97,98,99	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.
A1.2	100,101,102, 103,104,105, 106,107	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.
A1.3	102,107	The entity tests recovery plan procedures supporting system recovery to meet its objectives.

Criteria	Supporting Control Activity	Criteria Description
C1.0 - Additional Criteria Related to Confidentiality		
C1.1	1,12,23,63, 77,78	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.

Criteria	Supporting Control Activity	Criteria Description
C1.0 - Additional Criteria Related to Confidentiality		
C1.2	1,12,23,63, 77,78	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
1	New Hires - NDA and Code of Business Conduct: New hires are required to read and sign the Non-Disclosure Agreement (NDA) and Code of Conduct Policy at the time of joining, towards preserving the confidentiality and integrity of information within the organization.	CC1.1 CC2.2 C1.1 C1.2	Inspected the Code of Conduct document to determine whether ethical values and integrity were documented. For a sample of new hires, inspected the signed NDA and Code of Conduct policy to determine whether the new hires had signed and agreed to maintain confidentiality and integrity of information within the organization.	No deviations noted. No deviations noted.
2	New Hires - Internet Usage and Acceptable Usage Policy: New hires read and acknowledge over email the Internet Usage and Acceptable Usage policy at the time of employment agreeing to maintain confidentiality and integrity of	CC1.1	For a sample of new hires, inspected the email communication between new hires and the Human Resources team to determine whether new hires had read and acknowledged the Internet Usage and Acceptable	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	information of NTT GDC & CI's information.		Usage policy at the time of employment agreeing to maintain confidentiality and integrity of information of NTT GDC & CI's information.	
3	New Hires - Background Check: The third-party vendor conducts the background checks and sends the reports to Human Resources Team. Following background checks are performed: • Verification of prior employment, • Education verification, • Residential verification • Criminal verification • CIBIL Check	CC1.1 CC1.4	For a sample of new hires, inspected the background check reports to determine whether listed background checks were conducted as per the policy.	No deviations noted.
4	Information Security Trainings:	CC1.1 CC1.4	Inspected induction training material to determine whether	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	New hires are made aware about information security policies during induction training program which include elements of information security, confidentiality, integrity, and availability of data. An attendance record is maintained post the induction training. Additionally, on a periodic basis GRC Team sends mailers to notify all employees on the latest Information Security awareness.	CC2.2	new hires were made aware of information security practices and their obligations towards security, availability, and confidentiality principles at NTT GDC & CI. Further, for a sample of new hires, inspected the induction training attendance sheet and Information Security awareness test record to determine whether the new hires attended the induction training program. For a sample of months, inspected the Information Security awareness mailers sent by GRC Team to determine whether employees were notified on the	No deviations noted. No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
			latest Information Security guidelines.	
5	Induction Training - Reporting Incidents: Employees are made aware about their responsibility to report security, availability, and confidentiality incidents through a session on Information Security policy during the Induction program.	CC1.1 CC1.4 CC2.2	Inspected the induction training material to determine whether the material included topics related to employee's responsibility to report security, availability, and confidentiality incidents. For a sample of new hires, inspected the induction attendance records to determine whether the new hires attended the induction program.	No deviations noted. No deviations noted.
6	Whistle-Blower Policy: Formalized Whistle-blower Policy exists for handling sensitive incidents within NTT GDC & CI and protection of whistle blower identity. The policy is	CC1.1 CC2.2	Inspected the Whistle Blower policy to determine whether it contained details on handling sensitive incidents.	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	published on corporate intranet portal accessible by all employees. The Senior Management reviews and approves the policy at least annually or as needed.		Further, inspected the policy to determine whether it was approved by Senior Management. Additionally, inspected the intranet portal to determine whether the policy was maintained on the portal.	No deviations noted. No deviations noted.
7	Management Review Meeting: On a Quarterly basis, a Management Review Meeting (MRM) is conducted amongst the Senior Management to discuss security incidents, their impact, root cause analysis and the respective corrective actions.	CC1.2 CC2.2 CC3.3 CC3.4 CC4.1 CC4.2 CC5.1 CC5.2 CC5.3	For a sample of quarters, inspected agenda, meeting invite and MoM of the Management Review meeting (MRM) to determine whether details of the security incidents were discussed.	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
8	Organization Chart: NTT GDC & CI has defined an organizational structure which describes the line of authority and the individual roles and responsibilities to help meet its commitments and requirements related to system security, availability, and confidentiality.	CC1.3 CC1.5	Inspected NTT GDC & CI organizational chart to determine whether NTT GDC & CI had defined an organizational structure, reporting lines, authorities, and responsibilities to help meet its commitments and requirements related to system security, availability, and confidentiality.	No Deviations noted.
9	Roles and responsibilities: Roles and responsibilities for various positions within the organization are defined within Job descriptions to assign responsibility for security, availability and confidentiality. These job descriptions are maintained by the Human Resources Team within NTT SharePoint and are reviewed and updated when needed. Access to the NTT SharePoint is restricted to	CC1.3 CC1.5 CC5.3	For a sample of job postings, inspected the job descriptions maintained by Human Resources Team to determine whether roles and responsibilities were defined. Further, inquired with the Senior member of the Human Resources team to determine whether the job descriptions were updated and	No deviations noted. No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	authorized members of the Human Resources team.		reflect the current job responsibilities. Additionally, inspected the NTT SharePoint, the list of users having access to the SharePoint and the HR list to determine whether Job descriptions were maintained by the Human Resources team within NTT SharePoint and access to the NTT SharePoint was restricted to authorized members of the Human Resources team.	No deviations noted.
10	Information Security Policy: NTT GDC & CI has developed an organization wide Information Security Policy to implement confidentiality, integrity, and availability of NTT GDC & CI information assets. The Information	CC1.3 CC1.5 CC2.2 CC5.3	Inspected the Information Security Management policy to determine whether the policy and procedures for managing information security was documented, reviewed and approved by Senior Director & CISO - GRC on an annual basis.	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	Security Policy is reviewed and approved by Senior Director & CISO - GRC on an annual basis.			
11	System Boundaries: Information regarding the design and operation of the system and its boundaries are defined within Information Security policy and related policies to help address security, availability, and confidentiality commitments. These policies and procedures are communicated to internal users by publishing them on corporate Intranet.	CC1.3 CC1.5 CC2.1 CC2.2 CC5.3	Inspected the Information Security policy and other related policies and procedures on the intranet to determine whether they addressed areas related to system security, availability, and confidentiality.	No deviations noted.
12	MSA / SOF – User Organizations: NTT GDC & CI's security, availability, and confidentiality commitments if any regarding the system are	CC1.3 CC2.1 CC2.3	For a sample of newly onboarded User Organizations, inspected the MSA / SOF, as applicable, to determine whether NTT GDC & CI's	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	included within Master Service Agreement (MSA) / Service Order Form (SOF).	CC9.2 C1.1 C1.2	security, availability, and confidentiality commitments, regarding the system were documented and communicated to User Organizations.	
13	Employee Screening Policy: Formalized policy and procedures exist for managing the employee screening process prior to their selection. These policies and procedures are reviewed and approved by Senior Director – Human Resources on an annual basis.	CC1.4	Inspected the Employee Screening policy to determine whether the procedures for managing employee screening were documented, reviewed and approved by Senior Management on an annual basis.	No deviations noted.
14	Employee Screening: Candidates are interviewed and assessed to evaluate qualifications against job requirements. Human Resources Team help ensure that skillsets of the candidate match	CC1.4	For a sample of new hires, inspected the interview assessment form or email communication between members of Human Resources team and the reporting manager (as applicable)	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	with job requirements prior to their appointment and assessment records of the candidates are maintained within an Interview Assessment form or over email.		to determine whether qualifications of the new hires were evaluated against the job requirements.	
15	Active Employees - Annual Refresher Training: On an annual basis, all employees undergo Information Security refresher awareness training program which includes information security practices and their obligations towards security, availability, and confidentiality principles at NTT GDC & CI.	CC1.4 CC2.2	Inspected the information security refresher awareness training material to determine whether employees are made aware of information security practices and their obligations towards security, availability, and confidentiality principles at NTT GDC & CI. Further, for a sample of active employees, inspected the training completion records of the information security refresher awareness training to determine whether the employee had	No deviations noted. No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
			successfully completed the training.	
16	Domain Knowledge Training: Information regarding the design and operation related to job responsibilities of the operations team is communicated to the employees through periodic domain knowledge trainings conducted for them.	CC1.4 CC2.2	For a sample of active employees, inspected the attendance sheet of employees to determine whether domain knowledge training was successfully completed.	No deviations noted.
17	Process SOPs: NTT GDC & CI has defined, and documented policies and procedures related to various functions. These policies and procedures are saved on the corporate intranet and reviewed periodically.	CC1.5 CC2.1 CC2.2	Inspected the policy and procedure documents related to various functions to determine whether documented policies and procedures were saved on the corporate intranet and reviewed periodically.	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
18	Internal Audit: GRC Team carries out Internal Audit across various functions of NTT GDC & CI on a yearly basis. Based on the findings, internal control recommendations are given to the respective functions. Auditee prepares a Corrective Action Plan which is reviewed and tracked to closure by GRC Team. The Internal Audit report is shared with the respective department heads for review. The Internal Audit report covers the following aspects: ► Significant findings on internal audits during the year for the respective teams ► Internal control recommendations that need to be	CC2.2 CC4.1 CC4.2 CC7.1 CC7.2 CC7.3 CC7.4 CC7.5	Inspected the internal audit reports to determine whether audit findings and recommendations were documented in the report and covered the following aspects: ► Significant findings on internal audits during the year for the respective teams ► Internal control recommendations that need to be implemented by the respective teams. Further, inspected the internal audit report to determine whether details such as Root Cause of the audit findings, Corrective Actions required, Target Date & details of individuals responsible for	No deviations noted. No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	implemented by the respective teams. The team prepares a "Corrective Action Plan" with details such as Root Cause of the audit findings, Corrective Actions required, Target Date & details of individuals responsible for mitigation and implementation of identified controls. GRC Team tracks the closure of the action items.		mitigation and implementation of identified controls were documented within the "Corrective Action Plan". Additionally, inspected the email communications by GRC Team to determine whether the internal audit findings were shared with the respective stakeholders and tracked to closure by the GRC Team.	No deviations noted.
19	Information Security Awareness – Mailers: On a periodic basis, the GRC Team sends emails on Information Security updates and best practices to help ensure Information Security awareness among employees.	CC2.2	Inspected the Information Security awareness mailers sent by the GRC Team to determine whether employees were made aware of the updates and best practices on Information Security.	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
20	Policies on Intranet: NTT GDC & CI has published all relevant policies and procedures on intranet. Any updates to the policies and procedures are updated on the intranet.	CC2.2	Inspected the NTT GDC & CI intranet to determine whether relevant policies and procedures were updated and reviewed on an annual basis.	No deviations noted.
21	Changes to NTT GDC & CI Policies: Major updates or changes to NTT GDC & CI's policies related to system security, availability, or confidentiality are communicated to employees through emails sent by GRC Team in case of any changes to policies.	CC2.2	Inspected the emails sent by GRC Team to determine whether any major changes or updates to NTT GDC & CI's policies were communicated to the employees.	No deviations noted.
22	MSA / SOF - Reporting breaches / incidents: The security, availability, and confidentiality obligations of user	CC2.3	For a sample of newly onboarded User Organizations, inspected the MSA / SOF as applicable, to determine whether security, availability and confidentiality	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	organizations are defined in the Master Service agreement (MSA) / Service Order Form (SOF). As a part of the MSA/ (SOF), User Organizations are instructed to report any breaches / issues / complaints to NTT GDC & CI.		obligations of user organizations were defined and the process of reporting breaches to NTT GDC & CI by User Organizations was documented and communicated to the User Organizations.	
23	NDA – Contractors: Third-party vendors, who work at the company premises, are also required to sign an NDA to help ensure that third party contractors / vendors abide by the confidentiality requirements of NTT GDC & CI.	CC2.3 C1.1 C1.2	For a sample of newly onboarded third-party vendors, inspected the signed NDA to determine whether third party contractors / vendors had agreed to abide by the confidentiality requirements of NTT GDC & CI.	No deviations noted.
24	MSA - Changes to NTT GDC & CI Policies: As a part of MSA / SOF with User Organizations, NTT GDC & CI has defined the point of contact to	CC2.3	For a sample of newly onboarded User Organizations, inspected the MSA / SOF to determine whether it had a defined point of contact for	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	communicate changes / updates to NTT GDC & CI policies to User Organizations.		both NTT GDC & CI and User Organization.	
25	User Organization - Performance Reporting: On a monthly basis, a Service Performance report is sent to NTT GDC & CI's Premium and Advance User Organizations which highlights the status on the User Organization's services.	CC2.3 CC4.1 CC4.2	For a sample of months and User Organizations, inspected the Service Performance report shared with the Premium and Advance User Organizations to determine whether the report highlighted the status on the User Organization's services.	No deviations noted.
26	Vendor Due Diligence: Service providers, vendors or suppliers are subject to review as a part of the Supplier Risk Assessment process based on certain defined risk criteria. This review includes obtaining and evaluating information related to their management, quality	CC2.3 CC3.3 CC4.1 CC4.2 CC5.1 CC5.2 CC9.1	For a sample of service providers, vendors or suppliers, inspected the Supplier Risk Assessment report to determine whether risk assessment was conducted.	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	system, safety and health environment, information security, business continuity management and human resources.	CC9.2		
27	Risk Assessment Policy and Procedure: NTT GDC & CI has developed a Risk Assessment Matrix to help ensure applicable risks are identified, addressed, and monitored to ensure protection of information assets. Risk Assessment Matrix is approved by NTT GDC & CI Senior Management and reviewed at-least on an annual basis.	CC3.1 CC5.1 CC5.2 CC9.1	Inspected the Risk Assessment Policy to determine whether methodology for identifying, addressing, monitoring risks to ensure protection of information assets is documented, reviewed and approved by NTT GDC & CI Senior Management at-least on an annual basis.	No deviations noted.
28	Subscription to external bodies: NTT GDC & CI has subscribed to external reporting service like Indian Computer Emergency Response	CC3.1	Inspected the emails received by Chief Information Security Officer from external reporting services to determine whether changes to	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	Team (Cert-In) that identifies changes to applicable regulations / compliance standards relating to the services provided to User Organization.		applicable regulations / compliance standards relating to the services provided to User Organization were communicated.	
29	Vendor Governance Framework: NTT GDC & CI has developed a Vendor Management policy. The identification, assessment and management of vendor risks are carried out on an annual basis by Vendor Governance Team (part of the GRC Team), based on the documented Vendor Management policy. This policy is approved by management and reviewed periodically.	CC3.1 CC5.1 CC5.2 CC9.1	Inspected the Vendor Management Policy to determine whether methodology for identifying, addressing, monitoring of vendor risks is documented. Further, inspected whether this policy document is approved and uploaded on the internal intranet portal of NTT GDC & CI.	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
30	Risk Assessment Matrix: NTT GDC & CI has developed a Risk Assessment Matrix to help ensure that applicable risks are identified, addressed, and monitored for protection of information assets.	CC3.2 CC3.3 CC5.1 CC5.2	Inspected the Risk Management Matrix to determine whether the process of identifying risks, addressing and monitoring them was documented.	No deviations noted.
31	Risk Treatment Plan: On an annual basis, NTT GDC & CI identifies the risks associated with their various functions and facilities on Yajnetra portal an Enterprise Risk Management (ERM) portal. Based on the risks identified during the risk assessment, a Risk Assessment report is prepared for each function and facilities. Risks identified are categorized as Critical, High, Medium or Low. Based on the risk level, a Risk Treatment Plan is prepared in Yajnetra by GRC Team along with the	CC3.2 CC3.3 CC4.1 CC4.2 CC5.1 CC5.2	Inspected the Risk Assessment report to determine whether risks were identified, and their corresponding Risk Treatment plans were documented within the report on Yajnetra. Further, inspected the Risk Treatment plan to determine whether risk treatment methods and internal controls were identified to mitigate the risks.	No deviations noted. No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	respective functions where risk treatment methods and controls are identified to mitigate the risks for Critical and High Risks.			
32	Risk due to change to environment: The risks arising due to inadequate infrastructure or obsolete machinery / equipment, developments in operating, regulatory, and technology environment, or changes to policies and procedures are addressed during the Risk Assessment performed by the GRC Team for the Facility function.	CC3.2 CC3.3 CC3.4 CC4.1 CC4.2 CC5.1 CC5.2 CC9.2	Inspected the Risk Assessment report to determine whether risks arising due to inadequate infrastructure or obsolete machinery / equipment, developments in operating, regulatory, and technology environment, or changes to policies and procedures were addressed during the Risk Assessment performed by GRC Team for the Facility function.	No deviations noted.
33	Fraud Risk Assessment: On an annual basis, Information Security Team conducts Information	CC3.2 CC3.3	Inspected the Risk Assessment Report to determine whether Information Security Team	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	Security Risk Assessment exercises as part of ISO 27001 certification program. Risks are ranked on the basis of impact to confidentiality, integrity, and availability of information assets. Factors such as fraud, natural disasters, theft, etc. are also considered while performing risk assessment.		performed risk assessment for risks related to fraud, identified and rated fraud risks and documented risk mitigation measures.	
34	Internal and External Vulnerability Assessment: On a Monthly basis, a member of the Security Operations Center (SOC) team performs vulnerability assessment using Qualys tool on various servers. Nessus tool is used for Firewalls, Network Device & Storage Device Scan which is happening on Quarterly basis by SOC Team Based on the severity of the	CC3.2 CC3.3 CC4.1 CC4.2 CC6.6 CC7.1 CC7.2 CC7.3 CC7.4	For a sample of months and quarters, inspected the internal VA report from Qualys tool and Nessus tool and external VA report from PCI council approved vendor using Hacker guardian tool to determine whether VA was conducted, and the identified vulnerabilities, if any were emailed to the respective functional teams for their review and action.	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	Vulnerabilities, member of the SOC team emails the list of identified vulnerabilities to respective functional teams and functional team tracks it to closure. An external vulnerability assessment is also performed using PCI council approved vendor using Hacker guardian tool, where IP addresses are entered. Upon completion of the assessment, the vulnerabilities identified in the generated report are notified to the respective functional teams. Closure of vulnerabilities is monitored in the subsequent quarter to check for their recurrence, if any.	CC7.5		
35	Penetration Testing: On a half yearly basis, a third-party vendor conducts Penetration Testing	CC3.2 CC3.3 CC4.1	For a sample half year, inspected the email communication between the third-party vendor and GRC Team to determine whether the	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	(PT) and shares the results identified with GRC Team. Upon completion of the assessment, the vulnerabilities rated as "Critical", "High", "Medium" and "Low" in the generated report are notified to the respective functional teams by the GRC Team. Closure of vulnerabilities is monitored by the GRC Team, if any.	CC4.2 CC6.6 CC7.1 CC7.2 CC7.3 CC7.4 CC7.5	results were shared with GRC Team. Further, inspected the email communication between the GRC Team and respective functional teams to determine whether the vulnerabilities identified were notified to the respective functional teams by the GRC Team. Further, inspected the relevant snapshots of Penetration Testing report to determine whether the identified vulnerabilities, if any, were closed in the rescan report.	No deviations noted. No deviations noted.
36	Physical Access Policy and Procedures:	CC5.3 CC6.4	Inspected the Business Facility Security Management policy to determine whether the policies and procedures for managing	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	Formalized policies and procedures exist for managing physical access to NTT GDC & CI facilities. These policies and procedures are reviewed and approved by Senior Management of NTT GDC & CI on an annual basis.		physical access to NTT GDC & CI facilities were documented, reviewed, and approved by Senior Management on an annual basis.	
37	Logical Access Policy: Formalized policies and procedures exist for managing logical access to IT infrastructure of NTT GDC & CI, to restrict inappropriate and unauthorized access. These policies and procedures are reviewed and approved by Senior Director & CISO - GRC on an annual basis.	CC5.3 CC6.1	Inspected the Logical Access Management policy to determine whether the policies and procedures for managing logical access were documented, reviewed and approved by Senior Director & CISO - GRC on an annual basis.	No deviations noted.
38	Incident Management Policy: Formalized policies and procedures exist for managing security, availability, and confidentiality	CC5.3 CC7.1 CC7.2	Inspected the Incident Management Policy to determine whether policies and procedures for managing security, availability,	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	related incidents within the organization. These policies and procedures are reviewed and approved by Operation Leadership team on an annual basis.	CC7.3 CC7.4 CC7.5	and confidentiality related incidents were documented, reviewed and approved by Operation Leadership team on an annual basis.	
39	Problem Management Policy: Formalized policies and procedures exist for managing Problems within the organization. These policies and procedures are reviewed and approved by Managed Service Operations Director on an annual basis.	CC5.3	Inspected the Problem Management Policy to determine whether policies and procedures for managing problems was documented, reviewed and approved by Managed Service Operations Director on an annual basis.	No deviations noted.
40	Change Management Policy: Formalized policies and procedures exist for managing infrastructure changes in NTT GDC & CI. These policies and procedures are reviewed and approved by Senior MS	CC5.3 CC8.1	Inspected the Change Management Policy to determine whether policies and procedures for managing infrastructure changes were documented, reviewed and approved by Senior	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	Operations Director on an annual basis.		MS Operations Director on an annual basis.	
41	Business Continuity Policy: Formalized Business Continuity Management (BCM) policy and procedure has been documented to help ensure availability commitments and requirements are met for NTT GDC & CI facilities and Data Centers. This policy is approved by Senior Management of NTT GDC & CI.	CC5.3	Inspected the Business Continuity Management policy addressing availability commitments and requirements to determine whether the policy and procedure was approved by Senior Management of NTT GDC & CI.	No deviations noted.
42	Authentication: NTT AD is used to authenticate users' login into NTT GDC & CI domain.	CC6.1	Observed user authentication process to determine whether the active directory was used to authenticate users' login on to NTT domain. Further, inspected the user listing on the AD to determine whether	No deviations noted. No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
			unique user IDs were created on NTT domain.	
43	Remote Access: Remote access to NTT GDC & CI systems is provided through Fortigate VPN. VPN credentials and Two factor authentication via SafeNet tool is used to establish connection with NTT GDC & CI systems from both internal and external network.	CC6.1 CC6.6	Inspected the configuration within Fortigate VPN to determine SafeNet two factor authentication was implemented. Further, observed the process of authentication to NTT GDC & CI systems to determine whether VPN credentials and SafeNet two factor authentication was used to establish connection with NTT GDC & CI systems.	No deviations noted. No deviations noted.
44	Administrative Access – NTT AD: Administrative privileges on the NTT AD are restricted to authorized	CC6.1	Inspected user listings from the NTT AD and the HR list to determine whether administrative privileges to the AD were restricted to authorized personnel	No deviations noted

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	personnel of NTT GDC & CI's Microsoft Team.		from NTT GDC & CI's Microsoft Team.	
45	Administrative Access to CyberArk: Administrative access to network devices and perimeter firewalls through CyberArk tool is restricted to authorized personnel from Network and SOC teams and Product Engineering and Innovation Team.	CC6.1 CC6.6	Inspected the list of personnel having access to network devices through CyberArk tool and the HR list to determine whether administrative access to network devices including switches, routers and firewall was restricted to authorized personnel from Network and SOC teams and Product and Innovation Teams.	No deviations noted.
46	Password Policy: Formal password policy has been defined and established for access to domain, network devices and servers. There are separate domain controllers for servers and workstations. Passwords are	CC6.1	Inspected the password policy and password settings on NTT GDC & CI domain controllers for workstations and servers to determine whether the password settings included password expiry, password length, password	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	controlled through group policy settings which include password expiry, password length, password history, and password complexity requirements.		history, password complexity requirements and account lockout period and configured as per the password policy.	
47	Unsuccessful Logon: User account is locked after a limited number of unsuccessful logon attempts.	CC6.1	Inspected the settings on NTT domain controllers for workstations and servers to determine whether the user account was configured for lockout after a limited number of unsuccessful logon attempts.	No deviations noted.
48	Account Lockout Policy: Unattended desktops and laptops are locked after a stipulated time of inactivity.	CC6.1	Inspected the password settings on NTT domain controllers for workstations and servers to determine whether unattended desktops and laptops were configured for lockout after a stipulated time of inactivity.	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
49	Guest and Anonymous account: Guest account and anonymous logins are disabled on domain controller.	CC6.1	Inspected the active directory to determine whether the default administrator and guest account on domain controller was disabled.	No deviations noted.
50	Default accounts: Default administrator accounts on servers are renamed / disabled for security purposes.	CC6.1	Inspected the policy settings on the AD to determine whether default administrators account on servers were renamed / disabled.	No deviations noted.
51	Data Encryption – MyNTT GDC & CI: NTT GDC & CI has enabled data encryption on MyNTT portal using Secured Socket Layer (SSL) using Advanced Encryption Standard (AES) 128-bit encryption.	CC6.1 CC6.6 CC6.7	Inspected the SSL certificate for MyNTT portal to determine whether the data transmitted over the network was secured using Secured Socket Layer (SSL) using Advanced Encryption Standard (AES) 128-bit encryption.	No deviations noted.
52	Encryption of Data at Rest:	CC6.1 CC6.6	For a sample of workstations, inspected the settings / console to	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	Endpoint systems are encrypted using Bit locker / Trusted Platform Module (TPM) chip.	CC6.7	determine whether encryption is used for workstations.	
53	Email Encryption: Email communications are transmitted over the Internet using Transport Layer Security (TLS) encryption protocol using in-built feature of Microsoft Outlook.	CC6.1 CC6.6 CC6.7	For a sample email inspected the email exchange in Microsoft Outlook to determine whether encryption is used for email communications.	No deviations noted.
54	Backup Encryption: The backup is encrypted using in-built encryption within CommVault.	CC6.1 CC6.6 CC6.7	Inspected the CommVault software to determine whether backup media is encrypted.	No deviations noted.
55	Segregation of User Organization environments: Dedicated Virtual Local Area Networks (VLAN) are configured to segregate one User Organization	CC6.1	For a sample of User Organizations, inspected the VLAN configuration to determine whether the User Organization networks were segregated from	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	network from the other User Organization network.		other User Organization networks through dedicated VLANs.	
56	Administrative Privileges on Workstations: Users are not granted administrative privileges on local workstations and cannot install software / applications on local workstations.	CC6.1 CC6.8	Inspected the settings on AD to determine whether users on local machines are not given administrative privileges and cannot download software on local machines.	No deviations noted.
57	User Account creation in AD: When a new hire joins, Human Resources team sends an email to Internal IT Team with a copy to new hires reporting manager for domain account and remote access creation. Based on the authorized request from the Human Resources team, Internal IT Team creates the NTT GDC & CI domain account and grants access to the new hire.	CC6.2 CC6.3	For a sample of new hires, inspected the email communication between Human Resources Team and Internal IT team to determine whether employees reporting manager was copied on the email and NTT GDC & CI domain account creation and remote access for new hires was granted based on authorized	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
			request from the Human Resources team. Further, inspected the user creation log from AD to determine whether the NTT GDC & CI domain account was created post approval.	No deviations noted.
58	User Account revocation from AD: On the last working day of the resigned employee, Human Resources Team sends an email to the Internal IT Team for disabling the user account in NTT AD and resetting LDAP password of the user. The Internal IT Team disables the user account on the last working day, resets the LDAP Password for the resigned employee and signs off the	CC6.2 CC6.3	For a sample of resigned employees, inspected the email sent by Human Resources Team for disabling the user account in NTT AD to determine whether resignation of employees was notified to Internal IT Team on a timely basis. Further, for a sample of resigned employees inspected the Handover checklist to determine	No Deviation noted. No Deviation noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	completed Handover checklist on Ramco Fusion.		whether the checklist was signed off by Internal IT Team on the last working day indicating the timely deactivation of the domain user account. Additionally, for a sample of resigned employees, inspected the disabled date from the Active Directory to determine whether the AD account was timely disabled.	No Deviation noted.
59	Privilege Access Creation: Access to database and application servers and firewall and other network devices (switches and routers) through CyberArk Tool is provided based on approval from the Department Team Leads over ServiceNow ticket/email. The	CC6.2 CC6.3	For a sample of access requests for application/ database server, firewall and other network devices (switches and routers) through CyberArk Tool, inspected the email approvals to determine whether access provided was approved by	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	approval is then sent to IT Team for adding the user to defined security groups on domain controller.		the respective Department Team Leads. Further, for sample of access requests, inspected PIM security group to determine whether access granted was as per the access approved.	No deviations noted.
60	Privilege Access Revocation: CyberArk Tool uses the NTT AD for authentication. Access to database / application servers and network devices such as switches, routers, and firewall through CyberArk Tool is automatically disabled when AD access gets disabled.	CC6.2 CC6.3	Inspected the configuration within CyberArk Tool to determine whether the CyberArk Tool is integrated with the NTT AD. Further, for a sample of resigned employees having access to CyberArk Tool, inspected the ServiceNow tool and email sent Human Resources Team for disabling the user account in AD and for resetting LDAP password	No deviations noted. No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
			for the resigned employee to determine whether resignation of employees was notified to Internal IT Team on a timely basis. Additionally, for a sample of resigned employees having access to CyberArk tool inspected the Handover checklist to determine whether the checklist was signed off by Internal IT Team on the last working day indicating the timely deactivation domain user account. Additionally, for a sample of resigned employees, inspected the disabled date from the Active Directory to determine whether the AD account was timely disabled.	No deviations noted. No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
61	CyberArk – Restricted Access: Administrative Access to network devices through CyberArk Tool has been restricted to authorized personnel from Network, SOC and Product Engineering & Innovation teams.	CC6.2 CC6.3	Inspected the list of personnel having access to network devices through CyberArk Tool and HR list to determine whether access to network devices including switches, routers and firewall was restricted to authorized personnel from Network, SOC and Product Engineering & Innovation teams.	No deviations noted.
62	Server Commissioning: User Organizations are provided access to their servers through Implementation Request (IR) which is raised in ServiceNow tool at the time of server installation.	CC6.2 CC6.3	For a sample of User Organizations, inspected the Implementation Request (IR) raised in Service Now tool to determine whether server login credentials were shared with the User Organization as per the request.	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
63	Decommissioning Services: On decommissioning of User Organization's services, a confirmation email is sent to the User Organization indicating discontinuation of their services.	CC6.2 CC6.3 CC6.5 C1.1 C1.2	For a sample of User Organizations, inspected the decommissioning request and email communication between NTT GDC & CI and the User Organization to determine whether the services were discontinued as requested.	No deviations noted.
64	Domain Access Reconciliation: On a quarterly basis, Human Resources Team extracts a list of resigned employees from Workday tool sends it to GRC Team for access reconciliation. GRC Team compares the list of resigned employees with the active users within the AD and sends the results of this comparison to Internal IT Team. Basis the results received from GRC Team; Internal IT	CC6.2 CC6.3	For a sample of quarters, inspected the email communication between Human Resources Team, GRC Team and Internal IT Team to determine whether list of resigned employees from Workday tool was reconciled with the active users from the AD and corrective actions were communicated to Internal IT Team in case of discrepancies identified.	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	Team takes corrective action in case of any discrepancies.		Further, for a sample of quarters, inspected the email communication between GRC Team and Internal IT Team to determine whether corrective actions taken by Internal IT Team in case of any discrepancies identified.	No deviations noted.
65	PIM Access Review: On a quarterly basis, PIM Team (part of IT Operations Team) sends the active user list from CyberArk Tool to all the Tower Leads from IT Operations Team for review. The Tower Leads verify the appropriateness of the access and confirm to PIM Team. In case of discrepancies, Team Leads raise a ServiceNow ticket and corrective	CC6.2 CC6.3	For a sample of quarters, inspected the email communication between PIM Team and the respective Tower Leads to determine whether the Tower Leads reviewed the active user list from respective CyberArk Tool groups and necessary actions were communicated to the PIM Team in case of any discrepancies noted via ServiceNow ticket.	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	actions are taken by IT Support Team.			
66	Security Guards: Security guards are stationed at entry and exit points and work in shifts to monitor the physical access to NTT GDC & CI facilities & Data Centers. A shift register is maintained to record the work shifts of the security guards.	CC6.4	Visited the Data Center premises (for Mumbai and Delhi DCs) and through the use of video streaming technology (for other than Mumbai and Chennai location DCs) assisted by NTT GDC & CI Administration Team and GRC Team personnel, inspected the facilities & Data Centers to determine whether security guards were stationed at entry and exit points of the NTT GDC & CI facilities & Data Centers. Further, for a sample of days and Data Centers, inspected the shift register for security guards to determine whether security guards work in shifts to monitor	No deviations noted. No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
			the physical access to NTT GDC & CI facilities and Data Centers.	
67	CCTV: Closed Circuit Television (CCTV) surveillance equipment is used by the security guard to monitor the entry and exit points at NTT GDC & CI facilities. CCTV logs are retained by Administration team for a period of 90 days.	CC6.4	Visited the Data Center premises (for Mumbai and Delhi DCs) and through the use of video streaming technology (for other than Mumbai and Chennai location DCs) assisted by NTT GDC & CI Administration Team and GRC Team personnel and inspected the NTT GDC & CI facilities and BMS rooms to determine whether CCTV surveillance equipment was installed at the entry and exit points and the CCTV recordings were being monitored by the security guard in the BMS rooms. Further, for a sample of data centres, inspected CCTV console	No deviations noted. No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
			to determine whether the CCTV logs were retained as per NTT GDC & CI's CCTV retention policy.	
68	Access Control System – Facility: Proximity card-based access control systems are installed at entry and exit points to restrict unauthorized entry into NTT GDC & CI facilities. Additionally, parking spaces are maintained at a safe distance from the Data Centers and vehicles entering the facility are scanned.	CC6.4	Visited the Data Center premises (for Mumbai and Delhi DCs) and through the use of video streaming technology (for other than Mumbai and Chennai location DCs) assisted by NTT GDC & CI Administration Team and GRC Team personnel, inspected the NTT GDC & CI facilities to determine whether proximity card-based access control systems were installed at entry and exit points, parking spaces were maintained at a safe distance from the Data Centers and vehicles entering the facility were scanned.	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
			Further, for a sample of days, inspected the proximity card-based access control system logs to determine whether the proximity card-based access control system was operational.	No deviations noted.
69	Access Control System – Data Center: Access to Data Center Server Hall is controlled by proximity card-based access control system.	CC6.4	Visited the Data Center premises (for Mumbai and Delhi DCs) and through the use of video streaming technology (for other than Mumbai and Chennai location DCs) assisted by NTT GDC & CI Administration Team and GRC Team personnel, inspected the Data Centers to determine whether access to Data Centers was controlled by biometric and proximity card-based access control system.	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
			For a sample of days, inspected the proximity card-based access control system logs to determine whether the proximity card-based access control system was operational.	No deviations noted.
70	Physical Access creation: When an employee joins, Human Resources Team sends an email to Physical Security Team with a copy to employee's reporting manager for physical access creation for a new employee. Based on the authorized request Physical Security Team grants default access to common area to the new employee.	CC6.4	For a sample of new hires, inspected the email communication between Human Resources Team, Physical Security Team and employee's reporting manager to determine whether default access to common area for new hires was authorized by the Human Resources team. Further, for a sample of new hires, inspected the card activation date in Solus application to determine whether physical access card was	No deviations noted. No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
			activated post authorization from Human Resources team.	
71	Data Center: Access to Data Centers is restricted to authorized personnel from Facilities Operations, IT Operations and Global Service Desk, Service Account Management and Product Engineering & Innovation teams only.	CC6.4	Inspected the list of personnel having access to Data Centers to determine whether access to Data Centers was restricted to authorized personnel from Facilities Operations, IT Operations and Global Service Desk, Service Account Management and Product Engineering & Innovation teams only.	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
72	Access Revocation: On the last working day of the resigned employee, Human Resources Team sends an email to Physical Security Team for deactivating the physical access to NTT GDC & CI facilities and Data Centers. Physical Security Team signs off the completed Handover checklist and confirms to Human Resources Team on Ramco Fusion / Workday tool post deactivation of the access associated with the card.	CC6.4	For a sample of resigned employees, inspected the email sent by the Human Resources Team to determine whether resignation of employees was notified to Physical Security Team on a timely basis for access deactivation. Further, for a sample of resigned employees inspected the Handover checklist to determine whether the checklist was signed off by Physical security Team on the last working day indicating the timely deactivation of the physical access.	No deviations noted. No deviations noted.
73	Visitor Access: Security guards at the reception are responsible to help ensure that the	CC6.4	Visited the Data Center premises (for Mumbai and Chennai DCs) and through the use of video streaming	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	details of the visitors or vendors such as name of visitor or vendor, organization name, contact details, contact person, entry & exit time are recorded within the VMS maintained at the reception for permitting entry to NTT GDC & CI facilities & Data Centers.		technology (for other than Mumbai and Chennai location DCs) assisted by NTT GDC & CI Administration Team and GRC Team personnel, inspected the NTT GDC & CI facilities and Data Centers to determine whether the security guards at the reception supervised the details entered by visitor or vendor such as name of visitor or vendor, organization name, contact details, contact person, entry & exit time in the Visitor Management System (VMS) prior to allowing entry inside the Data Centers. Further, for a sample of days, inspected the logs from the VMS to determine whether name of visitor or vendor, organization name,	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
			contact details, contact person, entry and exit time were recorded.	
74	Material Movement: Material movement is recorded in the Material Movement Register / Physical Challan copies. Outward material movement is approved by authorized personnel from User Organization or Facilities Team.	CC6.4	For a sample of days, inspected the Material Movement Register / Physical Challan copies to determine whether material movement details including company name, material details, quantity and time in/time out were recorded within the register. Further, for a sample of days, inspected the outward challan copies to determine whether the outward movement of material was either approved by authorized personnel from User Organization or Facilities Team.	No deviations noted. No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
75	Access Validity: Access given to employees is valid for a maximum period of six months.	CC6.4	For a sample of new hires, inspected the access validity from the Solus to determine whether the access granted was valid for a maximum period of six months.	No deviations noted.
76	Access Reconciliation: Access given to employees are renewed on a half-yearly basis by Human Resources Team. Physical Security Team emails the list of active employees having access to NTT GDC & CI facilities from the Solus tool to Human Resources Team. Human Resources Team extracts the list of resigned employees and active employees from the Fusion tool and compares it with active users within the Solus tool. Human Resources Team emails the discrepancies to Physical Security Team for	CC6.4	Inspected the email communication between Physical Security Team and Human Resources Team, resigned employees and active employees list extracted from the Fusion tool and active employees list extracted from Solus tool to determine whether access reconciliation and renewal was performed and approved by Human Resources Team, and corrective actions, if any were taken by the Physical Security Team.	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	revocation of inappropriate access. Physical Security Team takes the necessary corrective actions			
77	Asset Disposal Policy: NTT GDC & CI has a formal asset classification and disposal policy stating procedures for secure disposal of assets. The Policy is approved by Senior Management of NTT GDC & CI and available on the intranet portal for employee access.	CC6.5 C1.1 C1.2	Inspected the Asset Disposal Policy to determine whether procedures for secure disposal of assets were documented and approved by senior management of NTT GDC & CI. Further, Inspected the intranet portal to determine whether the policy was uploaded on the intranet portal for employees to access.	No deviations noted. No deviations noted.
78	Secure Disposal: All assets (laptops / desktops / servers, etc.) are disposed off using secure sanitization methods prior to	CC6.5 C1.1 C1.2	For a sample of disposed assets, inspected the asset disposal certificates to determine whether	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	removal of these assets from NTT GDC & CI environment.		the data was wiped clean from the asset prior to disposal.	
79	Firewall: NTT GDC & CI has implemented firewall on the Internet gateway to protect against security, availability, and confidentiality threats from sources outside the NTT GDC & CI network perimeter boundaries. Rules are configured on Fortigate firewall, to regulate traffic in and out of NTT GDC & CI network. Rules are enforced on firewall to 'deny all' accesses to NTT GDC & CI network with access enabled for specific services as per business requirements.	CC6.6	Inspected the NTT GDC & CI network diagram and the configurations within Fortigate Firewall to determine whether firewalls have been implemented on the Internet gateway. Inspected the firewall configuration from FortiGate tool to determine whether rules were defined and enforced to regulate traffic in and out of NTT GDC & CI's network. Further, inspected the firewall rules to determine whether rules were enforced on firewall to 'deny all' accesses to NTT GDC & CI network with access enabled for	No deviations noted. No deviations noted. No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
			specific services as per business requirements.	
80	IPS / IDS: NTT GDC & CI has deployed network based IPS/IDS at the external network perimeter to monitor the network traffic and prevent and detect intrusions into their network. NTT GDC & CI uses FortiGuard tool to manage IPS/IDS. The IPS/IDS is updated by NTT GDC & CI with signatures received from the vendor as and when they are released.	CC6.6 CC6.8 CC7.1 CC7.2 CC7.3 CC7.4 CC7.5	Inspected FortiGuard tool configuration for IPS/IDS to determine whether the IPS/IDS feature was enabled in the firewall. Further, inspected the IPS/IDS settings in FortiGuard tool to determine whether the IPS/IDS was configured to be updated with signatures as and when received from the vendor.	No deviations noted. No deviations noted.
81	URL Filtering: URL filtering has been enabled within the firewall to regulate internet usage.	CC6.6	Inspected the firewall settings to determine whether URL filtering had been enabled within the firewall to regulate internet usage.	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
			For a sample workstation, reperformed the process to access the blocked websites to determine whether the access was blocked.	No deviations noted.
82	Active Directory event monitoring: Logging has been enabled for network devices, servers and firewalls on Logstash Server. The logs are sent to a remote syslog server from where Monitoring Team reviews the logs on a daily basis for any exceptions within the Kibana Tool. Monitoring Team shares the log review report with CISO. On a daily basis, CISO reviews the log review report and communicates the exceptions noted, if any to the monitoring team.	CC6.6	Inspected the Logstash server to determine whether logging was enabled for network devices, servers and firewalls on Logstash Server. The logs are sent to a remote syslog server. For a sample of day, inspected the email communication between the Monitoring Team and GRC Team to determine whether the log review report was reviewed by GRC Team.	No deviations noted. No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
83	System Availability monitoring: NTT GDC & CI uses CheckMK tool to manage the capacity of its servers as a part of system availability monitoring process. SOC Team monitors the dashboard of the CheckMK tool which shows the status of servers. Based on the thresholds defined, the dashboard shows the status of parameters such as disk space, memory usage, and CPU usage of the servers.	CC6.6 CC7.1 CC7.2 CC7.3 CC7.4 CC7.5	Inspected the CheckMK tool to determine whether the parameter thresholds were configured as per the defined thresholds.	No deviations noted.
84	Data Security: Removable media devices, such as Universal Serial Bus (USB) mass storage devices are disabled on the end-user workstations through the AD group policies.	CC6.7	Inspected the configuration on domain controller to determine whether USB was disabled on the end user workstations.	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
85	Endpoint Protection Solution: NTT GDC & CI has implemented CrowdStrike Falcon EDR solution on its workstations, laptops, and servers. CrowdStrike is a cloud-delivered solution that unifies next generation antivirus (NGAV) and provides protection against viruses and malware. CrowdStrike uses NGAV analysis to scan for vulnerabilities in real time to prevent any installation of virus or malware.	CC6.8	Inspected the CrowdStrike Falcon EDR antivirus server configuration to determine whether the next generation antivirus is used as an end point security solution for NTT GDC & CI's workstation, laptops, and servers.	No deviations Noted.
86	Hardening Policies: A formal hardening policy exists for NTT GDC & CI servers and network devices. The hardening policy is approved by senior management and is available on intranet portal accessible to all employees.	CC7.1 CC7.2 CC7.3 CC7.4 CC7.5	Inspected the hardening document to determine whether configurations are documented to help ensure server and network device security.	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
87	Logging and Monitoring: Logging has been enabled for network devices, servers and firewalls etc to forward logs to ELK Stack. Log review team reviews the logs on daily basis for any exceptions/errors within the Kibana tool. Monitoring Team shares the log review report with the CISO. On a daily basis, CISO reviews the log review report and communicates the exceptions noted, if any to the monitoring team.	CC7.1 CC7.2 CC7.3 CC7.4 CC7.5	Inspected the Logstash server to determine whether logging was enabled for network devices, servers and firewalls on Logstash Server. The logs are sent to a remote syslog server. Further, for a sample of days, inspected the log review report prepared by the Monitoring Team to determine whether logs were reviewed by the Network Operations Centre (NOC) team on a daily basis. For a sample of days inspected the email communication between the Monitoring Team and GRC team to determine whether the log review report was reviewed by GRC team.	No deviations noted. No deviations noted. No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
88	Security Incident Policy: Formalized policies and procedures exist for managing the information security incidents logged by User Organizations' or NTT GDC & CI employees.	CC7.1 CC7.2 CC7.3 CC7.4 CC7.5	Inspected the Incident Management policy to determine whether policies and procedures for managing information security incidents were documented.	No deviations noted.
89	Incident Resolution: For Incident tickets with severity S1, a workaround resolution is provided within an incident ticket in line with the defined Service Level Agreement (SLA). A problem ticket is created for all S1 category incidents and Root Cause Analysis (RCA) is performed. The RCA is reviewed and approved by a member of Incident management team, and the problem ticket is marked as resolved. For incident tickets with severity S2, S3 and S4, resolution is given based	CC7.1 CC7.2 CC7.3 CC7.4 CC7.5	For a sample of Incident tickets, inspected incident tickets to determine whether the resolution was provided within the defined SLAs, as per the severity and documented within the ticket. Performed inquiry with Manager – Compliance team and determined that SLAs defined within MSA for resolution of S2, S3 and S4 incidents are common for all NTT GDC & CI user organization.	No deviations noted. No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	on the defined SLAs and comments are documented within the incident ticket. The SLAs are defined in the Master Service Agreement (MSA) signed with the user organization.		Further, for sample Incident tickets with S2, S3 and S4 severity, inspected the incident tickets and MSA signed with a user organization to determine whether SLA was defined within the MSA, and incident was resolved as per the defined SLAs and comments were documented within the ticket.	No deviations noted.
90	Security Incidents: Physical security incidents are logged within ServiceNow ticketing tool. A Root Cause Analysis (RCA) is performed for the incidents and the action taken is documented within the ServiceNow ticket. Administration Head reviews and approves the RCA and actions taken	CC7.1 CC7.2 CC7.3 CC7.4 CC7.5	For a sample of physical security incidents, inspected the incident ticket to determine whether RCA was performed and actions taken were documented within the security incident ticket. Further, inspected the incident ticket to determine whether	No deviations noted. No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	within the ServiceNow ticketing tool. Based on approval, a member of the Administration team marks the ticket as resolved.		Administration Head reviewed and approved the RCA and actions taken within the incident ticket and the ticket was marked as resolved based on approval from the Administration head.	
91	MIS Reporting - Incident Management: On a monthly basis, IT Operations Team prepares a Management Information System (MIS) report which details the list of incidents which are open / closed, and key activities performed during the month. This report is shared with the IT Operations Head.	CC7.1 CC7.2 CC7.3 CC7.4 CC7.5	For a sample of months, inspected the MIS report to determine whether the list of incidents which were open/closed and key activities performed were recorded in the report. Further, inspected the email communication to determine whether the MIS report was shared with the IT Operations Head.	No deviations noted. No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
92	Change Authorization: The Change Requestor logs the Change Request (CR) in ServiceNow Tool with details such as severity, description, location and change type. The Team Leader (TL) approves the CR in ServiceNow Tool, and the Change Requestor receives an automatic notification of change approval from ServiceNow tool.	CC7.5	For a sample of Change Requests, inspected the ServiceNow Tool to determine whether the Change requestor had mentioned details such as severity, description, location, change type and whether the CR was approved by the TL.	No deviations noted.
93	Change Advisory Board (CAB) Review: The CM initiates CAB review. Changes planned for the week are approved in the weekly CAB / ECAB review meeting.	CC8.1	For a sample of Change Requests, inspected the ServiceNow Tool to determine whether the changes were approved by CAB / ECAB as per the policy. For a sample of weeks, inspected the CAB / ECAB meeting invites and MOMs to determine whether	No deviations noted. No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
			the changes planned for the week were discussed in the CAB / ECAB meeting.	
94	Change Testing: Testing is performed, wherever applicable and test results are documented in ServiceNow Tool.	CC8.1	For a sample of Change Requests, inspected the Test results in ServiceNow Tool to determine whether testing was performed, and results were documented.	No deviations noted.
95	MIS Reporting - Change Management: On a monthly basis, Operations Team prepares a Management Information System (MIS) report which details of the list of changes open / close, and key activities performed during the month. This report is shared with the IT Operations Head.	CC8.1	For a sample of months, inspected the MIS report to determine whether the list of changes which were open/closed and key activities performed were recorded in the report. Further, inspected the email communication to determine that the MIS report was shared with IT Operations Head.	No deviations noted. No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
96	Availability and Capacity Monitoring: NTT GDC & CI uses CheckMK tool to manage the capacity of its servers including File system, memory utilization, CPU load, network devices, ports, CPU utilizations, SNMP information, etc. as a part of its system availability monitoring process. SOC Team monitors the dashboard of the CheckMK tool which shows the status of servers. Based on the thresholds defined, the dashboard reports on parameters such as disk space, memory usage, and CPU usage of the servers. In case of parameter breaches, the dashboard generates an alert, and an auto Incident is logged in the ServiceNow Tool. Based on the email alert, the ServiceNow tool notifies	A1.1	For a sample of threshold parameters defined by NTT GDC & CI, inspected the CheckMK tool to determine whether the parameter thresholds were configured as per the defined thresholds. Further, for a sample of auto incident tickets logged in the ServiceNow tool inspected the tickets to determine whether the threshold breaches were logged as incidents and followed the incident management process for corrective actions.	No deviations noted. No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	relevant server owners of corrective actions. The ticket then follows the Incident Management Process.			
97	Network Redundancy: For critical utilities / equipment supporting NTT GDC & CI business operations, NTT GDC & CI has built NTT GDC & CI Data Center facilities which are designed to support resiliency and redundancy. The redundancy is intended to minimize the impact of common equipment failures and environmental risks.	A1.1	Inspected the network diagram to determine whether NTT GDC & CI has built NTT GDC & CI facilities and Data Centers which were designed to support resiliency and redundancy.	No deviations noted.
98	Capacity Utilization Reports: On a monthly basis, "Capacity Utilized Reports" are sent to the vendor and internal stakeholders by the Backup Team. The report	A1.1	For a sample of months, inspected the email communication between Backup Team, vendor and Internal Stakeholders and capacity utilization report to determine	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	highlights the space utilization in CommVault.		whether the "Capacity Utilized Reports" were sent to the vendor and internal stakeholders.	
99	Backup and Restoration Policy: Formalized process and policy document exists for Backup and Restoration to assist in the continuity of business operations by maintaining backup. This process is reviewed and approved by Senior Director GRC & CISO on an annual basis.	A1.1	Inspected the Backup and Restoration policy to determine whether the policies and procedures for managing backup and restoration were documented, reviewed and approved by Senior Director GRC & CISO on an annual basis.	No deviations noted.
100	Fire Detection and Prevention: Smoke detectors and hand-held fire extinguishers are installed within the Data Center at strategic points. Fire detection and suppression units such as fire alarm, Novec 1230 fire suppression fluid and water	A1.2	Visited the Data Center premises (for Mumbai and Delhi DCs) and through the use of video streaming technology (for other than Mumbai and Delhi location DCs) assisted by NTT GDC & CI Administration Team and GRC Team personnel,	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	sprinklers are installed at various locations within the Data Centers. Servers within the Data Center Server halls are placed on raised floors. Water leak detection system is installed to detect water leakage. Rodent system is installed to avoid rats.		inspected the facilities & Data Centers to determine whether smoke detectors, hand-held fire extinguishers, fire alarm, Novec 1230 fire suppression fluid, water sprinklers, water leak detection system and rodent system. Further, visited the Data Center premises (for Mumbai and Delhi DCs) and through the use of video streaming technology (for other than Mumbai and Chennai location DCs) assisted by NTT GDC & CI Administration Team and GRC Team personnel, inspected the Data Centers to determine whether servers within the Data Center Server halls were placed on raised floors.	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
101	Fire Drills: On a half yearly basis, fire drills are carried out at the NTT GDC & CI facilities in scope.	A1.2 A1.3	For a sample of delivery centers, inspected the fire drill reports for the NTT GDC & CI facilities in scope to determine whether fire drills were successfully carried out during the review period.	No deviations noted.
102	UPS and Diesel Generators: Data Centers are supported by UPS and Diesel Generators for continuous operation of information processing equipment in the event of power failure.	A1.2	Visited the Data Center premises (for Mumbai and Chennai DCs) and through the use of video streaming technology (for other than Mumbai and Chennai location DCs) assisted by NTT GDC & CI Administration Team and GRC Team personnel, inspected the Data Centers to determine whether UPS and Diesel Generators existed to help ensure continuous operation of information processing equipment in the event of power failure.	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
103	Temperature & Humidity Monitoring: Facilities Team monitors the temperature and humidity monitoring tool. Every two to four hours, a security guard visits the Data Centers to help ensure that the temperature and humidity conditions are maintained in the system.	A1.2	For a sample of days, inspected the logs from the temperature and humidity monitoring tool, to determine whether the monitoring system was operational, and security guards visited the data centres every two to four hours to help ensure that the temperature and humidity conditions are maintained in the system.	No deviations noted.
104	Preventive Maintenance: For the Data Centers, NTT GDC & CI has documented a preventive maintenance calendar maintaining the list of critical equipments important for maintaining business continuity. Critical equipments such as UPS, power generators, smoke detectors, fire extinguishers, power supply, access control, humidity	A1.2	For a sample of delivery centres, inspected the preventive maintenance calendar to determine whether list of critical equipments important for maintaining business continuity was maintained. Further, for a sample of equipments and delivery centres, inspected the preventive	No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	monitoring and temperature monitoring are serviced as per the preventive calendar.		maintenance report to determine whether Critical equipments such as UPS, power generators, smoke detectors, fire extinguishers, power supply, access control, humidity monitoring and temperature monitoring were serviced as per the preventive calendar.	
105	Daily / Weekly Backup: Daily incremental and/or weekly full backup is scheduled using CommVault Tool as agreed with respective server owners. Backup Team is notified with backup status post completion of the backup and in case of backup failure, an incident ticket is automatically raised in ServiceNow Tool. Based on the ticket	A1.2	For a sample of servers, inspected the backup configuration to determine whether daily incremental and /or weekly full backup was scheduled. Further, for a sample of backup failure incident tickets, inspected the ticket logs to determine whether corrective actions were	No deviations noted. No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	raised, Backup Team takes corrective actions.		taken by Backup Team in case of backup failure.	
106	Data Restoration: Backup Team raises a ticket in ServiceNow to perform restoration of data on NTT GDC & CI servers' basis on Customer request. A Backup Team member performs the data restoration activity and updates the resolution in the ticket post successful completion of the restoration.	A1.2 A1.3	For a sample of backup restoration tickets, inspected the ServiceNow Tool to determine whether the restoration of Customer data was performed successfully by Backup Team.	No deviations noted.
107	BCP Drills: NTT GDC & CI Facility Team performs BCP drills for covering business disruption and continuity risks on basis of the internal BCP test calendar. Infrastructure availability, system and data availability,	A1.3	Inspected the BCP drill report to determine whether BCP drill was carried out by the Facility Team during the review period. Further, inspected the BCP drill report to determine whether Test	No deviations noted. No deviations noted.

Applicable Trust Service Criteria Mapped to NTT GDC & CI Controls & Independent Auditor's Tests and Results of Tests				
Control #	Controls specified by NTT GDC & CI	Control Criteria	Tests Performed by EY	Results of Tests
	uninterrupted process flow and training of personnel to handle disaster are areas covered as a part of the BCP activity. A BCP test report which highlights the tests conducted and their test results is prepared post the activity. Improvement areas are also documented within the report.		results and improvement areas were documented in the report.	
108	Internal Audit Calendar: GRC Team creates an Internal Audit calendar at the beginning of the financial year, which contains the list of audits to be carried out during the year. The audit calendar is finalized on basis of external audit schedules and inputs from other risk management functions of the company. Internal Audit is performed through the Yajnetra portal.	CC2.2 CC4.1 CC4.2 CC7.1 CC7.2 CC7.3 CC7.4 CC7.5	Inspected the Internal Audit calendar to determine whether internal audit was planned for different functions for the year. Further, inspected the Yajnetra portal and performed inquiry with GRC team to determine whether Yajnetra portal was used to perform the Internal Audit.	No deviations noted. No deviations noted.