TISAX® Assessment Report

Follow-Up

Cyient Limited

SMYMPH

A1L42C-3

10th May 2024

Version 1.0

Initial Remarks

This Assessment Report and its underlying assessment was created by qualified experts of an TISAX audit provider. It expresses professional judgement of the effectiveness of control procedures based on the current state of implementation and in accordance to the Audit Provider Criteria and Assessment Requirements (ACAR) of the Trusted Information Security Assessment Exchange (TISAX) as defined and published by ENX Association at the time of the issuance of this report.

The Trusted Information Security Assessment Exchange (TISAX) is operated and governed by ENX Association. TISAX was created to provide commonly accepted assessments based on the ISA control catalogue conducted by trustworthy competing audit providers. Detailed information about TISAX can be found at http://www.enx.com/tisax/.

This Assessment Report is intended exclusively for use within TISAX. All distribution or exchange of TISAX Assessment Results must follow the rules for information exchange established for TISAX Participants and TISAX Audit Providers within the applicable TISAX agreements and guidelines.

No exchange of TISAX Assessment Results outside the defined TISAX information exchange proceedings or exchange with third parties outside the TISAX shall take place. Please be aware that certain rights provided by the applicable TISAX legal framework may cease when exchanging TISAX Assessment Results outside the set guidelines.

The underlying assessment engagement is not designed to detect all weaknesses in control procedures because it is not performed continuously throughout the period and the checks performed on the control procedures are on a sample basis. As such, even though checks are conducted with due diligence, misstatements due to errors or fraud may occur and go undetected.

Additionally, the assessment was based on the situation at the day of the assessment and does not account for any changes in the future. Any projections of any evaluation to future periods are subject to the risk that the report may become inadequate because of changes in conditions, or that the level of compliance with the policies or procedures may deteriorate.

Report Structure

This report is structured as follows:

A. Assessment Related Information
B. Summarized Results
C. Assessment Result Summary
D. Maturity Levels of VDA ISA (Result Tab)
E. Detailed Assessment Results

The structure and headlines reflect different levels of possible disclosure regarding its content towards other TISAX Participants.

Starting with general information about the assessment (A. Assessment-Related Information), it spans from a summary of results (B. Summarized Results, C. Assessment Result Summary) to the very details of the assessment (D. Maturity Levels of ISA and E. Detailed Assessment Results).

A. Assessment Related Information

1.1 Assessment Scope

TISAX® Scope-ID	SMYMPH
Scope Type	☒ Standard Scope 2.0 *The TISAX Scope defines the scope of the assessment. The assessment includes all processes, procedures and resources under responsibility of the assessed organization that are relevant to the security of the protection objects and their protection goals as defined in the listed assessment objectives at the listed locations.* *The assessment is conducted at least in the highest Assessment Level listed in any of the listed Assessment Objectives. All assessment criteria listed in the listed assessment objectives are subject to the assessment.* ☐ Custom Extended Scope ☐ Full Custom Scope
Assessment Objectives	☒ Handling of Information with High Protection Level ☐ Handling of Information with Very High Protection Level ☐ Handling of Prototype Components and Parts ☐ Handling of Prototype Vehicles ☐ Use of Test Vehicles ☐ Events and Photo Shootings with Objects in Need of Protection ☐ Handling of Personal Data according to article 28 GDPR (“processor”) ☐ Handling with Special Categories of Personal Data (article 9 GDPR) according to article 28 GDPR (“processor”)
Assessment Requirements	ACAR – TISAX Specification of Assessment Version 2.1: Family-ID: ISA, Version 5.0

1.2 Assessed Locations

Company Name	Address	Location-ID	Contact Person
Cyient Limited	Plot Nos. 11, Infocity, Madhapur 500082 Hyderabad	LWX7V8	Srinivasa Rao Mathi Srinivasa.Mathi@cyient.com
Cyient Limited	Plot Nos. 2,Nanakramguda Manikonda 500032 Hyderabad Telengana India	L9ZM27	Srinivasa Rao Mathi Srinivasa.Mathi@cyient.com
Cyient Limited	Plot Nos. 110A, 110B Phase 1, Electronics city	LT21ZC	Srinivasa Rao Mathi Srinivasa.Mathi@cyient.com

	Hosur Road, 560100 Bangalore Karnataka		

The auditor confirms that all information above is verified to be accurate.

1.3 Initial Assessment

TISAX® Assessment-ID	A1L42C-1
Assessment Level	AL2
Assessment Method	☒ Plausibility check of self-assessment using evidences and documentation ☒ Detailed evaluation of evidence ☒ Interviews with persons involved in the processes of the auditee ☐ On-site Inspection ☐ Video based remote site inspection
Date of Kick-Off Meeting	12th April 2024
Date of Opening Meeting	03rd May 2024
Date of Closing Meeting (Effective Date)	04th May 2024
Consent of Auditee	The auditee ☒ unqualifiedly agrees on the documented conclusions. ☐ qualifiedly agrees on assessment conclusions (auditee's dissenting comments are included and marked in the report).

TISAX® Assessment-ID	A1L42C-2
Corrective Action Plan Date	<09th May 2024>
Consent of Auditee	The auditee ☒ unqualifiedly agrees on the documented conclusions. ☐ qualifiedly agrees on assessment conclusions (auditee's dissenting comments are included and marked in the report).

Corrective Action Plan Assessment

Preparations	Estimated amount of audit days: <1hrs> Type of Follow-Up: ☐ **on-site** ☒ **off-site** Expected Datum: <09th May 2024>
TISAX® Assessment-ID	A1L42C-3

Assessment Method	☒ Based on available documentation ☐ Based on Interviews with persons involved in the processes of the auditee ☐ On-site Inspection
Follow-Up Date	10th May 2024
Consent of Auditee	The auditee ☒ unqualifiedly agrees on the documented conclusions. ☐ qualifiedly agrees on assessment conclusions (auditee's dissenting comments are included and marked in the report).

Authors

Auditor
Girija Togarati- Lead Auditor Vijay Reddy- Observer Auditor
Quality Assurance
DQS GmbH, Ulrich Merz

Frankfurt, 8th May 2024

signed: Girija Togarati
Signature

signed: Ulrich Merz
Signature

B. Summarized Results

2.1 Initial Assessment

AL2: Based on the observations during the initial assessment the overall assessment of the scope is:

☐ Conform

☒ Minor non-conform (only minor non-conformities exist)

- ☐ Minor non-conformities without defined corrective actions exist.
- ☒ All minor non-conformities have defined corrective actions. Latest corrective action is due on <09th May 2024> (temporary labels may be issued until this date).
- ☐ A video supported remote assessment method has been conducted and an on-site inspection has been scheduled as part of corrective actions.
- ☐ The overall maturity level is less than 10% of the target maturity level (<2,7).

☐ Major Non-conform

- ☐ Some of the non-conformities create immediate significant risks, in addition to a suitable corrective action plan, compensating measures must be implemented before the status can change to “Minor Non-conform”
- ☐ The overall maturity level is less than 30% of the target maturity level (<2,1).

In total, **0** major and **1** minor non-conformities to the assessed catalogue were identified.

After the initial assessment an average maturity level of **2.98** was calculated.

2.2 Corrective Action Plan Assessment

Based on the observations during the corrective action plan assessment the overall assessment of the scope is:

☐ Minor non-conform (only minor non-conformities exist)

- ☐ Minor non-conformities without defined corrective actions exist.
- ☒ All minor non-conformities have defined corrective actions. Latest corrective action is due on <09th May 2024> (temporary labels may be issued until this date).
- ☐ The overall maturity level is less than 10% of the target maturity level (<2,7).

☒ Major Non-conform

- ☒ Some of the non-conformities create immediate significant risks, in addition to a suitable corrective action plan, compensating measures must be implemented before the status can change to “Minor Non-conform”.
- ☐ The overall maturity level is less than 30% of the target maturity level (<2,1).

In total, {0 major and 1 minor non-conformities to the assessed catalogue were identified.

A corrective action plan was presented by the auditee to the auditor during the initial assessment.

2.3 First Follow-Up

Based on the observations during the follow-up on <date> the overall assessment of the scope is:

☒ Conform

☐ Minor non-conform (only minor non-conformities exist)

☐ Minor non-conformities without defined corrective actions exist.

☐ All minor non-conformities have defined corrective actions. Latest corrective action is due on <date> (temporary labels may be issued until this date).

☐ The overall maturity level is less than 10% of the target maturity level (<2,7).

☐ Major Non-conform

☐ Some of the non-conformities create immediate significant risks, in addition to a suitable corrective action plan, compensating measures must be implemented before the status can change to “Minor Non-conform”.

☐ The overall maturity level is less than 30% of the target maturity level (<2,1).

There are no longer deviations to the requirements.

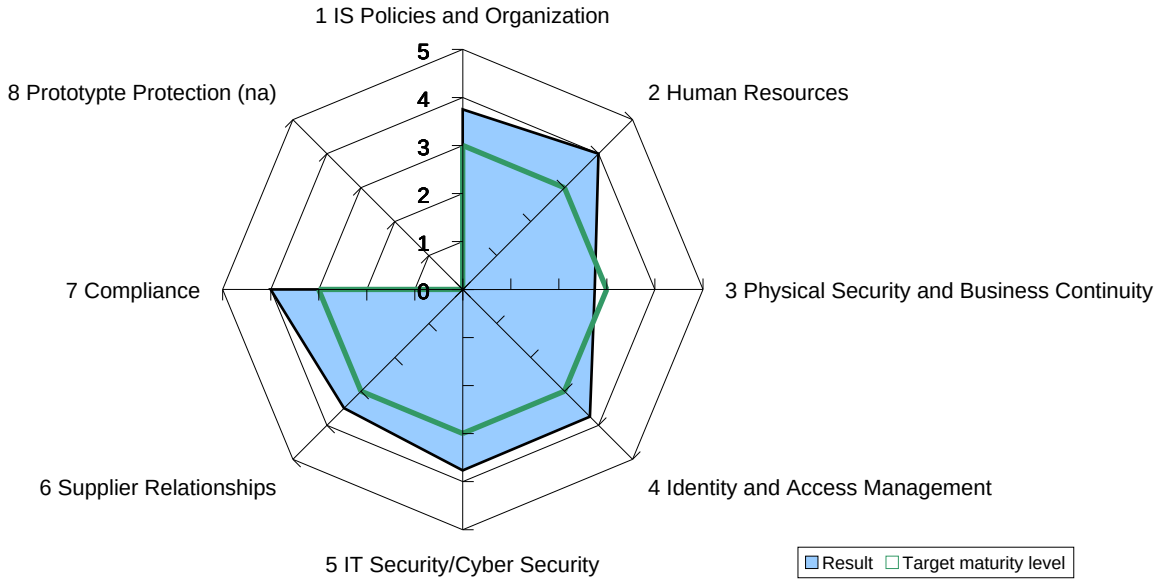
A total of **0** major and **0** minor non-conformities to the assessed requirements remain.

After the follow-up assessment an average maturity level of 3 is calculated

C. Assessment Result Summary

3.1 Initial Assessment

The individual areas of the initial maturity levels can be found in the spider web diagram below.



The major and/or minor non-conformities, as applicable, were identified in the following Areas:

No.	Area	Number of major non-conformities	Number of minor non-conformities
1	IS Policies and Organization	0	0
2	Human Resources	0	0
3	Physical Security and Business Continuity	0	1
4	Identity and Access Management	0	0
5	IT Security / Cyber Security	0	0
6	Supplier Relationships	0	0
7	Compliance	0	0
8	Prototype Protection	NA	NA
9	Data Protection	NA	NA

3.2 Corrective Action Plan Assessment

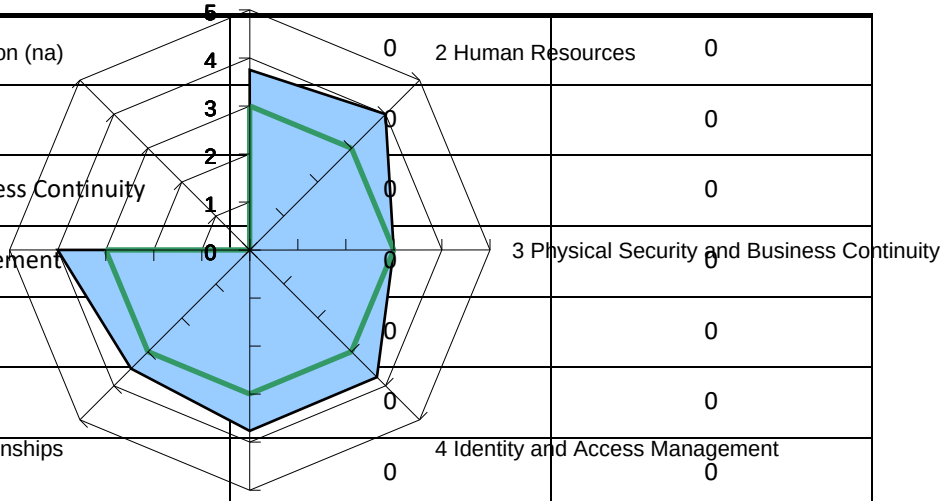
The major and/or minor non-conformities, as applicable, were identified in the following Areas:

No.	Area	Number of major non-conformities	Number of minor non-conformities
1	IS Policies and Organization	0	0
2	Human Ressources	0	0
3	Physical Security and Business Continuity	0	1
4	Identity and Access Management	0	0
5	IT Security / Cyber Security	0	0
6	Supplier Relationships	0	0
7	Compliance	0	0
8	Prototype Protection	NA	NA
9	Data Protection	NA	NA

3.3 First Follow-Up

The individual areas of the initial maturity levels can be found in the spider web diagram below.

The major and/or minor non-conformities, as applicable, were determined in the following Areas:



1	IS Policies and Organization	0	0
2	Human Ressources	0	0
3	Physical Security and Business Continuity	0	0
4	Identity and Access Management	0	0
5	IT Security / Cyber Security	0	0
6	Supplier Relationships	0	0
7	Compliance	0	0
8	Prototype Protection	NA	NA
9	Data Protection	NA	NA

D. Maturity Levels of ISA (Result Tab)

4.1 ISMS

Based on the current status of implementation, the following maturity levels result for the controls listed in the ISMS Area:

No.	Control Question	Target maturity level	Result
1	***IS Policies and Organization***		
1.1	***Information Security Policies***		
1.1.1	To what extent are information security policies available?	3	**3**
1.2	***Organization of Information Security***		
1.2.1	To what extent is information security managed within the organization?	3	3
1.2.2	To what extent are information security responsibilities organized?	3	3
1.2.3	To what extent are information security requirements taken into account in projects?	3	3
1.2.4	To what extent are responsibilities between external IT service providers and the own organization defined?	3	3
1.3	***Asset Management***		
1.3.1	To what extent are information assets identified and recorded?	3	3
1.3.2	To what extent are information assets classified and managed in terms of their protection needs?	3	3
1.3.3	To what extent is it ensured that only evaluated and approved external IT services are used for processing the organization's information assets?	3	3
1.4	***IS Risk Management***		
1.4.1	To what extent are information security risks managed?	3	**3**
1.5	***Assessments***		
1.5.1	To what extent is compliance with information security ensured in procedures and processes?	3	3
1.5.2	To what extent is the ISMS reviewed by an independent entity?	3	3
1.6	***Incident Management***		
1.6.1	To what extent are information security events processed?	3	**3**

2	***Human Resources***		
2.1.1	To what extent is the suitability of employees for sensitive work fields ensured?	3	3
2.1.2	To what extent is all staff contractually bound to comply with information security policies?	3	3
2.1.3	To what extent is staff made aware of and trained with respect to the risks arising from the handling of information?	3	3
2.1.4	To what extent is teleworking regulated?	3	3
3	***Physical Security and Business Continuity***		
3.1.1	To what extent are security zones managed to protect information assets?	3	2
3.1.2	To what extent is information security ensured in exceptional situations?	3	3
3.1.3	To what extent is the handling of supporting assets managed?	3	3
3.1.4	To what extent is the handling of mobile IT devices and mobile data storage devices managed?	3	3
4	***Identity and Access Management***		
4.1	***Identity Management***		
4.1.1	To what extent is the use of identification means managed?	3	3
4.1.2	To what extent is the user access to network services, IT systems and IT applications secured?	3	3
4.1.3	To what extent are user accounts and login information securely managed and applied?	3	3
4.2	***Access Management***		
4.2.1	To what extent are access rights assigned and managed?	3	**3**
5	***IT Security/Cyber Security***		
5.1	***Cryptography***		
5.1.1	To what extent is the use of cryptographic procedures managed?	3	3
5.1.2	To what extent is information protected during transport?	3	3
5.2	***Operations Security***		

5.2.1	To what extent are changes managed?	3	**3**
5.2.2	To what extent are development and testing environments separated from operational environments?	3	NA
5.2.3	To what extent are IT systems protected against malware?	3	3
5.2.4	To what extent are event logs recorded and analyzed?	3	3
5.2.5	To what extent are vulnerabilities identified and addressed?	3	3
5.2.6	To what extent are IT systems technically checked (system audit)?	3	3
5.2.7	To what extent is the network of the organization managed?	3	3
5.3	***System acquisitions, requirement management and development***		
5.3.1	To what extent is information security considered in new or further development of IT systems?	3	NA
5.3.2	To what extent are requirements for network services defined?	3	3
5.3.3	To what extent is the return and secure removal of information assets from external IT services regulated?	3	3
5.3.4	To what extent is information protected in shared external IT services?	3	NA
6	***Supplier Relationships***		
6.1.1	To what extent is information security ensured among suppliers and cooperation partners?	3	3
6.1.2	To what extent is non-disclosure regarding the exchange of information contractually agreed?	3	3
7	***Compliance***		
7.1.1	To what extent is compliance with regulatory and contractual provisions ensured?	3	3
7.1.2	To what extent is the protection of personal data taken into account when implementing information security?	3	3

4.2 Handling of Prototypes

The module has not been assessed.

4.3 Data Protection

The Data Protection Module is not following the ISA maturity levels and therefore not listed here.

E. Detailed Assessment Results

1 IS Policies and Organization

1.1 Information Security Policies

1.1.1 To what extent are information security policies available?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** High level ISMS Policy is designed keeping in view of Organizations information security objectives aligned to the ISO 27001, constantly changing threat Landscapes, and our Client(s) information security requirements covering also the education, competent resources required for safeguarding the information assets and continual improvements that are required to strengthen the information security at Cyient. This was reviewed by the Security Council, approved by CEO & MD and the final policy was shared to all the relevant stakeholders of Cyient. This ISMS Policy is made available for all associates to go through any time, in our intranet portal called 'Cyient Process Artefacts Library - CyientPAL" . Awareness mailers to Cyient Associates are released at periodic intervals regarding the availability of ISMS Processes in CyientPAL, and safeguarding the information asset(s) in their possession.. **The following evidences were provided:** '"Cyient’s Commitment to Information Security" available in CyientPAL. Awareness mail to associates is appended for reference.CISO
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.**
Planned measures (including implementation period)
Evaluation at Follow-Up

1.2 Organization of Information Security

1.2.1 To what extent is information security managed within the organization?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** While the High level ISMS Policy is approved by CEO & MD, a detailed “Cyient Information Security Manual-CISM" is established aligning to the ISO 27001, NIST and other standard requirements Within this CISM, a detailed ISMS purpose, scope, requirements, governance, roles, responsibilities, and management of ISMS are discussed for implementation. ISMS governance/management reviews are performed at periodic intervals among the identified council members, referred to as "Information security and Data Privacy Security Council". In alignment to ISO 27001 Standard, all the applicable controls are determined, and SR-020-SOA (Statement of Applicability) is created, reviewed periodically and made available in CyientPAL. The effectiveness of the ISMS is regularly reviewed and monitored through various inputs from the established controls, regularly reviewed through the Internal, External audits and suitable measures/corrective actions are taken to mitigate the identified risks and improve the effectiveness of implemented controls. **The following evidences were provided:** **Description** SM-001-CISM (Cyient Information Security Manual) available in CyientPAL. SR-020-SOA (Statement of Applicability) "Security Council Minutes of meeting" and related summary inputs are provided as evidence. Security Council representation list is appended. Internal and External Audit(s) related artefacts shall be evidenced while interviews.
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.**

Planned measures (including implementation period)
Evaluation at Follow-Up

1.2.2 To what extent are information security responsibilities organized?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** 'The roles and responsibilities of relevant stakeholders for ISMS implementation are defined in the Cyient Information Security Manual (CISM). Corporate-ISMS team comprising of analysts and managers along with Director acting as ISO are competent, experienced and certified on relevant competencies aligned to Information security (viz, ISO/IEC 27001:2022 LA, CISA, CISM, CRISC, Cyber Law etc.) At all business delivery units, depart level Information security officers (DISO's) are identified to support information security requirements of Cyient Customers. These DISO's will act at internal SPOCs for the business teams for the ISMS enablement for their respective areas. **The following evidences were provided:** **Description:** Roles and Responsibilities are defined in "SM-001-CISM (Cyient Information Security Manual) available in CyientPAL" at Section 5.3 - Information Security Organization - Roles, Responsibilities and Authorities. Security Council list is appended, which is represented by the Senior Leadership of the Cyient. List of DISO's and their Training evidences.
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible**
Planned measures (including implementation period)
Evaluation at Follow-Up

1.2.3 To what extent are information security requirements taken into account in projects?

Detailed Description (Including Assessment Procedure)

AL2:

The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:

Description

Information security requirements are considered in the life cycle activities of the Projects that are delivered to the Customers.

Key artefacts maintained by the project teams include, Risk Management Plan; User Access review list; User Training and Awareness records related to Information security; Customer specific Information security requirements captured as part of the Contract / Agreement; additionally as part of the Governance process, the Projects undergo the Internal ISMS audits at periodic intervals.

The following evidences were provided:

Description:

'QP-041-RMP(Information Security Operational Risk Management) process

Project / Account RMP

Project / Account team - GRNT - Access Management process

Project / Account team - Onboarding and Offboarding process and samples.

Project / Account team - DCafe records

Project / Account team - Internal Audit records

Finding

Based on the observations, no deviation was found.

Project Classification can be more clearly defined based on the Infosec risk assessments

AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

☐ Major non-conformity ☐ Minor non-conformity ☒ Observation ☐ Room for improvement

Planned measures (including implementation period)

Evaluation at Follow-Up

1.2.4 To what extent are responsibilities between external IT service providers and the own organization defined?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** Representatives from various business and functional teams will identify the requirements within their respective area for seeking services from external IT Service providers/vendors. These requirements are reviewed by the internal sourcing team and IT Service providers/vendors shall be finalized through Vendor identification and further finalized through Vendor Risk Management Process to ensure that the Cyient's information security requirements are complied. Both parties will agree on a contract holding all relevant information security requirement clauses, duly reviewed, and authorized by the global corporate legal head. Each of the stakeholder execute their duties as defined in the contract document. suitable documentation shall be obtained and maintained during the engagement for the purpose of internal security reviews. **The following evidences were provided:** **Description:** FP-033-VRA (Vendor Risk Assessment Policy) FG-009-VRM (Standard Work -Vendor Risk Management Process).
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.**
Planned measures (including implementation period)
Evaluation at Follow-Up

1.3 Asset Management

1.3.1 To what extent are information assets identified and recorded?

Detailed Description (Including Assessment Procedure)

AL2:

The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:

Description

'All information assets (not limiting to Hardware, Software, Services, and people) are identified, inventoried and classified as per the information that is being processed by these assets.

Hardware Asset Management (IT-HAM) and Software Asset Management (IT-SAM) team's are responsible and shall performs their activities related to information assets management, which includes maintenance of the inventory.

All asset allocations and de-allocations will go through a central request management system, duly approved by the respective Asset owners and Risk owners.

Hardware asset catalogue is managed centrally within the "Asset management System (AMS)" and the software asset catalogue is managed within Flexera, Flex Net manager suite(FNMS) and the respective asset configurations are managed through the "Manage Engine Desktop Central" Asset configuration management system

The following evidences were provided:

Description

'ITP-008-SAM (Software Asset Management)

ITP-010-IHM (IT Hardware Asset Management Policy Procedure)

SP-002-AMIC (Asset Management & Information Classification Procedure)

Asset inventory (Hardware and Software) is appended.

GHD ticket samples on Hardware requests and Software requests.

Flexera Screen Shots on Software Inventory

AMS Screen Shots on Hardware inventory is evident

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

Planned measures (including implementation period)
Evaluation at Follow-Up

1.3.2 To what extent are information assets classified and managed in terms of their protection needs?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** Information assets are handled (data records) are classified as per the defined process and labelled using the Microsoft Information Protection (MIP). Information assets are handled all through the life cycle activities of the asset (identification to secure disposal of the supporting assets) are performed by the respective teams (IT, Facilities and Admin) as per the defined process. For Information assets participating in the processing activities, their risks are evaluated, assessed and appropriate mitigation controls are identified and established. **The following evidences were provided:** **Description:** Data Labelling and classification referred in SP-002-AMIC (Asset Management & Information Classification Procedure) to be evidenced. Asset disposal is performed as per ITP-010-IHM (IT Hardware Asset Management Policy Procedure) with reference of the Section 8 IT Asset Retirement and Disposal Process QP-041-RMP (Information Security, Operational Risk Management) procedure QR-059-RMP (Risk Management Plan)
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.**
Planned measures (including implementation period)
Evaluation at Follow-Up

1.3.3 To what extent is it ensured that only evaluated and approved external IT services are used for processing the organization’s information assets?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** 'External IT services are availed as per the defined Vendor onboarding process, which includes ensuring that a valid Contract / agreement is available and the information security requirements are part of such agreements. Vendor Security risk assessment is performed while onboarding the vendors for IT Services. **The following evidences were provided:** **Description:** 'FP-033-VRA (Vendor Risk Assessment Policy) FG-009-VRM (Standard Work-Vendor Risk Management Process) Sample Vendor Risk Management Plan appended.
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.**
Planned measures (including implementation period)
Evaluation at Follow-Up

1.4 IS Risk Management

1.4.1 To what extent are information security risks managed?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** 'Cyient has established the Risk management process which is aligned to the best practices for the applicable management systems / processes. Information security risk is embedded to the project management life cycle activities including the enabling functions. all the applicable information security risks are identified, analyzed and appropriate mitigation strategy is established. Risk Assessment is maintained, performed, reviewed, and updated at periodic intervals and the validation of the Risk Management Plans are part of the internal audit process as well. **The following evidences were provided:** **Description**. QP-041-RMP(Information Security Operational Risk Management) is available. QR-059-RMP(Risk Management Plan) template is available. Project Specific, Functional group (IT, HR, Procurement) RMPs are appended for reference
Finding
Based on the observations, no deviation was found. **Existing Controls and Implemented controls can be mapped to ISMS Annex A Controls in the InfoSec Risk register** **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.** ☐ Major non-conformity ☐ Minor non-conformity ☒ Observation ☐ Room for improvement
Planned measures (including implementation period)
Evaluation at Follow-Up

1.5 Assessments

1.5.1 To what extent is compliance with information security ensured in procedures and processes?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** Cyient's ISMS team performs the periodic review and update of the ISMS Process artefacts, i.e., policies, procedures, guidelines, templates etc., These policies and procedures are published in CyientPAL, central process artefacts repository or library accessible to all Cyient Associates. All these Process artefacts are published through BET - Business Enablement team (Quality) and the change management process is followed as well. Internal ISMS audits are performed, and non-conformities are tracked to the closure, through the in-house developed internal audit tool. Summary of Non-conformances are part of the management review process (Security council). **The following evidences were provided:** **Description:** 1. CP-002-AUD (Internal Audit Procedure) 2. ISMS Internal audit portal tool (in-house tool), 3. Summary snap of 2023-24 Internal Audits is appended.(Quarterly Audit plan shall be evidenced while interviews) 4. Sample Audit reports appended. 5. Sample process artefacts shared with BET for publishing in CyientPAL appended. 6. Internal audits summary report (Slide # 20) shared to Security council is appended
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.**
Planned measures (including implementation period)

Evaluation at Follow-Up

1.5.2 To what extent is the ISMS reviewed by an independent entity?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** 'Cyient's ISMS is verified and validated by an independent and competent certified body annually. Annually, Cyient undergoes the ISO/IEC 27001:2013 and SOC - 2 Type 2 external assessments. The outcome of the audit / assessments and any actions required for corrections shall be initiated and pursued by the respective user groups in coordination with Corporate ISMS team. The assessment outcomes and corrections take are discussed in Security Council reviews for further improvement opportunities. **The following evidences were provided:** **Description.** 'Cyient's ISO/IEC 27001:2013 Certificate copy is appended. SOC 2 Type 2 report will be evidenced during the interview discussions. Management Assertion is appended. BitSight score (780) as of 1st April 2024
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.**
Planned measures (including implementation period)
Evaluation at Follow-Up

1.6 Incident Management

1.6.1 To what extent are information security events processed?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** Cyient has established a comprehensive Incident Management Process. All Security incidents are logged in the Incident Management Portal accessible the Cyient Associates. Security incidents are classified according to the nature of the Incidents (Physical, Human, Data, etc.,) Role players are identified for addressing the Security Incidents, which includes Security Incident Facilitator; Security Incident Manager; Security Incident Reviewed. All the security incidents have to be addressed as per the defined incident Management process and an appropriate Root Cause Analysis to be provided including Correction and Correction Action for each of the incidents, which are reviewed and validated prior to considering the incident as closed. **The following evidences were provided:** **Description:** 'SP-010-SIMP (Security Incident Management Procedure). SW-010-SIMP(Security Incident management Work Flow) Samples of Incidents along with RCA, CA and correction are appended.
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.**
Planned measures (including implementation period)
Evaluation at Follow-Up

2 Human Ressources

2.1.1 To what extent is the suitability of employees for sensitive work fields ensured?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** Employee onboarding process is established, and the associates are recruited based on the Job requests that are applicable or available for a particular function. Employee Job descriptions are defined and articulated, which includes their roles and responsibilities. HR team manages the staff augmentation process (employee onboarding to off boarding). Every employee is sensitized and must go through a mandatory education on Cyient's Information Security process while the time of joining and during the employment as well. As part of the onboarding, Background verification checks are performed on the prospective employees and accordingly the associates are onboarded. **The following evidences were provided:** **Description:** HP-003-RES Talent Acquisition Procedure (Job Requisition to Offer Release) – Lateral Talent and Off-Campus Samples of recruited employees is appended. Samples of employee background verification is appended. HR-IN-G-BGV-C4-POL (Background Verification Policy Guidelines)
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.**
Planned measures (including implementation period)

Evaluation at Follow-Up

2.1.2 To what extent is all staff contractually bound to comply with information security policies?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** Employee onboarding process is established, and the associates are recruited based on the Job requests that are applicable or available for a particular function. Employee Job descriptions are defined and articulated, which includes their roles and responsibilities. HR team manages the staff augmentation process (employee onboarding to off boarding). Every employee is sensitized and must go through a mandatory education on Cyient's Information Security process while the time of joining and during the employment as well. As part of the onboarding, Background verification checks are performed on the prospective employees and accordingly the associates are onboarded. **The following evidences were provided:** **Description:** HP-003-RES Talent Acquisition Procedure (Job Requisition to Offer Release) – Lateral Talent and Off-Campus Samples of recruited employees is appended. Samples of employee background verification is appended. HR-IN-G-BGV-C4-POL (Background Verification Policy Guidelines)
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.**
Planned measures (including implementation period)
Evaluation at Follow-Up

2.1.3 To what extent is staff made aware of and trained with respect to the risks arising from the handling of information?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** Cyient associates must complete the Information Security Management System trainings when they join the Organization and attend an annual refresher. The employees also receive periodic Email flyers to inform them about Information security aspects. The L&D team keeps the employee training records in the centralized portal, called DCafe. The training modules include topics such as intellectual property rights, Cyber Security, Information security, and General Data Protection Regulation (GDPR) from Security perspective. The Organization also provides account specific information security training and awareness sessions as required. Role specific training sessions highlight the key information security aspects for the relevant role players. The Organization records the participation details and gives learning credits to the Users / participants. **The following evidences were provided:** **Description** 'Training details of DISO - Department Information Security Officer session participation info is appended. Dcafe Link is provided. Sample of associates training records submitted. Samples of Email Flyers shared with Cyient's Associates are appended.
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.**
Planned measures (including implementation period)
Evaluation at Follow-Up

2.1.4 To what extent is teleworking regulated?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** Cyient has established the remote working policy to meet the business needs or requirements and ensure the work deliverables are performed seamlessly, ensuring the information security requirements are fulfilled. All users connecting from outside the Cyient network need to authenticate using their credentials and multi-factor authentication is enabled. Users are sensitized to consider security precautions while accessing the Cyient business systems from outside the Cyient network.. **The following evidences were provided:** **Description** Intune Mobile policies to be evident. SP-023-RWP (Remote Working Policy Procedure) SP-020-AUP covering the behavioral aspects while in public or private surroundings. LP-010-COC (CODE OF ETHICS AND BUSINESS CONDUCT)
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.**
Planned measures (including implementation period)
Evaluation at Follow-Up

3 Physical Security and Business Continuity

3.1.1 To what extent are security zones managed to protect information assets?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** Cyient has secured its locations - physically and logically. Where appropriate, CCTV surveillance systems are deployed and managed centrally from the respective campus/building. Badge access is enforced with different color tags to quickly identify Employees, Visitors, Guests etc. and Visitor access is verified and allowed upon approvals from the respective associate to the Maing gate Security. Round the clock perimeter security is enforced at all the Cyient premises to prevent unauthorized entry and exit into Cyient premises and further to safeguard the assets Individual information processing work areas within the building are enabled with anti-pass back swipe access. Physical Access logs are maintained by the Facilities and Admin(F&S) team for the movement of the users / visitors inside or outside the Cyient premises. IT Asset movement within the Cyient premises is handled by the IT Infra team in collaboration with the F&A team. Physical Security personnel will check the material movement (Inward/Outward) at the entry and exit gates of the premise. Vehicles entering into the Cyient premises shall be checked (randomly) by the Security personnel to ensure that unauthorized asset movement is happening in uncontrolled manner. Security personnel shall check the baggage randomly carried by associates during entry and exit into Cyient premises to ensure controlled asset movement is happening. Logical access to the IT systems of Cyient is enabled as per the Identity and Access Management Process. IT Infra team manages the process, which includes enabling and disabling the logical access of the users against the Service requests which are approved by the concerned stakeholders. Access to the business systems is enabled on "Need to Know" basis, against the approvals. **The following evidences were provided:** **Description** 'SP-011-IAM (Identity and Access Management procedure) SP-001-PES Physical security and access control policy SP-017-SOP (Facilities & Services Standard Operating Procedure)

FSP-001-VMS-Visitor Management Policy and Procedure

Samples of Access enabled to users and visitors including disabled access to the users.

Samples of Privilege access to the users at scoped locations is appended.

Finding

Based on the observations, deviation was found.

Minor NCs: Zone identification as part of the floor plan is not evidenced.

AL2: The description of the implementation in relation to the evidences provided is ☐ plausible ☒ not plausible. Description:

☐ Major non-conformity ☒ Minor non-conformity ☐ Observation ☐ Room for improvement

Planned measures (including implementation period)

The assessed company has implemented the following compensating measures (temporary):

1. Security zones have been identified and marked.

The assessed company has planned the implementation of the following mitigating measures (lasting):

1. Update the SP-001-PES (Physical Access Control Policy and Procedure) for classification of security zones. Make sure that all floor plans having the security zones as per defined policy during the internal audits

According to planning, the implementation will be completed by <2024.05.10> at the latest.

The result remains/changes to a ☐ Major non-conformity ☒ Minor non-conformity ☐ Observation ☐ Room for improvement

Evaluation at Follow-Up

Evidence check on <10th May 2024>

Provided Evidences:

- As attached in the email (Manikonda - Admin block ground floor, Manikonda TOWER -1 FIRST FLOOR C BLOCK (002), Madhapur ph. 2 south wing-Updated (002)yy (003), Madhapur - Kaveri Block, BLR -4th floor Layout with identification of Security zones as RED, YELLOW and GREEN

There are no more deviations from the requirements.

3.1.2 To what extent is information security ensured in exceptional situations?

Detailed Description (Including Assessment Procedure)

AL2:

The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:

Description

'Cyient has implemented a robust and resilient information security management system that ensures the security of the information assets in normal and exceptional situations. Cyient is constantly monitoring and improving its information security posture, to cope with the evolving and emerging challenges and threats.

- Business continuity and disaster recovery plan: This plan outlines the procedures and actions that Cyient takes to ensure the continuity of the critical business functions and the recovery of the essential data and systems in the event of a disaster or an emergency. The plan identifies the potential risks and scenarios, the recovery objectives and strategies, the roles and responsibilities of the stakeholders, and the testing and maintenance of the plan.
- Backup and restoration: Cyient performs regular backups of the data and systems that are stored on-premises or in the cloud, and ensures that the backups are encrypted, secured, and accessible. Cyient also has the capability to restore the data and systems from the backups in a timely manner, in case of any loss or corruption of the original data and systems.
- Remote access and VPN: Cyient enables its employees to access the data and systems remotely, using a secure virtual private network (VPN) connection that encrypts the traffic and prevents any unauthorized or malicious access. Cyient also enforces strong authentication and authorization mechanisms, such as passwords, tokens, or biometrics, to verify the identity and access rights of the remote users.
- Encryption and data protection: Cyient encrypts the data and systems that are stored or transmitted, using industry-standard algorithms and protocols, such as AES, SSL, or TLS. Cyient also applies data protection measures, such as masking, anonymizing, or pseudonymizing, to reduce the sensitivity or identifiability of the data, especially when dealing with personal or confidential data.
- Security awareness and training: Cyient provides regular security awareness and training programs to its employees, to educate them about the information security policies and practices, the potential threats and risks, and the best practices and behaviors to protect the information assets. Cyient also conducts security audits and assessments, to evaluate the effectiveness and compliance of the information security measures.

The following evidences were provided:

Description

'SP-010-SIMP (Security Incident Management Procedure)

SP-003B-OMP(Operations Management Procedure)

SP-001-PES (Physical Access Control Policy and Procedure).

QP-041-RMP(Information Security Operational Risk Management)

SG-006-BKUP (Backup Policy & Guidelines)
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.**
Planned measures (including implementation period)
Evaluation at Follow-Up

3.1.3 To what extent is the handling of supporting assets managed?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** IT Assets handling is performed in alignment to ISO 19770-1 (ITAM), in relation to deployment & allocating the assets to users, Storage, Maintenance, Return, Repair, Retire and disposal, etc., and these activities are part of the Hardware asset management process. For assets which are lost are handled as appropriate to the defined procedure in HAM and will attract Incident Management process. Asset inventory is being managed accordingly by the Hardware Asset Management - HAM Team. E-Waste safe disposal activity is handled through the certified e-waste disposal vendor after duly erasing the data/degassing the hard disks containing the information and necessary documents are furnished to the regulatory bodies (PCB) per defined frequency once disposed. **The following evidences were provided:** **Description:** SP-010-SIMP (Security Incident Management Procedure) ITP-010-IHM (IT Hardware Asset Management Policy Procedure) ITP-008-SAM (Software Asset management) Sample of an Asset Lost recorded in the Incident Management tool is appended.
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.**
Planned measures (including implementation period)
Evaluation at Follow-Up

3.1.4 To what extent is the handling of mobile IT devices and mobile data storage devices managed?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** All mobile IT devices and mobile data storage devices that are used for Cyient's business are registered and approved by the IT department. All such devices are encrypted and password-protected using BitLocker full disk encryption and windows hello as multifactor access protection. Microsoft Defender for Endpoint security as Antivirus and Antimalware protection is enforced and updated regularly. Suitable Group policies are enforced through central active directory for auto screen locking or logged off when in idle state for certain duration. All users are mad aware on safe handling procedures and suitable 'Acceptable Use policies' accepted to protect these devices while commuting or when not in use. User must report immediately to the IT department in case of loss, theft, or damage. All these devices must be returned to the IT department when no longer needed or upon termination of employment. All data shall be wiped off from the disks before seeking any disk replacements or asset disposal or asset reuse. **The following evidences were provided:** **Description:** 1. SP-022-PWP (Password Policy Procedure) 2. SP-003B-OMP(Operations Management Procedure) 3. SP-010-SIMP (Security Incident Management Procedure) 4. SP-020-AUP (Acceptable Use Policy - General Use of IT Resources) 5. ITP-010-IHM (IT Hardware Asset Management Policy Procedure) AUP Samples shall be evident while interviews
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.**

Planned measures (including implementation period)
Evaluation at Follow-Up

4 Identity and Access Management

4.1 Identity Management

4.1.1 To what extent is the use of identification means managed?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** 'Physical Access: Badge Access cards: All associates are provided with physical badge access that contain the employee's name, photo, date of joining and office address. These badges are limited to access all common areas and the information processing blocks as appropriate to the associates need. Access to these blocks is tracked and logs are centrally managed by the F&A team. Biometric authentication: For all restricted and Sensitive areas like, Data Centre, server rooms the identity of the users are captured based on their unique physical characteristics, such as fingerprints. Also, Cyient uses biometric authentication for supporting IT systems (Laptops) as part of technology improvements for enhancing the security and authorization. Logical Access: Unique Identity and Authentication: All associates are assigned a unique userID and a confidential password that is required to log into the system. Cyient follows the industry best practices of centrally enforced password management and full disk encryption technologies to protect the user accounts and data. Multi-factor authentication is part of the additional security measure which is enabled for all users to authenticate the user while accessing the Cyient's business systems and applications exposed to Internet. Identity creation is completely under the control of Central IT Infra Active Directory team. **The following evidences were provided:** **Description:** 'SP-001-PES (Physical Access Control Policy and Procedure). SP-011-IAM (Identity and Access Management procedure)
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.**

Planned measures (including implementation period)
Evaluation at Follow-Up

4.1.2 To what extent is the user access to network services, IT systems and IT applications secured?

Detailed Description (Including Assessment Procedure)

AL2:

The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:

Description

'The users access to the IS Services and IT systems is secured through multiple modes or mechanism to ensure that the secured user access helps to protect the confidentiality, integrity, and availability of the IT resources and data from unauthorized or malicious access.

Conditional access is enabled for all associates requesting for privileged access on the cloud resources.

The process of secured user access involves the following steps:

Identification: The user provides a unique identifier, such as a username, email address, or employee ID, to the IT service or system that they want to access.

Authentication: The user proves their identity by providing a secret key or a token, such as a password, PIN, biometric to the IT service or system.

Authorization: The user requests access to a specific IT service or system function through Help desk, such as reading, writing, or deleting data. The IT service team (GHD) checks the user's access rights and permissions, based on the approvals for their role, group, or policy, and grants or denies access accordingly.

Auditing: The user's access activities, such as login, logout, access request, access grant, or access denial, are recorded and logged by the IT service or system. The logs provide evidence and traceability of the user's access behavior and can be used for monitoring, reporting, or investigation purposes.

Passwords must adhere to the password policy and procedure and the control requirements to manage these passwords shall be enforced through the centrally managed group policies by IT. Guidelines w.r.t., to its complexity, historical password usage, length etc. shall be manage appropriately.

The following evidences were provided:

Description:

'SP-011-IAM (Identity and Access Management procedure)

SP-022-PWP (Password Policy Procedure)

Samples of User Access password policy rules including the privileged users is shared.

IT GHD team responses for the Users requests is shared.

Finding

Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

Planned measures (including implementation period)
Evaluation at Follow-Up

4.1.3 To what extent are user accounts and login information securely managed and applied?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** Cyient has established the process of securely maintaining and managing the User access management to ensure maintenance of Confidentiality, Integrity and availability of IT systems and information. Some of the key measures considered to protect the user accounts and login information are ... Unique user accounts are created or disabled as per the Onboarding and offboarding process managed by the HR team synced through Workday system. First time password change is mandated and enforced through AD For the existing user, privilege changes or other systems access is routed through Service Request, which is raised through the Self-service portal and access is enabled as per the approvals from the concerned stakeholders. User accounts are enforced with the password management policy and guidelines. Windows Hellow, multi-factor authentication (MFA) are enabled as required for allowing access to the Cyient IT systems. Access to the systems is enabled on "Need to Know" basis to limit the privileges of users based on their roles and responsibilities. Review of user access rights are performed at periodic intervals by the respective teams and this control adherence is verified during Internal ISMS Audits to detect and prevent any unauthorized or suspicious changes. Users are provided with training and awareness programs on adhering to the policies for creating and maintaining secure login credentials. **The following evidences were provided:** **Description:** 'SP-011-IAM (Identity and Access Management procedure) SP-022-PWP (Password Policy Procedure) SP-020-AUP(Acceptable Use Policy) Samples of the users Access enablement and disablement is provided
Finding
Based on the observations, no deviation was found.

AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.
Planned measures (including implementation period)
Evaluation at Follow-Up

4.2 Access Management

4.2.1 To what extent are access rights assigned and managed?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** Access to the systems is enabled on "Need to Know" basis limiting the access and privileges of users based on their roles and responsibilities. Privileged access requirements are controlled through Help desk ticket followed by approval workflow and automated review for revocation of access. Review of user access rights are performed at periodic intervals by the respective teams and covered through the Internal ISMS Audits to detect and prevent any unauthorized or suspicious actions. **The following evidences were provided:** **Description:** SP-011-IAM (Identity and Access Management procedure) Samples of the users Access enablement and disablement is provided
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.**
Planned measures (including implementation period)
Evaluation at Follow-Up

5 IT Security / Cyber Security

5.1 Cryptography

5.1.1 To what extent is the use of cryptographic procedures managed?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** Cyient uses various cryptographic controls to ensure the security and integrity of its data, systems, and communications while at rest, and in transit . Prominently the IT teams have deployed: Encryption and decryption of data at rest and in transit using industry-standard algorithms and protocols such as AES, RSA, SSL/TLS, and VPN. Hashing and digital signing of data and documents using cryptographic functions such as SHA, MD5, and DSA to verify their authenticity and prevent tampering and maintain the integrity of the data. Key management and distribution is performed using secure methods such as public key infrastructure (PKI), certificate authorities (CA), and hardware security modules (HSM). Access control and authentication using cryptographic mechanisms such as maintaining and using the complex password mechanism, multi-factor authentication, biometrics. **The following evidences were provided:** **Description:** 'SP-003B-OMP (Operations Management Procedure) Related Evidences
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.**
Planned measures (including implementation period)
Evaluation at Follow-Up

5.1.2 To what extent is information protected during transport?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** Data transfer refers to the process of sending or receiving information between different devices, networks, or locations. This can include email, cloud storage, file sharing, remote access, web browsing, and other online activities. The network services used to transfer information are identified and documented. Policies and procedures in accordance with the classification requirements for the use of network services are defined and implemented. Measures for the protection of transferred contents against unauthorized access are implemented. Networking & Systems / IT Infrastructure ensures the security of data in networks and the protection of connected services from unauthorized access and disclosure by adhering to the guidelines. **The following evidences were provided:** **Description:** SP-003A-COM (Information communications management procedure) SG-020-SDD (Guidelines on Secure by Design and Default Best Practices) - refer to Encryption. SP-011-IAM (Identity and Access Management procedure) - refer for access management. SG-006-BKUP (Backup Policy & Guidelines) SP-003B-OMP (Operations Management Procedure) - refer for Malware protection
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.**
Planned measures (including implementation period)
Evaluation at Follow-Up

5.2 Operations Security

5.2.1 To what extent are changes managed?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** Cyient's IT team follows the change management process which covers a wide range of aspects, such as hardware, software, network, data, security, configuration and supporting infrastructure. Some examples of changes that are managed for IT systems at Cyient are: Upgrading or replacing IT equipment, such as servers, routers, switches, laptops, etc. Installing or updating operating systems, databases, enterprise resource planning (ERP) systems, etc. Modifying or enhancing network configurations, such as bandwidth, firewall, VPN, etc. Implementing or improving security measures, such as encryption, authentication, backup, etc. **The following evidences were provided:** **Description** ITP-003-CMC(IT Change Management _ Control Procedure) samples of changes performed by the team appended.
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.**
Planned measures (including implementation period)
Evaluation at Follow-Up

5.2.2 To what extent are development and testing environments separated from operational environments?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** 'Cyient maintains different environments for different stages of the software development life cycle (SDLC), such as development, testing and production and configuration is maintained appropriately by the respective teams. The segregated environments help Cyient to ensure and Prevent unauthorized access and modification of data and code. Reduce the risk of errors, bugs, and failures in the operational environment. Improve the performance and scalability of the software and systems. Facilitate the testing and verification of the systems and information. Enable the smooth deployment and transition of the systems to production environment. By separating the development and testing environments from the operational environments, Cyient ensures the delivery of high-quality and secure software and systems to its clients and stakeholders by adhering to the relevant policies, procedures, and guidelines for the security, privacy, and compliance of the environments. **The following evidences were provided:** **Description:** SG-020-SDD (Guidelines on Secure by Design and Default Best Practices) SP-005-SDM (Information systems acquisition and maintenance Procedure) Evidences related to SAP environment and Cyient - SAP on GCP Architecture are appended.
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.**
Planned measures (including implementation period)
Evaluation at Follow-Up

5.2.3 To what extent are IT systems protected against malware?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** Cyient has established sufficient process and controls to ensure the IT systems are protected from malware infections or attacks. Cyient's end points (computing devices) are protected and uses Microsoft Defender for Endpoint protection to ensure that the end point is protected, and any unauthorized malicious executions are monitored and alerted from any malware infections. Comprehensive policies and rules are established in the Endpoint detection and response (EDR) which are updated at periodic intervals and pushed to the end points. All cyient systems that are connecting to the Cyient network are by default protected with this end point protection solution. The Network connectivity - bi-directional and lateral movements are monitored and reviewed as part of the Managed SOC operations through "Security Information and Event Management-SIEM" (IBM QRadar) by the Cyber Security Team. All abnormal events are notified to the respective asset owners to apply remediation for ensuring or preventing from any potential incidents. **The following evidences were provided:** **Description** SP-003B-OMP (Operations Management Procedure) refer to Section 5.2.1 Protection against malware refer to 5.7.1 Encryption Requirements Evidences related to End point protection and IDS / IPS logs are shared
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.**
Planned measures (including implementation period)
Evaluation at Follow-Up

5.2.4 To what extent are event logs recorded and analyzed?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** Managed Security Operations Center (SOC) activities are performed by external Service Provider (MSSP) monitor event logs in real-time to identify suspicious or anomalous activities. a. All the security telemetry event logs are recorded & analyzed extensively as part of the MSSP deliverables. b. Integrated all critical infrastructure log sources to this service provider, including firewalls, Intrusion detection systems (IDS), End Point Detection and Response (EDR), AD servers, endpoints & Cloud Native Security e.g. – Azure AD, Message Trace, Intune, MFA etc. c. Log aggregation and log correlation from multiple sources are used for detecting potential security incidents. d. Cyient Cyber Security team Interface with MSSP for additional triaging and Incident response activities. e. Log retention as per the statutory requirements is maintained as "hot" & "cold" storages for log retention which is 9 months (Min 180 days per CERT-IN requirements).**The following evidences were provided:** **Description:** SP-003B-OMP(Operations Management Procedure) SP-003SG-020-SDD (Guidelines on Secure by Design and Default Best Practices)
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible**
Planned measures (including implementation period)
Evaluation at Follow-Up

5.2.5 To what extent are vulnerabilities identified and addressed?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** Cyient has a detailed Threat, Vulnerability and Patch management process in place. Threat Intel is received daily through multiple sources, and we leverage scanning internal networks using Nessus professional and Expert (Infrastructure) along with Burp Suit for Web-Application tools to identify vulnerabilities within the organization's network, systems, web applications, and infrastructure. Suitable automated scanning configurations are in place for Monthly scans on the identified VLANS. On Demand manual assessments shall also be performed to quickly scan for any new vulnerabilities, misconfigurations, weakness in the systems. Annual Vulnerability assessments are carried out by identified third party on the publicly exposed services and infrastructure which are duly remediated by the respective asset owners. Manage Engine Desktop Central (MEDC) is used to automate the patch deployments of IT systems. All deployments are carried out post testing of any newly released patches on the test environment. Continual scans of machines across the estate using MEDC help us in keeping the missing deployments to complete and upkeep the security hygiene of the IT estate. **The following evidences were provided:** **Description** ITP-004-VAPT (Threat, Vulnerability and Patch Management) SG-020-SDD (Guidelines on Secure by Design and Default Best Practices) Manage Engine Desktop Central Screen Shots appended. Sample VA PT reports along with summary reports are appended
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.**
Planned measures (including implementation period)

Evaluation at Follow-Up

5.2.6 To what extent are IT systems technically checked (system audit)?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** IT General controls of the business-critical systems are performed annually by the third party. While ISMS teams collaborate with these teams and provide necessary support to complete the ITGC audits, Cyient's Cyber Security team will also perform internal VAPT activities to verify the systems and services adherence to the Defined policies and processes. All these assessment reports will be shared to the Cyient management and Leadership as appropriate and are discussed during the governance calls and Audit Committee meetings to consider strategic decisions. **The following evidences were provided:** **Description** 'ITP-004-VAPT (Threat Vulnerability and Patch Management) Evidences of VA PT reports, internal and external are shared. Evidences of external ITGC assessments shall be showcased while interviews.
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.**
Planned measures (including implementation period)
Evaluation at Follow-Up

5.2.7 To what extent is the network of the organization managed?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** Cyient's network is managed completely by the internal capacities called Network Support team (NWSupport). Centrally managed corporate Network architecture with all segregated VLAN's and extended networks including "Center Of Excellences" will be reviewed periodically by the NWSupport team. Network segmentation is managed through VLAN's and CoE's using latest configuration firewalls and Routers. **The following evidences were provided:** **Description:** 'ITP-020-NET (Network Operations Procedure) SP-003A-COM (Information communications management procedure) SG-020-SDD (Guidelines on Secure by Design and Default Best Practices) Reports from the OpManager; IDS and IPS logs; SIEM Logs are shared.
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.**
Planned measures (including implementation period)
Evaluation at Follow-Up

5.3. System acquisitions, requirement management and development

5.3.1 To what extent is information security considered in new or further development of IT systems?

Detailed Description (Including Assessment Procedure)

AL2:

The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:

Description

At Cyient, security requirements and risks in the development or acquisition of new or further developed IT systems is considered aptly.

During the planning phase teams will identify and address the security requirements and risks of IT systems in their lifecycle, Risk analysis is performed and for the implementation of mitigating information security controls viz.

- Authentication, authorization, and access control (Identity and Access management)
- Data protection and encryption
- Input validation and output filtering
- Error handling and logging
- Audit and monitoring
- Backup and recovery
- Patch management and vulnerability remediation
- Incident response and contingency planning

The following evidences were provided:

Description:

1. SG-020-SDD (Guidelines on Secure by Design and Default Best Practices)

2. SP-005-SDM(Information systems acquisition and maintenance Procedure)

3. SG-019-SCC (Secure Cloud Adoption and Cloud Security Best Practices)

4. ITP-004-VAPT (Threat Vulnerability and Patch Management)

5. SP-011-IAM (Identity and Access Management procedure)

6. SG-006-BKUP (Backup Policy & Guidelines)

Finding

Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.**
Planned measures (including implementation period)
Evaluation at Follow-Up

5.3.2 To what extent are requirements for network services defined?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** 'To ensure the security and integrity of the network services, which include internet access, email, file sharing, remote access, and cloud computing, Cyient's Network services are adequately protected and measured at periodic intervals. The documented procedure helps in maintaining, securing, and using the network services at Cyient seamlessly. All network services are protected by firewalls, antivirus software, encryption, and authentication mechanisms. Configuration management is followed for all network devices, such as routers, switches, servers, and workstations which are maintained according to the best practices and standards. Users performing the Network services are assigned with unique usernames and passwords and follow the password management process. Access to these users is enabled to network services based on the principle of least privilege, i.e., access is enabled to the resources on a "Need to know" basis to perform their tasks. The teams performing the Network services are subject matter experts in the domain and are expected to comply with them at all times. Network services are monitored and logged, and any suspicious or unauthorized events are reported and investigated as per the Incident Management Process. Additionally, the network services are regularly tested and audited for vulnerabilities and performance issues, and any identified gaps are remediated. **The following evidences were provided:** **Description** ITP-020-NET (Network Operations Procedure) Sample reports of Audit, IT DR test, Configuration management, Monitoring reports are shared
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.**
Planned measures (including implementation period)

Evaluation at Follow-Up

5.3.3 To what extent is the return and secure removal of information assets from external IT services regulated?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** Information assets which include any data, documents, or devices that contain or process information related to Cyient's business operations, customers, or partners is maintained and managed by the relevant stakeholders, which includes the users as well. Therefore, Cyient has established the proper procedures for returning and securely removing information assets when they are no longer needed or authorized. From a user perspective, once the user is offboarded the access to the IT systems is disabled following the offboarding process. These may include files, folders, databases, emails, messages, or accounts. IT Assets which are no longer required or needed for business purpose, which includes the asset retirement or due for disposal, are returned to HAM – Hardware asset management team for secure removal of information assets. For example, delete, erase, overwrite, or encrypt the information assets. Any IT asset that is returned is verified and validated with the Asset inventory and updated accordingly. Document the process and outcome of returning or securely removing information assets from the IT service. Record the date, time, method, and verification of the action. Store the documentation in a secure location for future reference or audit. **The following evidences were provided:** **Description:** ITP-010-IHM (IT Hardware Asset Management Policy Procedure). Refer to Section 8 - IT Asset Retirement and Disposal Process. Sample evidences of Assets returns and securely disposed are shared
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.**
Planned measures (including implementation period)
Evaluation at Follow-Up

5.3.4 To what extent is information protected in shared external IT services?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** All SAAS based cloud applications and IT Infrastructure hosted on cloud platforms are having clear isolation with multi tenancy capabilities. Client environments inside Cyient on-premise are segregated over VLAN's with access limited by controlling the required ports to access any IT services. Based on the contractual requirements, there are Physically and logically isolated environments, which are treated as separate 'Center of Excellence (CoE)'s" and for such environments Cyient will collaborate with the respective customers in establishing the required "Technology Control Plan". **The following evidences were provided:** **Description:** 1. SG-019-SCC (Secure Cloud Adoption and Cloud Security Best Practices) 2. SG-010-TCP (Technology Control Plan)
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.**
Planned measures (including implementation period)
Evaluation at Follow-Up

6 Supplier Relationships

6.1.1 To what extent is information security ensured among suppliers and cooperation partners?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** Information security requirements with the Contractors is part of the Contract / Agreement, which are verified and validated as per the Legal and Compliance activities. Contractual obligations with the Customers is part of the Contract requirements register which is verified and validated based on the contractual requirements. The relevant stakeholders will be provided access to the tool "simplicontract" to verify and validate the compliance requirements. All Contractors or vendors will have a valid Contract and an NDA is signed. **The following evidences were provided:** **Description:** Screenshot of the Simplicontract is appended. Sample NDA for a Vendor / contractor is appended.
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.**
Planned measures (including implementation period)
Evaluation at Follow-Up

6.1.2 To what extent is non-disclosure regarding the exchange of information contractually agreed?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** Cyient 's team has established the process of obtaining and maintaining the non-disclosure agreement while sharing the Cyient's information with any of the stakeholders as part of the Legal and Compliance. NDA is obtained from Employees or Associates at the time of joining. NDA is obtained from Vendor teams while engaging them for any of the Services with Cyient NDA is obtained from Customers or Contractors while engaging them for any of the Services with Cyient. **The following evidences were provided:** **Description:** A non-disclosure agreement template is appended. Samples of the NDA signed by the Associates; Vendor teams or other relevant stakeholders are appended for reference.
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.**
Planned measures (including implementation period)
Evaluation at Follow-Up

7 Compliance

7.1.1 To what extent is compliance with regulatory and contractual provisions ensured?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** 'Cyient has an established process of capturing, tracking, analyzing, and assessing the compliance requirements from legal, regulatory or contractual obligations. These obligations are captured in the Centralized tool by the Legal and Compliance team for verification and validation by the respective stakeholders. the tool referred is Complyent tool. Access to this tool is enabled to the relevant stakeholders by the Legal and Compliance team. Periodic updates are shared with the Management by the Legal and Compliance team at an organizational level. **The following evidences were provided:** **Description:** • LP-011-COM (Complyent Tool Process Document) • SP-007-SCL(Legal Compliance Procedure) • Complyent tool snapshot appended • SP-018-IPR(Interested Parties & Their Requirements)
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.**
Planned measures (including implementation period)
Evaluation at Follow-Up

7.1.2 To what extent is the protection of personal data taken into account when implementing information security?

Detailed Description (Including Assessment Procedure)
AL2: **The control was evaluated by a plausibility check of the self-assessment. The following implementation was described according to the documentation:** **Description** 'Cyient has established the legal and contractual information security requirements through a documented process to ensure that all of the stakeholders comply to it. Individual's personal identifiable information is protected through appropriate security controls and processes like DLP; Information asset labelling and classification. Users are sensitized and made aware of the Data privacy requirements through Email Flyers and training and awareness interventions. **The following evidences were provided:** **Description:** • 'GP-017-GDP (Global Data Privacy Policy) • SP-007-SCL(Legal Compliance Procedure) • Email Flyers - sample shared. .
Finding
Based on the observations, no deviation was found. **AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.**
Planned measures (including implementation period)
Evaluation at Follow-Up