KPMG Assurance and Consulting Services LLP
9th floor, Business Plaza,
Westin Hotel Campus,
36/3-B, Koregaon Park Annex,
Mundhwa Road, Ghorpadi,
Pune - 411 001, India
Telephone: +91 (20) 6747 7000
Fax: +91 (20) 6747 7100

HighRadius Technologies Private Limited
Unit-2, 1st Floor, Building No: 12C
Mindspace, Hitech City
Madhapur, Hyderabad
Telangana 500081
India

19 December 2023

Attention: Mr. Bhanu Bobba, Managing Director

KPMG Assurance and Consulting Services LLP (herein after referred to as "KPMG", "We", "Our") have completed SOC 2 Type 2 examination for HighRadius Technologies Private Limited (a wholly owned subsidiary of HighRadius Corporation) and HighRadius Corporation (herein after collectively referred to as "HighRadius" or "service organization", "you") as outlined in our engagement letter dated 20 April 2023. This report to you represents our final report for SOC 2 Type 2 examination.

The data included in this report was obtained from you, on or before 4 December 2023. We have no obligation to update our report or to revise the information contained therein to reflect events and transactions occurring subsequent to 4 December 2023. The attached report is the electronic version of our signed deliverable, which has been issued to you in the hard copy format.

This report sets forth our views based on the completeness and accuracy of the facts stated to KPMG and any assumptions that were included. If any of the facts and assumptions is not complete or accurate, it is imperative that we be informed accordingly, as the inaccuracy or incompleteness thereof could have a material effect on our conclusions. While performing the work, we assumed the genuineness of all signatures and the authenticity of all original documents. We have not independently verified the correctness or authenticity of the same.

This report is intended solely for the information and use of the management of HighRadius, its user entities and the independent auditors of user entities (collectively referred to as authorized parties) and is not intended to be, and should not be, used by anyone other than these authorized parties. If this report is received by anyone other than authorized parties, the recipient is placed on notice that the attached SOC 2 Type 2 report has been prepared solely for authorized parties for their internal use and this report and its contents shall not be shared with or disclosed to anyone by the recipient without the express written consent of HighRadius and KPMG. KPMG shall have no liability and shall pursue all available legal and equitable remedies against recipient, for the unauthorized use or distribution of this report. We have been engaged by HighRadius for the Services and to the fullest extent permitted by law, we will not accept responsibility or liability to any other party in respect of our Services or the report. We thus disclaim all responsibility or liability for any costs, damages, losses, liabilities, expenses incurred by such other party arising out of or in connection with the report or any part thereof. By reading our report the reader of the report shall be deemed to have accepted the terms mentioned hereinabove.

Please contact me at sumantdutta@kpmg.com if you have any questions or comments. We look forward to providing services to your company.

Yours sincerely,

Sumant Dutta
Director, KPMG Assurance and Consulting Services LLP

SYSTEM AND ORGANIZATION CONTROLS (SOC 2) TYPE 2 Report

Report on description of HighRadius Technologies Private Limited and HighRadius Corporation's system supporting application implementation services and on suitability of design and operating effectiveness of its controls relevant to Security, Availability, Confidentiality and Processing Integrity from the following delivery centers located at Bhubaneswar, India; Hyderabad, India; and Houston, USA.

For the period 1 November 2022 to 31 October 2023

TABLE OF CONTENTS

SECTION 1

INDEPENDENT SERVICE AUDITOR'S ASSURANCE REPORT

KPMG Assurance and Consulting Services LLP
9th floor, Business Plaza,
Westin Hotel Campus,
36/3-B, Koregaon Park Annex,
Mundhwa Road, Ghorpadi,
Pune - 411 001, India
Telephone: +91 (20) 6747 7000
Fax: +91 (20) 6747 7100

INDEPENDENT SERVICE AUDITOR'S ASSURANCE REPORT

To:
The Board of Directors,
HighRadius Corporation

Scope

We have been engaged to report on HighRadius Technologies Private Limited (a wholly owned subsidy of HighRadius Corporation) and HighRadius Corporation (hereinafter collectively referred to as "HighRadius" or "service organization") description in section 3 of its system for providing cloud-based application implementation and hosting services, application support services and supporting General Operating Environment for processing user entities' transactions to user entities from the delivery centers located in Hyderabad, India; Bhubaneswar, India; and Houston, USA throughout the period 1 November 2022, to 31 October 2023, (the description) based on the criteria for a description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2®Report (AICPA, Description Criteria), (description criteria) and on the design and operation of controls stated in the description to provide reasonable assurance that HighRadius' service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, and confidentiality set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria) (applicable trust services criteria).

HighRadius uses subservice organization(s) namely Equinix at Texas, USA; Datapipe at New Jersey, USA; Azure data centers at USA, Europe; Google Cloud Provider (GCP) data centers at USA; and Amazon Web Services (AWS) data centers at USA, Europe, and Canada for hosting the application servers and databases in the data centers. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at HighRadius, to achieve HighRadius' service commitments and system requirements based on the applicable trust services criteria. The description presents HighRadius' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of HighRadius' controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at HighRadius, to achieve HighRadius' service commitments and system requirements based on the applicable trust services criteria. The description presents HighRadius' controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of HighRadius' controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

The information included in Section 5 of the report, "Other Information Provided by HighRadius" is presented by management of HighRadius to provide additional information and is not a part of HighRadius' description. The information

about HighRadius' mapping of its controls with security and privacy requirements in Health Insurance Portability and Accountability Act (HIPAA) has not been subjected to the procedures applied in the examination of the description and of the suitability of the design and operating effectiveness of controls to achieve HighRadius' service commitments and system requirements based on the applicable trust services criteria, and accordingly, we express no opinion on it.

Service Organization's Responsibilities

HighRadius is responsible for: preparing the description and accompanying statement in section 2, including the completeness, accuracy, and method of presentation of the description and statement; providing the services covered by the description; selecting the applicable trust services category or categories and stating the related controls in the description; identifying the risks that would threaten the achievement of the service organization's service commitments and system requirements; and designing, implementing, and operating controls that are suitably designed and operating effectively to provide reasonable assurance that its service commitments and system requirements were achieved.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the design and operation of controls related to the service commitments and system requirements stated in that description, based on our procedures. We conducted our engagement in accordance with International Standard on Assurance Engagements 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board. That standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented in accordance with the description criteria and the controls are 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.

An assurance engagement to report on the description and the design and operating effectiveness of controls at a service organization involves performing procedures to obtain evidence about the disclosures in the service organization's description of its system and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgment, including the assessment of the risks that the description is not presented in accordance with the description criteria and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to obtain reasonable assurance that the service commitments and system requirements stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Service Auditor's Independence and Quality Control

We have complied with the independence and other ethical requirements of the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants (including International Independence Standards) (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

The firm applies International Standard on Quality Management 1, which requires the firm to design, implement and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Limitations of Controls at a Service Organization

The description is prepared to meet the common needs of a broad range of user entities and their auditors and may not, therefore, include every aspect of the system that individual user entity may consider important in its own environment. Also, because of their nature, service organization controls 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 of any evaluation of the suitability of design or operating effectiveness of controls to future periods is subject to the risk that controls at a service organization may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. In our opinion, in all material respects,

a. the description presents HighRadius' system for providing cloud-based application implementation and hosting services, application support services and supporting General Operating Environment for processing user entities' transactions that was designed and implemented throughout the period 1 November 2022 to 31 October 2023 in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period 1 November 2022 to 31 October 2023 to provide reasonable assurance that HighRadius' 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 the subservice organization(s) and user entities applied the complementary controls assumed in the design of HighRadius' controls throughout that period; and

c. the controls, which were those necessary to provide reasonable assurance that HighRadius' service commitments and system requirements were achieved based on the applicable trust services criteria, operated effectively throughout the period from 1 November 2022 to 31 October 2023, if complementary subservice organization controls and complementary user entity controls assumed in the design of HighRadius' controls operated effectively throughout that period.

Description of Tests of Controls

The specific controls tested, and the nature, timing, and results of those tests are listed in section 4.

Intended Users and Purpose

This report and the description of tests of controls in section 4 are intended only for HighRadius, user entities who have used HighRadius' system for providing cloud-based application implementation and hosting services, application support services and supporting General Operating Environment for processing user entities' transactions and their auditors, 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 entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- 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.

KPMG Assurance and Consulting Services LLP
Date: 4 December 2023

SECTION 2

STATEMENT BY THE SERVICE ORGANIZATION

STATEMENT BY THE SERVICE ORGANIZATION

We have prepared the accompanying description of HighRadius Technologies Private Limited (a wholly owned subsidy of HighRadius Corporation) and HighRadius Corporation (hereinafter collectively referred to as "HighRadius" or "service organization") in section 3 for providing cloud-based application implementation and hosting services, application support services and supporting General Operating Environment for processing user entities' transactions from the delivery centers located in Hyderabad, India; Bhubaneswar, India; and Houston, USA throughout the period 1 November 2022 to 31 October 2023 (description), based on the criteria for a description of a service organization's system in DC section 200, 2018 *Description Criteria for a Description of a Service Organization's System in a SOC 2®Report* (AICPA, *Description Criteria*) ("description criteria"). The description is intended to provide report users with information about the HighRadius' system that may be useful when assessing the risks arising from interactions with HighRadius' system, particularly information about system controls that HighRadius has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to *Security, Availability, Processing Integrity, and Confidentiality* ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).*

HighRadius uses subservice organization namely Equinix at Texas, USA; Datapipe at New Jersey, USA; Azure data centers at USA, Europe; Google Cloud Provider (GCP) data centers at USA; and Amazon Web Services (AWS) data centers at USA, Europe, and Canada for hosting the application servers and databases in the data centers. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at HighRadius, to achieve HighRadius' service commitments and system requirements based on the applicable trust services criteria. The description presents HighRadius' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of HighRadius' controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at HighRadius, to achieve HighRadius' service commitments and system requirements based on the applicable trust services criteria. The description presents HighRadius' controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of HighRadius' controls.

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

a. the description presents HighRadius' system for providing cloud-based application implementation and hosting services, application support services and supporting General Operating Environment for processing user entities' transactions that was designed and implemented throughout the period 1 November 2022 to 31 October 2023 in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period 1 November 2022 to 31 October 2023 to provide reasonable assurance that HighRadius' 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 the subservice organization(s) and user entities applied the complementary controls assumed in the design of HighRadius' controls throughout that period.

c. the controls stated in the description operated effectively throughout the period 1 November 2022 to 31 October 2023 to provide reasonable assurance that HighRadius' service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of HighRadius' controls, operated effectively throughout that period.

SECTION 3

HIGHRADIUS' DESCRIPTION OF THE SYSTEM

INTRODUCTION

Scope

This report focuses on application implementation and hosting services, application support services and supporting general operating environment rendered to user entities by HighRadius Technologies Private Limited and HighRadius Corporation (Collectively referred as "HighRadius") intended to meet the applicable trust service criteria for the services provided from HighRadius delivery centres at Hyderabad and Bhubaneswar in India and Houston in USA during the period 1 November 2022, to 31 October 2023. HighRadius management is responsible for designing, implementing, and documenting the controls to meet the applicable trust service criteria.

The scope of the report is restricted to below HighRadius cloud products and locations:

Platform Name	Cloud Products
Autonomous Receivables	• Credit • EIPP (E-Invoice Presentment & Payment) • Cash App • Deductions • Collections • Payment Gateway or Payment Cloud
RadiusOne AR Suite	• Collection App • Cash Reconciliation • Credit Risk App • E-Invoicing App
Freeda	• Digital Assistant Platform
dotONE Performance	• Analytics
Rivana	• Artificial Intelligence Platform

Location	Address
Hyderabad, India	DLF Cyber City, Indira Nagar, Gachibowli, Hyderabad, Telangana 500032
Hyderabad, India[1]	Unit-2, 1st Floor, Building No: 12C, Mindspace, Hitech City, Madhapur, Hyderabad, Telangana, PIN-500081
Bhubaneswar, India	KIIT Bhubaneswar, 4th Floor, Campus 3, Khordha, Odisha, 751024
Houston, USA	Westlake 4 Building (BP Campus) 200 Westlake Park Blvd 8th floor Houston, TX 77079
Houston, USA[2]	2107 CityWest Blvd Suite 1100, Houston, TX 77042

The report does not include any other services, locations, or facilities of HighRadius apart from the above mentioned.

Overview of HighRadius

HighRadius specializes in developing SaaS based software application products that optimize receivables management for corporations and enables them to modernize the entire process through highly integrated technology and automation. By adoption

[1] *HighRadius relocated to a new office in Hyderabad, India during the audit period and moved from DLF Cyber City, Indira Nagar, Gachibowli, Hyderabad to Unit-2, 1st Floor, Building No: 12C, Mindspace, Hitech City, Madhapur, Hyderabad on 21 August 2023*

[2] *HighRadius relocated to a new office in Houston, USA during the audit period and moved from Westlake 4 Building (BP Campus) 200 Westlake Park Blvd 8th floor Houston (previous facility) to 2107 CityWest Blvd Suite 1100, Houston (current facility) on 5 July 2023*

of innovative products, Accounts Receivables and Credit departments of user entities can become more strategic and streamlined which in turn helps in lowering their Days Sales Outstanding (DSO), minimize write-offs, and reduce operating expenses. HighRadius products deliver value to a wide range of customers in varied industry sectors like Financial Services, Consumer Products, Manufacturing, Distribution, Energy, and Retail. Products are suited to large enterprises that process thousands of invoices each day and are suited to mid-size enterprises as well who do not have resources to consolidate on an Enterprise Resource Planning (ERP) platform but still seek to streamline the receivable process. HighRadius has 4600+ professionals working from different locations spread across India, US and EMEA. HighRadius provides services to 800+ global clients including Fortune 500 companies. HighRadius operates on three core principles: to reduce the Total Cost of Ownership (TCO) of receivables solutions, to deliver a concrete Return on Investment (RoI) and fast payback periods to its customers, and to provide innovative functionality to its customers. HighRadius has adopted ISO 27001:2013 to establish a management framework for the Information Security Management System (ISMS). HighRadius development centre at Hyderabad is certified against the ISO (International Organization for Standardization) 27001:2013 standard.

Sub-service Organization

HighRadius uses subservice organizations for hosting cloud product servers and databases in data centers of Equinix at Texas, USA; Datapipe at New Jersey, USA; Azure data centers at USA, Europe; Google Cloud Provider (GCP) data centers at USA; and Amazon Web Services (AWS) data centers at USA, Europe, and Canada. This description includes only controls of HighRadius and excludes the relevant controls of the sub-service organizations. The controls pertaining to Physical Security and Environmental Safeguards for application servers and databases hosted at Equinix at Texas, USA; Datapipe at New Jersey, USA; Azure data centers at USA, Europe; Google Cloud Provider (GCP) data centers at USA; and Amazon Web Services (AWS) data centers at USA, Europe, and Canada are not covered in this report.

Managed Security Services

HighRadius uses Price Waterhouse Coopers (PwC) as its Managed Security Service Provider (MSSP) for the logs which includes server, firewall and end user logs monitoring. Alerts, in case of any malicious activity noted, are generated, and shared by the MSSP with HighRadius Cyber Security – Operations team using the Securonix Security Information and Event Monitoring (SIEM) tool. The alerts are categorized into Critical, High, Medium, and Low severities within the SIEM tool. Appropriate actions are taken by the HighRadius Cyber Security – Operations team for alerts reported.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

A Master Service Agreement (MSA) communicates the security, availability, confidentiality, and processing integrity commitments between HighRadius and its user entities. The agreement covers the scope and definition of services related to application implementation services.

HighRadius designs its processes and procedures related to application implementation services and general operating environment supporting for HighRadius' applications as listed below under scope to meet its objectives. These objectives are based on the service commitments agreed between HighRadius and its user entities. Services provided by HighRadius to its user entities are subject to security, availability, confidentiality and processing integrity requirements as documented in the MSA signed between HighRadius and its user entities.

The security, availability and confidentiality requirements are communicated to HighRadius employees via contractual agreements or Non-Disclosure Agreements (NDA). These commitments are considered by HighRadius while providing services to its user entities.

HighRadius has Information Security policies that define the organization-wide approach for protecting systems and data. These policies govern how the products are designed and developed, how the systems are operated, how the internal business systems and network are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented for executing various processes.

COMPONENTS OF THE SYSTEM IN SCOPE

Infrastructure

Application implementation services are provided to user entities using IT equipment, and network devices such as firewall, IDS/IPS, and switches located in respective third-party data centers. This infrastructure includes devices providing connectivity into the hosting environment needed to make services available to user entities as needed. Network and infrastructure changes were initiated, approved, and tracked within the ManageEngine – Genie tool. Upon receipt of approval from Line Manager, IMS team implements the change.

People

The application development, application implementation and application support services are supported by the development team, operations support team, implementation team and Infrastructure Management Service (IMS) team. HighRadius provides support services to its user entities from delivery centers in Hyderabad and Bhubaneswar, India and Houston, USA.

Software

HighRadius has documented 'Server and Firewall Hardening Standard' policy and procedures for its servers and 'End User Device Hardening Standard' for its end user systems in order to provide a controlled operating environment and to prevent any unauthorized access to critical system resources.

Relevant security patches are updated on workstations and servers. The changes are implemented post approval from the respective department heads and post testing of patches in the staging environment.

Remote access of data by HighRadius employees is in line with the defined 'Remote Access Guidelines' which requires the usage of a secure Virtual Private Network (VPN) to access the HighRadius network through AES 256 encryption.

Data

User entity data is held in accordance with the relevant data protection and other regulations, with any specific requirements being set out in the user entity MSA.

HighRadius has documented information classification policy for classification of data based upon the sensitivity and confidentiality of data. Data or information in HighRadius is classified into four categories given below:

- Public
- Internal
- Confidential
- Restricted

Data handling requirements is documented in the policy which covers guidelines to identify the level of protection, controls requirement and handling in various scenarios. HighRadius has documented and established procedures to dispose confidential information post retention period.

Policies and Procedures

HighRadius has a corporate intranet portal where the information security policies and related procedures are made available to the associates. Induction program for new associates includes session on information security to provide awareness on HighRadius information security policies and related procedures. On an annual basis, HighRadius associates undergo information security awareness program and an assessment. The program covers various aspects of Information Security defined at HighRadius such as acceptable use of assets, protection of information, security incident management and general information security guidelines. Associates are required to complete the assessment.

SYSTEM OVERVIEW

HighRadius operates within a defined Information Security Management System (ISMS) to provide application implementation services and general operating environment for HighRadius's applications as listed below under scope.

The ISMS consists of multiple components such as policies and procedures, governance structure, support functions and application systems. The policies and procedures provide guidance to the users regarding the process to be followed for providing the services and ensures their consistent implementation. The governance model of HighRadius provides direction for operating its system and assists in demonstrating management commitments. The defined processes for information systems, including information security, network security, logical security, physical security, environmental safeguards, and human resources are implemented by HighRadius to provide services in a secure IT environment to its customers.

Internal control consists of five interrelated components. These are derived from the way management runs a business and are integrated with the management process. HighRadius has established an internal controls framework that reflects the five components which includes:

Control Environment

The control environment is the set of standards, processes, and structures that provide the basis for defining, implementing, and operating internal control system across the organization. The Board of Directors (BoD) and senior management establish the tone at the top regarding the importance of internal controls including expected standards of conduct. Management reinforces expectations at the various levels of the organization. The control environment comprises the integrity and ethical values of the organization; the parameters enabling the BoD to carry out its governance oversight responsibilities; the organizational structure and assignment of authority and responsibility; the process for attracting, developing, and retaining competent individuals; and the rigor around performance measures, incentives, and rewards to drive accountability for performance. The resulting control environment has a pervasive impact on the overall system of internal control.

Risk Assessment

Every entity faces a variety of risks from external and internal sources. Risk is defined as the possibility that an event will occur and adversely affect the achievement of objectives. Risk assessment involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives. Risks to the achievement of these objectives from across the entity are considered relative to established risk tolerances. Thus, risk assessment forms the basis for determining how risks will be managed. A precondition to risk assessment is establishment of objectives, linked at different levels of the entity. Management specifies objectives within categories relating to operations, reporting and compliance with sufficient clarity to be able to identify and analyse risks to those objectives. Management also considers the suitability of the objectives for the entity. Risk assessment also requires management to consider the impact of possible changes in the external environment and within its own business model that may render internal control ineffective.

Information and Communication

Information is necessary for the entity to carry out internal control responsibilities to support the achievement of its objectives. Management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of other components of internal control. Communication is the continual, iterative process of providing, sharing, and obtaining necessary information. Internal communication is the means by which information is disseminated throughout the organization, flowing up, down, and across the entity. It enables personnel to receive a clear message from senior management that control responsibilities must be taken seriously. External communication is twofold: it enables inbound communication of relevant external information, and it provides information to external parties in response to requirements and expectations.

Monitoring Activities

Regular internal audits, evaluations and external audits, or some combination of the two are used to ascertain whether each of the five components of internal control, including controls to affect the principles within each component, is present and functioning. Ongoing evaluations, built into business processes at different levels of the entity, provide timely information. Separate evaluations, conducted periodically, will vary in scope and frequency depending on assessment of risks, effectiveness of ongoing evaluations, and other management considerations. Findings are evaluated against criteria established by regulators, recognized standard-setting

bodies or management and the board of directors; deficiencies are communicated to management and the board of directors as appropriate.

With respect to the sub service organizations, HighRadius obtains the System and Organization Controls assessment reports of Equinix, Datapipe, Google Cloud Platform, Azure, and AWS to verify the controls which are performed by sub-service organizations.

Control Activities

Control activities are the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out. Control activities are performed at all levels of the entity, at various stages within business processes, and over the technology environment. They may be preventive or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations, and business performance reviews. Segregation of duties is typically built into the selection and development of control activities. Where segregation of duties is not practical, management selects and develops alternative control activities.

There is synergy and linkage among these components, forming an integrated system that reacts dynamically to changing conditions. The internal control system is intertwined with the entity's operating activities and exists for fundamental business reasons.

The components mentioned above are described in detail in the succeeding sections.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

Control Environment

Security Policies

HighRadius has defined an organization wide Information Security Management System (ISMS) based on International Organization for Standardization (ISO) 27001:2013 framework.

Information Security policies and related procedures have been developed in line with ISO27001 standard. Information Security policies and related procedures are periodically reviewed by the Vice President – Cyber Security - Risk & Compliance and approved by Chief Information Security Officer.

The below policies are in place at HighRadius:

- Information Security Policy
- Organization of Information Security Policy
- Human Resources Security Policy
- Asset Management Policy
- Access Control Policy
- Cryptography Policy
- Physical and Environment Security Policy
- Clear Desk and Clear Screen Policy
- Operations Security Policy
- Communication Security policy
- Information Systems Acquisition Development and Maintenance Policy
- Supplier Relationships Policy
- Incident Management Policy
- Information Security Aspect of Business Continuity Management Policy
- Compliance Policy
- Privacy Policy
- Social Media Policy
- Acceptable Usage standard

Organization Structure

The organization structure of HighRadius, which provides the overall framework for planning, directing, and controlling operations, has segregated personnel and business functions into functional groups according to job responsibilities. This approach allows HighRadius to clearly define responsibilities, lines of reporting, and communication. HighRadius operates under the general direction and supervision of its Chief Executive Officer. The organization structure of HighRadius as on 31 October 2023 showing the various functional groups is shown below:

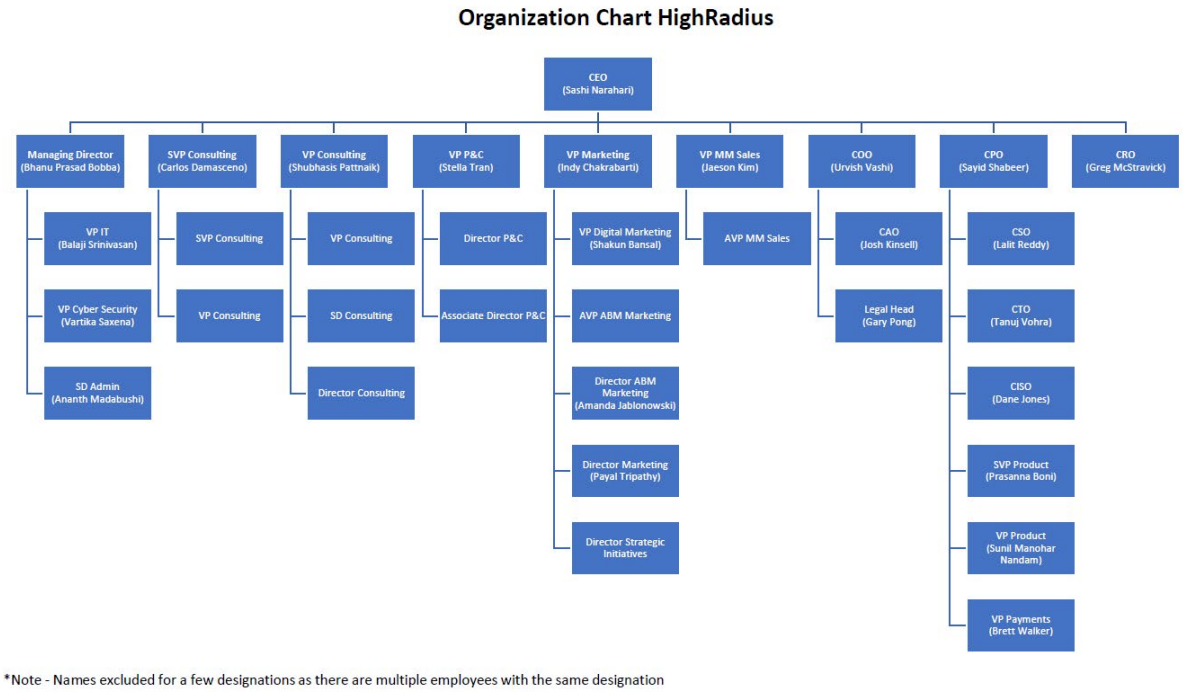

Figure 1 – Organization Structure

Acronyms used in HighRadius organization structure:

- CEO – Chief Executive Officer
- COO – Chief Operating Officer
- CAO – Chief Administrative Officer
- CPO – Chief Product Officer
- CSO – Chief Strategy Officer
- CTO – Chief Technology Officer
- CISO – Chief Information Security Officer
- CRO – Chief Revenue Officer
- SVP – Senior Vice President
- VP – Vice President
- SD – Senior Director
- P&C – People and Culture
- ABM – Account Based Marketing
- MM – Mid Market

Senior Management Group

HighRadius operates under the direction of the Chief Executive Officer (CEO), Chief Operating Officer (COO) and Managing Director (MD). The senior management group is instrumental in formulating and executing the company's global strategy and growth. They are responsible for evaluating corporate governance policies and establishing a number of committees for addressing specific areas with well-defined objectives and activities. The company has put in place a risk management process. Reports are presented to the senior management group at regular intervals. Senior management group reviews whether systems and controls are in place for safeguarding the information assets of the company and for preventing and detecting any major weaknesses in the system.

The responsibilities of senior management group include the following:

- Reviewing, approving, monitoring, fundamental, financial, and business strategies, and major corporate actions,
- Assessing major risks facing HighRadius and reviewing options for their mitigation, and,

- Ensuring that processes are in place for maintaining the integrity and confidentiality of the entity, the financial statements, compliance with laws and ethics, relationship with user entity and suppliers, and relationship with stake holders.

Cyber Security team

The Cyber Security group is headed by the functional head of Cyber Security and has two different functions:

- Cyber Security - Risk & Compliance
- Cyber Security - Operations

Cyber Security - Risk & Compliance

The team comprises of Cyber Security - Risk & Compliance - CISO, Vice President, Senior Managers, Associate Managers, and Cyber Security team members.

Cyber Security - Compliance

- Cyber Security - Risk & Compliance team performs regular audits and assessments of internal controls, the audit process, the process for monitoring compliance with laws & regulations. Suggestions are provided by the team and the Audit Committee follows-up on the implementation of corrective actions.
- The team manages Vendor Risk Assessment through Sourcing Assessments as a due diligence activity for new vendors before finalizing the vendor and performs subsequent annual Vendor Assessments for the existing vendors.
- The team addresses information security related queries by prospective clients and contributes to pre-sales activities.
- The team is responsible for assigning security induction training modules for new joiners post user data upload on the portal by HR team and information security awareness annual refresher training, phishing campaigns, and security advisories for existing employees of HighRadius through the Knowbe4 training portal.
- The team is responsible for phishing alerts review to cut through the mailbox spam and respond to threats more quickly.
- The team is also responsible to perform the annual risk assessments and semi-annual asset inventory reviews.

Cyber Security - Operations

- Cyber Security - Operations team is responsible for information security related initiatives and maintaining security posture of the organization.
- The team performs vulnerability assessments and penetration testing on HighRadius applications, networks, database servers, and operating systems on a periodic basis. Issues of non-compliance from the vulnerability assessments and penetration tests are tracked to closure.
- The team is also responsible for performing wireless scans and software scans on a quarterly basis.
- The team also performs a monthly full static code analysis and a weekly incremental static code security analysis of the changes in the development environment prior to pushing the change to production. Issues of non-compliance from the static code security analysis are tracked to closure.
- Cyber Security – Operations team is responsible for monitoring the alerts shared by HighRadius' MSSP within the Security Information and Event Management (SIEM) tool. Appropriate actions are taken, as required.
- Generation and management of Advanced Encryption Standard (AES) keys for encrypting customer data hosted within HighRadius' application servers and databases is automated and managed by Customer Value Managers (CVMs). Further, Pretty Good Privacy (PGP) public and private keys are also generated by the CVMs for encrypting the files shared with and received from customers. The AES and PGP keys are generated basis the requests received from HighRadius Consulting team for customer accounts. Additionally, key rotation is performed on an annual basis prior to expiration.
- Cyber Security – Operations team leverages the BitSight tool to track HighRadius' Cyber Security performance. Alerts received are monitored by Cyber Security – Operations team and appropriate actions are taken, as required.
- Cyber Security – Operations team is also responsible for monitoring Network and Endpoint Security using Cloud Access Security Broker (CASB) solution, Anti-Malware and Anti Malware solutions.

- The team is further responsible for the security incident management which includes recording, categorizing, root cause analysis and tracking to closure of incidents affecting security, availability, confidentiality, and processing integrity of information systems.

People and Culture (Human Resources)

The People and Culture (P&C) department is responsible for competency development, new joiner's induction, security induction (security awareness) to new joiners, exit formalities of resigned associates, disciplinary activities, and yearly appraisal of associates. The P&C department is also responsible for initiating physical access card request for new associates, initiating domain user ID creation for new associates, and initiating exit formalities for associates exiting HighRadius. Further, P&C department conducts yearly Prevention of Sexual Harassment (POSH) at workplace training. POSH training is also covered as part of the new joiner induction conducted by the HR team at HighRadius. Additionally, background checks are performed, and references are checked prior to hiring new personnel to validate their academic qualifications, past work experiences and suitability for HighRadius operations.

Talent Acquisition Group

Talent Acquisition team is responsible for identifying appropriate resources for various functions/products based on requirement of resources in the organization. P&C team has defined formal hiring policies and guidelines that assist in selecting qualified applicants for specific job responsibilities, as per business requirements. Each job candidate is interviewed to determine if background and experience is appropriate for the job function.

Training and Development

HighRadius associates who are involved in supporting the IT infrastructure and environment are trained in their respective areas of expertise. HighRadius encourages its associates to enhance their skills on a continuous basis. Training programs are conducted on a regular basis to enable associates to develop their competencies. Cyber Security team members are encouraged to achieve certifications from vendors and independent certification organizations. On an annual basis, HighRadius associates undergo an information security awareness program and assessment using the Knowbe4 tool. The program covers various aspects of information security defined at HighRadius such as acceptable use of assets, protection of information, incident management and general information security guidelines. Associates are required to complete the assessment. Further, the Learning and Development (L&D) team at HighRadius provides and prepares employee self-development initiatives, manages events and communications to HighRadius.

Administration team

The Administration team at HighRadius consists of Facilities team and Commercial team.

Facilities

The Facilities team is responsible for implementing and managing adequate controls for physical and environmental security and performing physical access reviews for users on a semi-annual basis. The team is also responsible for issuance and configuration of access cards and monitoring the entry/exit to the premises by deploying security guards at the facilities. They are also responsible for managing the backup power sources and environmental safeguards implemented within the premises of HighRadius. The Facilities team also reviews the visitor register and material in/out register maintained on a weekly basis.

Commercial

The Commercial team handles the procurement of IT and Non-IT assets. Requests for the procurement are received through the Service Desk tool or via e-mail. The commercial team then contacts the vendor and quotations are discussed/received. After finalising the vendor, sourcing of the requirements is performed by the Commercial team.

Corporate Legal Counsel

The Corporate Legal Counsel looks after compliance with legal requirements, compliance with regulations of the different geographies and assists with customer compliance for any applicable regulations. The contractual and legal compliance aspects related to information security are handled by the Head of Legal and Legal team.

Infrastructure Management Services (IMS) team

The IMS team is represented by VP Technology and is responsible for designing, deploying, and maintaining IT infrastructure aligned to HighRadius business needs across its locations. IT security controls at HighRadius are implemented by the IMS. Logical access security to systems, servers and applications, maintenance, and upkeep of servers, managing logical security and network security at HighRadius premises is being governed by the IMS team.

Service Delivery Functions

Service Delivery at HighRadius consists of various teams such as Sales & Marketing, Consulting & Implementation, TechSupport, Implementation, Quality Assurance and Product Management. Each team is headed by respective Vice Presidents and strives to achieve excellence in service delivery and support. HighRadius provides application implementation and support services to its user entity. HighRadius' associates provide the support services from the HighRadius facilities located at Hyderabad and Bhubaneswar, India and Houston, USA. Further, the teams and departments are responsible for performing quarterly user entitlement reviews.

Risk Assessment

Entity Level Risk Assessment

HighRadius understands that risk assessment is a critical component of its operations that helps ensure that business is properly managed and secured. HighRadius management has incorporated risk management procedures across its functional areas. Risk management standard is updated on an annual basis or if there is a significant change in the process. Risks are reviewed and updated on an annual basis. The consolidated risk assessment report is prepared by the risk management team and is reviewed by the VP – Cyber Security. The management is responsible for implementing procedures to identify risks inherent in the operations and for implementing procedures to monitor and mitigate the identified risks. The foundation for this process is management's knowledge of its operations, its close working relationship with its clients, and its understanding of the industry in which it operates.

Information Risk Assessment

HighRadius has a formal Risk Management standard document that defines the procedure for performing the risk assessment of information assets. For assets, Asset Value is computed based on three attributes: confidentiality, integrity, and availability. For each information asset, a number of possible threats are identified. For each threat, Risk Value is computed based on the probability of occurrence and the impact of consequence. For each threat, a number of possible vulnerabilities are identified. For each vulnerability, an Impact Value and Probability Value are assigned based on the likelihood of the vulnerability being exploited as per current practices. Risk Value is computed based on the Asset Value, Impact Value, and Probability Value. Further, HighRadius has defined a threshold limit for acceptable Risk Value. For risks that are above the threshold limit, suitable risk treatment plans are identified and implemented. Risk treatment assessment plan is reviewed and updated at least once a year or whenever there is a significant change regarding the assets being added in the company. Further, on a semi-annual basis, Cyber Security - Risk & Compliance team performs asset inventory reconciliation. Results of the reconciliation are documented, and remediation actions are taken as appropriate.

Business Risks

Contracts and proposals are reviewed by the Sales, Legal and Cyber Security - Risk & Compliance teams to identify and mitigate risks. The Sales and Legal teams review the performance of projects against contractual commitments and takes appropriate corrective actions as necessary.

Business Continuity Planning and Disaster Recovery

HighRadius has documented and approved Business Continuity Plan, which describes the process on business continuity and Disaster Recovery. The following are documented in detail within the BCP/DRP (Disaster Recovery Plan):

- Business Continuity Planning
- Recovery Time Objective (4 hours) and Recovery Point Objective (1 hour)

Emergency Management Team (EMT) and Disaster Recovery (DR) team are responsible for the development, testing and implementation of BCP/DRP for the organization's critical infrastructure included but not limited to IT, Systems, Process and Resources. The BCP/DR team determines the services/ processes / technology and systems considered as critical and impacts the

continuity of business. This exercise also determines the project and related data systems need to be recovered in the event of disruption. BCP/DR plan is reviewed and updated annually or whenever there is a change in the infrastructure and facilities. BCP/DR plan is tested on an annual basis. Observations are documented and reviewed by the VP – Cyber Security.

Environmental, Regulatory and Technological Review

Environmental, regulatory, and technological change, and its effect on system security is closely monitored by MD, CEO, COO, and other members of the Senior Management group via webcast, seminars, and printed media, and relevant issues are discussed in review meetings.

Information and Communication

Personnel Security

Recruitment process

As part of joining formalities, new employees and contractors are required to sign a Non-Disclosure Agreement (NDA) that addresses the confidentiality requirement of HighRadius and customer information.

Background verification

HighRadius has defined a formal 'Background Verification' policy to provide guidance for performing background verification for new hires. Background verification includes verifying identity, education, employment, and criminal checks. The Human Resources (HR) department initiates the Background Verification Checks (BGV) for associates who have joined HighRadius. As per 'Background Verification' policy, the associates joining directly from campus, are subject to identity and criminal checks. For immediate or ad hoc joiners, BGV is initiated post offer acceptance and uploading of relevant documents by the candidate. Background verification is performed by approved third party service providers. A detailed BGV report is provided by the third-party service provider upon completion of the background verification.

Master Service Agreements

Terms and Conditions are presented through Master Service Agreements (MSA) to provide a mechanism for communicating the terms of service between HighRadius and its user entities. The terms and conditions outline the terms and payments for services, use of services, enforcement, intellectual property rights, and warranties. HighRadius presents a description of its systems, services, and terms of usage on its website www.highradius.com, which can be referred by its prospective clients, associates, and website users.

Environmental and Physical Security[3][4]

Fire Detection and Suppression

Smoke detectors and fire extinguishers are available in the work area where computer systems are housed and are installed at strategic points where they can be accessed easily. Fire safety equipment is checked on a quarterly basis for Hyderabad, India and semi-annual basis for Houston, USA. Checks are conducted in accordance with manufacturer's instructions and test results are documented. Fire and emergency instructions are displayed in prominent locations within the facility. The smoke detectors are rated by the manufacturer to produce an audible alarm when activated.

Power Backup

UPS is installed within the premises to support during a power failure or shutdown. Backup UPS equipment is used to help ensure continuous functioning of sensitive or critical systems in case the original UPS equipment fails.

[3] *HighRadius relocated to a new office in Hyderabad, India during the audit period and moved from DLF Cyber City, Indira Nagar, Gachibowli, Hyderabad to Unit-2, 1st Floor, Building No: 12C, Mindspace, Hitech City, Madhapur, Hyderabad on 21 August 2023.*
[4] *HighRadius relocated to a new office in Houston, USA during the audit period and moved from Westlake 4 Building (BP Campus) 200 Westlake Park Blvd 8th floor Houston (previous facility) to 2107 CityWest Blvd Suite 1100, Houston (current facility) on 5 July 2023*

Temperature Monitoring

Air-conditioners are installed inside the network and hub rooms to control and maintain temperature. A physical security personnel monitors and records the temperature in the server and hub rooms every six hours.

Physical Access Security

Administration team is responsible for implementing physical security controls at HighRadius facilities. HighRadius facilities are safeguarded on a continuous basis by security guards. Entry to the facility is restricted to authorized personnel by a proximity card-based access control system. Proximity based access control systems are installed to restrict unauthorized entry to HighRadius premises and network/hub room. Physical access to the network/hub/UPS room is restricted to authorized personnel from the IMS team and physical security personnel. CCTV cameras are positioned in the facilities and are monitored on a continuous basis by security personnel.

Visitor Access

A separate visitor register is maintained by security guards for capturing entry and exit time of vendors/ consultants/ visitors along with name, purpose, and contact person. The visitors/ consultants/ vendors are escorted by the HighRadius' associates in the facilities. Electronic devices (laptop) brought by the visitors/vendors are declared at the entrance of the facility in the visitor register.

Further, from 5 July 2023, the building security team of HighRadius' Houston office is responsible for providing temporary/visitor access cards to visitors of HighRadius based on the email requests raised by the HR.

Process for Granting & Revoking Physical Access

Administration team manages the proximity access card-based access control system, and the HR team initiates the access registration process. Administration team issues access cards to new associates based on the requests raised by the HR through email or ManageEngine – Genie tool. Physical access to the HighRadius facility is revoked and the proximity card is returned to the administration team on or before the last working day of the associate.

Further, from 5 July 2023, the building security team of HighRadius' Houston office is responsible for creating physical access for new associates joining the Houston office based on the email requests raised by the HR and provides an email confirmation upon creation. Additionally, the building security team is responsible for revoking physical access for leavers based on the email requests raised by the HR and provides an email confirmation upon revocation. Also, physical access cards are collected by the HR on the last working day of the associate.

System Account Management

User Access Creation

For new joiners prior to joining HighRadius, the HR department initiates a request the IT helpdesk for providing logical access to the new joiner. via e-mail and the IT helpdesk raises a request on the ManageEngine – Genie Tool. The access request consists of associate's details including employee ID, first name, last name, location, designation, and date of joining. The system administrator creates the user ID based on e-mail communication from HR. Access to client production and non-production environments is granted to users after obtaining approval from respective line managers in the Privileged Access Management Solutions (PAMS) tool. Time-bound access is granted to the users and revoked automatically based on the timeout duration configured as per the job role of the users within the PAMS tool.

User Account Maintenance

User accounts are configured to lock-out after five unsuccessful logon attempts. Local administrative rights on desktops and laptops are restricted and exceptions are provided based on approval from the line manager and IMS team. Default guest or anonymous logins are disabled on desktops and laptops.

User Account Deletion

When an associate leaves HighRadius, a request for revocation of access is raised as part of the associate's exit formalities in the Genie tool by HR. Process for revoking user access in case of termination and absconding are the same as voluntary exit. Upon receiving information from the portal, the associate's user ID is disabled, and access is revoked by the IMS teams from the LDAP and Active Directory on associate's last working date.

Endpoint security

Administrative access on employee workstations is restricted to authorized internal IMS team. Trend Micro Apex Central anti-malware solution is installed on HighRadius workstations and servers. The malware definitions required by the anti-malware solution are automatically updated on workstations at the time of logging-in. Administrative access to the anti-malware server is restricted to the IMS team. Firewalls are used in the perimeter of the core network to block traffic unless specifically configured to permit. Incoming and outgoing e-mails are scanned for malwares through the anti-malware system. Access to the internet is restricted to business-critical sites by the IMS team through Uniform Resource Locator (URL) filtering. Hardening procedure is enforced on servers, end user systems and network devices, including restrictions on access to diagnostic/configuration/auxiliary ports. Regular review and monitoring of compliance to security and hardening standards for systems and devices is being performed. Removable media devices, such as Compact Disk writers, Universal Serial Bus (USB) mass storage devices, and Compact Disk – Read Only Memory (CD-ROM) readers are disabled on individual workstations. User access review for standard and privileged users on AD and LDAP are performed by the Cyber Security - Risk & Compliance team on a quarterly basis.

Clear desk policy

A Clear Desk and Clear Screen Policy is documented and implemented to ensure that a user entity's confidential information is not left unattended on user workstation desks during and after working hours and is safeguarded.

Logging and Retention Policy

HighRadius has defined policy to establish a requirement to enable, review and storage of the logs of IT systems and services. The policy covers system components for which logs are to be generated, retention, review of logs, monitoring, and access control. A centralized syslog server is in place to maintain or manage the logs generated. These logs are integrated with SIEM and monitored by HighRadius' MSSP to identify security events that may have a potential impact on the system security. Cyber Security – Operations team monitors the alerts received in the SIEM tool and takes appropriate actions, as required.

Cloud Application Implementation Services and Request Management

The requests received by HighRadius from user entity are categorized as follows:

Cloud Application Implementation

User Acceptance Testing

In cases of cloud application implementations, User Acceptance Testing (UAT) is performed by the user entity in HighRadius' UAT environment. Upon successful completion of UAT, a UAT sign-off is obtained from the user entity.

Cutover Plan Communication and Go-live Confirmation

Once a UAT sign-off is obtained from the user entity, HighRadius communicates the cutover plan to the user entity prior to implementation in the production environment and receives a go-live confirmation from the user entity post successful migration of the final product by the Cloud Engineering team onto the on-demand cloud portal.

Service Request Management

New Implementation Requests

New Implementation requests are registered by HighRadius' customers using the Salesforce ticketing tool if customer needs additional functionality in the system to handle additional use cases. HighRadius is not contractually obligated to perform work within a certain period.

Past Implementation Issue

Past implementation issues are registered by HighRadius' customers using the Salesforce ticketing tool if customer needs support in configurational changes from a previous implementation. HighRadius is not contractually obligated to perform work within a certain period.

Admin Tasks

Admin tasks are registered by HighRadius' customers using the Salesforce ticketing tool if customer needs help to perform a task. HighRadius is not contractually obligated to perform work within a certain period.

Service requests are resolved by the TechSupport team in coordination with the respective customer support teams at HighRadius.

Defects and Service Disruption Management

Defects

Defects are registered by HighRadius' customers using the Salesforce ticketing tool in case the existing product functionality is broken. Defects have a contractual SLA commitment.

Service Disruptions

Service disruptions are registered by HighRadius' customers using the Salesforce ticketing tool in case 60% or more users are not able to access the HighRadius system. Service disruptions have a contractual SLA commitment.

For defects and service disruptions, priorities are assigned to each ticket within the ticketing tool, and they are acknowledged and resolved by the respective customer support teams in HighRadius within the defined SLAs. Upon closure of defects and service disruptions, TechSupport team performs the Root Cause Analysis (RCA) and communicates the results to affected users through the ticketing tool.

Change Management

HighRadius has defined an organization-wide change management procedure to regulate changes across applications and infrastructure components for ensuring that changes are assessed, approved, implemented, and reviewed in a controlled manner. The change management policy for the HighRadius applications detailing the procedures for raising a change request, development, testing and necessary approvals prior to implementation are covered as part of the 'Operations Security procedure' document. The policy document is updated and reviewed by the Vice President – Cyber Security – Risk & Compliance and approved by the Chief Information Security Officer on an annual basis or as and when required. Any change to the components of the network & systems requires prior approval from the line manager. JIRA tool is used for tracking the product related changes involved in the Software Development Life Cycle (SDLC). Changes to network and security devices such as Firewall, OS and IDS/IPS are initiated based on a request in ManageEngine – Genie tool. The changes are logged, categorized as scheduled or emergency, analysed, tested, and released by the IMS team. The changes are implemented only after communicating to management and users who will be affected. Changes to HighRadius corporate infrastructure components follow the standard change management procedure and such changes are authorized, tested, and documented along with approvals from IMS Manager and Manager – Cyber Security - Operations wherever applicable. Also, access to the development environment and to migrate changes to production environments is segregated and restricted to authorized individuals. HighRadius Architecture, Product Development and Quality Assurance teams support in the change management process.

The below mentioned change management procedure refers to application changes for both HighRadius and user entities.

CR Registration

Change Request (CR) is registered within a tracking tool by user entity or Product team. CR contains detailed information such as priority, impact (based upon criticality of change request), ownership, and description of the change. The changes are classified by the Product teams within the ticketing tool

Development and testing of changes

Change is worked upon by the development team. The JIRA ticketing tool is used for tracking the complete development process for the CR and is updated by the Product team**.** Once the change is developed, it is moved to the QA environment by the build and development team. Changes are tested in the test environment by the QA team and QA sign-off is obtained prior to migration of changes into the stage environment. QA team performs further testing in the stage environment and approves the change for migration of the change to production.

CR Resolution

Upon QA sign-off, Product team updates the CR with a brief description of the solution provided and changes the status within the tracking tool to "Closed" and the change is moved into the production environment in the subsequent release cycle.

Network and Infrastructure

Network and infrastructure changes were initiated, approved, and tracked within the ManageEngine – Genie tool. Upon receipt of approval from the line manager, IMS team implements the change. The changes are authorized, tested, and documented. The

changes are categorized based on the criticality, and are implemented, communicated to management and the users who will be affected by the changes.

Functional Changes

HighRadius categorizes functional changes as configuration level changes to specific customer environments basis requests received from respective customer POCs. Requests are raised by the customers on Salesforce tool and a priority level is assigned to each request. HighRadius functional consultants are responsible for making the required configuration level change post authorization from the Value Com team. In case a customer request cannot be accommodated at configuration level, then appropriate product enhancement change requests are raised and standard change management process is followed.

Patch Management

Patch management policy is defined to regulate changes across applications and infrastructure components for ensuring that changes are assessed, approved, implemented, and reviewed in a controlled manner. Desktop Central tool pushes patches to end user systems. The patches are tested and observed in staging machines prior to deployment to HighRadius end user systems. Scheduled restart alert is sent to HighRadius users 48 hours prior to deployment of patch to prevent loss of work. Relevant security patches are updated on servers and other infrastructure devices through patch management process. The patches are deployed based on the severity level (Critical – 5 days, High – 30 days, Medium – 90 days and Low – 180 days) post approval from the IMS team manager and successful testing in the staging environment.

Patch Requisition

Patch requests are raised as tickets in the internal IT helpdesk ticketing tool by Infrastructure Management Service (IMS) team / Cyber Security – Operations team.

Migration to production

Patches to be applied are authorized by respective department heads prior to migration of patch in production environment.

Security Incident Management

HighRadius has defined a 'Incident Management Procedure' which includes procedures for reporting, categorization, resolution, and escalation of security incidents. The Security Incident Management policy is available on intranet. The details of policy are also covered as part of the initial induction program.

Job description and responsibility of SIRT (Security Incident Response Team) is defined in the 'Information Security' policy. The 'Information Security' policy is hosted on the corporate intranet and is available to employees.

Information security incidents affecting security, confidentiality, processing integrity, and availability of information systems are recorded, categorized, analysed for root cause, and tracked to closure by the Cyber Security team. Any incidents that involve suspected issues related to protected data or personally identifiable information (PII) are e-mailed to a dedicated mailbox.

For incidents having impact on user entities, the HighRadius TechSupport team reports the incident to appropriate client stakeholders. Clients are informed about these procedures during the contracting phase.

Security Incident Reporting

At HighRadius, associates are instructed to report and communicate security breaches and other incidents via e-mail or using the internal ticketing tool. The e-mail IDs are group e-mail IDs; members of the Cyber Security team have access to this e-mail. In case any incident is reported, the incident is reviewed immediately by the Cyber Security teams and decide on the necessary action to be taken. Further, the incident reports are shared with relevant stakeholders.

Security Management

Vulnerability Assessment & Penetration Testing

Quarterly Vulnerability Assessment and Penetration Test (VAPT) are performed on HighRadius applications, networks, database server and operating system by the Cyber Security – Operations team. Third party VAPT is conducted semi-annually to assess vulnerabilities and evaluate network security risks. Issues of non-compliance from assessments are tracked to closure.

Static Code Analysis

Cyber Security – Operations team performs a monthly full static code analysis and a weekly incremental static code analysis of the changes in the development environment prior to pushing the change to production. Issues of non-compliance from assessments are tracked to closure.

Network Controls

Remote access to the data centre, corporate network and other servers is restricted through the use of VPN and appropriate access control measures. These access control measures help in restricting remote connection to production servers and corporate network. Access to production servers and corporate network is restricted to authorized personnel only.

Password Control

Password parameters are defined for operating systems, databases, and applications that include the following: Minimum length, password history, password complexity, and password age. The domain password policy stipulates minimum length, password history, change of password after first successful logon, account lockout settings and password complexity. The domain password policy is implemented on workstations within the HighRadius domain.

Network

HighRadius uses redundant leased lines from Tier–I Internet Service Provider (ISP) for maintaining connection with the Internet. Bandwidth requirements are evaluated based on utilization and threshold statistics. Site to site Virtual Private Networks (VPN) have been established to enable data transmission between HighRadius and Data Centres. A firewall has been deployed to control access to the HighRadius network and to allow only restricted services. The rules of the firewall are configured and maintained by the IMS team.

HighRadius has implemented network-based IPs within its firewall to prevent intrusions into the HighRadius network and is monitored by the IMS team, log review is performed by Cyber Security teams through SIEM tools.

Network monitoring tool 'Nagios' is used to monitor the utilization and availability of network. The IMS team is responsible for monitoring the network on a continuous basis. The monitoring tool is configured to perform latency checks, port availability, URL monitoring, disk space verification, CPU load monitoring and memory on the servers. Thresholds for resource usage and availability are set in the tool for generating alerts which are sent to the IMS team. Cyber Security – Operations team performs Vulnerability Assessment on HighRadius network and servers on a monthly basis and web applications on weekly basis. Issues of non-compliance from assessments are tracked to closure. Cyber Security – Operations team on a half yearly basis performs Penetration Testing on HighRadius network, servers, and web applications. Issues of non-compliance from assessments are tracked to closure. Third party Vulnerability Assessment and Penetration Test is conducted semi-annually to assess vulnerabilities and evaluate network security risks. Issues of non-compliance from assessments are tracked to closure. Results of such assessment are reviewed by the Vice President – Cyber Security - Operations and senior security engineer and corrective action are taken based on the assessment report. DoS/DDoS tests are performed against HighRadius infrastructure by Cyber Security – Operations team on an annual basis and reviewed by the Vice President, Cyber Security – Operations and senior security engineer.

Firewall

Firewalls are installed at the perimeter level at HighRadius Development Centres and third-party Data Centers. HighRadius uses whitelisting technique to allow access. On a semi-annual basis, the Cyber Security – Risk & Compliance team reviews the firewall rule set configuration. In case of any change in the firewall ruleset, standard Change Management procedure is followed.

IMS and Cyber Security – Operations team is responsible for monitoring firewall alerts on an ongoing (24/7) basis through SIEM tool. SIEM tool is maintained and managed by third party service providers. Changes to the firewall rule base follow the defined "Change Management" process and rules are reviewed by Cyber Security – Risk & Compliance team every six months.

Cloud Security

HighRadius implemented a Cloud Access Security Broker (CASB) solution from Netskope, which serves as an extended security for applications (SaaS) used within HighRadius. These applications are integrated with the CASB solution, which logs the activities performed by HighRadius users within the applications. The solution is also configured to restrict the activities of users on various social media platforms, G-Suite, and prevents users from accessing blacklisted websites, as per the rulesets defined by HighRadius within the solution.

HighRadius also implemented a Cloud Security Posture Management (CSPM) solution, CloudGuard Dome9, for security and compliance automation in the public cloud. It is an API based SaaS platform that is natively integrated with Amazon Web Services (AWS), Microsoft Azure and Google cloud. The solution provides visibility on cloud configuration, constant adherence to compliance in view of industry standards such as National Institute of Standards and Technology (NIST), Health Insurance Portability and Accountability Act of 1996 (HIPAA), International Organization for Standardization (ISO), and others, along with providing active security and threat detection. It also provides guardrails to minimize attack surface and ensures HighRadius meets compliance and governance standards in the public cloud.

Web Application Firewall

HighRadius implemented a Web Application Firewall (WAF) solution to protect its infrastructure and applications from web based cyber-attacks. The solution filters, monitors, and blocks malicious traffic and allows safe web traffic to reach HighRadius infrastructure and its applications.

Anti-Malware Monitoring

Trend Micro Apex Central anti-malware software is installed and activated on servers and workstations. Computer malwares and worms are a major threat to information security and may result in data loss, damage to system and networks, and service disruptions. Latest malware definitions are automatically updated on windows server and workstations for new releases.

Anti-malware servers with XDR (Extended Detection & Response) and XDR (Advanced Threat Protection) are configured to generate alerts upon malware detection and manage defences from anti-malware server. Anti-malware logs are sent to the SIEM tool for continuous monitoring. The Cyber Security – Operations team reviews the anti-malware logs for issues and concerns related information security across locations and sends the report to respective process owners on a weekly basis.

Data Loss Prevention

To detect leakage of confidential data, GTB (DLP) tool is installed in the desktops and laptops within the infrastructure, database, and banking support teams of HighRadius to keep in check that unauthorized transmission of sensitive client data does not occur accidentally or deliberately. The Cyber Security - Operations team is responsible for monitoring DLP alerts on a real time basis.

Code Monitoring

Code analysis and track code changes are done in real time using Overops. Cyber Security - Operations team performs a monthly full static code analysis and a weekly incremental static code analysis of the changes in the development environment prior to pushing the change to production. Issues of non-compliance from assessments are tracked to closure.

Performance Logs

Log servers are in place to maintain or manage the logs generated. The logs are integrated with SIEM and are monitored by HighRadius' MSSP on an ongoing basis (24/7) to identify trends that may have a potential impact on the system security. File Integrity Monitoring (FIM) is in place that keeps track of system components and notify the stakeholders on a continuous basis. Cyber Security – Operations team monitors the alerts received in the SIEM tool and takes appropriate actions, as required.

System Monitoring

SDLC Methodology and Procedures

The Software Development Lifecycle (SDLC) methodology of HighRadius contains procedures for internal reviews and quality assurance reviews to ensure completeness, accuracy, timeliness, and authorization of services provided to user entities. HighRadius have formalized internal reviews across the SDLC process for the services delivered to user entities. HighRadius uses Jira software as their change management tool to issue and track the change requests of the in-scope applications and products. It follows HighRadius' SDLC Methodology. Bizops team is responsible for maintaining the Jira workflow life cycle to ensure sustainability.

Bots like Claims and POD Automation (CPA), Retail Trade Agreement (RTA), and Invoice Tracing Automation (ITA) agents are developed in-house by HighRadius which essentially serve as addons to applications for the ease of business-as-usual (BAU) and follow the same SDLC methodology using the Jira workflow. For Application Development, Maintenance and Support, the requirements or requests for maintenance and support are communicated by user entities. The requirements are tracked and maintained for reference within HighRadius systems.

As part of development, HighRadius prepares the test cases with expected results, performs testing, and reviews the results of testing. Developers are responsible for fixing the results of review performed by Line Manager and Cyber Security operations team wherever applicable. Access to the development environment for HighRadius application products is restricted to respective development team members only. Changes to code are tracked using the Gitlab tool which also supports versioning with check-in and check-out history and different development branches. A cutover plan is also communicated to the user entities prior to production implementation. The Product team is responsible for migration of the build from development to testing. Build and Release team is responsible for migration from testing to the production environment. Upon successful completion of UAT, migration to the production environment is performed by the Build and Release team, based on e-mail confirmation from the user entity.

Data Backup and Recovery

Backup and Restoration

The Database (DB) & IMS teams are responsible for scheduling of backup jobs. The IMS team has a standard retention schedule for backups. Real time sync to Disaster Recovery (DR) system and monthly, weekly, and daily backups are performed. An automatic e-mail notification is sent out to the IMS and DB teams communicating the backup status. Restorations tests are performed by the DB team on a quarterly basis to ensure that the backed-up data is readable and restorable. The backup data is retained as per the backup retention procedure. Any discrepancies identified are reported by DB team to the IMS team for resolution.

Disaster Recovery (DR) Plan

Disaster Recovery measures are in place to restore the system and client data in minimal time from the secondary hosting facility. IT Disaster Recovery (DR) Plan is established, documented, reviewed by Senior Director – Infrastructure (IMS) and approved by the Chief Information Security Officer. HighRadius has a documented and approved DR plan to minimize the effect of disruptions on HighRadius information systems.

The following are documented in detail within the DR Plan:

- Critical Systems
- Plan Review
- Annual frequency of DR test
- Process summary for failover
- Evaluation Criteria

The IMS and Cyber Security teams are responsible for the implementation of DR and testing its effectiveness. The IMS and Cyber Security teams determine the services, processes, technology, and systems considered as critical. This exercise also determines the critical operational systems and related infrastructure that needs to be recovered in the event of disruption. DR plan is reviewed and updated on an annual basis or at the time of any major change in the existing environment. The DR plan is tested on an annual basis. Observations are documented and reviewed by senior management. On an annual basis, a DR Test is conducted by the IMS team to test effectiveness of the DR site by switching the application and its database instances from production to DR. RTO (Recovery Time Objective) is defined as 4 hours and RPO (Recovery Point Objective) as 1 hour.

Capacity Monitoring

Monitoring tool ‘Nagios’ is used to monitor the utilization and availability of the network. The IMS team is responsible for monitoring the network on a continuous basis. The monitoring tool is configured to perform latency checks, port availability, URL monitoring, disk space verification, CPU load monitoring and memory on the servers. Thresholds for resource usage and availability are set in the tool for generating alerts which are sent to the IMS team.

Application version

HighRadius releases an update for the in-scope applications and products monthly and increments the minor version number. Correspondingly, the major version number gets updated on an annual basis. The in-scope applications and products are currently on version 23.4.0.

Operating Systems and Software

The following operating systems are used in HighRadius:

- Windows 10 Professional Edition for laptops/desktops
- Cent OS 7.9 for servers
- Windows 2016 and 2019 for Servers running Windows OS
- Windows 10 Enterprise N version 2004 for Virtual Desktop Infrastructure (VDI)

The following tools were used by HighRadius to support the general IT environment and are not subject to the general IT controls covered as part of this report:

S. No	Tools	Description
1	ManageEngine – Genie tool	IT helpdesk ticketing tool
2	Prometheus	Infrastructure monitoring tool
3	NetXs	Physical access control system.
4	Trend Micro	Anti-malware tool for production environment & end user devices
5	Open LDAP	Open-source directory access protocol
6	AD	Domain controller
7	SCP	Secure data transfer utility tool
8	Crontab	Job scheduling utility tool
9	Nessus	Vulnerability assessment tool
10	Secure Trust	Approved scanning vendor for PCI scans
11	Qualys Guard	Web application vulnerability scanner
12	Wi-Fi guard	Wireless scanning tool
13	CVS	Version control system for development
14	Gitlab	Code repository and version control system
15	RSYSLOG	Logging utility for Linux systems
16	Jira	Used to track and manage changes
17	Desktop Central	Used to push patches to end user systems
18	ESSL	Physical access control system (For Hyderabad)

S. No	Tools	Description
19	Brivio	Physical access control system (For Westlake)
20	Monyog	DB monitoring tool
21	Bouncer	Query management system
22	Selenium	Automation testing tool
23	Salesforce	Customer relationship management system and used to track configuration changes, defects, and service disruptions
24	WhiteSource	Bug detecting tool
25	Checkmarx	Static code analysis tool
26	GTB and Netskope	Data Loss Prevention tool
27	Jenkins	Build & deployment tool
28	Securonix	Security Information and Event Monitoring tool
29	BitSight	Security ratings solution
30	NetSuite	Tool for creation of Invoices
31	Smartsheets	Project planning & delivery tracking tool
32	G-Suite	Business e-mail
33	New Relic	Application performance monitoring tool
34	PAMS	Privileged access management to HighRadius applications
35	CloudGuard Dome9	Cloud Security Posture Management solution
36	Netskope CASB	Cloud Access Security Broker solution
37	Knowbe4	Security training tool
38	Akamai	Web Application Firewall and DoS prevention
39	JFrog	Manages and automates artifacts and binaries from start to finish during the application delivery process.

S. No	Tools	Description
40	HADAM	HADAM (HighRadius Automated Deployment and Management) is an internal tool for scheduled and emergency production deployments.
41	Eclipse	The tool is used for Build and Deployment.
42	Sophos	The tool is used to monitor and permit/block incoming.
43	Fortigate	The tool is used to monitor and permit/block incoming
44	Global Protect	VPN to provide secure access to corporate networks & resources for remote users
45	FortiClient	VPN to provide secure access to corporate networks & resources for remote users (From 22 Aug 2023)

Cryptography

Data is encrypted while in transit with Transport Layer Security (TLS) v1.2. Data at rest is encrypted with 256-bit AES cipher standard. Further, PGP public and private keys are used for encrypting the files shared with and received from customers.
The keys are generated through automation and managed by Customer Value Managers basis the requests received from HighRadius Consulting team for customer accounts. Generated keys are shared with Cloud Engineering team, who is responsible for encrypting these generated keys using a separate management key and store them in HighRadius' AWS S3 bucket. The path of the AWS S3 bucket where the respective keys are stored is shared by the Cloud Engineering team with the corresponding requester from the HighRadius Consulting team. The Consulting team member then incorporates the key in the customer account for the respective HighRadius application. Further, key rotation is performed on an annual basis prior to expiration.

Database

The following databases are used in HighRadius:

- MySQL 5.7.39
- Aurora 3.04/3.05

Information Technology Environment

HighRadius product team members perform the services from the development centers located in Hyderabad. Applications used for processing are hosted and maintained by HighRadius. Site to site Virtual Private Networks (VPN) have been established to enable data transmission between HighRadius and Data Centers.

Internal Communication

HighRadius maintains communication with associates using the corporate intranet portal, e-mail, and notice boards. The communications include but not limited to communication and training of HighRadius policies and procedures, corporate events, awareness of new initiatives. Security obligations of users are communicated through Induction program, employee contracts, Non-Disclosure Agreements (NDA) and information security awareness training. HighRadius has a corporate intranet where relevant information security policies are made available to associates. Induction program for new associates includes a session on information security to provide awareness on HighRadius' information security policies. Changes and updates to HighRadius policies and procedures, and implementation of changes on HighRadius infrastructure are communicated to relevant users through internal portals and share drives. Awareness on security, availability, and confidentiality of information is provided to HighRadius associates at the time of joining as part of induction, and in e-mails on a regular basis.

Application Communication

Payers (HighRadius' customers' customers) send remittances via email to HighRadius' email server, which is subsequently consumed by HighRadius' applications. Remittances uploaded to customer web portals are also downloaded by HighRadius applications via a web crawler and transmitted to the same via HighRadius' email server. Further, HighRadius customers send and receive data feeds with/from HighRadius over Secure File Transfer Protocol (SFTP) streams using TLS 1.2 or higher. The respective HighRadius application agents in turn retrieve data from these SFTP streams.

Non-Disclosure Agreement

New associates are required to sign an NDA document as a part of the on-boarding process that includes confidentiality and intellectual property right clauses. NDA prohibits any disclosures of confidential information and other data that an associate has access, to any unauthorised users.

Policies and Procedures

HighRadius has a corporate intranet portal where relevant information security policies are made available to associates. Induction program for new associates includes a session on information security to provide awareness on HighRadius information security policies. On an annual basis, HighRadius associates undergo information security awareness program and an assessment. The program covers various aspects of information security defined at HighRadius such as acceptable use of assets, protection of information, security incident management and general information security guidelines. Associates are required to complete the assessment at the end of the awareness training, that is considered complete only if the assessment is passed by the associate.

Electronic Mail (e-mail)

Important corporate events, employee news, and cultural updates are some of the messages communicated using e-mail. E-mail is also a means to draw the attention of associates towards adherence to specific procedural requirements such as information security.

External Communication

External Communication is critical to facilitate communication between end user and HighRadius to track progress, and to identify and resolve issues, if any, on a timely basis. Communications with the end user are maintained using a ticket tracking tool, website, e-mail, and newsletters.

Security Awareness Trainings and Assessments

On an annual basis and during onboarding, HighRadius associates undergo an information security awareness program using the Knowbe4 tool. The program covers various aspects of information security defined at HighRadius such as acceptable use of assets, protection of information, security incident management and general information security guidelines. Associates are required to complete an assessment at the end.

Monitoring Activities

Surveillance audits

HighRadius development centers at Hyderabad certified against ISO 27001:2013. Surveillance audits and certification audits are performed by the Certifying Authority at the organization level.

Internal Assessments

Operations are monitored on a periodic basis by the Cyber Security – Risk & Compliance team in HighRadius to help ensure compliance with the security requirements. Cyber Security – Risk & Compliance team, depending on the assessment, schedules and performs review of operations of various functions in HighRadius, and the findings are documented in the internal assessment reports. The status of the observations in the Internal Assessment reports and corrective actions taken are presented to HighRadius' senior management group on a periodic basis.

Vulnerability Assessment and Penetration Testing (VAPT)

Cyber Security – Operations team performs vulnerability assessments on HighRadius network and servers on a monthly basis and web applications on weekly basis. Issues of non-compliance from assessments are tracked to closure. Cyber Security – Operations

team performs penetration testing on HighRadius network, servers, and web applications on half yearly basis. Issues of non-compliance from assessments are tracked to closure. A third-party conducts VAPT semi-annually to assess vulnerabilities and evaluate network security risks. Issues of non-compliance from assessments are tracked to closure.

Subservice Organization

HighRadius uses subservice organizations for hosting the application servers and databases in data centers of Equinix at Texas, USA; Datapipe at New Jersey, USA; Azure data centers at USA, Europe; Google Cloud Provider (GCP) data centers at USA; and Amazon Web Services (AWS) data centers at USA, Europe, and Canada. SOC reports of these data centers are reviewed on an annual basis by the Cyber Security – Risk & Compliance team to verify whether the security, availability, confidentiality and processing integrity commitments and requirements of the data centers are in line with HighRadius' commitments.

Control Activities

The specific controls tested, and the nature, timing, and results of those tests are included in Section 4 of this report, "Trust Services Criteria, Controls, Test Procedures and Test Results", to eliminate the redundancy that would result from listing them in this section and repeating them in Section 4.

Although the controls are included in Section 4, they are, nevertheless, an integral part of HighRadius' description of the system.

Complementary User Entity Controls

In designing its system, HighRadius has contemplated that certain complementary controls would be implemented by user entities in their respective environments, as per the SOW, in order to meet certain criteria applicable to Security, Availability, Confidentiality, and Processing Integrity. The responsibility for design, implementation, and operating effectiveness of these controls' rests with the user entity. This information has been provided to user entities and to their auditors to be taken into consideration when making assessments of control risk for the user entity.

While the complementary user entity controls (CUEC) have been stated below, these are not operated by HighRadius and therefore, the design and operating effectiveness has not been tested. The list of complementary user entity controls presented do not represent a comprehensive set of all the controls that should be employed by the user entity. Other controls may be required at the user entity.

- User entity is responsible for UAT testing and providing UAT sign-off to HighRadius.
- User entity is responsible for go-live date finalization.
- User entity is responsible for registration of service requests through the ticketing tool.
- User entity is responsible for registration of defects and service disruptions through the ticketing tool.
- User entity is responsible for enabling multifactor authentication to HighRadius applications.
- User entity is responsible for performing and managing user access review for users having access to HighRadius applications.
- User entity is responsible for performing and managing role management and roles review for users having access to HighRadius applications.
- User entities with administrative access rights are responsible for managing and reviewing users having administrative access periodically.

Complementary Subservice Organization Controls

In the design of its controls, HighRadius has envisaged certain controls to be exercised by subservice organizations. The responsibility for design, implementation, and operating effectiveness of these controls rests with the subservice organizations. This information has been provided to user entities and to their auditors to be taken into consideration when making assessments of control risk for user entities.

While the subservice organization controls have been stated below, these are not operated by HighRadius and therefore the design and operating effectiveness has not been tested. The list of subservice organization controls presented do not represent a comprehensive set of all the controls that should be employed by user entities. Other controls may be required at the subservice organizations. The complementary subservice organization controls required to achieve the criteria are outlined as below:

Controls maintained by subservice organizations:
Physical security of Data Center: • Perimeter Security • Primary Access Control System • Secondary Access Control System • Periodic reconciliation of access permissions granted through the access control system • Monitoring of premises using CCTV • Tracking of Material Movement • Visitor Management System
Environmental safeguard of Data Center: • Fire Detection and Suppression System • Fire Fighting Equipment • Temperature and Humidity Control System • Backup power supply mechanism

Subservice organizations are responsible for ensuring appropriate actions are taken to mitigate risks associated with exceptions identified as agreed with HighRadius.

.

SECTION 4

TRUST SERVICES CRITERIA, CONTROLS, TEST PROCEDURES AND TEST RESULTS

1.0 Common Criteria Related to Control Environment			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
1.1 The entity demonstrates a commitment to integrity and ethical values.	HighRadius has an organization structure that provides overall framework for planning, directing, and controlling operations and has segregated personnel and business functions into functional groups according to job responsibilities.	• Inquired of the People and Culture Manager regarding the organization structure at HighRadius. • Inspected the organization structure to determine whether the organization has segregated personnel and business functions into functional groups according to job responsibilities.	No relevant exceptions noted
	Induction program for new employees includes session on 'Acceptable Use policy' and 'Disciplinary Procedure' to provide awareness on the workplace standards at HighRadius.	• Inquired of the People and Culture Manager regarding the induction program for new employees at HighRadius. • Inspected the HR induction program material to determine whether the induction program includes session on of 'Acceptable Use policy' and 'Disciplinary Procedure'.	No relevant exceptions noted
	HighRadius has documented 'Acceptable Use policy' and 'HR policy' related to workplace conduct standards.	• Inquired of the People and Culture Manager regarding the 'Acceptable Use policy' and 'HR policy' related to workplace conduct standards at HighRadius. • Inspected the 'Acceptable Use policy' and 'HR policy' documents to determine whether they covered the aspects of the policies. • Inspected the intranet portal to determine whether 'Acceptable Use policy' and 'HR policy' documents were available on the intranet.	No relevant exceptions noted

1.0 Common Criteria Related to Control Environment			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	Training sessions on 'Information Security' policies and related procedures are conducted as a part of induction program and the annual information security awareness program held over HighRadius' training platform.	• Inquired of the People and Culture Manager regarding the information security induction program and the annual information security awareness program held over HighRadius' platform. • Inspected material for induction training and annual information security awareness program to determine whether information security policy and related procedures were covered as a part of induction program and the annual information security awareness program held over HighRadius' platform. • For a selection of new joiners, inspected the induction training records to determine whether the new joiners attended the training on 'Information Security' policy and procedures as a part of their initial induction program. • For a selection of existing employees, inspected the training records to determine whether annual refresher training on 'Information Security' policy and procedures were completed.	No relevant exceptions noted
	As part of joining formalities, new employees and contractors are required to sign a 'Non-Disclosure Agreement' (NDA) that addresses the confidentiality of HighRadius and customer information.	• Inquired of the People and Culture Manager regarding the signing of 'Non-Disclosure Agreement' by new employees and contractors at HighRadius. • Inspected the 'Non-Disclosure Agreement' to determine whether NDA addresses the confidentiality of HighRadius and customer information.	No relevant exceptions noted

1.0 Common Criteria Related to Control Environment			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		• For a selection of new joiners, inspected the records for 'Non-Disclosure Agreements' to determine whether NDAs were signed as part of the joining formalities.	
	Background checks for identity, address, criminal, education, and employment verification are carried out for new employees as per the defined procedures. Also, identity and criminal checks are performed for interns.	• Inquired of the People and Culture Manager regarding the process followed for performing background checks for employees at HighRadius. • For a selection of new joiners, inspected the background verification reports to determine whether background checks for identity, employment, education verification and criminal checks were conducted as per the policy. • For the above selection of new joiners, inspected the background verification reports to determine whether the report was completed and submitted to HR as per the defined procedures. • For a selection of interns, inspected the background verification reports to determine whether background checks for identity and criminal checks were conducted as per the policy. • For the above selection of interns, inspected the background verification reports to determine whether the report was completed and submitted to HR as per the defined procedures.	No relevant exceptions noted

1.0 Common Criteria Related to Control Environment			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	'Master Service Agreements' are established with HighRadius and user entities that include clearly defined terms, conditions, and responsibilities for service providers and user entities.	• Inquired of the Cyber Security – Risk & Compliance team regarding the 'Master Service Agreements' (MSA). • For a selection of user entities, inspected the MSA signed between HighRadius and the user entity to determine whether there were terms, conditions, and responsibilities defined for service provider and user entities as part of the executed MSA documents.	No relevant exceptions noted
1.2 The board of directors demonstrates independence from management and exercises oversight of the development and performance of the internal control.	HighRadius has an organization structure that provides overall framework for planning, directing, and controlling operations and has segregated personnel and business functions into functional groups according to job responsibilities.	• Inquired of the People and Culture Manager regarding the organization structure at HighRadius. • Inspected the organization structure to determine whether the organization has segregated personnel and business functions into functional groups according to job responsibilities.	No relevant exceptions noted
	HighRadius has established Senior Management Group (SMG), which consists of Chief Executive Officer (CEO), Chief Financial Officer (CFO) and Managing Director (MD) for providing overall directions on organization and business operations who are responsible for decision making and ensuring commitment to security, availability, confidentiality and processing integrity at the entity level.	• Inquired of the People and Culture Manager regarding the Senior Management Group (SMG) and its responsibilities. • Inspected the 'Roles and Responsibilities' document to determine whether the roles and responsibilities of the members of SMG were defined as part of the document.	No relevant exceptions noted

1.0 Common Criteria Related to Control Environment			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
1.3 Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	HighRadius has an organization structure that provides overall framework for planning, directing, and controlling operations and has segregated personnel and business functions into functional groups according to job responsibilities.	• Inquired of the People and Culture Manager regarding the organization structure at HighRadius. • Inspected the organization structure to determine whether the organization has segregated personnel and business functions into functional groups according to job responsibilities.	No relevant exceptions noted
	Job description of key positions in Product Implementation and Support Operations are documented in corresponding job description documents.	• Inquired of the People and Culture Manager regarding the job description of key positions in Product Implementation and Support Operations teams. • For a selection of key positions in Product Implementation and Support Operations teams, inspected the job description documents to determine whether the job description was defined as part of the document.	No relevant exceptions noted
	The objective description of the HighRadius system and its boundaries are communicated to authorized internal and external system users as follows: Internal: 'Information Security' policies and procedures are documented and available on corporate intranet for authorized users. Employees joining HighRadius attend training sessions on 'Information Security' policies and related procedures.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the communication of objective description to authorized internal and external system users. • Inspected the 'Information Security' policies and procedures defined and documented to determine whether aspects of the policy were covered as part of the documents. • Inspected the intranet to determine whether the 'Information Security' policy and procedure documents	No relevant exceptions noted

1.0 Common Criteria Related to Control Environment			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	User Entity: · HighRadius enters into a 'Master Service Agreement' (MSA) with the user entities for the services relating to on-demand receivables. The agreement covers the scope and definition of services related to hosting and support services of the on- demand receivables. · Project scope, deliverables, roles and responsibilities are documented in the SOW along with detailed service commitments from HighRadius.	were available on the intranet portal. • For a selection of new joiners, inspected the induction training records to determine whether the new joiners attended the training on 'Information Security' policy and procedures as a part of their initial induction program. • For a selection of user entities, inspected the MSA signed between HighRadius and user entities to determine whether the agreement covered the scope and definition of services related to hosting and support services of the on-demand receivables. • Inspected the SOW to determine whether project scope, deliverables, roles and responsibilities were documented in the SOW along with detailed service commitments from HighRadius.	
1.4 The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The security, availability, confidentiality and processing integrity policies and related procedures are documented and hosted on the HighRadius intranet.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the security, availability, confidentiality, and processing integrity policies and related procedures. • Inspected the security, availability, confidentiality, and processing integrity related policies and related procedure documents to determine whether they were approved, and the aspects were covered. • Inspected the intranet portal to determine whether security, availability, confidentiality, and processing integrity policies and related procedure documents	No relevant exceptions noted

1.0 Common Criteria Related to Control Environment			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		were available on intranet.	
	Job description of key positions in Product Implementation and Support Operations are documented in corresponding job description documents.	• Inquired of the People and Culture Manager regarding the job description of key positions in Product Implementation and Support Operations teams. • For a selection of key positions in Product Implementation and Support Operations teams, inspected the job description documents to determine whether the job description was defined as part of the document.	No relevant exceptions noted
	Induction program for new employees includes session on 'Acceptable Use policy' and 'Disciplinary Procedure' to provide awareness on the workplace standards at HighRadius.	• Inquired of the People and Culture Manager regarding the induction program procedure for new employees at HighRadius. • Inspected the HR induction program material to determine whether the induction program includes session on of 'Acceptable Use policy' and 'Disciplinary Procedure'.	No relevant exceptions noted
	HighRadius has documented 'Acceptable Use policy' and 'HR policy' related to workplace conduct standards.	• Inquired of the People and Culture Manager regarding the 'Acceptable Use policy' and 'HR policy' related to workplace conduct standards at HighRadius. • Inspected the 'Acceptable Use policy' and 'HR policy' documents to determine whether they covered the aspects of the policies. • Inspected the intranet portal to determine whether 'Acceptable Use policy' and 'HR policy' documents	No relevant exceptions noted

1.0 Common Criteria Related to Control Environment			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		were available on the intranet.	
	As part of joining formalities, new employees and contractors are required to sign a 'Non-Disclosure Agreement' (NDA) that addresses the confidentiality of HighRadius and customer information.	• Inquired of the People and Culture Manager regarding the signing of 'Non-Disclosure Agreement' by new employees and contractors at HighRadius. • Inspected the 'Non-Disclosure Agreement' to determine whether NDA addresses the confidentiality of HighRadius and customer information. • For a selection of new joiners, inspected the records for 'Non-Disclosure Agreements' to determine whether NDAs were signed as part of the joining formalities.	No relevant exceptions noted
	Background checks for identity, address, criminal, education, and employment verification are carried out for new employees as per the defined procedures. Also, identity and criminal checks are performed for interns.	• Inquired of the People and Culture Manager regarding the process followed for performing background checks for employees at HighRadius. • For a selection of new joiners, inspected the background verification reports to determine whether background checks for identity, employment, education verification and criminal checks were conducted as per the policy. • For the above selection of new joiners, inspected the background verification reports to determine whether the report was completed and submitted to HR as per the defined procedures. • For a selection of interns, inspected the background	No relevant exceptions noted

1.0 Common Criteria Related to Control Environment			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		verification reports to determine whether background checks for identity and criminal checks were conducted as per the policy. • For the above selection of interns, inspected the background verification reports to determine whether the report was completed and submitted to HR as per the defined procedures.	
	HighRadius has defined process for training to ensure that personnel fulfil their responsibilities.	• Inquired of the People and Culture Manager regarding the process for training. • Inspected the policies and procedure documents pertaining to training activities to determine whether the process for training was documented such that personnel fulfil their responsibilities.	No relevant exceptions noted
	HighRadius has formal 'Business Continuity Plan' (BCP) in place. BCP is reviewed and approved by VP - Cyber Security on a yearly basis.	• Inquired of the Cyber Security – Risk & Compliance Team Manager regarding the 'Business Continuity Plan'. • Inspected the 'Business Continuity Plan' (BCP) to determine whether the plan was documented, reviewed, and approved. • Further, inspected the approval records to determine whether the BCP was reviewed and approved by VP - Cyber Security on a yearly basis.	No relevant exceptions noted

1.0 Common Criteria Related to Control Environment			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	HighRadius' security, availability and confidentiality commitments are communicated to employees through information security awareness trainings while joining HighRadius and thereafter on an annual basis through information security awareness training sessions. The related procedures are placed in the central repository. 'Information Security policy' is part of induction program and the annual information security awareness program.	• Inquired of the People and Culture Manager regarding the information security induction program and the annual information security awareness program at HighRadius. • Inspected material for induction training and annual information security awareness program to determine whether information security policy and related procedures were covered as a part of induction program and the annual information security awareness program. • For a selection of new joiners, inspected the induction training records to determine whether the new joiners attended the training on information security policy and procedures as a part of their initial induction program. • For a selection of existing employees, inspected the training records to determine whether annual refresher training on information security policy and procedures were completed.	No relevant exceptions noted
1.5 The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	HighRadius has an organization structure that provides overall framework for planning, directing, and controlling operations and has segregated personnel and business functions into functional groups according to job responsibilities.	• Inquired of the People and Culture Manager regarding the organization structure at HighRadius. • Inspected the organization structure to determine whether the organization has segregated personnel and business functions into functional groups according to job responsibilities.	No relevant exceptions noted

1.0 Common Criteria Related to Control Environment			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	HighRadius has documented 'Acceptable Use policy' and 'HR policy' related to workplace conduct standards.	• Inquired of the People and Culture Manager regarding the 'Acceptable Use policy' and 'HR policy' related to workplace conduct standards at HighRadius. • Inspected the 'Acceptable Use policy' and 'HR policy' documents to determine whether they covered the aspects of the policies. • Inspected the intranet portal to determine whether 'Acceptable Use policy' and 'HR policy' documents were available on the intranet.	No relevant exceptions noted
	As part of joining formalities, new employees and contractors are required to sign a 'Non-Disclosure Agreement' (NDA) that addresses the confidentiality of HighRadius and customer information.	• Inquired of the People and Culture Manager regarding the signing of 'Non-Disclosure Agreement' by new employees and contractors at HighRadius. • Inspected the 'Non-Disclosure Agreement' to determine whether NDA addresses the confidentiality of HighRadius and customer information. • For a selection of new joiners, inspected the records for 'Non-Disclosure Agreements' to determine whether NDAs were signed as part of the joining formalities.	No relevant exceptions noted
	Background checks for identity, address, criminal, education, and employment verification are carried out for new employees as per the defined procedures. Also, identity and criminal checks are performed for interns.	• Inquired of the People and Culture Manager regarding the process followed for performing background checks for employees at HighRadius. • For a selection of new joiners, inspected the background verification reports to determine whether background checks for identity, employment, education	No relevant exceptions noted

1.0 Common Criteria Related to Control Environment			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		verification and criminal checks were conducted as per the policy. • For the above selection of new joiners, inspected the background verification reports to determine whether the report was completed and submitted to HR as per the defined procedures. • For a selection of interns, inspected the background verification reports to determine whether background checks for identity and criminal checks were conducted as per the policy. • For the above selection of interns, inspected the background verification reports to determine whether the report was completed and submitted to HR as per the defined procedures.	
	Job description of key positions in Product Implementation and Support Operations are documented in corresponding job description documents.	• Inquired of the People and Culture Manager regarding the job description of key positions in Product Implementation and Support Operations teams. • For a selection of key positions in Product Implementation and Support Operations teams, inspected the job description documents to determine whether the job description was defined as part of the document.	No relevant exceptions noted
	Induction program for new employees includes session on 'Acceptable Use policy' and 'Disciplinary Procedure' to provide awareness on the workplace standards at HighRadius.	• Inquired of the People and Culture Manager regarding the induction program procedure for new employees at HighRadius.	No relevant exceptions noted

1.0 Common Criteria Related to Control Environment			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		• Inspected the HR induction program material to determine whether the induction program includes session on of 'Acceptable Use policy' and 'Disciplinary Procedure'.	
	Cyber Security – Risk & Compliance team conducts internal audits on an annual basis. Results and recommendations for improvement are documented and shared with respective teams.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the internal audit conducted on an annual basis. • Inspected the annual internal audit reports to determine whether the results and recommendations for improvement were reported to respective teams. • For a selection of improvement points, inspected the remediation tracker to determine whether the improvement points reported in the internal audit were resolved and tracked to closure.	No relevant exceptions noted

2.0 Common Criteria Related to Communication and Information			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
2.1 The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	HighRadius has defined 'Incident Management' policy which includes procedures for reporting, categorization and resolution of security incidents. The 'Incident Management' policy is available on Intranet. The process for reporting the incidents is also covered as part of annual refresher training.	• Inquired of the Cyber Security – Operations team manager regarding the 'Incident Management' policy and procedures document. • Inspected the 'Incident Management' policy document to determine whether it covered the aspects of the policy. • Inspected the 'Incident Management' policy and procedures documents to determine whether the guidelines for reporting, categorization, and resolution of security incidents were defined. • Inspected the intranet portal to determine whether the 'Incident Management' policy and procedure documents were available on the intranet. • Inspected the training content for refresher training to determine whether incident management guidelines were covered as part of the training. • For a selection of employees, inspected the attendance sheet to determine if the incident management guidelines were communicated to the employees.	No relevant exceptions noted

2.0 Common Criteria Related to Communication and Information			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	Cyber Security – Risk & Compliance team conducts internal audits on an annual basis. Results and recommendations for improvement are documented and shared with respective teams.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the internal audit conducted on an annual basis. • Inspected the annual internal audit reports to determine whether the results and recommendations for improvement were reported to respective teams. • For a selection of improvement points, inspected the remediation tracker to determine whether the improvement points reported in the internal audit were resolved and tracked to closure.	No relevant exceptions noted
	HighRadius has defined an organization wide Information Security Management System (ISMS) based on International Organization for Standardization (ISO) 27001:2013 framework.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding Information Security Management System (ISMS) based on International Organization for Standardization (ISO) 27001:2013 framework. • Inspected the ISO 27001 certificate to determine whether the ISO 27001 certification was valid during the audit period.	No relevant exceptions noted

2.0 Common Criteria Related to Communication and Information			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
2.2 The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	HighRadius' security, availability and confidentiality commitments are communicated to employees through information security awareness trainings while joining HighRadius and thereafter on an annual basis through information security awareness training sessions. The related procedures are placed in the central repository. 'Information Security' policy is part of induction program and the annual information security awareness program.	• Inquired of the People and Culture Manager regarding the information security induction program and the annual information security awareness program at HighRadius. • Inspected material for induction training and annual information security awareness program to determine whether information security policy and related procedures were covered as a part of induction program and the annual information security awareness program. • For a selection of new joiners, inspected the induction training records to determine whether the new joiners attended the training on 'Information Security' policy and procedures as a part of their initial induction program. • For a selection of existing employees, inspected the training records to determine whether annual refresher training on 'Information Security' policy and procedures were completed.	No relevant exceptions noted

2.0 Common Criteria Related to Communication and Information			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	Roles and responsibilities of Cyber Security team members is defined within the' Information Security' policy. The 'Information Security' policy is available on intranet.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the 'Information Security' policy and procedure documents. • Inspected the 'Information Security' policy and procedure documents to determine whether the roles and responsibilities of Cyber Security team members were documented within 'Information Security' policy. • Inspected the intranet portal to determine whether the 'Information Security' policy was available on the intranet.	No relevant exceptions noted
	Security obligations of employees are communicated through 'Information Security' policies. 'Information Security' policies and related procedures are hosted on corporate intranet and are available to the employees.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the 'Information Security' policies and related procedures. • Inspected the 'Information Security' policies and related procedures to determine whether the security obligations of employees were covered as part of the document. • Inspected the intranet portal to determine whether the 'Information Security' policies and related procedure documents were available on intranet for the employees.	No relevant exceptions noted

2.0 Common Criteria Related to Communication and Information			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	Training sessions on 'Information Security' policies and related procedures are conducted as a part of induction program and the annual information security awareness program held over HighRadius' training platform.	• Inquired of the People and Culture Manager regarding the information security induction program and the annual information security awareness program held over HighRadius' platform. • Inspected material for induction training and annual information security awareness program to determine whether information security policy and related procedures were covered as a part of induction program and the annual information security awareness program held over HighRadius' platform. • For a selection of new joiners, inspected the induction training records to determine whether the new joiners attended the training on 'Information Security' policy and procedures as a part of their initial induction program. • For a selection of existing employees, inspected the training records to determine whether annual refresher training on 'Information Security' policy and procedures were completed.	No relevant exceptions noted

2.0 Common Criteria Related to Communication and Information			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	Job description and responsibility of SIRT (Security Incident Response Team) is defined in the 'Information Security' policy. The 'Information Security' policy is hosted on corporate intranet and is available to the employees.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the 'Information Security' policy and procedure documents. • Inspected the 'Information Security' policy and procedure documents to determine whether the job description and responsibilities of the members of SIRT were defined. • Inspected the intranet portal to determine whether the 'Information Security' policy and procedure documents were available on intranet for the employees.	No relevant exceptions noted
	Job description of key positions in Product Implementation and Support Operations are documented in corresponding job description documents.	• Inquired of the People and Culture Manager regarding the job description of key positions in Product Implementation and Support Operations teams. • For a selection of key positions in Product Implementation and Support Operations teams, inspected the job description documents to determine whether the job description was defined as part of the document.	No relevant exceptions noted

2.0 Common Criteria Related to Communication and Information			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	HighRadius has defined 'Incident Management' policy which includes procedures for reporting, categorization and resolution of security incidents. The 'Incident Management' policy is available on Intranet. The process for reporting the incidents is also covered as part of annual refresher training.	• Inquired of the Cyber Security – Operations team manager regarding the 'Incident Management' policy and procedures document. • Inspected the 'Incident Management' policy document to determine whether it covered the aspects of the policy. • Inspected the 'Incident Management' policy and procedures documents to determine whether the guidelines for reporting, categorization, and resolution of security incidents were defined. • Inspected the intranet portal to determine whether the 'Incident Management' policy and procedure documents were available on the intranet. • Inspected the training content for refresher training to determine whether incident management guidelines were covered as part of the training. • For a selection of employees, inspected the attendance sheet to determine if the incident management guidelines were communicated to the employees.	No relevant exceptions noted

2.0 Common Criteria Related to Communication and Information			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	HighRadius has a formal change management procedure documented within the 'Operations Security' policy, which describes the procedures designed to help ensure that only authorized, tested, and documented changes are made to the system.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the change management procedure at HighRadius. • Inspected the change management process within the 'Operations Security' policy and procedure documents to determine whether the procedure designed to help ensure that only authorized, tested, and documented changes were made to the system was defined.	No relevant exceptions noted
	HighRadius' security, availability, and confidentiality commitments are communicated to employees through information security awareness trainings while joining HighRadius and thereafter on an annual basis through information security awareness training sessions. The related procedures are placed in the central repository. 'Information Security' policy is part of induction program and the annual information security awareness program.	• Inquired of the People and Culture Manager regarding the information security induction program and the annual information security awareness program at HighRadius. • Inspected material for induction training and annual information security awareness program to determine whether 'Information Security' policy and related procedures were covered as a part of induction program and the annual information security awareness program. • For a selection of new joiners, inspected the induction training records to determine whether the new joiners attended the training on 'Information Security' policy and procedures as a part of their initial induction program. • For a selection of existing employees, inspected the training records to determine whether annual refresher training on 'Information Security' policy and	No relevant exceptions noted

2.0 Common Criteria Related to Communication and Information			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		procedures were completed.	
	The objective description of the HighRadius system and its boundaries are communicated to authorized internal and external system users as follows: Internal: · 'Information Security' policies and procedures are documented and available on corporate intranet for authorized users. · Employees joining HighRadius attend training sessions on 'Information Security' policies and related procedures. User Entity: · HighRadius enters into a 'Master Service Agreement' (MSA) with the user entities for the services relating to on-demand receivables. The agreement covers the scope and definition of services related to hosting and support services of the on- demand receivables. · Project scope, deliverables, roles and responsibilities are documented in the SOW along with detailed service commitments from HighRadius.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the communication of objective description to authorized internal and external system users. • Inspected the 'Information Security' policies and procedures defined and documented to determine whether the aspects of the policy were covered as part of the documents. • Inspected the intranet to determine whether the 'Information Security' policy and procedure documents were available on the intranet portal. • For a selection of new joiners, inspected the induction training records to determine whether the new joiners attended the training on 'Information Security' policy and procedures as a part of their initial induction program. • For a selection of user entities, inspected the MSA signed between HighRadius and user entities to determine whether the agreement covered the scope and definition of services related to hosting and support services of the on-demand receivables. • Inspected the SOW to determine whether project scope, deliverables, roles and responsibilities were documented in the SOW along with detailed service	No relevant exceptions noted

2.0 Common Criteria Related to Communication and Information			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		commitments from HighRadius.	
	Changes that may affect system security, availability, and confidentiality are discussed in the weekly status meetings- 'CPCI' (Cross Product Changes and Impacts) conducted by HighRadius' QA team and are tracked in the internal tracking tool until closure.	• Inquired of the QA team manager regarding the changes that may affect system security, availability, and confidentiality. • For a selection of weeks, inspected the calendar invites and minutes of the meeting to determine whether weekly status meetings- 'CPCI' (Cross Product Changes and Impacts) were conducted by the HighRadius change management team to discuss the changes that may affect system's security, availability, and confidentiality.	No relevant exceptions noted
2.3 The entity communicates with external parties regarding matters affecting the functioning of internal control.	Changes that may affect system security, availability, and confidentiality are discussed in the weekly status meetings- 'CPCI' (Cross Product Changes and Impacts) conducted by HighRadius' QA team and are tracked in the internal tracking tool until closure.	• Inquired of the QA team manager regarding the changes that may affect system security, availability, and confidentiality. • For a selection of weeks, inspected the calendar invites and minutes of the meeting to determine whether weekly status meetings- 'CPCI' (Cross Product Changes and Impacts) were conducted by the HighRadius change management team to discuss the changes that may affect system's security, availability, and confidentiality.	No relevant exceptions noted

2.0 Common Criteria Related to Communication and Information			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	The objective description of the HighRadius system and its boundaries are communicated to authorized internal and external system users as follows: Internal: · 'Information Security' policies and procedures are documented and available on corporate intranet for authorized users. · Employees joining HighRadius attend training sessions on 'Information Security' policies and related procedures. User Entity: · HighRadius enters into a 'Master Service Agreement' (MSA) with the user entities for the services relating to on-demand receivables. The agreement covers the scope and definition of services related to hosting and support services of the on- demand receivables. · Project scope, deliverables, roles and responsibilities are documented in the SOW along with detailed service commitments from HighRadius.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the communication of objective description to authorized internal and external system users. • Inspected the 'Information Security' policies and procedures defined and documented to determine whether the aspects of the policy were covered as part of the documents. • Inspected the intranet to determine whether the 'Information Security' policy and procedure documents were available on the intranet portal. • For a selection of new joiners, inspected the induction training records to determine whether the new joiners attended the training on 'Information Security' policy and procedures as a part of their initial induction program. • For a selection of user entities, inspected the MSA signed between HighRadius and user entities to determine whether the agreement covered the scope and definition of services related to hosting and support services of the on-demand receivables. • Inspected the SOW to determine whether project scope, deliverables, roles and responsibilities were documented in the SOW along with detailed service commitments from HighRadius.	No relevant exceptions noted

2.0 Common Criteria Related to Communication and Information			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	'Master Service Agreements' are established with HighRadius and user entities that include clearly defined terms, conditions, and responsibilities for service providers and user entities.	• Inquired of the Cyber Security – Risk & Compliance team regarding the 'Master Service Agreements' (MSA). • For a selection of user entities, inspected the MSA signed between HighRadius and the user entity to determine whether there were terms, conditions, and responsibilities defined for service provider and user entities as part of the executed MSA documents.	No relevant exceptions noted
	Cyber Security – Risk & Compliance team performs information security risk assessment for new vendors at the time of onboarding and for existing vendors on an annual basis. Appropriate actions are taken, if any.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the information security risk assessment process for new and existing vendors. • For a selection of new vendors of HighRadius, inspected the risk assessment report to determine whether information security risk assessment was performed, and appropriate actions were taken, if any. • For a selection of existing vendors of HighRadius, inspected the annual vendor risk assessment report to determine whether information security risk assessment was performed, and appropriate actions were taken, if any.	No relevant exceptions noted
	As part of joining formalities, new employees and contractors are required to sign a 'Non-Disclosure Agreement' (NDA) that addresses the confidentiality of HighRadius and customer information.	• Inquired of the People and Culture Manager regarding the signing of 'Non-Disclosure Agreement' by new employees and contractors at HighRadius. • Inspected the 'Non-Disclosure Agreement' to determine whether NDA addresses the confidentiality of HighRadius and customer information.	No relevant exceptions noted

2.0 Common Criteria Related to Communication and Information			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		• For a selection of new joiners, inspected the records for 'Non-Disclosure Agreements' to determine whether NDAs were signed as part of the joining formalities.	
	HighRadius has defined 'Incident Management' policy which includes procedures for reporting, categorization and resolution of security incidents. The 'Incident Management' policy is available on Intranet. The process for reporting the incidents is also covered as part of annual refresher training.	• Inquired of the Cyber Security – Operations team manager regarding the 'Incident Management' policy and procedures document. • Inspected the 'Incident Management' policy document to determine whether it covered the aspects of the policy. • Inspected the 'Incident Management' policy and procedures documents to determine whether the guidelines for reporting, categorization, and resolution of security incidents were defined. • Inspected the intranet portal to determine whether the 'Incident Management' policy and procedure documents were available on the intranet. • Inspected the training content for refresher training to determine whether incident management guidelines were covered as part of the training. • For a selection of employees, inspected the attendance sheet to determine if the incident management guidelines were communicated to the employees.	No relevant exceptions noted

3.0 Common Criteria Related to Risk Assessment			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
3.1 The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	HighRadius has detailed 'Risk Management standard' document.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the 'Risk Management standard' document. • Inspected the 'Risk Management' standard document to determine whether the document covered areas pertaining to risk management in detail. • Inspected the 'Risk Management' standard document to determine whether the document was reviewed and approved on an annual basis.	No relevant exceptions noted
	As a part of risk assessment, VP – Cyber Security - Risk & Compliance team in concurrence with department heads of various departments / functions, assess the risk with their preview and share the findings / draft report / risk assessment plan / risk treatment plan with Cyber Security team.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding findings / draft report / risk assessment plan / risk treatment plan prepared in concurrence with department heads of various departments / functions post assessing the risk with their preview. • Inspected the risk assessment report and treatment plan to determine whether the department heads assessed the risk and shared the findings with the Cyber Security team.	No relevant exceptions noted

3.0 Common Criteria Related to Risk Assessment			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	Cyber Security – Risk & Compliance team conducts internal audits on an annual basis. Results and recommendations for improvement are documented and shared with respective teams.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the internal audit conducted on an annual basis. • Inspected the annual internal audit reports to determine whether the results and recommendations for improvement were reported to respective teams. • For a selection of improvement points, inspected the remediation tracker to determine whether the improvement points reported in the internal audit were resolved and tracked to closure.	No relevant exceptions noted
	'Information Security' policy and related procedures have been developed in line with ISO27001 standard. 'Information Security' policy is annually reviewed by Manager - Cyber Security – Risk & Compliance and approved by VP – Cyber Security.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the 'Information Security' policies and related procedures. • Inspected the ISO 27001 certificate to determine whether the ISO 27001 certification was valid during the audit period. • Inspected the 'Information Security' policies to determine whether they were developed in line with ISO27001 standards. • Inspected the 'Information Security' policies and related procedures to determine whether the document was reviewed by Manager - Cyber Security – Risk & Compliance and were approved by VP – Cyber Security on an annual basis.	No relevant exceptions noted

3.0 Common Criteria Related to Risk Assessment			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	HighRadius network, servers and web applications undergo third party Vulnerability Assessment and Penetration Testing on a semi-annual basis. Issues of non-compliance from assessments are tracked to closure.	• Inquired of the Cyber Security – Operations team manager regarding the third-party Vulnerability Assessment and Penetration Testing (VAPT). • Inspected the semi-annual third party VAPT report to determine whether HighRadius network, servers and web applications were covered as part of the report. • Inspected the remediation report to determine whether issues of non-compliance from the assessments were resolved and tracked to closure.	No relevant exceptions noted
	Cyber Security – Operations team performs penetration testing on the HighRadius network and servers on a quarterly basis and performs penetration testing on HighRadius web applications on a semi-annual basis. Issues of non-compliance from assessments are tracked to closure.	• Inquired of the Cyber Security – Operations team manager regarding penetration testing performed on HighRadius network, servers, and web applications. • For a selection of quarters and semi-annual web application penetration testing, inspected the reports of penetration testing to determine whether Cyber Security team conducted penetration testing on HighRadius network, servers, and web applications. • For the above selection of reports, inspected the remediation activities to determine whether issues of non-compliance from testing were resolved and tracked to closure.	No relevant exceptions noted
	Cyber Security – Operations team performs vulnerability assessment on the HighRadius web applications on a weekly basis and network, servers on a monthly basis. Issues of	• Inquired of the Cyber Security – Operations team manager regarding vulnerability assessments performed HighRadius network, servers, and web applications.	No relevant exceptions noted

3.0 Common Criteria Related to Risk Assessment			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	non-compliance from assessments are tracked to closure.	• For a selection of weeks, inspected the reports of vulnerability assessment to determine whether Cyber Security – Operations team conducted vulnerability assessment on HighRadius web applications • For the above selection of weeks, inspected the remediation report to determine whether issues of non-compliance from assessments were resolved and tracked to closure. • For a selection of months, inspected the reports of vulnerability assessment to determine whether Cyber Security – Operations team conducted vulnerability assessment on HighRadius network and servers. • For the above selection of months, inspected the remediation report to determine whether issues of non-compliance from assessments were resolved and tracked to closure.	
	Cyber Security – Operations team performs a full static code analysis (security) on a monthly basis and an incremental static code analysis (security) on a weekly basis of changes prior to release. Issues of non-compliance from analysis are tracked to closure.	• Inquired of the Cyber Security – Operations team manager regarding the static security code review process. • For a selection of months, inspected the reports for static security code review to determine whether monthly full static security code reviews were performed on changes prior to release by the Cyber Security – Operations team. • Further, inspected the communication for remediation to determine whether the non-compliances from assessments were getting resolved and tracked to	No relevant exceptions noted

3.0 Common Criteria Related to Risk Assessment			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		closure. • For a selection of weeks, inspected the reports for static security code review to determine whether weekly incremental static security code reviews were performed on changes prior to release by the Cyber Security team. • Further, inspected the communication for remediation to determine whether the non-compliances from assessments were getting resolved and tracked to closure.	
	On an annual basis, DoS/DDoS tests are performed on HighRadius infrastructure by Cyber Security team and reviewed by the Manager – Cyber Security.	• Inquired of the Cyber Security Team Manager regarding the DoS/DDoS tests performed on HighRadius infrastructure. • For the audit period, inspected the DoS/DDoS test report to determine whether the Cyber Security team performed the DoS/DDoS tests on an annual basis and the result was reviewed by the Manager – Cyber Security.	No relevant exceptions noted
3.2 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.	As a part of risk assessment, VP – Cyber Security - Risk & Compliance team in concurrence with department heads of various departments / functions, assess the risk with their preview and share the findings / draft report / risk assessment plan / risk treatment plan with Cyber Security team.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding findings / draft report / risk assessment plan / risk treatment plan prepared in concurrence with department heads of various departments / functions post assessing the risk with their preview. • Inspected the risk assessment report and treatment plan to determine whether the department heads assessed the	No relevant exceptions noted

3.0 Common Criteria Related to Risk Assessment			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		risk and shared the findings with the Cyber Security team.	
	HighRadius network, servers and web applications undergo third party Vulnerability Assessment and Penetration Testing on a semi-annual basis. Issues of non-compliance from assessments are tracked to closure.	• Inquired of the Cyber Security – Operations team manager regarding the third-party Vulnerability Assessment and Penetration Testing (VAPT). • Inspected the semi-annual third party VAPT report to determine whether HighRadius network, servers and web applications were covered as part of the report. • Inspected the remediation report to determine whether issues of non-compliance from the assessments were resolved and tracked to closure.	No relevant exceptions noted
	Cyber Security – Operations team performs penetration testing on the HighRadius network and servers on a quarterly basis and performs penetration testing on HighRadius web applications on a semi-annual basis. Issues of non-compliance from assessments are tracked to closure.	• Inquired of the Cyber Security – Operations team manager regarding penetration testing performed on HighRadius network, servers, and web applications. • For a selection of quarters and semi-annual web application penetration testing, inspected the reports of penetration testing to determine whether Cyber Security team conducted penetration testing on HighRadius network, servers, and web applications. • For the above selection of reports, inspected the remediation activities to determine whether issues of non-compliance from testing were resolved and tracked to closure.	No relevant exceptions noted

3.0 Common Criteria Related to Risk Assessment			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	Cyber Security – Operations team performs vulnerability assessment on the HighRadius web applications on a weekly basis and network, servers on a monthly basis. Issues of non-compliance from assessments are tracked to closure.	• Inquired of the Cyber Security – Operations team manager regarding vulnerability assessments performed HighRadius network, servers, and web applications. • For a selection of weeks, inspected the reports of vulnerability assessment to determine whether Cyber Security – Operations team conducted vulnerability assessment on HighRadius web applications • For the above selection of weeks, inspected the remediation report to determine whether issues of non-compliance from assessments were resolved and tracked to closure. • For a selection of months, inspected the reports of vulnerability assessment to determine whether Cyber Security – Operations team conducted vulnerability assessment on HighRadius network and servers. • For the above selection of months, inspected the remediation report to determine whether issues of non-compliance from assessments were resolved and tracked to closure.	No relevant exceptions noted

3.0 Common Criteria Related to Risk Assessment			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	On an annual basis, DoS/DDoS tests are performed on HighRadius infrastructure by Cyber Security team and reviewed by the Manager – Cyber Security.	• Inquired of the Cyber Security Team Manager regarding the DoS/DDoS tests performed on HighRadius infrastructure. • For the audit period, inspected the DoS/DDoS test report to determine whether the Cyber Security team performed the DoS/DDoS tests on an annual basis and the result was reviewed by the Manager – Cyber Security.	No relevant exceptions noted
	HighRadius has documented 'Information Classification' policy based upon the sensitivity and confidentiality of data. Data or information in HighRadius is classified into four categories given below: Public; Internal; Confidential; and Restricted.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding 'Information Classification' policy. • Inspected the 'Information Classification' policy to determine whether data or information in HighRadius is classified into four categories as Public, Internal, Confidential and Restricted.	No relevant exceptions noted
	Cyber Security – Operations team performs a full static code analysis (security) on a monthly basis and an incremental static code analysis (security) on a weekly basis of changes prior to release. Issues of non-compliance from analysis are tracked to closure.	• Inquired of the Cyber Security – Operations team manager regarding the static security code review process. • For a selection of months, inspected the reports for static security code review to determine whether monthly full static security code reviews were performed on changes prior to release by the Cyber	No relevant exceptions noted

3.0 Common Criteria Related to Risk Assessment			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		Security – Operations team. • Further, inspected the communication for remediation to determine whether the non-compliances from assessments were getting resolved and tracked to closure. • For a selection of weeks, inspected the reports for static security code review to determine whether weekly incremental static security code reviews were performed on changes prior to release by the Cyber Security team. • Further, inspected the communication for remediation to determine whether the non-compliances from assessments were getting resolved and tracked to closure.	
3.3 The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Formal data retention and disposal procedures are defined and documented within 'Operation Security' procedure to guide the secure disposal of the company's data	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the formal data retention and disposal policy and procedure documents. • Inspected the data retention and disposal procedure within the 'Operation Security' policy and procedure documents to determine whether the guidelines to dispose company data securely were defined.	No relevant exceptions noted

3.0 Common Criteria Related to Risk Assessment			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	HighRadius has documented 'Information Classification' policy based upon the sensitivity and confidentiality of data. Data or information in HighRadius is classified into four categories given below: Public; Internal; Confidential; Restricted.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding 'Information Classification' policy. • Inspected the 'Information Classification' policy to determine whether data or information in HighRadius is classified into four categories as Public, Internal, Confidential and Restricted.	No relevant exceptions noted
	Background checks for identity, address, criminal, education, and employment verification are carried out for new employees as per the defined procedures. Also, identity and criminal checks are performed for interns.	• Inquired of the People and Culture Manager regarding the process followed for performing background checks for employees at HighRadius. • For a selection of new joiners, inspected the background verification reports to determine whether background checks for identity, employment, education verification and criminal checks were conducted as per the policy. • For the above selection of new joiners, inspected the background verification reports to determine whether the report was completed and submitted to HR as per the defined procedures. • For a selection of interns, inspected the background verification reports to determine whether background checks for identity and criminal checks were conducted	No relevant exceptions noted

3.0 Common Criteria Related to Risk Assessment			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		as per the policy. • For the above selection of interns, inspected the background verification reports to determine whether the report was completed and submitted to HR as per the defined procedures.	
	HighRadius has defined 'Incident Management' policy which includes procedures for reporting, categorization and resolution of security incidents. The 'Incident Management' policy is available on Intranet. The process for reporting the incidents is also covered as part of annual refresher training.	• Inquired of the Cyber Security – Operations team manager regarding the 'Incident Management' policy and procedures document. • Inspected the 'Incident Management' policy document to determine whether it covered the aspects of the policy. • Inspected the 'Incident Management' policy and procedures documents to determine whether the guidelines for reporting, categorization, and resolution of security incidents were defined. • Inspected the intranet portal to determine whether the 'Incident Management' policy and procedure documents were available on the intranet. • Inspected the training content for refresher training to determine whether incident management guidelines were covered as part of the training. • For a selection of employees, inspected the attendance sheet to determine if the incident management guidelines were communicated to the employees.	No relevant exceptions noted

3.0 Common Criteria Related to Risk Assessment			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
3.4 The entity identifies and assesses changes that could significantly impact the system of internal control.	HighRadius network, servers and web applications undergo third party Vulnerability Assessment and Penetration Testing on a semi-annual basis. Issues of non-compliance from assessments are tracked to closure.	• Inquired of the Cyber Security – Operations team manager regarding the third-party Vulnerability Assessment and Penetration Testing (VAPT). • Inspected the semi-annual third party VAPT report to determine whether HighRadius network, servers and web applications were covered as part of the report. • Inspected the remediation report to determine whether issues of non-compliance from the assessments were resolved and tracked to closure.	No relevant exceptions noted
	Cyber Security – Operations team performs penetration testing on the HighRadius network and servers on a quarterly basis and performs penetration testing on HighRadius web applications on a semi-annual basis. Issues of non-compliance from assessments are tracked to closure.	• Inquired of the Cyber Security – Operations team manager regarding penetration testing performed on HighRadius network, servers, and web applications. • For a selection of quarters and semi-annual web application penetration testing, inspected the reports of penetration testing to determine whether Cyber Security team conducted penetration testing on HighRadius network, servers, and web applications. • For the above selection of reports, inspected the remediation activities to determine whether issues of non-compliance from testing were resolved and tracked to closure.	No relevant exceptions noted
	Cyber Security – Operations team performs vulnerability assessment on the HighRadius web applications on a weekly basis and network, servers on a monthly basis. Issues of	• Inquired of the Cyber Security – Operations team manager regarding vulnerability assessments performed HighRadius network, servers, and web applications.	No relevant exceptions noted

3.0 Common Criteria Related to Risk Assessment			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	non-compliance from assessments are tracked to closure.	• For a selection of weeks, inspected the reports of vulnerability assessment to determine whether Cyber Security – Operations team conducted vulnerability assessment on HighRadius web applications • For the above selection of weeks, inspected the remediation report to determine whether issues of non-compliance from assessments were resolved and tracked to closure. • For a selection of months, inspected the reports of vulnerability assessment to determine whether Cyber Security – Operations team conducted vulnerability assessment on HighRadius network and servers. • For the above selection of months, inspected the remediation report to determine whether issues of non-compliance from assessments were resolved and tracked to closure.	
	Cyber Security – Operations team performs a full static code analysis (security) on a monthly basis and an incremental static code analysis (security) on a weekly basis of changes prior to release. Issues of non-compliance from analysis are tracked to closure.	• Inquired of the Cyber Security – Operations team manager regarding the static security code review process. • For a selection of months, inspected the reports for static security code review to determine whether monthly full static security code reviews were performed on changes prior to release by the Cyber Security – Operations team. • Further, inspected the communication for remediation to determine whether the non-compliances from assessments were getting resolved and tracked to	No relevant exceptions noted

3.0 Common Criteria Related to Risk Assessment			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		closure. • For a selection of weeks, inspected the reports for static security code review to determine whether weekly incremental static security code reviews were performed on changes prior to release by the Cyber Security team. • Further, inspected the communication for remediation to determine whether the non-compliances from assessments were getting resolved and tracked to closure.	
	On an annual basis, DoS/DDoS tests are performed on HighRadius infrastructure by Cyber Security team and reviewed by the Manager – Cyber Security.	• Inquired of the Cyber Security Team Manager regarding the DoS/DDoS tests performed on HighRadius infrastructure. • For the audit period, inspected the DoS/DDoS test report to determine whether the Cyber Security team performed the DoS/DDoS tests on an annual basis and the result was reviewed by the Manager – Cyber Security.	No relevant exceptions noted
	HighRadius has detailed 'Risk Management standard' document.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the 'Risk Management standard' document. • Inspected the 'Risk Management' standard document to determine whether the document covered areas pertaining to risk management in detail. • Inspected the 'Risk Management' standard document to	No relevant exceptions noted

3.0 Common Criteria Related to Risk Assessment			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		determine whether the document was reviewed and approved on an annual basis.	
	HighRadius has a formal change management procedure documented within the 'Operations Security' policy, which describes the procedures designed to help ensure that only authorized, tested, and documented changes are made to the system.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the change management procedure at HighRadius. • Inspected the change management process within the 'Operations Security' policy and procedure documents to determine whether the procedure designed to help ensure that only authorized, tested, and documented changes were made to the system was defined.	No relevant exceptions noted
	Changes that may affect system security, availability, and confidentiality are discussed in the weekly status meetings- 'CPCI' (Cross Product Changes and Impacts) conducted by HighRadius' QA team and are tracked in the internal tracking tool until closure.	• Inquired of the QA team manager regarding the changes that may affect system security, availability, and confidentiality. • For a selection of weeks, inspected the calendar invites and minutes of the meeting to determine whether weekly status meetings- 'CPCI' (Cross Product Changes and Impacts) were conducted by the HighRadius change management team to discuss the changes that may affect system's security, availability, and confidentiality.	No relevant exceptions noted

4.0 Common Criteria Related to Monitoring Activities			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
4.1 The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	HighRadius network, servers and web applications undergo third party Vulnerability Assessment and Penetration Testing on a semi-annual basis. Issues of non-compliance from assessments are tracked to closure.	• Inquired of the Cyber Security – Operations team manager regarding the third-party Vulnerability Assessment and Penetration Testing (VAPT). • Inspected the semi-annual third party VAPT report to determine whether HighRadius network, servers and web applications were covered as part of the report. • Inspected the remediation report to determine whether issues of non-compliance from the assessments were resolved and tracked to closure.	No relevant exceptions noted
	Cyber Security – Operations team performs penetration testing on the HighRadius network and servers on a quarterly basis and performs penetration testing on HighRadius web applications on a semi-annual basis. Issues of non-compliance from assessments are tracked to closure.	• Inquired of the Cyber Security – Operations team manager regarding penetration testing performed on HighRadius network, servers, and web applications. • For a selection of quarters and semi-annual web application penetration testing, inspected the reports of penetration testing to determine whether Cyber Security team conducted penetration testing on HighRadius network, servers, and web applications. • For the above selection of reports, inspected the remediation activities to determine whether issues of non-compliance from testing were resolved and tracked to closure.	No relevant exceptions noted

4.0 Common Criteria Related to Monitoring Activities			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	Cyber Security – Operations team performs vulnerability assessment on the HighRadius web applications on a weekly basis and network, servers on a monthly basis. Issues of non-compliance from assessments are tracked to closure.	• Inquired of the Cyber Security – Operations team manager regarding vulnerability assessments performed HighRadius network, servers, and web applications. • For a selection of weeks, inspected the reports of vulnerability assessment to determine whether Cyber Security – Operations team conducted vulnerability assessment on HighRadius web applications • For the above selection of weeks, inspected the remediation report to determine whether issues of non-compliance from assessments were resolved and tracked to closure. • For a selection of months, inspected the reports of vulnerability assessment to determine whether Cyber Security – Operations team conducted vulnerability assessment on HighRadius network and servers. • For the above selection of months, inspected the remediation report to determine whether issues of non-compliance from assessments were resolved and tracked to closure.	No relevant exceptions noted
	Cyber Security – Operations team performs a full static code analysis (security) on a monthly basis and an incremental static code analysis (security) on a weekly basis of changes prior to release. Issues of non-compliance from analysis are tracked to closure.	• Inquired of the Cyber Security – Operations team manager regarding the static security code review process. • For a selection of months, inspected the reports for static security code review to determine whether monthly full static security code reviews were performed on changes prior to release by the Cyber	No relevant exceptions noted

4.0 Common Criteria Related to Monitoring Activities			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		Security – Operations team. • Further, inspected the communication for remediation to determine whether the non-compliances from assessments were getting resolved and tracked to closure. • For a selection of weeks, inspected the reports for static security code review to determine whether weekly incremental static security code reviews were performed on changes prior to release by the Cyber Security team. • Further, inspected the communication for remediation to determine whether the non-compliances from assessments were getting resolved and tracked to closure.	
	On an annual basis, DoS/DDoS tests are performed on HighRadius infrastructure by Cyber Security team and reviewed by the Manager – Cyber Security.	• Inquired of the Cyber Security Team Manager regarding the DoS/DDoS tests performed on HighRadius infrastructure. • For the audit period, inspected the DoS/DDoS test report to determine whether the Cyber Security team performed the DoS/DDoS tests on an annual basis and the result was reviewed by the Manager – Cyber Security.	No relevant exceptions noted
	Cyber Security – Risk & Compliance team conducts internal audits on an annual basis. Results and recommendations for improvement are documented and shared with respective teams.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the internal audit conducted on an annual basis. • Inspected the annual internal audit reports to determine	No relevant exceptions noted

4.0 Common Criteria Related to Monitoring Activities			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		whether the results and recommendations for improvement were reported to respective teams. • For a selection of improvement points, inspected the remediation tracker to determine whether the improvement points reported in the internal audit were resolved and tracked to closure.	
	As a part of risk assessment, VP – Cyber Security - Risk & Compliance team in concurrence with department heads of various departments / functions, assess the risk with their preview and share the findings / draft report / risk assessment plan / risk treatment plan with Cyber Security team.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding findings / draft report / risk assessment plan / risk treatment plan prepared in concurrence with department heads of various departments / functions post assessing the risk with their preview. • Inspected the risk assessment report and treatment plan to determine whether the department heads assessed the risk and shared the findings with the Cyber Security team.	No relevant exceptions noted
4.2 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.	As a part of risk assessment, VP – Cyber Security - Risk & Compliance team in concurrence with department heads of various departments / functions, assess the risk with their preview and share the findings / draft report / risk assessment plan / risk treatment plan with Cyber Security team.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding findings / draft report / risk assessment plan / risk treatment plan prepared in concurrence with department heads of various departments / functions post assessing the risk with their preview. • Inspected the risk assessment report and treatment plan to determine whether the department heads assessed the risk and shared the findings with the Cyber Security team.	No relevant exceptions noted

4.0 Common Criteria Related to Monitoring Activities			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	HighRadius network, servers and web applications undergo third party Vulnerability Assessment and Penetration Testing on a semi-annual basis. Issues of non-compliance from assessments are tracked to closure.	• Inquired of the Cyber Security – Operations team manager regarding the third-party Vulnerability Assessment and Penetration Testing (VAPT). • Inspected the semi-annual third party VAPT report to determine whether HighRadius network, servers and web applications were covered as part of the report. • Inspected the remediation report to determine whether issues of non-compliance from the assessments were resolved and tracked to closure.	No relevant exceptions noted
	Cyber Security – Operations team performs penetration testing on the HighRadius network and servers on a quarterly basis and performs penetration testing on HighRadius web applications on a semi-annual basis. Issues of non-compliance from assessments are tracked to closure.	• Inquired of the Cyber Security – Operations team manager regarding penetration testing performed on HighRadius network, servers, and web applications. • For a selection of quarters and semi-annual web application penetration testing, inspected the reports of penetration testing to determine whether Cyber Security team conducted penetration testing on HighRadius network, servers, and web applications. • For the above selection of reports, inspected the remediation activities to determine whether issues of non-compliance from testing were resolved and tracked to closure.	No relevant exceptions noted

4.0 Common Criteria Related to Monitoring Activities			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	Cyber Security – Operations team performs vulnerability assessment on the HighRadius web applications on a weekly basis and network, servers on a monthly basis. Issues of non-compliance from assessments are tracked to closure.	• Inquire Inquired of the Cyber Security – Operations team manager regarding vulnerability assessments performed HighRadius network, servers, and web applications. • For a selection of weeks, inspected the reports of vulnerability assessment to determine whether Cyber Security – Operations team conducted vulnerability assessment on HighRadius web applications • For the above selection of weeks, inspected the remediation report to determine whether issues of non-compliance from assessments were resolved and tracked to closure. • For a selection of months, inspected the reports of vulnerability assessment to determine whether Cyber Security – Operations team conducted vulnerability assessment on HighRadius network and servers. • For the above selection of months, inspected the remediation report to determine whether issues of non-compliance from assessments were resolved and tracked to closure.	No relevant exceptions noted
	On an annual basis, DoS/DDoS tests are performed on HighRadius infrastructure by Cyber Security team and reviewed by the Manager – Cyber Security.	• Inquired of the Cyber Security Team Manager regarding the DoS/DDoS tests performed on HighRadius infrastructure. • For the audit period, inspected the DoS/DDoS test report to determine whether the Cyber Security team performed the DoS/DDoS tests on an annual basis and the result was reviewed by the Manager – Cyber Security.	No relevant exceptions noted

4.0 Common Criteria Related to Monitoring Activities			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	Cyber Security – Operations team performs a full static code analysis (security) on a monthly basis and an incremental static code analysis (security) on a weekly basis of changes prior to release. Issues of non-compliance from analysis are tracked to closure.	• Inquired of the Cyber Security – Operations team manager regarding the static security code review process. • For a selection of months, inspected the reports for static security code review to determine whether monthly full static security code reviews were performed on changes prior to release by the Cyber Security – Operations team. • Further, inspected the communication for remediation to determine whether the non-compliances from assessments were getting resolved and tracked to closure. • For a selection of weeks, inspected the reports for static security code review to determine whether weekly incremental static security code reviews were performed on changes prior to release by the Cyber Security team. • Further, inspected the communication for remediation to determine whether the non-compliances from assessments were getting resolved and tracked to closure.	No relevant exceptions noted
	Cyber Security – Risk & Compliance team conducts internal audits on an annual basis. Results and recommendations for improvement are documented and shared with respective teams.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the internal audit conducted on an annual basis. • Inspected the annual internal audit reports to determine whether the results and recommendations for improvement were reported to respective teams.	No relevant exceptions noted

4.0 Common Criteria Related to Monitoring Activities			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		• For a selection of improvement points, inspected the remediation tracker to determine whether the improvement points reported in the internal audit were resolved and tracked to closure.	

5.0 Common Criteria Related to Control Activities			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
5.1 The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	HighRadius has detailed 'Risk Management standard' document.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the 'Risk Management standard' document. • Inspected the 'Risk Management standard' document to determine whether the document covered the areas pertaining to risk management in detail. • Inspected the 'Risk Management standard' document to determine whether the document was reviewed and approved on an annual basis.	No relevant exceptions noted
	As a part of risk assessment, VP – Cyber Security - Risk & Compliance team in concurrence with department heads of various departments / functions, assess the risk with their preview and share the findings / draft report / risk assessment plan / risk treatment plan with Cyber Security team.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding findings / draft report / risk assessment plan / risk treatment plan prepared in concurrence with department heads of various departments / functions post assessing the risk with their preview. • Inspected the risk assessment report and treatment plan to determine whether the department heads assessed the risk and shared the findings with the Cyber Security team.	No relevant exceptions noted

5.0 Common Criteria Related to Control Activities			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
5.2 The entity also selects and develops general control activities over technology to support the achievement of objectives.	HighRadius has a formal change management procedure documented within the 'Operations Security' policy, which describes the procedures designed to help ensure that only authorized, tested, and documented changes are made to the system.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the change management procedure at HighRadius. • Inspected the change management process within the 'Operations Security' policy and procedure documents to determine whether the procedure designed to help ensure that only authorized, tested, and documented changes were made to the system was defined.	No relevant exceptions noted
5.3 The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Information security policies are reviewed on an annual basis.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the review of 'Information Security' policies. • Inspected the 'Information Security' policy documents to determine whether the policies were reviewed at least on an annual basis.	No relevant exceptions noted
	Induction program for new employees includes session on 'Acceptable Use' policy and 'Disciplinary Procedure' to provide awareness on the workplace standards at HighRadius.	• Inquired of the People and Culture Manager regarding the induction program procedure for new employees at HighRadius. • Inspected the HR Induction program material to determine whether the induction program includes session on of 'Acceptable Use' policy and 'Disciplinary Procedure'.	No relevant exceptions noted

5.0 Common Criteria Related to Control Activities			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	HighRadius has documented 'Acceptable Use policy' and 'HR policy' related to workplace conduct standards.	• Inquired of the People and Culture Manager regarding the 'Acceptable Use policy' and 'HR policy' related to workplace conduct standards at HighRadius. • Inspected the 'Acceptable Use policy' and 'HR policy' documents to determine whether they covered the aspects of the policies. • Inspected the intranet portal to determine whether 'Acceptable Use policy' and 'HR policy' documents were available on the intranet.	No relevant exceptions noted
	HighRadius' security, availability and confidentiality commitments are communicated to employees through information security awareness trainings while joining HighRadius and thereafter on an annual basis through information security awareness training sessions. The related procedures are placed in the central repository. 'Information Security' policy is part of induction program and the annual information security awareness program.	• Inquired of the People and Culture Manager regarding the information security induction program and the annual information security awareness program at HighRadius. • Inspected material for induction training and annual information security awareness program to determine whether information security policy and related procedures were covered as a part of induction program and the annual information security awareness program. • For a selection of new joiners, inspected the induction training records to determine whether the new joiners attended the training on 'Information Security' policy and procedures as a part of their initial induction program. • For a selection of existing employees, inspected the training records to determine whether annual refresher training on 'Information Security' policy and procedures were completed.	No relevant exceptions noted
	HighRadius has defined 'Incident Management' policy which includes	• Inquired of the Cyber Security – Operations team manager regarding the 'Incident Management' policy and	No relevant exceptions noted

5.0 Common Criteria Related to Control Activities			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	procedures for reporting, categorization and resolution of security incidents. The 'Incident Management' policy is available on Intranet. The process for reporting the incidents is also covered as part of annual refresher training.	procedures document. • Inspected the 'Incident Management' policy document to determine whether it covered the aspects of the policy. • Inspected the 'Incident Management' policy and procedures documents to determine whether the guidelines for reporting, categorization, and resolution of security incidents were defined. • Inspected the intranet portal to determine whether the 'Incident Management' policy and procedure documents were available on the intranet. • Inspected the training content for refresher training to determine whether incident management guidelines were covered as part of the training. • For a selection of employees, inspected the attendance sheet to determine if the incident management guidelines were communicated to the employees.	
	Roles and responsibilities of Information Security team members is defined within the' Information Security' policy. The 'Information Security' policy is available on intranet.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the 'Information Security' policy and procedure documents. • Inspected the 'Information Security' policy and procedure documents to determine whether the roles and responsibilities of Information Security team members were documented within 'Information Security' policy. • Inspected the intranet portal to determine whether the 'Information Security' policy was available on the intranet.	No relevant exceptions noted

5.0 Common Criteria Related to Control Activities			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	Job description and responsibility of SIRT (Security Incident Response Team) is defined in the 'Information Security' policy. The 'Information Security' policy is hosted on corporate intranet and is available to the employees.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the 'Information Security' policy and procedure documents. • Inspected the 'Information Security' policy and procedure documents to determine whether the job description and responsibilities of the members of SIRT were defined. • Inspected the intranet portal to determine whether the 'Information Security' policy and procedure documents were available on intranet for the employees.	No relevant exceptions noted
	HighRadius has defined 'Incident Management' policy which includes procedures for reporting, categorization and resolution of security incidents. The 'Incident Management' policy is available on Intranet. The process for reporting the incidents is also covered as part of annual refresher training.	• Inquired of the Cyber Security – Operations team manager regarding the 'Incident Management' policy and procedures document. • Inspected the 'Incident Management' policy document to determine whether it covered the aspects of the policy. • Inspected the 'Incident Management' policy and procedures documents to determine whether the guidelines for reporting, categorization, and resolution of security incidents were defined. • Inspected the intranet portal to determine whether the 'Incident Management' policy and procedure documents were available on the intranet. • Inspected the training content for refresher training to determine whether incident management guidelines were covered as part of the training. • For a selection of employees, inspected the attendance sheet to determine if the incident management guidelines were communicated to the employees.	No relevant exceptions noted

5.0 Common Criteria Related to Control Activities			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	'Information Security' policy and related procedures have been developed in line with ISO27001 standard. 'Information Security' policy is annually reviewed by Manager - Cyber Security – Risk & Compliance and approved by VP – Cyber Security.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the 'Information Security' policies and related procedures. • Inspected the ISO 27001 certificate to determine whether the ISO 27001 certification was valid during the audit period. • Inspected the 'Information Security' policies to determine whether they were developed in line with ISO27001 standards. • Inspected the 'Information Security' policies and related procedures to determine whether the document was reviewed by Manager - Cyber Security – Risk & Compliance and were approved by VP – Cyber Security on an annual basis.	No relevant exceptions noted
	HighRadius has documented 'Information Classification' policy based upon the sensitivity and confidentiality of data. Data or information in HighRadius is classified into four categories given below: Public; Internal; Confidential; and Restricted.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding 'Information Classification' policy. • Inspected the 'Information Classification' policy to determine whether data or information in HighRadius is classified into four categories as Public, Internal, Confidential and Restricted.	No relevant exceptions noted

5.0 Common Criteria Related to Control Activities			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	HighRadius has a documented 'Clear Desk and Clear Screen' policy to ensure that information is not left unattended on user workstation desks during and after working hours.	• Inquired of the Cyber Security – Risk & Compliance Team Manager regarding the 'Clean Desk and Clear Screen' policy. • Inspected the 'Clean Desk and Clear Screen' policy document to determine whether procedure to maintain a clear desk was documented such that information is not left unattended on user workstation desks during and after working hours.	No relevant exceptions noted
	HighRadius has a formal change management procedure documented within the 'Operations Security' policy, which describes the procedures designed to help ensure that only authorized, tested, and documented changes are made to the system.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the change management procedure at HighRadius. • Inspected the change management process within the 'Operations Security' policy and procedure documents to determine whether the procedure designed to help ensure that only authorized, tested, and documented changes were made to the system was defined.	No relevant exceptions noted
	HighRadius has a documented policy and procedure for managing physical security within the organization.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the physical security policies and procedures. • Inspected the 'Physical and Environmental Security' document to determine whether HighRadius has documented policy and procedures for managing physical security within the organization.	No relevant exceptions noted

6.0 Common Criteria Related to Logical and Physical Access[5][6]			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
6.1 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.	Firewalls are installed at the perimeter of the corporate servers and network to block traffic unless specifically whitelisted.	• Inquired of the IMS team manager regarding the firewall implemented on HighRadius' corporate servers and network. • Inspected the network diagram to determine whether firewalls were installed on the perimeter of the corporate servers and network. • Inspected the firewall configuration to determine whether traffic to the corporate servers and network was blocked unless specifically whitelisted.	No relevant exceptions noted
	Firewalls are installed at the perimeter of the production and non-production servers and network to block traffic unless specifically whitelisted.	• Inquired of the IMS team manager regarding the firewall implemented on HighRadius' production and non-production servers. • Inspected the network diagram to determine whether firewalls were installed on the perimeter of the production and non-production servers and network. • Inspected the firewall configuration to determine whether traffic to the production and non-production servers was blocked unless specifically whitelisted.	No relevant exceptions noted

[5] *HighRadius relocated to a new office in Hyderabad, India during the audit period and moved from DLF Cyber City, Indira Nagar, Gachibowli, Hyderabad to Unit-2, 1st Floor, Building No: 12C, Mindspace, Hitech City, Madhapur, Hyderabad on 21 August 2023.*

[6] *HighRadius relocated to a new office in Houston, USA during the audit period and moved from Westlake 4 Building (BP Campus) 200 Westlake Park Blvd 8th floor Houston (previous facility) to 2107 CityWest Blvd Suite 1100, Houston (current facility) on 5 July 2023*

6.0 Common Criteria Related to Logical and Physical Access[56]			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	A network monitoring tool is configured to perform ping test, port availability, verification of partition sizes of the hard disk, CPU monitoring and memory on the servers. For any exceptions noted, the monitoring tool is configured to generate a request within tracking tool for the alerts.	• Inquired of the Cloud Engineering team manager regarding the network monitoring tool in place for HighRadius network. • Inspected the configuration of the monitoring tool to determine whether tool was configured to perform ping test, port availability, verification of partition sizes of the hard disk, CPU monitoring and memory on the servers. • Inspected the configuration of the monitoring tool to determine whether it is configured to generate a request within the tracking tool for the alerts in case of any exceptions. • For a selection of exceptions noted, inspected the requests generated within the tracking tool to determine whether the monitoring tool was configured to generate a request within tracking tool for the alerts.	No relevant exceptions noted
	HighRadius has corporate network security policies that include password length, password complexity requirements, periodic forced password changes, password history, and account lock out after a minimum number of invalid attempts.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the password policy. • Inspected the password policy for HighRadius corporate network to determine whether corporate network security policies have been defined. • Inspected the domain password policy to determine whether the password length, password complexity requirements, periodic forced password changes, password history, and account lock out after a minimum number of invalid attempts parameters were implemented as per the policy.	No relevant exceptions noted

6.0 Common Criteria Related to Logical and Physical Access[56]			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		• Performed a workstation walkthrough for negative testing of password configuration to determine whether user was not able to change the password outside enforced password policy.	
	HighRadius has implemented a Cloud Access Security Broker (CASB) solution which is responsible for logging activities performed by HighRadius' employees on the applications (SaaS). The solution is also configured to prevent users from accessing blacklisted websites.	• Inquired of the Cyber Security – Operations team manager regarding the CASB solution implemented within HighRadius. • For a selection of applications, inspected the CASB portal to determine whether activities performed on the applications (SaaS) were getting logged. • Inspected the rulesets in the CASB portal to determine whether the solution was configured to prevent users from accessing blacklisted websites.	No relevant exceptions noted
	Remote access of data by HighRadius employees is in line with the defined remote access guidelines which requires the usage of a secure Virtual Private Network (VPN) to access the HighRadius network through encrypted means.	• Inquired of the IMS team manager regarding the remote access guidelines which requires the usage of a secure (VPN and Extranet) to access the HighRadius network through encrypted means. • Inspected remote access guidelines to determine whether usage of a secure VPN to access the HighRadius network through AES 256 encryption was documented. • Inspected the VPN configuration to determine whether encryption was enabled on the remote connections.	No relevant exceptions noted

6.0 Common Criteria Related to Logical and Physical Access[56]			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	Appropriate actions are taken by the HighRadius Cyber Security – Operations team for alerts reported by HighRadius' Managed Security Service Provider (MSSP).	• Inquired of the Cyber Security – Operations Team Manager regarding HighRadius' Managed Security Service Provider (MSSP). • For a selection of "High", "Medium" and "Low" alerts reported, inspected the email communication to determine whether the alerts were acknowledged, and appropriate actions were taken by the Cyber Security – Operations team.	No relevant exceptions noted
	On a semi-annual basis, Cyber Security – Risk & Compliance team performs asset inventory reconciliation. Results of the reconciliation are documented and authorized, and remediation actions are taken, if any.	• Inquired of the Cyber Security – Risk & Compliance Team Manager regarding the asset inventory reconciliation process. • Inspected the semi-annual asset inventory reconciliation reports to determine whether the results of reconciliation were documented and authorized, and remediation actions are taken, if any.	No relevant exceptions noted
6.2 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	Access control policies and procedures are documented to protect against unauthorized access to system resources.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the access control policies and procedures. • Inspected the access control policies and procedure documents to determine whether access control procedures were defined to protect against unauthorized access to system resources.	No relevant exceptions noted

6.0 Common Criteria Related to Logical and Physical Access[56]			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
system credentials are removed when user access is no longer authorized.	Physical access for new joiners is created by Administration team for Hyderabad, Bhubaneswar, and Houston (previous facility) offices basis HR notification. Further, the building security team of HighRadius' Houston office (current facility) is responsible for creating physical access for new joiners joining the Houston office based on the email requests raised by the HR and provides an email confirmation upon creation.	• Inquired of the Administration team regarding the process followed for providing physical access to HighRadius premises. • For a selection of new joiners, inspected notification from HR team and date of physical access creation to determine whether the physical access to HighRadius premises was provided based on request from HR. • For a selection of new joiners at the Houston office (current facility), inspected the email requests raised by the HR and email confirmation of physical access creation from the building security team of HighRadius' Houston office (current facility) to determine whether the physical access was created based on the email requests raised by the HR.	No relevant exceptions noted
	Upon receipt of logical access creation request from HR for a new associate, IMS team creates a unique user ID basis the details provided by the HR.	• Inquired of the IMS Team Manager regarding the process followed for logical access creation. • For a selection of new joiners, inspected the HR email, logical access creation tickets, and logical access creation dates to determine whether the IMS team created unique user ID in HighRadius Active Directory and LDAP based on the request received from HR and whether the creation details of the user ID were communicated to the associate.	No relevant exceptions noted
	Upon receipt of an access revocation request from HR, the associate's user ID is disabled by the IMS team from the Active Directory and LDAP on the user's last working date.	• Inquired of the IMS team manager regarding the process followed for logical access revocation. • Inspected the system generated list of active users in Active Directory and LDAP and compared it with the list	**Exception noted:** For one out of 25 selections of logical access revocations, it was

6.0 Common Criteria Related to Logical and Physical Access[56]			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		of users resigned to determine whether terminated users continued to hold access. • For the above selection of resigned users inspected the revocation dates from Active Directory and LDAP to determine whether the user IDs of the employees who left the organization was disabled by IMS team from the Active Directory and LDAP on the user's last working date. • For the selection of resigned users where delay was noted, inspected the activity log to determine whether activities were performed from the user ID post the user's last working date and noted that no activities were performed.	noted that LDAP access was revoked after the last working day with a delay of 42 days. Further, inspected the LDAP activity log for the identified user and noted that no activities were logged post the user's last working day. **Management response:** The access revocation request for the above sample was delayed due to an error in the HR notification, where the username did not exactly match with the exit employee and hence, it required validation. Further, the exit employee's AD user ID was deleted on the last working day and the user could not log in to the network. It was determined that there was no activity logged as well, after the last working day.

6.0 Common Criteria Related to Logical and Physical Access[56]			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
			Action taken: A formal notice has been communicated to the respective teams to ensure that any such issues going forward are to be dealt promptly and with more caution.
	Physical access for leavers is revoked and proximity card is returned to the Administration team for Hyderabad, Bhubaneswar, and Houston (previous facility) offices on the last working day of the leaver basis HR notification. Further, the building security team of HighRadius' Houston office (current facility) is responsible for revoking physical access for leavers based on the email requests raised by the HR and provides an email confirmation upon revocation.	• Inquired of the Administration Team Manager regarding the process followed for physical access revocation. • Inspected the system generated list of active users with physical access to HighRadius premises and compared it with HR's list of terminated users during the audit period to determine whether any terminated users continued to hold the physical access. • For a selection of physical access revocations, inspected the last working day of the terminated user and their physical access revocation date from the admin tool to determine whether the physical access to HighRadius premises of the employees who left the organization was revoked on or before the last working date and whether the proximity card was returned to the Administration team. • For a selection of leavers at the Houston office (current facility), inspected the email requests raised by the HR and email confirmation of physical access revocation from the building security team of HighRadius' Houston office (current facility) to determine whether the physical	No relevant exceptions noted

6.0 Common Criteria Related to Logical and Physical Access[56]			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		access was revoked based on the email requests raised by the HR.	
	Access to the client production and non-production environment is granted after obtaining approval from respective line managers using the PAMS tool.	• Inquired of the Platform Technical Team Manager regarding the process followed for access provisioning to the client production and non-production environments. • Inspected the configuration in PAMS to determine whether the tool is configured to provision access only after the line manager's approval. • For a selection of client production and non-production environment access requests, inspected the PAMS tool to determine whether access was granted after obtaining approval from the respective line managers.	No relevant exceptions noted
	Access to the client production and non-production environment is revoked automatically based on the timeout duration configured as per the job role.	• Inquired of the Platform Technical Team Manager regarding the process followed for access revocation to the client production and non-production environment. • Inspected the access control procedure document to determine whether access timeout duration was defined as per the job role. • Inspected the access timeout duration configured in the PAMS to determine whether the duration was configured as per the access control procedure document. • For a selection of client production and non-production environment access requests, inspected the PAMS tool to determine whether access was revoked as per the timeout duration configured for the respective job role.	No relevant exceptions noted

6.0 Common Criteria Related to Logical and Physical Access[56]			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	Closed Circuit Televisions (CCTV) cameras have been installed at the entry/ exit points and work area of HighRadius facilities.	• Inquired of the Administration team manager regarding the CCTV monitoring on HighRadius premises. • Performed walkthrough of HighRadius Bhubaneswar, Hyderabad, and Houston facilities through physical observation and video conferencing to determine whether CCTV cameras were installed at the entry/ exit points and work area.	No relevant exceptions noted
	Access to application production servers is restricted to Cloud Engineering team.	• Inquired of the Cloud Engineering team manager regarding the access to application production servers. • Inspected the system generated list of user IDs with access to application production servers and compared it with the HR active list of users to determine whether access to application production servers was restricted to Cloud Engineering team.	No relevant exceptions noted
	Access to network devices is provided only to authorized personnel. Users with access to the network devices must authenticate to the network with a unique user identifier and password.	• Inquired of the IMS team and Cloud Engineering team managers regarding the access to corporate and production network devices respectively. • Inspected the system generated list of user IDs with access to network devices and compared it with the HR active list of users to determine whether access to network devices was granted only to the authorized personnel. • Inspected the system generated list of user IDs with access to network devices to determine whether unique user ids were allocated to users.	No relevant exceptions noted

6.0 Common Criteria Related to Logical and Physical Access[56]			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	Access to HighRadius' Active Directory (AD), Unified End-point Management (UEM) System, Anti-Malware Console, and Network devices is provided to users based on their job responsibilities and approved by the IMS team manager.	• Inquired of the IMS team manager regarding the access to Active Directory (AD), Unified End-point Management (UEM) System, Anti-Malware Console and Network devices. • For a selection of new joiner user ids created, inspected the communication of approval for users having access to Active Directory (AD), Unified End-point Management (UEM) System, Anti-Malware Console and Network devices to determine whether the access was provided based on approval from IMS team manager.	No relevant exceptions noted
	User access review for standard and privileged users having access to AD & LDAP are performed by IMS and Cloud Engineering teams on a quarterly basis.	• Inquired of the IMS team and Cloud Engineering team managers regarding the quarterly user access review performed. • For a selection of quarters, inspected the user access review report to determine whether the IMS and Cloud Engineering teams performed the user access review of standard and privileged users having access to AD & LDAP.	No relevant exceptions noted
6.3 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, considering the concepts of least	HighRadius has a documented policy and procedure for managing physical security within the organization.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the physical security policies and procedures. • Inspected the 'Physical and Environmental Security' document to determine whether HighRadius has documented policy and procedures for managing physical security within the organization.	No relevant exceptions noted

6.0 Common Criteria Related to Logical and Physical Access[56]			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
privilegeand segregation of duties, to meet the entity's objectives.	Remote access of data by HighRadius employees is in line with the defined remote access guidelines which requires the usage of a secure Virtual Private Network (VPN) to access the HighRadius network through encrypted means.	• Inquired of the IMS team manager regarding the remote access guidelines which requires the usage of a secure (VPN and Extranet) to access the HighRadius network through encrypted means. • Inspected remote access guidelines to determine whether usage of a secure VPN to access the HighRadius network through AES 256 encryption was documented. • Inspected the VPN configuration to determine whether encryption was enabled on the remote connections.	No relevant exceptions noted
	Access to the development environment and to migrate changes to the production environments is segregated.	• Inquired of the IMS team manager regarding the segregation of access to development and production environment. • Inspected the system generated list of users with access to the development environment and compared it with the system generated list of users having access to migrate changes to the production environments to determine whether there were any common users, and whether the access was segregated.	No relevant exceptions noted.
	Upon receipt of logical access creation request from HR for a new associate, IMS team creates a unique user ID basis the details provided by the HR.	• Inquired of the IMS Team Manager regarding the process followed for logical access creation. • For a selection of new joiners, inspected the HR email, logical access creation tickets, and logical access creation dates to determine whether the IMS team created unique user ID in HighRadius Active Directory and LDAP based on the request received from HR and whether the creation details of the user ID were communicated to the associate.	No relevant exceptions noted

6.0 Common Criteria Related to Logical and Physical Access[56]			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	Upon receipt of an access revocation request from HR, the associate's user ID is disabled by the IMS team from the Active Directory and LDAP on the user's last working date.	• Inquired of the IMS team manager regarding the process followed for logical access revocation. • Inspected the system generated list of active users in Active Directory and LDAP and compared it with the list of users resigned to determine whether terminated users continued to hold access. • For the above selection of resigned users inspected the revocation dates from Active Directory and LDAP to determine whether the user IDs of the employees who left the organization was disabled by IMS team from the Active Directory and LDAP on the user's last working date. • For the selection of resigned users where delay was noted, inspected the activity log to determine whether activities were performed from the user ID post the user's last working date and noted that no activities were performed.	**Exception noted:** For one out of 25 selections of logical access revocations, it was noted that LDAP access was revoked after the last working day with a delay of 42 days. Further, inspected the LDAP activity log for the identified user and noted that no activities were logged post the user's last working day. **Management response:** The access revocation request for the above sample was delayed due to an error in the HR notification, where the username did not exactly match with the exit employee and hence, it required validation. Further, the exit employee's AD user ID was deleted on the last working day and the user could not log in to the network. It was

6.0 Common Criteria Related to Logical and Physical Access[56]			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
			determined that there was no activity logged as well, after the last working day. **Action taken:** A formal notice has been communicated to the respective teams to ensure that any such issues going forward are to be dealt promptly and with more caution.
	Access to the client production and non-production environment is granted after obtaining approval from respective line managers using the PAMS tool.	• Inquired of the Platform Technical Team Manager regarding the process followed for access provisioning to the client production and non-production environments. • Inspected the configuration in PAMS to determine whether the tool is configured to provision access only after the line manager's approval. • For a selection of client production and non-production environment access requests, inspected the PAMS tool to determine whether access was granted after obtaining approval from the respective line managers.	No relevant exceptions noted
	Access to the client production and non-production environment is revoked automatically based on the timeout duration configured as per the job role.	• Inquired of the Platform Technical Team Manager regarding the process followed for access revocation to the client production and non-production environment. • Inspected the access control procedure document to determine whether access timeout duration was defined	No relevant exceptions noted

6.0 Common Criteria Related to Logical and Physical Access[56]			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		as per the job role. • Inspected the access timeout duration configured in the PAMS to determine whether the duration was configured as per the access control procedure document. • For a selection of client production and non-production environment access requests, inspected the PAMS tool to determine whether access was revoked as per the timeout duration configured for the respective job role.	
	Access to network devices is provided only to authorized personnel. Users with access to the network devices must authenticate to the network with a unique user identifier and password.	• Inquired of the IMS team and Cloud Engineering team managers regarding the access to corporate and production network devices respectively. • Inspected the system generated list of user IDs with access to network devices and compared it with the HR active list of users to determine whether access to network devices was granted only to the authorized personnel. • Inspected the system generated list of user IDs with access to network devices to determine whether unique user ids were allocated to users.	No relevant exceptions noted
	Access to application production servers is restricted to Cloud Engineering team.	• Inquired of the Cloud Engineering team manager regarding the access to application production servers. • Inspected the system generated list of user IDs with access to application production servers and compared it with the HR active list of users to determine whether access to application production servers was restricted to Cloud Engineering team.	No relevant exceptions noted

6.0 Common Criteria Related to Logical and Physical Access[56]			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	Access to HighRadius' Active Directory (AD), Unified End-point Management (UEM) System, Anti-Malware Console, and Network devices is provided to users based on their job responsibilities and approved by the IMS team manager.	• Inquired of the IMS team manager regarding the access to Active Directory (AD), Unified End-point Management (UEM) System, Anti-Malware Console and Network devices. • For a selection of new joiner user ids created, inspected the communication of approval for users having access to Active Directory (AD), Unified End-point Management (UEM) System, Anti-Malware Console and Network devices to determine whether the access was provided based on approval from IMS team manager.	No relevant exceptions noted
6.4 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.	Physical access for new joiners is created by Administration team for Hyderabad, Bhubaneswar, and Houston (previous facility) offices basis HR notification. Further, the building security team of HighRadius' Houston office (current facility) is responsible for creating physical access for new joiners joining the Houston office based on the email requests raised by the HR and provides an email confirmation upon creation.	• Inquired of the Administration team regarding the process followed for providing physical access to HighRadius premises. • For a selection of new joiners, inspected notification from HR team and date of physical access creation to determine whether the physical access to HighRadius premises was provided based on request from HR. • For a selection of new joiners at the Houston office (current facility), inspected the email requests raised by the HR and email confirmation of physical access creation from the building security team of HighRadius' Houston office (current facility) to determine whether the physical access was created based on the email requests raised by the HR.	No relevant exceptions noted
	Physical access for leavers is revoked and proximity card is returned to the Administration team for Hyderabad,	• Inquired of the Administration Team Manager regarding the process followed for physical access revocation.	No relevant exceptions noted

6.0 Common Criteria Related to Logical and Physical Access[56]			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	Bhubaneswar, and Houston (previous facility) offices on the last working day of the leaver basis HR notification. Further, the building security team of HighRadius' Houston office (current facility) is responsible for revoking physical access for leavers based on the email requests raised by the HR and provides an email confirmation upon revocation.	• Inspected the system generated list of active users with physical access to HighRadius premises and compared it with HR's list of terminated users during the audit period to determine whether any terminated users continued to hold the physical access. • For a selection of physical access revocations, inspected the last working day of the terminated user and their physical access revocation date from the admin tool to determine whether the physical access to HighRadius premises of the employees who left the organization was revoked on or before the last working date and whether the proximity card was returned to the Administration team. • For a selection of leavers at the Houston office (current facility), inspected the email requests raised by the HR and email confirmation of physical access revocation from the building security team of HighRadius' Houston office (current facility) to determine whether the physical access was revoked based on the email requests raised by the HR.	

6.0 Common Criteria Related to Logical and Physical Access[56]			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	HighRadius has a documented policy and procedure for managing physical security within the organization.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the physical security policies and procedures. • Inspected the 'Physical and Environmental Security' document to determine whether HighRadius has documented policy and procedures for managing physical security within the organization.	No relevant exceptions noted
	Physical access to the server rooms is restricted by proximity card-based access control system at Hyderabad, India and Houston, Texas offices.	• Inquired of the Administration team manager regarding the physical access to server rooms. • Performed walkthrough of HighRadius Bhubaneswar, Hyderabad, and Houston facilities through physical observation and video conferencing to determine whether access to server rooms were restricted by proximity card-based access control system. • For a selection of dates, inspected the visitor register being maintained for server rooms to determine whether logs were made to the visitor register upon each entry.	No relevant exceptions noted
	Physical access to the network Room, hub room and UPS room is restricted to authorized personnel from the IMS team and security personnel.	• Inquired of the Administration team manager regarding the physical access to network room, hub room and UPS room. • Inspected the list of users with access to network room, hub room and UPS room within HighRadius premises to determine whether access was restricted to users from IMS team and security personnel. • For a selection of dates, inspected the visitor register	No relevant exceptions noted

6.0 Common Criteria Related to Logical and Physical Access[56]			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		being maintained for network room, hub room and UPS room to determine whether logs were made to the visitor register upon each entry.	
	A visitor register is maintained by security guards at HighRadius reception area in Hyderabad, India and Bhubaneswar, India to record the name of the visitor, reason of visit, contact person, entry time, exit time, and electronic device details. Further, the building security team of HighRadius' Houston office (current facility) is responsible for providing temporary/visitor access cards to visitors of HighRadius based on the email requests raised by the HR.	• Inquired of the Administration Team Manager regarding the visitor registers maintained at HighRadius Bhubaneswar and Hyderabad facilities. • For a selection of days, inspected the visitor registers to determine whether the register was maintained by security guards to record the name of the visitor, reason of visit, contact person, entry time, exit time, and electronic device details. • For a selection of visitors, inspected the email requests raised by the HR and email confirmation of providing temporary/visitor access cards from the building security team of HighRadius' Houston office (current facility) to determine whether the building security team provided temporary/visitor access cards to visitors of HighRadius based on the email requests raised by the HR.	**Exception noted:** It was noted that the electronic device details were not captured as part of the visitor register maintained in Bhubaneswar, India during the audit period. **Management response:** HighRadius Bhubaneswar facility has been scoped in for physical security controls for the first time and the team missed on capturing the electronic device details as part of the visitor register. **Action taken:** As suggested by KPMG & HighRadius' Cyber Security team, we have started capturing the electronic device (laptop, mobile etc.) details in the visitor register from November 2023.

6.0 Common Criteria Related to Logical and Physical Access[56]			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	Closed Circuit Televisions (CCTV) cameras have been installed at the entry/ exit points and work area of HighRadius facilities.	• Inquired of the Administration team manager regarding the CCTV monitoring on HighRadius premises. • Performed walkthrough of HighRadius Bhubaneswar, Hyderabad, and Houston facilities through physical observation and video conferencing to determine whether CCTV cameras were installed at the entry/ exit points and work area.	No relevant exceptions noted
	Upon receipt of an access revocation request from HR, the associate's user ID is disabled by the IMS team from the Active Directory and LDAP on the user's last working date.	• Inquired of the IMS team manager regarding the process followed for logical access revocation. • Inspected the system generated list of active users in Active Directory and LDAP and compared it with the list of users resigned to determine whether terminated users continued to hold access. • For the above selection of resigned users inspected the revocation dates from Active Directory and LDAP to determine whether the user IDs of the employees who left the organization was disabled by IMS team from the Active Directory and LDAP on the user's last working date. • For the selection of resigned users where delay was noted, inspected the activity log to determine whether activities were performed from the user ID post the user's last working date and noted that no activities were performed.	**Exception noted:** For one out of 25 selections of logical access revocations, it was noted that LDAP access was revoked after the last working day with a delay of 42 days. Further, inspected the LDAP activity log for the identified user and noted that no activities were logged post the user's last working day. **Management response:** The access revocation request for the above sample was delayed due to an error in the HR notification, where the username did not exactly match with the exit

6.0 Common Criteria Related to Logical and Physical Access[56]			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
			employee and hence, it required validation. Further, the exit employee's AD user ID was deleted on the last working day and the user could not log in to the network. It was determined that there was no activity logged as well, after the last working day. **Action taken:** A formal notice has been communicated to the respective teams to ensure that any such issues going forward are to be dealt promptly and with more caution.
	Movement of material inward/ outward of the HighRadius premises is registered in the material movement (inward/outward) register.	• Inquired of the Administration team manager regarding the movement of material inward/outward of the HighRadius premises. • For a selection of dates, inspected the material movement register to determine whether details related to movement of material inward/outward of HighRadius premises were registered.	No relevant exceptions noted

6.0 Common Criteria Related to Logical and Physical Access[56]			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
6.5 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.	HighRadius has established documented procedures to dispose confidential information post retention period.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the policies and procedures for disposing of confidential information post retention period. • Inspected the 'Operations Security' policy and procedure documents to determine whether procedure for disposal of confidential information post retention period.	No relevant exceptions noted
	HighRadius has established documented procedures to dispose confidential information post retention period.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the policies and procedures for disposing of confidential information post retention period. • Inspected the 'Operations Security' policy and procedure documents to determine whether procedure for disposal of confidential information post retention period.	No relevant exceptions noted
	HighRadius has documented 'Information Classification' policy based upon the sensitivity and confidentiality of data. Data or information in HighRadius is classified into four categories given below: Public; Internal; Confidential; and Restricted.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding 'Information Classification' policy. • Inspected the 'Information Classification' policy to determine whether data or information in HighRadius is classified into four categories as Public, Internal, Confidential and Restricted.	No relevant exceptions noted

6.0 Common Criteria Related to Logical and Physical Access[56]			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Firewall rules are defined, and content filtering is enabled to restrict access to users on network.	• Inquired of the Cloud Engineering team manager regarding the firewall implemented to prevent unauthorized access on the HighRadius corporate network. • Inspected the firewall rule set to determine whether firewall rules were defined, and content filtering was enabled to restrict access of users on network.	No relevant exceptions noted
	Remote access of data by HighRadius employees is in line with the defined remote access guidelines which requires the usage of a secure Virtual Private Network (VPN) to access the HighRadius network through encrypted means.	• Inquired of the IMS team manager regarding the remote access guidelines which requires the usage of a secure (VPN and Extranet) to access the HighRadius network through encrypted means. • Inspected remote access guidelines to determine whether usage of a secure VPN to access the HighRadius network through AES 256 encryption was documented. • Inspected the VPN configuration to determine whether encryption was enabled on the remote connections.	No relevant exceptions noted
	Firewalls are installed at the perimeter of the corporate servers and network to block traffic unless specifically whitelisted.	• Inquired of the IMS team manager regarding the firewall implemented on HighRadius' corporate servers and network. • Inspected the network diagram to determine whether firewalls were installed on the perimeter of the corporate servers and network. • Inspected the firewall configuration to determine whether traffic to the corporate servers and network was blocked unless specifically whitelisted.	No relevant exceptions noted

6.0 Common Criteria Related to Logical and Physical Access[56]			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	Firewalls are installed at the perimeter of the production and non-production servers and network to block traffic unless specifically whitelisted.	• Inquired of the IMS team manager regarding the firewall implemented on HighRadius' production and non-production servers. • Inspected the network diagram to determine whether firewalls were installed on the perimeter of the production and non-production servers and network. • Inspected the firewall configuration to determine whether traffic to the production and non-production servers was blocked unless specifically whitelisted.	No relevant exceptions noted
	HighRadius has implemented a Cloud Access Security Broker (CASB) solution which is responsible for logging activities performed by HighRadius' employees on the applications (SaaS). The solution is also configured to prevent users from accessing blacklisted websites.	• Inquired of the Cyber Security – Operations team manager regarding the CASB solution implemented within HighRadius. • For a selection of applications, inspected the CASB portal to determine whether activities performed on the applications (SaaS) were getting logged. • Inspected the rulesets in the CASB portal to determine whether the solution was configured to prevent users from accessing blacklisted websites.	No relevant exceptions noted
6.7 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	GTB Data Leakage Prevention (DLP) Tool is installed in desktops and laptops within HighRadius to avoid unauthorized transmission of sensitive client data.	• Inquired of the Cyber Security - Operations team manager regarding the GTB Data Leakage Prevention (DLP) tool installed. • Inspected the configuration of DLP tool to determine whether transmission of confidential data is tracked through DLP tool to avoid unauthorized transmission of sensitive client data.	No relevant exceptions noted

6.0 Common Criteria Related to Logical and Physical Access[56]			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
the entity's objectives.	Remote access of data by HighRadius employees is in line with the defined remote access guidelines which requires the usage of a secure Virtual Private Network (VPN) to access the HighRadius network through encrypted means.	• Inquired of the IMS team manager regarding the remote access guidelines which requires the usage of a secure (VPN and Extranet) to access the HighRadius network through encrypted means. • Inspected remote access guidelines to determine whether usage of a secure VPN to access the HighRadius network through AES 256 encryption was documented. • Inspected the VPN configuration to determine whether encryption was enabled on the remote connections.	No relevant exceptions noted
	Removable media devices, such as compact disk writers, Universal Serial Bus (USB) mass storage devices, and Compact Disk – Read Only Memory (CD-ROM) readers are disabled on individual workstations.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the disabling of removable media devices on workstations. • Inspected the desktop central tool configuration to determine whether a policy was defined to disable removable media devices on individual workstations. • For a selection of workstations, inspected the system configuration to determine whether removable media devices, such as compact disk writers, Universal Serial Bus (USB) mass storage devices, and Compact Disk – Read Only Memory (CD-ROM) readers were disabled.	No relevant exceptions noted
	Admin access on desktops and laptops are restricted.	• Inquired of the IMS team manager regarding the disabling of admin access on workstations. • For a selection of workstations, inspected the system configuration to determine whether admin access was disabled on individual workstations.	No relevant exceptions noted

6.0 Common Criteria Related to Logical and Physical Access[56]			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Admin access on desktops and laptops are restricted.	• Inquired of the IMS team manager regarding the disabling of admin access on workstations. • For a selection of workstations, inspected the system configuration to determine whether admin access was disabled on individual workstations.	No relevant exceptions noted
	HighRadius has a formal change management procedure documented within the 'Operations Security' policy, which describes the procedures designed to help ensure that only authorized, tested, and documented changes are made to the system.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the change management procedure at HighRadius. • Inspected the change management process within the 'Operations Security' policy and procedure documents to determine whether the procedure designed to help ensure that only authorized, tested, and documented changes were made to the system was defined.	No relevant exceptions noted
	Change Requests are classified by the Product teams within the internal ticketing tool.	• Inquired of the Product Team Manager regarding the classification process for Change Requests (CR). • For a selection of change requests, inspected the JIRA ticketing tool to determine whether the change request was classified by the Product teams.	No relevant exceptions noted
	Product teams continuously monitor the internal ticketing tool for Change Requests logged and acknowledge the requests by changing the status of the ticket to "Open".	• Inquired of the Product Team Manager regarding the ticketing tool for Change Requests. • For a selection of change requests, inspected the JIRA ticketing tool to determine whether the Product team acknowledged the change requests by changing the status to 'Open'.	No relevant exceptions noted
	Product teams at HighRadius develop the required changes and communicate the same	• Inquired of the Product Team Manager regarding the	No relevant exceptions noted

6.0 Common Criteria Related to Logical and Physical Access[56]			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	to the user entity.	Change Requests (CR) management procedure. • For a selection of change requests, inspected the change tickets to determine whether the Product team developed the required changes and communicated the same to the user entity.	
	Emergency changes are logged, authorized, and documented as per the emergency change management procedure defined.	• Inquired of the Product Team Manager regarding the emergency change management procedure. • Inspected the emergency change management procedure within the 'Operations Security' policy and procedure documents to determine whether the procedure for emergency change management was defined and documented. • For a selection of emergency changes raised, inspected the change tickets to determine whether emergency changes were logged, authorized, and documented as per the emergency change management process defined.	No relevant exceptions noted
	Upon resolution of Change Request, Product teams update the requests with the solution provided along with details of the change release and then the status of the ticket is changed to "Closed" or "Resolved".	• Inquired of the Product manager regarding the Change Request (CR) management procedure. • For a selection of change requests, inspected the change tickets to determine whether the Product team updated the change requests with a brief description of the solution provided along with the details of the change release. • For the above selection of change requests, inspected the JIRA ticketing tool to determine whether the Product team changed the status of the change requests to 'Closed'	No relevant exceptions noted

6.0 Common Criteria Related to Logical and Physical Access[56]			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		or 'Resolved'.	
	Anti-malware software is installed and activated on workstations within HighRadius to protect the workstations from external threats. Anti-malware servers are configured to download the latest signature files from the vendor's site and deploy the same on the workstations at regular predefined intervals.	• Inquired of the IMS Team Manager regarding the anti-malware software installed and activated on workstations. • For a selection of workstations, inspected the anti-malware software settings to determine whether anti-malware software was installed and activated on workstations within HighRadius. • For the above selection of workstations, inspected the anti-malware software configuration to determine whether access to change the anti-malware settings was disabled. • Inspected the anti-malware configuration on the server to determine whether the server was configured to download the latest signature files from the vendor's site and deploy the same on the workstations at regular predefined intervals.	No relevant exceptions noted
	Anti-malware software is installed and activated on the production servers within HighRadius to protect the internal servers and network from external threats. Anti-malware servers are configured to download the latest signature files from the vendor's site and deploy the same on the servers at regular predefined intervals.	• Inquired of the IMS team manager regarding the anti-malware software installed and activated on the production servers within HighRadius. • Inspected the anti-malware configuration on the production servers to determine whether the anti-malware software was installed and activated. • Inspected the anti-malware software configuration to determine whether access to change the anti-malware settings was disabled.	No relevant exceptions noted

6.0 Common Criteria Related to Logical and Physical Access[56]			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		• Inspected the anti-malware configuration on the server to determine whether the server was configured to download the latest signature files from the vendor's site and deploy the same on the servers at regular predefined intervals.	
	Relevant security patches are updated on workstations. The patches are implemented as per predefined patch management process.	• Inquired of the IMS Team Manager regarding the security patch management process for workstations. • Inspected the security patch management procedure within the 'Patch Management' policy and procedure documents to determine whether the procedure for security patch management was defined and documented. • For a selection of workstations, inspected the system configuration to determine whether relevant security patches were updated as per predefined patch management process.	No relevant exceptions noted
	Relevant security patches are updated on servers. The patches are implemented post approval from the respective department heads and post testing of patches in the staging environment.	• Inquired of the IMS Team Manager regarding the security patch management process for HighRadius' servers. • For a selection of quarters, inspected the approval communication and patch test results for implementation of security patches on servers to determine whether the patches were implemented as per the defined patch management process. • For the above selection of quarters, inspected the list of patches deployed on servers to determine whether the security patches were pushed from the server post	**Exception noted:** For one out of two quarterly patching schedules selected, it was noted that 11 out of 12 production environments were not implemented with relevant security patches in Q2 2023. Further, we were informed by the CTO that a verbal approval for the same was granted by the

6.0 Common Criteria Related to Logical and Physical Access[56]			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		approvals.	CTO at the beginning of Q2 2023 to omit and reschedule the patching of the 11 production environments. **Management response:** The patching process is managed by the Cloud Engineering team. In Q2, the team was managing several critical programs in addition to working on identifying automation opportunities for the patching process. Hence, as an exception, the CTO had granted a verbal approval in Q2 to delay the planned patches since there were no critical security patches outstanding for Q2. This approval was also regularized through an email approval in Q3. **Action taken:** Subsequently, in Q3, the pending patches were deployed.

7.0 Common Criteria Related to System Operations			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
7.1 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.	HighRadius has documented 'Server and Firewall Hardening Standard' policy and procedures for its servers and 'End User Device Hardening Standards' document for its end user systems in order to provide a controlled operating environment and to prevent any unauthorized access to critical system resources.	• Inquired of Cyber Security – Risk & Compliance team manager regarding the hardening guidelines for servers and end user systems. • Inspected the 'Server and Firewall Hardening Standard' and 'End User Device Hardening Standards' document to determine whether hardening standards for servers and end user system were available to provide a controlled operating environment and to prevent any unauthorized access to critical system resources.	No relevant exceptions noted
	Network monitoring tool is installed to monitor the availability of the network devices and server. The monitoring tool is configured to generate an alert for any exceptions identified. Alerts generated are monitored by the IMS team.	• Inquired of the IMS team manager regarding the network monitoring tool in place for HighRadius network. • Inspected the configuration of the monitoring tool to determine whether tool was configured to monitor the availability of the network devices and servers. • Inspected the configuration of the monitoring tool to determine whether tool was configured to generate an alert for any exceptions identified. • Inspected the incident dashboard to determine whether the alerts generated were monitored. • Further, inspected the ticket raised to determine whether the alerts generated were tracked to closure.	No relevant exceptions noted

7.0 Common Criteria Related to System Operations			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	HighRadius network, servers and web applications undergo third party Vulnerability Assessment and Penetration Testing on a semi-annual basis. Issues of non-compliance from assessments are tracked to closure.	• Inquired of the Cyber Security – Operations team manager regarding the third-party Vulnerability Assessment and Penetration Testing (VAPT). • Inspected the semi-annual third party VAPT report to determine whether HighRadius network, servers and web applications were covered as part of the report. • Inspected the remediation report to determine whether issues of non-compliance from the assessments were resolved and tracked to closure.	No relevant exceptions noted
	Cyber Security – Operations team performs penetration testing on the HighRadius network and servers on a quarterly basis and performs penetration testing on HighRadius web applications on a semi-annual basis. Issues of non-compliance from assessments are tracked to closure.	• Inquired of the Cyber Security – Operations team manager regarding penetration testing performed on HighRadius network, servers, and web applications. • For a selection of quarters and semi-annual web application penetration testing, inspected the reports of penetration testing to determine whether Cyber Security team conducted penetration testing on HighRadius network, servers, and web applications. • For the above selection of reports, inspected the remediation activities to determine whether issues of non-compliance from testing were resolved and tracked to closure.	No relevant exceptions noted
	Cyber Security – Operations team performs vulnerability assessment on the HighRadius web applications on a weekly basis and network, servers on a monthly basis. Issues of non-compliance from assessments are tracked to closure.	• Inquired of the Cyber Security – Operations team manager regarding vulnerability assessments performed HighRadius network, servers, and web applications. • For a selection of weeks, inspected the reports of vulnerability assessment to determine whether Cyber Security – Operations team conducted vulnerability	No relevant exceptions noted

7.0 Common Criteria Related to System Operations			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		assessment on HighRadius web applications • For the above selection of weeks, inspected the remediation report to determine whether issues of non-compliance from assessments were resolved and tracked to closure. • For a selection of months, inspected the reports of vulnerability assessment to determine whether Cyber Security – Operations team conducted vulnerability assessment on HighRadius network and servers. • For the above selection of months, inspected the remediation report to determine whether issues of non-compliance from assessments were resolved and tracked to closure.	
	On an annual basis, DoS/DDoS tests are performed on HighRadius infrastructure by Cyber Security team and reviewed by the Manager – Cyber Security.	• Inquired of the Cyber Security Team Manager regarding the DoS/DDoS tests performed on HighRadius infrastructure. • For the audit period, inspected the DoS/DDoS test report to determine whether the Cyber Security team performed the DoS/DDoS tests on an annual basis and the result was reviewed by the Manager – Cyber Security.	No relevant exceptions noted
	Appropriate actions are taken by the HighRadius Cyber Security – Operations team for alerts reported by HighRadius' Managed Security Service Provider (MSSP).	• Inquired of the Cyber Security – Operations Team Manager regarding HighRadius' Managed Security Service Provider (MSSP). • For a selection of "High", "Medium" and "Low" alerts reported, inspected the email communication to determine whether the alerts were acknowledged, and	No relevant exceptions noted

7.0 Common Criteria Related to System Operations			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		appropriate actions were taken by the Cyber Security – Operations team.	
	Cyber Security – Operations team performs a full static code analysis (security) on a monthly basis and an incremental static code analysis (security) on a weekly basis of changes prior to release. Issues of non-compliance from analysis are tracked to closure.	• Inquired of the Cyber Security – Operations team manager regarding the static security code review process. • For a selection of months, inspected the reports for static security code review to determine whether monthly full static security code reviews were performed on changes prior to release by the Cyber Security – Operations team. • Further, inspected the communication for remediation to determine whether the non-compliances from assessments were getting resolved and tracked to closure. • For a selection of weeks, inspected the reports for static security code review to determine whether weekly incremental static security code reviews were performed on changes prior to release by the Cyber Security team. • Further, inspected the communication for remediation to determine whether the non-compliances from assessments were getting resolved and tracked to closure.	No relevant exceptions noted
7.2 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	HighRadius has defined 'Incident Management' policy which includes procedures for reporting, categorization and resolution of security incidents. The 'Incident Management' policy is available on Intranet. The process for reporting the incidents is also covered as part of annual refresher training.	• Inquired of the Cyber Security – Operations team manager regarding the 'Incident Management' policy and procedures document. • Inspected the 'Incident Management' policy document to determine whether it covered the aspects of the policy. • Inspected the 'Incident Management' policy and	No relevant exceptions noted

7.0 Common Criteria Related to System Operations			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
are analyzed to determine whether they represent security events.		procedures documents to determine whether the guidelines for reporting, categorization, and resolution of security incidents were defined. • Inspected the intranet portal to determine whether the 'Incident Management' policy and procedure documents were available on the Intranet. • Inspected the training content for refresher training to determine whether incident management guidelines were covered as part of the training. • For a selection of employees, inspected the attendance sheet to determine if the incident management guidelines were communicated to the employees.	
	HighRadius has documented 'Server and Firewall Hardening Standard' policy and procedures for its servers and 'End User Device Hardening Standards' document for its end user systems in order to provide a controlled operating environment and to prevent any unauthorized access to critical system resources.	• Inquired of Cyber Security – Risk & Compliance team manager regarding the hardening guidelines for servers and end user systems. • Inspected the 'Server and Firewall Hardening Standard' and 'End User Device Hardening Standards' document to determine whether hardening standards for servers and end user system were available to provide a controlled operating environment and to prevent any unauthorized access to critical system resources	No relevant exceptions noted
	HighRadius network, servers and web applications undergo third party Vulnerability Assessment and Penetration Testing on a semi-annual basis. Issues of non-compliance from assessments are tracked to closure.	• Inquired of the Cyber Security – Operations team manager regarding the third-party Vulnerability Assessment and Penetration Testing (VAPT). • Inspected the semi-annual third party VAPT report to determine whether HighRadius network, servers and web applications were covered as part of the report.	No relevant exceptions noted

7.0 Common Criteria Related to System Operations			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		• Inspected the remediation report to determine whether issues of non-compliance from the assessments were resolved and tracked to closure.	
	Cyber Security – Operations team performs penetration testing on the HighRadius network and servers on a quarterly basis and performs penetration testing on HighRadius web applications on a semi-annual basis. Issues of non-compliance from assessments are tracked to closure.	• Inquired of the Cyber Security – Operations team manager regarding penetration testing performed on HighRadius network, servers, and web applications. • For a selection of quarters and semi-annual web application penetration testing, inspected the reports of penetration testing to determine whether Cyber Security team conducted penetration testing on HighRadius network, servers, and web applications. • For the above selection of reports, inspected the remediation activities to determine whether issues of non-compliance from testing were resolved and tracked to closure.	No relevant exceptions noted
	Cyber Security – Operations team performs vulnerability assessment on the HighRadius web applications on a weekly basis and network, servers on a monthly basis. Issues of non-compliance from assessments are tracked to closure.	• Inquired of the Cyber Security – Operations team manager regarding vulnerability assessments performed HighRadius network, servers, and web applications. • For a selection of weeks, inspected the reports of vulnerability assessment to determine whether Cyber Security – Operations team conducted vulnerability assessment on HighRadius web applications • For the above selection of weeks, inspected the remediation report to determine whether issues of non-compliance from assessments were resolved and tracked to closure. • For a selection of months, inspected the reports of	No relevant exceptions noted

7.0 Common Criteria Related to System Operations			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		vulnerability assessment to determine whether Cyber Security – Operations team conducted vulnerability assessment on HighRadius network and servers. • For the above selection of months, inspected the remediation report to determine whether issues of non-compliance from assessments were resolved and tracked to closure.	
	On an annual basis, DoS/DDoS tests are performed on HighRadius infrastructure by Cyber Security team and reviewed by the Manager – Cyber Security.	• Inquired of the Cyber Security Team Manager regarding the DoS/DDoS tests performed on HighRadius infrastructure. • For the audit period, inspected the DoS/DDoS test report to determine whether the Cyber Security team performed the DoS/DDoS tests on an annual basis and the result was reviewed by the Manager – Cyber Security.	No relevant exceptions noted
	Cyber Security – Operations team performs a full static code analysis (security) on a monthly basis and an incremental static code analysis (security) on a weekly basis of changes prior to release. Issues of non-compliance from analysis are tracked to closure.	• Inquired of the Cyber Security – Operations team manager regarding the static security code review process. • For a selection of months, inspected the reports for static security code review to determine whether monthly full static security code reviews were performed on changes prior to release by the Cyber Security – Operations team. • Further, inspected the communication for remediation to determine whether the non-compliances from assessments were getting resolved and tracked to closure. • For a selection of weeks, inspected the reports for static security code review to determine whether weekly	No relevant exceptions noted

7.0 Common Criteria Related to System Operations			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		incremental static security code reviews were performed on changes prior to release by the Cyber Security team. • Further, inspected the communication for remediation to determine whether the non-compliances from assessments were getting resolved and tracked to closure.	
	Removable media devices, such as compact disk writers, Universal Serial Bus (USB) mass storage devices, and Compact Disk – Read Only Memory (CD-ROM) readers are disabled on individual workstations.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the disabling of removable media devices on workstations. • Inspected the desktop central tool configuration to determine whether a policy was defined to disable removable media devices on individual workstations. • For a selection of workstations, inspected the system configuration to determine whether removable media devices, such as compact disk writers, Universal Serial Bus (USB) mass storage devices, and Compact Disk – Read Only Memory (CD-ROM) readers were disabled.	No relevant exceptions noted
	A network monitoring tool is configured to perform ping test, port availability, verification of partition sizes of the hard disk, CPU monitoring and memory on the servers. For any exceptions noted, the monitoring tool is configured to generate a request within tracking tool for the alerts.	• Inquired of the Cloud Engineering team manager regarding the network monitoring tool in place for HighRadius network. • Inspected the configuration of the monitoring tool to determine whether tool was configured to perform ping test, port availability, verification of partition sizes of the hard disk, CPU monitoring and memory on the servers. • Inspected the configuration of the monitoring tool to determine whether it is configured to generate a request	No relevant exceptions noted

7.0 Common Criteria Related to System Operations			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		within the tracking tool for the alerts in case of any exceptions. • For a selection of exceptions noted, inspected the requests generated within the tracking tool to determine whether the monitoring tool was configured to generate a request within tracking tool for the alerts.	
	Anti-malware software is installed and activated on workstations within HighRadius to protect the workstations from external threats. Anti-malware servers are configured to download the latest signature files from the vendor's site and deploy the same on the workstations at regular predefined intervals.	• Inquired of the IMS Team Manager regarding the anti-malware software installed and activated on workstations. • For a selection of workstations, inspected the anti-malware software settings to determine whether anti-malware software was installed and activated on workstations within HighRadius. • For the above selection of workstations, inspected the anti-malware software configuration to determine whether access to change the anti-malware settings was disabled. • Inspected the anti-malware configuration on the server to determine whether the server was configured to download the latest signature files from the vendor's site and deploy the same on the workstations at regular predefined intervals.	No relevant exceptions noted
	Anti-malware software is installed and activated on the production servers within HighRadius to protect the internal servers and network from external threats. Anti-malware servers are configured to download the latest signature files from the vendor's site and	• Inquired of the IMS team manager regarding the anti-malware software installed and activated on the production servers within HighRadius. • Inspected the anti-malware configuration on the production servers to determine whether the anti-malware software was installed and activated.	No relevant exceptions noted

7.0 Common Criteria Related to System Operations			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	deploy the same on the servers at regular predefined intervals.	• Inspected the anti-malware software configuration to determine whether access to change the anti-malware settings was disabled. • Inspected the anti-malware configuration on the server to determine whether the server was configured to download the latest signature files from the vendor's site and deploy the same on the servers at regular predefined intervals.	
	HighRadius has implemented a Cloud Access Security Broker (CASB) solution which is responsible for logging activities performed by HighRadius' employees on the applications (SaaS). The solution is also configured to prevent users from accessing blacklisted websites.	• Inquired of the Cyber Security – Operations team manager regarding the CASB solution implemented within HighRadius. • For a selection of applications, inspected the CASB portal to determine whether activities performed on the applications (SaaS) were getting logged. • Inspected the rulesets in the CASB portal to determine whether the solution was configured to prevent users from accessing blacklisted websites.	No relevant exceptions noted
	Appropriate actions are taken by the HighRadius Cyber Security – Operations team for alerts reported by HighRadius' Managed Security Service Provider (MSSP).	• Inquired of the Cyber Security – Operations Team Manager regarding HighRadius' Managed Security Service Provider (MSSP). • For a selection of "High", "Medium" and "Low" alerts reported, inspected the email communication to determine whether the alerts were acknowledged, and appropriate actions were taken by the Cyber Security – Operations team.	No relevant exceptions noted
	XDR server is configured to correlate alerts and manage defenses from Anti-Malware	• Inquired of the IMS team manager regarding the XDR server.	No relevant exceptions noted

7.0 Common Criteria Related to System Operations			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	Server.	• Inspected the XDR server configuration to determine whether the XDR server was configured to correlate alerts and manage defenses from anti-malware server.	
	The Cyber Security - Operations team reviews the anti-malware and Extended Detection & Response (XDR) logs for issues and concerns related to information security across workstations and servers on a weekly basis, and remediation activities, if any, are performed.	• Inquired of the Cyber Security – Operations team manager regarding the reviews of anti-malware and XDR logs for issues and concerns related to information security. • For a selection of weeks, inspected the anti-malware and XDR log review reports to determine whether Cyber Security – Operations team performed weekly reviews and remediation activities, if any.	No relevant exceptions noted
7.3 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.	HighRadius has defined 'Incident Management' policy which includes procedures for reporting, categorization and resolution of security incidents. The 'Incident Management' policy is available on Intranet. The process for reporting the incidents is also covered as part of annual refresher training.	• Inquired of the Cyber Security – Operations team manager regarding the 'Incident Management' policy and procedures document. • Inspected the 'Incident Management' policy document to determine whether it covered the aspects of the policy. • Inspected the 'Incident Management' policy and procedures documents to determine whether the guidelines for reporting, categorization, and resolution of security incidents were defined. • Inspected the intranet portal to determine whether the 'Incident Management' policy and procedure documents were available on the intranet. • Inspected the training content for refresher training to determine whether incident management guidelines were covered as part of the training. • For a selection of employees, inspected the attendance	No relevant exceptions noted

7.0 Common Criteria Related to System Operations			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		sheet to determine if the incident management guidelines were communicated to the employees.	
	Security Incident Response Team (SIRT) is responsible for designing, developing, implementing and monitoring controls relevant to security, availability and confidentiality at HighRadius.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding SIRT. • Inspected the 'Roles and Responsibilities' policy and procedure documents to determine whether the responsibility for designing, developing, implementing and monitoring controls relevant to security, availability and confidentiality at HighRadius were assigned to SIRT.	No relevant exceptions noted
	For incidents having impact on user entities, the project manager / product development team for the user entities reports the incident to appropriate user entities.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding procedure for reporting of incidents to user entities. • For a selection of security incidents, inspected the communication between user entity and project manager/production development team to determine whether the incidents that impacted user entities were reported to the user entities.	No relevant exceptions noted
7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	HighRadius has defined 'Incident Management' policy which includes procedures for reporting, categorization and resolution of security incidents. The 'Incident Management' policy is available on Intranet. The process for reporting the incidents is also covered as part of annual refresher training.	• Inquired of the Cyber Security – Operations team manager regarding the 'Incident Management' policy and procedures document. • Inspected the 'Incident Management' policy document to determine whether it covered the aspects of the policy. • Inspected the 'Incident Management' policy and procedures documents to determine whether the guidelines for reporting, categorization, and resolution of security incidents were defined.	No relevant exceptions noted

7.0 Common Criteria Related to System Operations			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		• Inspected the intranet portal to determine whether the 'Incident Management' policy and procedure documents were available on the intranet. • Inspected the training content for refresher training to determine whether incident management guidelines were covered as part of the training. • For a selection of employees, inspected the attendance sheet to determine if the incident management guidelines were communicated to the employees.	
	Security Incident Response Team (SIRT) is responsible for designing, developing, implementing and monitoring controls relevant to security, availability and confidentiality at HighRadius.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding SIRT. • Inspected the 'Roles and Responsibilities' policy and procedure documents to determine whether the responsibility for designing, developing, implementing and monitoring controls relevant to security, availability and confidentiality at HighRadius were assigned to SIRT.	No relevant exceptions noted
	Priority for Defects and Service Disruptions are classified and documented by the TechSupport team within the ticketing tool.	• Inquired of the TechSupport Team Manager regarding the priorities defined for managing defects and service disruptions raised. • For a selection of defects and service disruptions, inspected the Genie ticketing tool to determine whether priority for defects and service disruptions were classified and documented within the tool by the TechSupport team.	No relevant exceptions noted

7.0 Common Criteria Related to System Operations			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	The TechSupport team resolves the Defect and Service Disruption requests and changes the status of the requests to 'Closed' within the ticketing tool.	• Inquired of the TechSupport team manager regarding the defects and service disruptions. • For a selection of defects and service disruptions raised, inspected the ticket details to determine whether the requests were resolved by the TechSupport team. • For the above selection of defects and service disruptions, inspected the Genie ticketing tool to determine whether TechSupport team changed the status of the defects and service disruptions to 'Closed' upon resolution.	No relevant exceptions noted
	Upon closure of Defect and Service Disruption requests, TechSupport team performs and documents the Root Cause Analysis (RCA) within the ticketing tool or communicates over an email.	• Inquired of the TechSupport Team Manager regarding the documentation of Root Cause Analysis (RCA) of defects and service disruptions. • For a selection of defects and service disruptions raised, inspected the ticket details to determine whether the TechSupport team performed and documented the RCA. • For the above selection of defects and service disruptions, inspected the ticket details to determine whether Tech Support team communicated the RCA details to affected users within the Genie ticketing tool or over an email.	No relevant exceptions noted
	Security incidents are registered with the Cyber Security - Operations team using the internal ticketing tool or by sending an e-mail.	• Inquired of the Cyber Security – Operations Team Manager regarding the reporting and tracking of security incidents. • For a selection of security incidents, inspected the internal incident ticketing tool, ticket details and Security	No relevant exceptions noted

7.0 Common Criteria Related to System Operations			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		incident e-mails to determine whether the security incidents were registered and tracked through the Genie ticketing tool or by e-mails.	
7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.	HighRadius has defined 'Incident Management' policy which includes procedures for reporting, categorization and resolution of security incidents. The 'Incident Management' policy is available on Intranet. The process for reporting the incidents is also covered as part of annual refresher training.	• Inquired of the Cyber Security – Operations team manager regarding the 'Incident Management' policy and procedures document. • Inspected the 'Incident Management' policy document to determine whether it covered the aspects of the policy. • Inspected the 'Incident Management' policy and procedures documents to determine whether the guidelines for reporting, categorization, and resolution of security incidents were defined. • Inspected the intranet portal to determine whether the 'Incident Management' policy and procedure documents were available on the intranet. • Inspected the training content for refresher training to determine whether incident management guidelines were covered as part of the training. • For a selection of employees, inspected the attendance sheet to determine if the incident management guidelines were communicated to the employees.	No relevant exceptions noted
	Security Incident Response Team (SIRT) is responsible for designing, developing, implementing and monitoring controls relevant to security, availability and confidentiality at HighRadius.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding SIRT. • Inspected the 'Roles and Responsibilities' policy and procedure documents to determine whether the responsibility for designing, developing, implementing	No relevant exceptions noted

7.0 Common Criteria Related to System Operations			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		and monitoring controls relevant to security, availability and confidentiality at HighRadius were assigned to SIRT.	
	Priority for Defects and Service Disruptions are classified and documented by the TechSupport team within the ticketing tool.	• Inquired of the TechSupport Team Manager regarding the priorities defined for managing defects and service disruptions raised. • For a selection of defects and service disruptions, inspected the Genie ticketing tool to determine whether priority for defects and service disruptions were classified and documented within the tool by the TechSupport team.	No relevant exceptions noted
	The TechSupport team resolves the Defect and Service Disruption requests and changes the status of the requests to 'Closed' within the ticketing tool.	• Inquired of the TechSupport team manager regarding the defects and service disruptions. • For a selection of defects and service disruptions raised, inspected the ticket details to determine whether the requests were resolved by the TechSupport team. • For the above selection of defects and service disruptions, inspected the Genie ticketing tool to determine whether TechSupport team changed the status of the defects and service disruptions to 'Closed' upon resolution.	No relevant exceptions noted
	Upon closure of Defect and Service Disruption requests, TechSupport team performs and documents the Root Cause Analysis (RCA) within the ticketing tool or communicates over an email.	• Inquired of the TechSupport Team Manager regarding the documentation of Root Cause Analysis (RCA) of defects and service disruptions. • For a selection of defects and service disruptions raised, inspected the ticket details to determine whether the	No relevant exceptions noted

7.0 Common Criteria Related to System Operations			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		TechSupport team performed and documented the RCA. • For the above selection of defects and service disruptions, inspected the ticket details to determine whether Tech Support team communicated the RCA details to affected users within the Genie ticketing tool or over an email.	
	Security incidents are registered with the Cyber Security - Operations team using the internal ticketing tool or by sending an e-mail.	• Inquired of the Cyber Security – Operations Team Manager regarding the reporting and tracking of security incidents. • For a selection of security incidents, inspected the internal incident ticketing tool, ticket details and Security incident e-mails to determine whether the security incidents were registered and tracked through the Genie ticketing tool or by e-mails.	No relevant exceptions noted
	HighRadius has a formal change management procedure documented within the 'Operations Security' policy, which describes the procedures designed to help ensure that only authorized, tested, and documented changes are made to the system.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the change management procedure at HighRadius. • Inspected the change management process within the 'Operations Security' policy and procedure documents to determine whether the procedure designed to help ensure that only authorized, tested, and documented changes were made to the system was defined.	No relevant exceptions noted

8.0 Common Criteria Related to Change Management			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	HighRadius has a formal change management procedure documented within the 'Operations Security' policy, which describes the procedures designed to help ensure that only authorized, tested, and documented changes are made to the system.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the change management procedure at HighRadius. • Inspected the change management process within the 'Operations Security' policy and procedure documents to determine whether the procedure designed to help ensure that only authorized, tested, and documented changes were made to the system was defined.	No relevant exceptions noted
	HighRadius production, non-production, and infrastructure changes are initiated, approved, and tracked within HighRadius' internal ManageEngine – Genie tool. Upon receipt of approval from line manager, IMS team member implements the change	• Inquired of the IMS team manager regarding the network and infrastructure changes. • For a selection of changes, inspected the change tickets raised in the tool to determine whether the network and infrastructure changes were initiated, documented and tracked within the tool. • For the above selection of changes, inspected the communication of approval from line manager to determine whether the network and infrastructure changes were implemented by the IMS team after the respective line manager approval.	No relevant exceptions noted
	Changes related to system software, firewall and network system services are raised as appropriate change requests by the IMS team in ManageEngine – Genie tool.	• Inquired of the IMS team manager regarding the changes related to system software, firewall and network system services. • For a selection of changes, inspected the change tickets raised in the tool to determine whether the changes were raised as per change requests by the IMS team in IT Helpdesk portal.	No relevant exceptions noted

8.0 Common Criteria Related to Change Management			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	Change Requests are classified by the Product teams within the internal ticketing tool.	• Inquired of the Product Team Manager regarding the classification process for Change Requests (CR). • For a selection of change requests, inspected the JIRA ticketing tool to determine whether the change request was classified by the Product teams.	No relevant exceptions noted
	Product teams continuously monitor the internal ticketing tool for Change Requests logged and acknowledge the requests by changing the status of the ticket to "Open".	• Inquired of the Product Team Manager regarding the ticketing tool for Change Requests. • For a selection of change requests, inspected the JIRA ticketing tool to determine whether the Product team acknowledged the change requests by changing the status to 'Open'.	No relevant exceptions noted
	Product teams at HighRadius develop the required changes and communicate the same to the user entity.	• Inquired of the Product Team Manager regarding the Change Requests (CR) management procedure. • For a selection of change requests, inspected the change tickets to determine whether the Product team developed the required changes and communicated the same to the user entity.	No relevant exceptions noted
	Emergency changes are logged, authorized, and documented as per the emergency change management procedure defined.	• Inquired of the Product Team Manager regarding the emergency change management procedure. • Inspected the emergency change management procedure within the 'Operations Security' policy and procedure documents to determine whether the procedure for emergency change management was defined and documented. • For a selection of emergency changes raised, inspected	No relevant exceptions noted

8.0 Common Criteria Related to Change Management			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		the change tickets to determine whether emergency changes were logged, authorized, and documented as per the emergency change management process defined.	
	Upon resolution of Change Request, Product teams update the requests with the solution provided along with details of the change release and then the status of the ticket is changed to "Closed" or "Resolved".	• Inquired of the Product manager regarding the Change Request (CR) management procedure. • For a selection of change requests, inspected the change tickets to determine whether the Product team updated the change requests with a brief description of the solution provided along with the details of the change release. • For the above selection of change requests, inspected the JIRA ticketing tool to determine whether the Product team changed the status of the change requests to 'Closed' or 'Resolved'.	No relevant exceptions noted
	User Acceptance Testing (UAT) is performed by the user entity in the UAT environment. Upon successful completion of UAT, UAT sign-off is obtained from the user entity.	• Inquired of the Vice President – Consulting team regarding the process of obtaining UAT signoffs for product related changes. • Inspected the 'Operation Security Procedure' document to determine whether steps for User Acceptance Testing (UAT) and go-live were defined and documented. • For a selection of cloud application implementations, inspected the UAT details to determine whether UAT was performed by the user entity in the UAT environment. • For the above selection of cloud application implementations, inspected the change records to	No relevant exceptions noted

8.0 Common Criteria Related to Change Management			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		determine whether UAT sign-off was obtained from the user entity upon successful completion of UAT.	
	Application products are designed in accordance with industry accepted security standards (i.e. OWASP for web applications) and comply with applicable regulatory and business requirements.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the designing of application products with industry accepted standards. • Inspected the 'Information Systems Acquisition Development and Maintenance' policy to determine whether a policy was in place to provide guidance in designing applications or products in accordance with Open Web Application Security Project (OWASP).	No relevant exceptions noted
	HighRadius communicates the cutover plan to the user entity prior to implementation and upon go-live confirmation, the Cloud Engineering team migrates the final product onto the on-demand cloud portal.	• Inquired of the Vice President – Consulting team regarding go-live approval for product related changes. • Inspected the 'Operation Security Procedure' document to determine whether steps for User Acceptance Testing (UAT) and go-live were defined and documented. • For a selection of cloud application implementations, inspected the records to determine whether the cutover plan was communicated by HighRadius prior to implementation. • For the above selection of cloud application implementations, inspected the records to determine whether the Cloud Engineering team migrated the final product onto the on-demand cloud portal in a timely manner.	No relevant exceptions noted

8.0 Common Criteria Related to Change Management			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	Relevant security patches are updated on workstations. The patches are implemented as per predefined patch management process.	• Inquired of the IMS Team Manager regarding the security patch management process for workstations. • Inspected the security patch management procedure within the 'Patch Management' policy and procedure documents to determine whether the procedure for security patch management was defined and documented. • For a selection of workstations, inspected the system configuration to determine whether relevant security patches were updated as per predefined patch management process.	No relevant exceptions noted
	Relevant security patches are updated on servers. The patches are implemented post approval from the respective department heads and post testing of patches in the staging environment.	• Inquired of the IMS Team Manager regarding the security patch management process for HighRadius' servers. • For a selection of quarters, inspected the approval communication and patch test results for implementation of security patches on servers to determine whether the patches were implemented as per the defined patch management process. • For the above selection of quarters, inspected the list of patches deployed on servers to determine whether the security patches were pushed from the server post approvals.	**Exception noted:** For one out of two quarterly patching schedules selected, it was noted that 11 out of 12 production environments were not implemented with relevant security patches in Q2 2023. Further, we were informed by the CTO that a verbal approval for the same was granted by the CTO at the beginning of Q2 2023 to omit and reschedule the patching of the 11 production

8.0 Common Criteria Related to Change Management			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
			environments. **Management response:** The patching process is managed by the Cloud Engineering team. In Q2, the team was managing several critical programs in addition to working on identifying automation opportunities for the patching process. Hence, as an exception, the CTO had granted a verbal approval in Q2 to delay the planned patches since there were no critical security patches outstanding for Q2. This approval was also regularized through an email approval in Q3. **Action taken:** Subsequently, in Q3, the pending patches were deployed.

8.0 Common Criteria Related to Change Management			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	Network monitoring tool is installed to monitor the availability of the network devices and server. The monitoring tool is configured to generate an alert for any exceptions identified. Alerts generated are monitored by the IMS team.	• Inquired of the IMS team manager regarding the network monitoring tool in place for HighRadius network. • Inspected the configuration of the monitoring tool to determine whether tool was configured to monitor the availability of the network devices and servers. • Inspected the configuration of the monitoring tool to determine whether tool was configured to generate an alert for any exceptions identified. • Inspected the incident dashboard to determine whether the alerts generated were monitored. • Further, inspected the ticket raised to determine whether the alerts generated were tracked to closure.	No relevant exceptions noted

9.0 Common Criteria Related to Risk Mitigation			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	HighRadius has a detailed 'Risk Management standard' document.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the 'Risk Management standard' document. • Inspected the 'Risk Management standard' document to determine whether the document covered the areas pertaining to risk management in detail. • Inspected the 'Risk Management standard' document to determine whether the document was reviewed and approved on an annual basis.	No relevant exceptions noted
	As a part of risk assessment, VP – Cyber Security - Risk & Compliance team in concurrence with department heads of various departments / functions, assess the risk with their preview and share the findings / draft report / risk assessment plan / risk treatment plan with Cyber Security team.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding findings / draft report / risk assessment plan / risk treatment plan prepared in concurrence with department heads of various departments / functions post assessing the risk with their preview. • Inspected the risk assessment report and treatment plan to determine whether the department heads assessed the risk and shared the findings with the Cyber Security team.	No relevant exceptions noted

9.0 Common Criteria Related to Risk Mitigation			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	HighRadius has formal 'Business Continuity Plan' (BCP) in place. BCP is reviewed and approved by VP - Cyber Security on a yearly basis.	• Inquired of the Cyber Security – Risk & Compliance Team Manager regarding the 'Business Continuity Plan'. • Inspected the 'Business Continuity Plan' (BCP) to determine whether the plan was documented, reviewed, and approved. • Further, inspected the approval records to determine whether the BCP was reviewed and approved by VP - Cyber Security on a yearly basis.	No relevant exceptions noted
9.2 The entity assesses and manages risks associated with vendors and business partners.	Cyber Security – Risk & Compliance team performs information security risk assessment for new vendors at the time of onboarding and for existing vendors on an annual basis. Issues of non-compliance from assessments are tracked to closure.	• Inquired of the Cyber Security – Risk & Compliance Team Manager regarding the information security risk assessment process followed for new and existing vendors. • For a selection of new vendors of HighRadius, inspected the risk assessment report to determine whether information security risk assessment was performed, and appropriate actions were taken, if any. • For a selection of existing vendors of HighRadius, inspected the annual vendor risk assessment report to determine whether information security risk assessment was performed, and appropriate actions were taken, if any.	No relevant exceptions noted
	The objective description of the HighRadius system and its boundaries are communicated to authorized internal and external system users as follows: Internal:	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the communication of objective description to authorized internal and external system users.	No relevant exceptions noted

9.0 Common Criteria Related to Risk Mitigation			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	· 'Information Security' policies and procedures are documented and available on corporate intranet for authorized users. · Employees joining HighRadius attend training sessions on 'Information Security' policies and related procedures. User Entity: · HighRadius enters into a 'Master Service Agreement' (MSA) with the user entities for the services relating to on-demand receivables. The agreement covers the scope and definition of services related to hosting and support services of the on- demand receivables. Project scope, deliverables, roles and responsibilities are documented in the SOW along with detailed service commitments from HighRadius.	• Inspected the 'Information Security' policies and procedures defined and documented to determine whether the aspects of the policy were covered as part of the documents. • Inspected the intranet to determine whether the 'Information Security' policy and procedure documents were available on the intranet portal. • For a selection of new joiners, inspected the induction training records to determine whether the new joiners attended the training on 'Information Security' policy and procedures as a part of their initial induction program. • For a selection of user entities, inspected the MSA signed between HighRadius and user entities to determine whether the agreement covered the scope and definition of services related to hosting and support services of the on-demand receivables. • Inspected the SOW to determine whether project scope, deliverables, roles and responsibilities were documented in the SOW along with detailed service commitments from HighRadius.	
	The security, availability, confidentiality commitments and processing integrity of HighRadius are communicated to user entities through relevant sections in the Master Service Agreements (MSA) and Statement of Work (SOW)	• Inquired of the Cyber Security – Risk & Compliance team manager regarding security, availability, confidentiality commitments and processing integrity of HighRadius to user entities. • Inspected the MSA and SOWs to determine whether the security, availability, confidentiality commitments and processing integrity of HighRadius were communicated to user entities through relevant sections in the Master	No relevant exceptions noted

9.0 Common Criteria Related to Risk Mitigation			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		Service Agreements and the SOWs	
	HighRadius reviews the System and Organization Control (SOC) reports of its data centers on an annual basis to verify whether the security, availability, confidentiality and processing integrity commitments and requirements of the data centers are in line with HighRadius' commitments.	• Inquired of Cyber Security – Risk & Compliance team regarding the review of SOC reports of its data centers. • Inspected the SOC review report to determine whether the Cyber Security – Risk & Compliance team reviews the SOC reports of its data centers on an annual basis to verify whether the security, availability, confidentiality and processing integrity commitments and requirements of the data centers are in line with HighRadius's commitments.	No relevant exceptions noted

Additional Criteria for Availability			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
1.1 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.	Network monitoring tool is installed to monitor the availability of the network devices and server. The monitoring tool is configured to generate an alert for any exceptions identified. Alerts generated are monitored by the IMS team.	• Inquired of the IMS team manager regarding the network monitoring tool in place for HighRadius network. • Inspected the configuration of the monitoring tool to determine whether tool was configured to monitor the availability of the network devices and servers. • Inspected the configuration of the monitoring tool to determine whether tool was configured to generate an alert for any exceptions identified. • Inspected the incident dashboard to determine whether the alerts generated were monitored.	No relevant exceptions noted
1.2 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.	HighRadius has defined policy and procedures which provide guidelines for performing backup and restoration of HighRadius information systems.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the 'Backup and Restoration' policy. • Inspected the 'Backup and Restoration' policy to determine whether the guidelines to perform backup and restoration were defined and documented.	No relevant exceptions noted
	UPS is installed within the premises of HighRadius facilities in Bhubaneswar, India and Hyderabad, India to support during a power failure or shutdown.	• Inquired of the Administration Team Manager regarding power backup facilities. • Performed physical walkthrough of HighRadius Bhubaneswar and Hyderabad facilities to determine whether UPS sets were installed. • For a selection of quarters, inspected the preventive maintenance records to determine whether quarterly	No relevant exceptions noted

Additional Criteria for Availability			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		checks were performed on the UPS and results were documented.	
	Air-conditioners are installed inside the network room and hub room to control and maintain temperature. A security personnel monitors and records the temperature in the server room and hub room every six hours.	• Inquired of the Administration Team Manager regarding the temperature monitoring within the network room and hub room. • Performed physical walkthrough of HighRadius Bhubaneswar and Hyderabad facilities to determine whether air conditioners were installed inside the network room and hub room. • For a selection of days, inspected the temperature register maintained within the network room and hub room to determine whether temperature was being monitored and logged by the administration team every six hours.	No relevant exceptions noted
	BMS team performs the fire drill on a yearly basis and records the results.	• Inquired of the BMS team manager regarding the fire drills. • Inspected the annual fire drill report to determine whether the annual fire drills were conducted, and results were documented.	No relevant exceptions noted

Additional Criteria for Availability			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	Automated full backups of HighRadius applications and data are performed as per the defined backup frequency.	• Inquired of the database team regarding backup of HighRadius applications and data. • Inspected the automated backup configuration of production databases and servers to determine whether the backups were configured as per the defined frequency. • For a selection of days, weeks and months inspected the backup log to determine whether daily, weekly, and monthly backups were performed.	No relevant exceptions noted
	Restorations tests are performed by database team on a quarterly basis to ensure that the back-up data is readable and restorable.	• Inquired of the database team regarding quarterly restoration test performed to ensure that the back-up data is readable and restorable. • For a selection of quarters, inspected the restoration reports to determine whether tests were performed to ensure that the back-up data was readable and restorable.	No relevant exceptions noted
	Smoke detectors and fire extinguishers are available in the work area where computer systems are housed and are installed at strategic points where they can be accessed easily.	• Inquired of the Administration Team Manager regarding the smoke detectors and fire extinguishers installed. • Performed walkthrough of HighRadius Bhubaneswar, Hyderabad, and Houston facilities through physical observation and video conferencing to determine whether smoke detectors and fire extinguishers were available in the work area where computer systems were housed and were installed at strategic points where they can be accessed easily.	No relevant exceptions noted

Additional Criteria for Availability			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	Fire safety equipment is checked on a quarterly basis for Hyderabad, India and semi-annual basis for Houston, USA. Checks are conducted and documented in accordance with the manufacturer's instructions.	• Inquired of the Administration Team Manager regarding the maintenance of fire safety equipment. • For a selection of quarters, inspected the maintenance records for Hyderabad location to determine whether the quarterly checks were performed on the fire safety equipment and results were documented. • Inspected the maintenance records for Houston location to determine whether the semi-annual checks were performed on the fire safety equipment and results were documented.	No relevant exceptions noted
	Fire and emergency instructions are displayed in prominent locations within facility.	• Inquired of the Administration Team Manager regarding display of fire and emergency instructions in prominent locations. • Performed walkthrough of Hyderabad and Houston facilities through physical observation and video conferencing respectively to determine whether fire and emergency instructions were displayed within the facilities in prominent locations.	No relevant exceptions noted
1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.	BMS team performs the fire drill on a yearly basis and records the results.	• Inquired of the BMS team manager regarding the fire drills. • Inspected the annual fire drill report to determine whether the annual fire drills were conducted, and results were documented.	No relevant exceptions noted
	On an annual basis, a mock drill is conducted by the Cloud Engineering team to test effectiveness of DR site by switching the	• Inquired of the Cloud Engineering team manager regarding the annual mock drill.	No relevant exceptions noted

Additional Criteria for Availability			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	critical application and its database instances from production environment to DR site.	• Inspected the annual mock drill report to determine whether IMS team tested effectiveness of DR site by switching the critical application and its database instances from production environment to DR site.	
	HighRadius has formal 'Business Continuity Plan' (BCP) in place. BCP is reviewed and approved by VP - Cyber Security on a yearly basis.	• Inquired of the Cyber Security – Risk & Compliance Team Manager regarding the 'Business Continuity Plan'. • Inspected the 'Business Continuity Plan' (BCP) to determine whether the plan was documented, reviewed, and approved. • Further, inspected the approval records to determine whether the BCP was reviewed and approved by VP - Cyber Security on a yearly basis.	No relevant exceptions noted
	'IT Disaster Recovery Plan' is established, documented, and approved by VP- Cyber Security.	• Inquired of IMS Team Manager regarding the 'IT Disaster Recovery Plan'. • Inspected the 'IT Disaster Recovery Plan' to determine whether disaster recovery plan was established and documented. • Further, inspected the approval records to determine whether 'IT Disaster Recovery Plan' was approved by the VP - Cyber Security – Risk & Compliance.	No relevant exceptions noted

Additional Criteria for Confidentiality			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
1.1 The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	Automated full backups of HighRadius applications and data are performed as per the defined backup frequency.	• Inquired of the database team regarding backup of HighRadius applications and data. • Inspected the automated backup configuration of production databases and servers to determine whether the backups were configured as per the defined frequency. • For a selection of days, weeks and months inspected the backup log to determine whether daily, weekly, and monthly backups were performed.	No relevant exceptions noted
	Restorations tests are performed by database team on a quarterly basis to ensure that the back-up data is readable and restorable.	• Inquired of the database team regarding quarterly restoration test performed to ensure that the back-up data is readable and restorable. • For a selection of quarters, inspected the restoration reports to determine whether tests were performed to ensure that the back-up data was readable and restorable.	No relevant exceptions noted
	HighRadius has documented 'Information Classification' policy based upon the sensitivity and confidentiality of data. Data or information in HighRadius is classified into four categories given below: Public; Internal; Confidential; and	• Inquired of the Cyber Security – Risk & Compliance team manager regarding 'Information Classification' policy. • Inspected the 'Information Classification' policy to determine whether data or information in HighRadius is classified into four categories as Public, Internal, Confidential and Restricted.	No relevant exceptions noted

Additional Criteria for Confidentiality			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	Restricted		
	Formal data retention and disposal procedures are defined and documented within 'Operation Security' procedure to guide the secure disposal of the company's data	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the formal data retention and disposal policy and procedure documents. • Inspected the data retention and disposal procedure within the 'Operation Security' policy and procedure documents to determine whether the guidelines to dispose company data securely were defined.	No relevant exceptions noted
	Cyber Security – Risk & Compliance team performs information security risk assessment for new vendors at the time of onboarding and for existing vendors on an annual basis. Issues of non-compliance from assessments are tracked to closure.	• Inquired of the Cyber Security – Risk & Compliance Team Manager regarding the information security risk assessment process followed for new and existing vendors. • For a selection of new vendors of HighRadius, inspected the risk assessment report to determine whether information security risk assessment was performed, and appropriate actions were taken, if any. • For a selection of existing vendors of HighRadius, inspected the annual vendor risk assessment report to determine whether information security risk assessment was performed, and appropriate actions were taken, if any.	No relevant exceptions noted

Additional Criteria for Confidentiality			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
1.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	HighRadius has documented 'Information Classification' policy based upon the sensitivity and confidentiality of data. Data or information in HighRadius is classified into four categories given below: Public; Internal; Confidential; and Restricted.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding 'Information Classification' policy. • Inspected the 'Information Classification' policy to determine whether data or information in HighRadius is classified into four categories as Public, Internal, Confidential and Restricted.	No relevant exceptions noted
	HighRadius has established documented procedures to dispose confidential information post retention period.	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the policies and procedures for disposing of confidential information post retention period. • Inspected the 'Operations Security' policy and procedure documents to determine whether procedure for disposal of confidential information post retention period.	No relevant exceptions noted
	Formal data retention and disposal procedures are defined and documented within 'Operation Security' procedure to guide the secure disposal of the company's data	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the formal data retention and disposal policy and procedure documents. • Inspected the data retention and disposal procedure within the 'Operation Security' policy and procedure documents to determine whether the guidelines to dispose company data securely were defined.	No relevant exceptions noted

Additional Criteria for Processing Integrity			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
1.1 The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.	HighRadius has documented 'Server and Firewall Hardening Standard' policy and procedures for its servers and 'End User Device Hardening Standards' document for its end user systems in order to provide a controlled operating environment and to prevent any unauthorized access to critical system resources.	• Inquired of Cyber Security – Risk & Compliance team manager regarding the hardening guidelines for servers and end user systems. • Inspected the 'Server and Firewall Hardening Standard' and 'End User Device Hardening Standards' document to determine whether hardening standards for servers and end user system were available to provide a controlled operating environment and to prevent any unauthorized access to critical system resources	No relevant exceptions noted
1.2 The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.	Cyber Security – Operations team performs a full static code analysis (security) on a monthly basis and an incremental static code analysis (security) on a weekly basis of changes prior to release. Issues of non-compliance from analysis are tracked to closure.	• Inquired of the Cyber Security – Operations team manager regarding the static security code review process. • For a selection of months, inspected the reports for static security code review to determine whether monthly full static security code reviews were performed on changes prior to release by the Cyber Security – Operations team. • Further, inspected the communication for remediation to determine whether the non-compliances from assessments were getting resolved and tracked to closure. • For a selection of weeks, inspected the reports for static security code review to determine whether weekly incremental static security code reviews were performed on changes prior to release by the Cyber Security team.	No relevant exceptions noted

Additional Criteria for Processing Integrity			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
		• Further, inspected the communication for remediation to determine whether the non-compliances from assessments were getting resolved and tracked to closure.	
1.3 The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.	Automated full backups of HighRadius applications and data are performed as per the defined backup frequency.	• Inquired of the database team regarding backup of HighRadius applications and data. • Inspected the automated backup configuration of production databases and servers to determine whether the backups were configured as per the defined frequency. • For a selection of days, weeks and months inspected the backup log to determine whether daily, weekly, and monthly backups were performed.	No relevant exceptions noted
1.4 The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.	Formal data retention and disposal procedures are defined and documented within 'Operation Security' procedure to guide the secure disposal of the company's data	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the formal data retention and disposal policy and procedure documents. • Inspected the data retention and disposal procedure within the 'Operation Security' policy and procedure documents to determine whether the guidelines to dispose company data securely were defined.	No relevant exceptions noted

Additional Criteria for Processing Integrity			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	Access to application production servers is restricted to Cloud Engineering team.	• Inquired of the Cloud Engineering team manager regarding the access to application production servers. • Inspected the system generated list of user IDs with access to application production servers and compared it with the HR active list of users to determine whether access to application production servers was restricted to Cloud Engineering team.	No relevant exceptions noted
1.5 The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.	User Acceptance Testing (UAT) is performed by the user entity in the UAT environment. Upon successful completion of UAT, UAT sign-off is obtained from the user entity.	• Inquired of the Vice President – Consulting team regarding the process of obtaining UAT signoffs for product related changes. • Inspected the 'Operation Security Procedure' document to determine whether steps for User Acceptance Testing (UAT) and go-live were defined and documented. • For a selection of cloud application implementations, inspected the UAT details to determine whether UAT was performed by the user entity in the UAT environment. • For the above selection of cloud application implementations, inspected the change records to determine whether UAT sign-off was obtained from the user entity upon successful completion of UAT.	No relevant exceptions noted

Additional Criteria for Processing Integrity			
Criteria Description	**HighRadius's Control Description**	**KPMG's Test Procedures**	**Results of Testing**
	HighRadius communicates the cutover plan to the user entity prior to implementation and upon go-live confirmation, the Cloud Engineering team migrates the final product onto the on-demand cloud portal.	• Inquired of the Vice President – Consulting team regarding go-live approval for product related changes. • Inspected the 'Operation Security Procedure' document to determine whether steps for User Acceptance Testing (UAT) and go-live were defined and documented. • For a selection of cloud application implementations, inspected the records to determine whether the cutover plan was communicated by HighRadius prior to implementation. • For the above selection of cloud application implementations, inspected the records to determine whether the Cloud Engineering team migrated the final product onto the on-demand cloud portal in a timely manner.	No relevant exceptions noted

ANNEXURE: LIST OF ABBREVIATIONS

Abbreviation	Expanded Form
AD	Active Directory
AES	Advanced Encryption Standard
AICPA	American Institute of Certified Public Accountants
AWS	Amazon Web Services
BAU	Business-as-usual
BCP	Business Continuity Plan
BGV	Background Verification Checks
BMS	Building Management System
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CI	Continuous Integration
CISO	Chief Information Security Officer
CPA	Claims and POD Automation
CR	Change Request
DoS	Denial-of-Service
DDoS	Distributed Denial-of-Service
DR	Disaster Recovery
EMT	Emergency Management Team
FIM	File Integrity Monitoring
HIPAA	Health Insurance Portability and Accountability Act
HR	Human Resource
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
IMS	Infrastructure Management System
IPS	Intrusion Prevention System
ISMS	Information Security Management System
ISO	International Standards Organization
ITA	Invoice Tracing Automation

Abbreviation	Expanded Form
MD	Managing Director
MSA	Master Service Agreement
MSS	Managed Security Services
NDA	Non-Disclosure Agreements
OS	Operating System
OWASP	Open Web Application Security Project
QA	Quality Assurance
RA	Risk Assessment
RCA	Root Cause Analysis
RoI	Return on Investment
RPO	Recovery Point Objective
RTA	Retail Trade Agreement
RTO	Recovery Time Objective
SDLC	Software Development Lifecycle
SIEM	Security Incident and Event Management
SIRT	Security Incident Response Team
SMG	Senior Management Group
SOC	System and Organization Controls
SOW	Statement of Work
TCO	Total Cost of Ownership
TSC	Trust Service Criteria
TSP	Trust Service Principles
UAT	User Acceptance Testing
VAPT	Vulnerability Assessment and Penetration Testing
VP	Vice President
VPN	Virtual Private Network