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

15 May 2024

Attention: Mr. Bhanu Bobba, Managing Director

KPMG Assurance and Consulting Services LLP (herein after referred to as "KPMG", "We", "Our") have completed SOC 1 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 SOC1 Type 2 examination.

The data included in this report was obtained from you, on or before 23 April 2024. We have no obligation to update our report or to revise the information contained therein to reflect events and transactions occurring subsequent to 23 April 2024. 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 1 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 1) Type 2 Report

Report on description of system, suitability of design and operating effectiveness of controls related to cloud-based application implementation and hosting services, application support services and supporting general operating environment provided by HighRadius Technologies Private Limited and HighRadius Corporation from the delivery centres located in Bhubaneswar, India; Hyderabad, India; and Houston, USA.

For the period 1 April 2023 to 31 March 2024

TABLE OF CONTENTS

SECTION 1

INDEPENDENT SERVICE AUDITOR'S 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 REPORT

To,

The Board of Directors,
HighRadius Technologies Private Limited

Scope

We have examined HighRadius Technologies Private Limited (a wholly owned subsidy of HighRadius Corporation) and HighRadius Corporation (hereinafter collectively referred to as "HighRadius" or "service organization") description of its system 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 its delivery centers located at Hyderabad, India; Bhubaneswar, India; and Houston, USA throughout the period 1 April 2023, to 31 March 2024 ("description") and the suitability of the design and operating effectiveness of the controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "HighRadius's assertion" ("assertion"). The controls and control objectives included in the description are those that management of HighRadius believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of HighRadius's system that are not likely to be relevant to user entities' internal control over financial reporting.

HighRadius uses 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 for hosting the application servers and databases in the datacenters to perform some of the services provided to user entities that are likely to be relevant to those user entities' internal control over financial reporting. The description includes only the control objectives and related controls of HighRadius and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by HighRadius can be achieved only if complementary subservice organization controls assumed in the design of HighRadius's controls are suitably designed and operating effectively, along with the related controls at HighRadius. Our examination did not extend to controls of the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of HighRadius's controls are suitably designed and operating effectively, along with related controls at HighRadius. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

In section 2, HighRadius has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. HighRadius is responsible for preparing the description and its assertion, including the completeness, accuracy, and method of presentation of the description and assertion, providing the services covered by the description, specifying the control

objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and International Standard on Assurance Engagements 3402, "Assurance Reports on Controls at a Service Organization," issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented, and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period 1 April 2023, to 31 March 2024. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion,
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description,
- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved,
- evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization in its assertion.

Service Auditor's Independence and Quality Management

We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA and International Ethics Standards Board for Accountants. We have also applied the statements on quality control standards established by the AICPA and International Standard on Quality Management 1 and accordingly maintain a comprehensive system of quality management.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives stated in the description is subject to the risk that controls at a service organization may become ineffective.

Description of Tests of Controls

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

Opinion

In our opinion, in all material respects, based on the criteria described in HighRadius's assertion:

a) the description fairly presents HighRadius's system for providing cloud-based application implementation and hosting services, application support services and supporting General Operating Environment that was designed and implemented throughout the period 1 April 2023, to 31 March 2024;

b) the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period from 1 April 2023 to 31 March 2024, and subservice organization(s) and user entities applied the complementary controls assumed in the design of HighRadius's controls throughout the period 1 April 2023, to 31 March 2024; and

c) the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period 1 April 2023, to 31 March 2024 if complementary subservice organization and user entity controls, assumed in the design of HighRadius's controls, operated effectively throughout the period 1 April 2023, to 31 March 2024.

Restricted Use

This report, including the description of tests of controls and results thereof in section 4, is intended solely for the information and use of management of HighRadius, user entities of HighRadius's system during some or all of the period 1 April 2023, to 31 March 2024, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. 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

23 April 2024

SECTION 2

STATEMENT BY THE SERVICE ORGANIZATION

HIGHRADIUS' ASSERTION[1]

We have prepared the 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") system for providing cloud-based application implementation and hosting services, application support services and supporting General Operating Environment for processing user entities' transactions from their delivery centers located at Hyderabad, India; Bhubaneswar, India; and Houston, USA throughout the period 1 April 2023, to 31 March 2024 (description) for user entities of the system during some or all of the period 1 April 2023, to 31 March 2024, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities of the system themselves, when assessing the risks of material misstatement of user entities' financial statements.

HighRadius uses 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 for hosting the application servers and databases in the datacenters to perform some of the services provided to user entities that are likely to be relevant to those user entities' internal control over financial reporting. The description includes only the control objectives and related controls of HighRadius and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified in the description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively along with the related controls at HighRadius. The description does not extend to controls of the subservice organizations.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of HighRadius's controls are suitably designed and operating effectively, along with related controls at HighRadius. The description does not extend to controls of the user entities.

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

(a) The description fairly presents HighRadius's system made available to user entities of the system during some or all of the period 1 April 2023, to 31 March 2024 for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description

   i. presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, if applicable,

      - the types of services provided including, as appropriate, the classes of transactions processed;
      - the procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system;
      - the information used in the performance of the procedures, including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities;
      - how the system captures and addresses significant events and conditions other than transactions;
      - the process used to prepare reports and other information for user entities;
      - services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them;
      - the specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the service organization's controls;

[1] *The service organization's "assertion" is equivalent to the service organization's "statement" as defined under ISAE 3402.*

- other aspects of our control environment, risk assessment process, information, and communications (including the related business processes), control activities and monitoring activities that are relevant to the services provided.

ii. includes relevant details of changes to HighRadius's system during the period covered by the description.

iii. does not omit or distort information relevant to HighRadius's system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their auditors, and may not, therefore, include every aspect of the HighRadius's system that each individual user entity of the system and its auditor may consider important in its own particular environment.

(b) The controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period 1 April 2023, to 31 March 2024 to achieve those control objectives if sub service organizations and user entities applied the complementary controls assumed in the design of HighRadius's controls throughout the period 1 April 2023, to 31 March 2024. The criteria used in making this assertion were that:

i. the risks that threatened the achievement of the control objectives stated in the description have been identified by management of HighRadius;

ii. the controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and

iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

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 control objectives for the services provided from HighRadius delivery centres at Hyderabad and Bhubaneswar in India and Houston in USA during the period 1 April 2023, to 31 March 2024. HighRadius management is responsible for designing, implementing, and documenting the controls to meet the applicable control objectives.

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

Platform Name	Cloud Products
Autonomous Receivables (Order to Cash)	• Credit Management • Electronic Invoicing or EIPP (E-Invoice Presentment & Payment) • Cash Application Management • Deductions Management • Collections Management
B2B Payments	• Payment Gateway
Autonomous Treasury (Treasury & Risk)	• Cash Management • Cash Forecasting
RadiusOne AR Suite[2]	• 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[3]	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[4]	2107 CityWest Blvd Suite 1100, Houston, TX 77042

[2] *RadiusOne AR Suite was decommissioned, and services were terminated on 23-Oct-2023*

[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.*

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 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 3800+ professionals working from separate locations spread across India, US and EMEA. HighRadius provides services to 850+ 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 control objectives and related controls of HighRadius and excludes the relevant control objectives and related controls of the sub-service organizations. The control objectives 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 monitoring, the logs generated at server, firewall and end user. 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.

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 various 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 relevant control objectives and related 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 the 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. The Vice President – Cyber Security - Risk & Compliance periodically reviews information Security policies and related procedures 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 organizational 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 March 2024 showing the various functional groups is shown below:

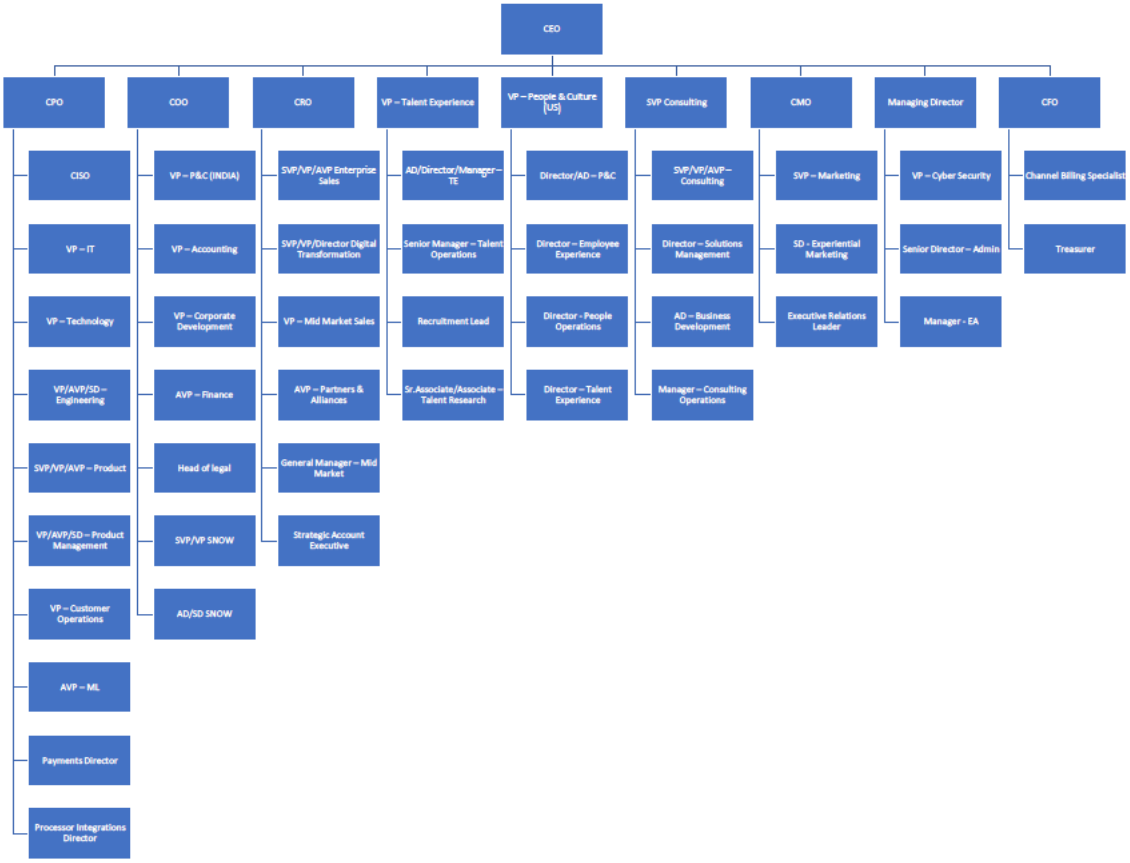

Figure 1 – Organization Structure

Acronyms used in HighRadius organization structure:

- CEO – Chief Executive Officer
- COO – Chief Operating Officer
- CAO – Chief Administrative Officer
- CPO – Chief Product Officer
- CMO - Chief Marketing Officer
- CFO – Chief Financial 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 distinct functions:

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

Cyber Security - Risk & Compliance

The team comprises of Cyber Security - Risk & Compliance - CISO, Vice President, 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. The team and the Audit Committee provide suggestions 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 joiner's 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-Virus, 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 take part 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. On the day of joining for new employees, security induction and POSH trainings are conducted by the L&D team and mandatory annual refresher POSH training is also conducted for existing employees of 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 manages 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, Commercial team performs sourcing of the requirements.

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 managed by the Head of Legal and Legal team.

Infrastructure Management Services (IMS) team

The IMS team is represented by VP IT 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 corporate 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.

Cloud Engineering team

The Cloud Engineering team is represented by VP Technology and is responsible for Cloud Operations, Service Reliability, Cloud Security, Customer Reliability, Database Operations and designing, deploying, maintaining cloud infrastructure aligned to HighRadius business needs across its locations.

Service Delivery Functions

Service Delivery at HighRadius consists of various teams such as Sales & Marketing, Consulting, TechSupport, Implementation, Quality Assurance and Product Development. 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[56]

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 Bhubaneswar, India. 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.

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.

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.

System Account Management (Logical Access)

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

[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.*

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. With effect from 30 November 2023, Trend Micro Apex Central has been decommissioned and replaced with SentinelOne. 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.

Go-live and Hypercare sign-off

Cloud Engineering team is responsible for managing and overseeing the migration of applications to the cloud. The team ensures that necessary components of the applications are successfully migrated to the HighRadius cloud applications onto the production environment post User Acceptance Testing (UAT) sign-off from the user entities. Post Go-Live, HighRadius obtains Hypercare sign-off from the user entity. Hypercare enables prompt resolution of any issues or concerns upon Go-Live.

Service Request Management/HighFive Change Requests

Service requests or HighFive Change Requests are raised by HighRadius' customers using the Salesforce ticketing tool (HighFive). These requests are resolved by the TechSupport team in coordination with the respective customer support teams at HighRadius. HighRadius is not contractually obligated to respond/resolve these requests within a certain period.

Upon providing the requested resolution, the request ticket status is changed to "Waiting for client confirmation" status. Post client confirmation or if the customer confirmation is not received post three follow ups by the TechSupport team, the request status is changed to "solved" and the customer has a 7-day window to re-open the resolved ticket in case of any further related issues. Post completion of the 7-day period, the request ticket status is changed to "Closed".

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.

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.

Admin Tasks

Admin tasks are registered by HighRadius' customers using the Salesforce ticketing tool if customer needs help to perform a task.

Defects and Service Disruption Management

For defects and service disruptions, priorities are assigned to each ticket within the Salesforce ticketing tool (HighFive), and they are acknowledged and resolved by the TechSupport team 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.

Upon providing the requested resolution, the request ticket status is changed to "Waiting for client confirmation" status. Post client confirmation or if the customer confirmation is not received post three follow ups by the TechSupport team, the request status is changed to "Resolved" and the customer has a 7-day window to re-open the resolved ticket in case of any further related issues. Post completion of the 7-day period, the request ticket status is changed to "Closed".

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.

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 Product SNOW, Quality Assurance, Build and Release, and Cloud Engineering 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 SNOW team. CR contains detailed information such as priority, impact (based upon criticality of change request), ownership, and description of the change. Application Change Requests are classified by the Product SNOW team within Jira ticketing tool.

Development and testing of changes

Change is worked upon by the Product SNOW team. The JIRA ticketing tool is used for tracking the complete development process for the CR and is updated by the Product SNOW team**.** Once the change is developed, it is moved to the QA environment by the 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 resolution of Change Request, Product SNOW teams update the requests with the solution provided with details of the change release and change the status of the JIRA ticket to “Ready for release".

Migration to Production

The Build and Release team adds the CR to the subsequent release cycle. Further, the Cloud Engineering team deploys the application change to production environment using HADAM tool as part of the monthly sprint cycles.

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. With effect from 11 May 2023, Desktop Central has been decommissioned and replaced with Microsoft Intune.

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. The Vice President – Cyber Security - Operations and senior security engineer reviews results of such assessment 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. With effect from 30 November 2023, Trend Micro Apex Central has been decommissioned and replaced with SentinelOne. 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 ATP (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, the IMS team conducts a DR Test 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 24.4.0.

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 (Decommissioned on 30 November 2023)
5	SentinelOne	Anti-malware tool for production environment & end user devices
6	Open LDAP	Open-source directory access protocol
7	AD	Domain controller
8	SCP	Secure data transfer utility tool
9	Crontab	Job scheduling utility tool
10	Nessus	Vulnerability assessment tool
11	Secure Trust	Approved scanning vendor for PCI scans
12	Qualys Guard	Web application vulnerability scanner
13	Wi-Fi guard	Wireless scanning tool
14	CVS	Version control system for development
15	Gitlab	Code repository and version control system

S. No	Tools	Description
16	RSYSLOG	Logging utility for Linux systems
17	Jira	Used to track and manage changes
18	Desktop Central	Used to push patches to end user systems (Decommissioned on 11 May 2023)
19	Microsoft Intune	Used to push patches to end user systems
19	ESSL	Physical access control system (For Hyderabad)
20	Brivio	Physical access control system (For Westlake)
21	Monyog	DB monitoring tool
22	Bouncer	Query management system
23	Selenium	Automation testing tool
24	Salesforce	Customer relationship management system and used to track configuration changes, defects, and service disruptions
25	WhiteSource	Bug detecting tool
26	Checkmarx	Static code analysis tool
27	GTB and Netskope	Data loss prevention tool
28	Jenkins	Build & deployment tool
29	Securonix	Security Information and Event Monitoring tool
30	BitSight	Security ratings solution
31	NetSuite	Tool for creation of Invoices
32	Smartsheets	Project planning & delivery tracking tool
33	G-Suite	Business e-mail
34	New Relic	Application performance monitoring tool
35	PAMS	Privileged access management to HighRadius applications
36	CloudGuard Dome9	Cloud Security Posture Management solution

S. No	Tools	Description
37	Netskope CASB	Cloud Access Security Broker solution
38	Knowbe4	Security training tool
39	Akamai	Web Application Firewall and DoS prevention
40	JFrog	Manages and automates artifacts and binaries from start to finish during the application delivery process.
41	HADAM	HADAM (HighRadius Automated Deployment and Management) is an internal tool for scheduled and emergency production deployments.
42	Eclipse	The tool is used for Build and Deployment.
43	Sophos	The tool is used to monitor and permit/block incoming.
44	Fortigate	The tool is used to monitor and permit/block incoming
45	Global Protect	VPN to provide secure access to corporate networks & resources for remote users
46	FortiClient	VPN to provide secure access to corporate networks & resources for remote users (From 22 Aug 2023)
47	Cohesity	The tool is used to backup Critical production servers

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 HighRadius IMS 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 IMS 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 5.7.44 / MySQL 8.0
- 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, which is considered complete only if the associate passes the assessment.

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 organizational 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 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 for hosting the application servers and databases in the datacenters to perform some of the services provided to user entities that are likely to be relevant to those user entities' internal control over financial reporting. SOC (Service Organization Controls) reports of these data centers are reviewed on an annual basis by the Cyber Security – Risk & Compliance team to verify whether the commitments and requirements of the data centers are in line with HighRadius' commitments.

Control Activities

The organization's control objectives and related controls are included in Section 4 of this report, "Control Objectives, Related Controls and Tests of Operating Effectiveness", to eliminate the redundancy that would result from listing them in this section and repeating them in Section 4.

Although the control objectives and 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 achieve certain control objectives included in this report. 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.

Control Objective 1 – Cloud Application Implementation

- User entity is responsible for UAT testing and providing UAT sign-off to HighRadius.
- User entity is responsible for go-live date finalization.

Control Objective 2 - Service Request Management (HighFive Change Requests)

- User entity is responsible for registration of service requests (HighFive Change Requests) through the ticketing tool.

Control Objective 3 – Defects & Service disruption Management

- User entity is responsible for registration of defects and service disruptions through the ticketing tool.

Control Objective 7 – Logical Security

- 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 control objectives 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

Controls maintained by subservice organizations:
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

CONTROL OBJECTIVES, RELATED CONTROLS AND TESTS OF OPERATING EFFECTIVENESS

Cloud Application Implementation	**Controls provide reasonable assurance that cloud application implementation is performed based on the requirements agreed with the user entity that are analysed, documented, tested, and approved prior to release.**

Control No	Control Description	Test Performed	Results of Testing
1.1	Customer master details are updated and maintained on SalesForce CRM. 'Master Service Agreements' are established between HighRadius and service providers or user entities that include clearly defined terms, conditions, and responsibilities for the parties involved.	• Inquired of the Cyber Security – Risk & Compliance team regarding the customer master details on SalesForce CRM and '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 exceptions noted.
1.2	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 exceptions noted.

Control No	Control Description	Test Performed	Results of Testing
1.3	Cloud Engineering team migrates the HighRadius cloud applications onto the production environment post UAT sign-off from the user entities. Post Go-Live HighRadius obtains Hypercare sign-off from user entity.	• 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 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. • For the above selection of cloud application implementations, inspected the records to determine whether Hypercare sign-off was obtained from the user entity.	No exceptions noted.

Complementary User Entity Controls	• User entity is responsible for performing UAT testing and providing UAT sign-off to HighRadius. • User entity is responsible for go-live date finalization.
Conclusion	Based on the tests of operating effectiveness described above, the controls were operating with sufficient effectiveness to achieve this control objective.

Service Request Management (HighFive Change Requests)	**Controls provide reasonable assurance that Service Requests (HighFive Change Requests) raised through the ticketing tool are acknowledged, classified, and resolved.**

Control No	Description of Controls	Test Performed	Results of Testing
2.1	Formal procedures for managing and resolving Service Requests (HighFive Change Requests) are documented and available to users.	• Inquired of the Cyber Security – Risk & Compliance Team Manager regarding the formal procedures for managing configuration changes. • Inspected the 'New Case Classification' document to determine whether formal Service Request management procedures were defined and documented. • Inspected the corporate intranet to determine whether 'New Case Classification' document was hosted on the intranet and available to the users.	No exceptions noted.
2.2	TechSupport team continuously monitors the Sales Force ticketing tool for Service Requests (HighFive Change Requests) logged and acknowledges them by changing the status of ticket to "Open".	• Inquired of the TechSupport Team Manager regarding the Service Requests (HighFive Change Requests) raised by the user entity in the SalesForce ticketing tool. • For a selection of Service Requests (HighFive Change Requests) raised, inspected the ticket details to determine whether the TechSupport team acknowledged the Service Requests (HighFive Change Requests) raised by changing the status to "Open" within the Sales Force ticketing tool.	No exceptions noted.

Control No	Description of Controls	Test Performed	Results of Testing
2.3	Upon resolution, the TechSupport team changes the status of the Service Request (HighFive Change Requests) within the SalesForce ticketing tool to "Solved."	• Inquired of the TechSupport Team Manager regarding the Service Requests (HighFive Change Requests) raised by the user entity in the SalesForce ticketing tool. • For a selection of Service Requests (HighFive Change Requests) raised, inspected the Service Request tickets to determine whether the requests were resolved by the TechSupport team. • For the above selection of Service Requests (HighFive Change Requests), inspected the ticketing tool to determine whether the status of the Service Requests was changed to 'Solved' in the SalesForce tracking tool upon resolution.	No exceptions noted.

Complementary User Entity Controls	• User entity is responsible for registration of Service Requests through the ticketing tool.
Conclusion	Based on the tests of operating effectiveness described above, the controls were operating with sufficient effectiveness to achieve this control objective.

Defects and Service Disruption Management	**Controls provide reasonable assurance that Defects and Service Disruptions raised within the ticketing tool are classified, acknowledged, and resolved in a timely manner.**

Control No	Description of Controls	Test Performed	Results of Testing
3.1	Priority for Defects and Service Disruptions are classified and documented by the TechSupport team within the SalesForce 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 SalesForce ticketing tool to determine whether priority for defects and service disruptions were classified and documented within the tool by the TechSupport team.	No exceptions noted.
3.2	TechSupport team provides acknowledgement against the Defect and Service Disruption Requests raised within the SalesForce ticketing tool.	• Inquired of the TechSupport Team Manager regarding the acknowledgement provided against the defects and service disruptions raised. • For a selection of defects and service disruptions raised, inspected the ticket details to determine whether TechSupport Team provided an acknowledgement to defects and service disruptions requests within the SalesForce ticketing tool.	No exceptions noted.
3.3	The TechSupport team resolves the Defect and Service Disruption requests and changes the status of the requests to 'Closed' within the SalesForce 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.	No exceptions noted.

Control No	Description of Controls	Test Performed	Results of Testing
		• For the above selection of defects and service disruptions, inspected the SalesForce ticketing tool to determine whether TechSupport team changed the status of the defects and service disruptions to 'Closed' upon resolution.	
3.4	Post closure of Defect and Service Disruption requests, TechSupport team performs and documents the Root Cause Analysis (RCA) within the SalesForce ticketing tool.	• 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 SalesForce ticketing tool or over an email.	No exceptions noted.

Complementary User Entity Controls	• User entity is responsible for registration of defects and service disruptions through the ticketing tool.
Conclusion	Based on the tests of operating effectiveness described above, the controls were operating with sufficient effectiveness to achieve this control objective.

Change Request Management	Controls provide reasonable assurance that Change Requests raised within the internal ticketing tool for cloud applications are acknowledged, classified, tested, and approved prior to implementation.

Control No	Description of Controls	Test Performed	Results of Testing
4.1	Application Change Requests are classified by the Product SNOW team within the Jira Service Desk.	• Inquired of the Product SNOW Team Manager regarding the classification process for Change Requests (CR). • For a selection of change requests, inspected the change tickets to determine whether the change request was classified by the Product teams.	No exceptions noted.
4.2	Product SNOW team continuously monitors the Jira Service Desk for Change Requests logged and acknowledge the requests by changing the status of the ticket to “Open”.	• Inquired of the Product SNOW Team Manager regarding the ticketing tool for Change Requests. • For a selection of change requests, inspected the change tickets to determine whether the Product SNOW team acknowledged the change requests by changing the status to 'Open'.	No exceptions noted.
4.3	Product SNOW team at HighRadius develops and tests the required application changes prior deployment to production environment.	• Inquired of the Product SNOW 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 develops and tests the required application changes prior deployment to production environment.	No exceptions noted.

Control No	Description of Controls	Test Performed	Results of Testing
4.4	Upon resolution of Change Request, Product SNOW team update the requests with the solution provided along with details of the change release and change the status of the Jira ticket to “Ready for release.	• Inquired of the Product SNOW Team Manager regarding the Change Request (CR) management procedure. • For a selection of change requests, inspected the change tickets to determine whether the Product SNOW 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 'Ready for release'.	No exceptions noted.
4.5	Cloud Engineering team deploys the application change to production environment using HADAM tool as part of the monthly sprint cycles.	• Inquired of the Cloud Engineering team manager regarding the application change to production environment. • For a selection of change requests, inspected the change tickets from HADAM tool to determine whether Cloud Engineering team deploys the application changes to production environment as part of the monthly sprint cycles.	No exceptions noted.
4.6	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 exceptions noted.

Control No	Description of Controls	Test Performed	Results of Testing
4.7	Cloud Engineering team deploys the Emergency changes are logged, authorized, developed, tested, and deployed as per the emergency change management procedure post approval from the product/environment owners.	• 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, developed, tested, and documented as per the emergency change management procedure post approval from the product/environment owners.	No exceptions noted.

Conclusion	Based on the tests of operating effectiveness described above, the controls were operating with sufficient effectiveness to achieve this control objective.

Physical Security[78]	**Controls provide reasonable assurance that physical access to the work areas and computer equipment at HighRadius facilities is restricted to authorized individuals.**

Control No	Description of Controls	Test Performed	Results of Testing
5.1	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 exceptions noted.
5.2	HighRadius facilities at Bhubaneswar, India and Hyderabad, India are guarded on a continuous basis by security guards at entry/exit points	• Inquired of the Administration Team Manager regarding the physical security controls at HighRadius facilities. • Performed physical walkthrough of HighRadius Bhubaneswar and Hyderabad facilities to determine whether physical security controls were set up on the premises. • Performed physical walkthrough of HighRadius Bhubaneswar and Hyderabad facilities to determine whether the facility was monitored by security guards at entry/exit points	No exceptions noted.

[7] *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.*

[8] *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.*

Control No	Description of Controls	Test Performed	Results of Testing
5.3	Entry to HighRadius facilities is restricted to authorized personnel by a proximity card-based access control system.	• Inquired of the Administration team manager regarding the entry restriction to the facility. • Performed walkthrough of HighRadius Bhubaneswar, Hyderabad, and Houston facilities through physical observation and video conferencing to determine whether entry to the facilities was restricted to authorized personnel by a proximity card-based access control system.	No exceptions noted.
5.4	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 exceptions noted.
5.5	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.	• 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.	**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

Control No	Description of Controls	Test Performed	Results of Testing
			the electronic device details as part of the visitor register. **Action taken:** HighRadius has started capturing the electronic device (laptop, mobile etc.) details in the visitor register from November 2023.
5.6	Physical access for new joiners is created by Administration team for Hyderabad, Bhubaneswar, and Houston (previous facility) offices basis HR notification.	• 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.	No exceptions noted.
5.7	Physical access for leavers is revoked and proximity card is returned to the Administration team for Hyderabad, Bhubaneswar, India offices on or before the last working day of the leaver basis HR notification.	• 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.	No exceptions noted.

Conclusion	Based on the tests of operating effectiveness described above, the controls were operating with sufficient effectiveness to achieve this control objective.

Environmental Safeguards and Backup[9][10]	Controls provide reasonable assurance that data, applications, infrastructure, and resources are protected against environmental threats and data backup, restoration is performed on a timely basis.

Control No	Description of Controls	Test Performed	Results of Testing
6.1	Smoke detectors and fire extinguishers are installed in the work areas and network/server/hub rooms within the HighRadius' facilities.	• Inquired of the Administration Team Manager regarding the smoke detectors and fire extinguishers installed. • Performed walkthrough of HighRadius Bhubaneswar, Hyderabad facilities through physical observation and video conferencing to determine whether smoke detectors and fire extinguishers were installed in the work areas and network/server/hub rooms within the HighRadius' facilities.	No exceptions noted.
6.2	Fire safety equipment is checked on a quarterly basis for Hyderabad, India and Bhubaneswar, India. '	• 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. • For a selection of months, inspected the maintenance records for Bhubaneswar location to determine whether the monthly checks were performed on the fire safety equipment and results were documented.	No exceptions noted.

[9] *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.*

[10] *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.*

Control No	Description of Controls	Test Performed	Results of Testing
6.3	Fire and emergency instructions are displayed in prominent locations within HighRadius facilities.	• Inquired of the Administration Team Manager regarding display of fire and emergency instructions in prominent locations. • Performed walkthrough of Hyderabad facility through physical observation to determine whether fire and emergency instructions were displayed within the facilities in prominent locations.	No exceptions noted.
6.4	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 checks were performed on the UPS and results were documented.	No exceptions noted.
6.5	HighRadius has defined policy and procedures which provide guidelines for performing backup and restoration of HighRadius information systems.	• Inquired of the IMS 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 exceptions noted.
6.6	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.	No exceptions noted.

Control No	Description of Controls	Test Performed	Results of Testing
		• For a selection of days, weeks and months inspected the backup log to determine whether daily, weekly, and monthly backups were performed.	
6.7	Restorations tests are performed by database team on a quarterly basis to verify that the back-up data is readable and restorable.	• Inquired of the database team regarding quarterly restoration test performed to verify that the back-up data is readable and restorable. • For a selection of quarters, inspected the restoration reports to determine whether restoration tests were performed to verify that the back-up data was readable and restorable.	No exceptions noted.
6.8	HighRadius has formal 'Business Continuity Plan' (BCP) in place. BCP is reviewed and approved by VP - Cyber Security on an annual basis. Cyber Security - Operations team performs a BCP test on an annual 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 exceptions noted.
6.9	'IT Disaster Recovery Plan' is established, documented, and approved by VP- Cyber Security on an annual basis. Cyber Security - Operations team performs a DR test on an annual basis.	• 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 exceptions noted.

Conclusion	Based on the tests of operating effectiveness described above, the controls were operating with sufficient effectiveness to achieve this control objective.

Logical Security	Controls provide reasonable assurance that logical access to HighRadius' systems is restricted to authorized individuals.

Control No	Description of Controls	Test Performed	Results of Testing
7.1	Based on logical access creation request from HR for a new associate, IMS team creates a unique user ID on Active Directory and Cloud Engineering team creates unique user ID on LDAP	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 Cloud Engineering team created on LDAP based on the request received from HR and whether the creation details of the user ID were communicated to the associate.	No exceptions noted.
7.2	Based on access revocation request from HR, the associate's user ID is disabled by the IMS team from the Active Directory and Cloud Engineering team from the LDAP on the associate's last working day.	• 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

Control No	Description of Controls	Test Performed	Results of Testing
			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. **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.
7.3	Access to the HighRadius' client's production and non-production environments is granted to associates after obtaining approval from respective line managers via Privileged Access Management (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 Privileged Access Management (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 Privileged Access Management (PAMS)	No exceptions noted.

Control No	Description of Controls	Test Performed	Results of Testing
		tool to determine whether access was granted after obtaining approval from the respective line managers.	
7.4	Access to the HighRadius' client's production and non-production environments is revoked automatically based on the timeout duration configured in Privileged Access Management (PAMS) tool 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 Privileged Access Management (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 Privileged Access Management (PAMS) tool to determine whether access was revoked as per the timeout duration configured for the respective job role.	No exceptions noted.
7.5	Admin access on desktops and laptops is restricted.	• Inquired of the Cyber Security – Risk & Compliance Team Manager regarding 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 exceptions noted.
7.6	HighRadius has corporate network security policy that include password length, password complexity requirements, password expiry,	• Inquired of the Cyber Security – Risk & Compliance team manager regarding the password policy.	No exceptions noted.

Control No	Description of Controls	Test Performed	Results of Testing
	password history, and after a minimum number of invalid attempts.	• Inspected the password policy for HighRadius corporate network to determine whether password complexity parameters and account lockout policies were documented. • Inspected the domain password policy to determine whether the password length, password complexity and account lockout parameters were configured as per the policy. • Performed a walkthrough of a workstation for negative testing of password configuration to determine whether the user was restricted from changing the password settings.	
7.7	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 exceptions noted.
7.8	Anti-malware software is installed and activated on workstations within HighRadius to protect the workstations from external threats. Anti-malware	• Inquired of the IMS Team Manager regarding the anti-malware software installed and activated on workstations.	No exceptions noted.

Control No	Description of Controls	Test Performed	Results of Testing
	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.	• 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.	
7.9	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.[11]	• 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 exceptions noted.
7.10	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.	No exceptions noted.

11 Control 7.10 is applicable only for the period 1st April 2023 to 30th November 2023 as activity was discontinued due to the implementation of new tool (SentinelOne) from 1st December 2023, for monitoring the XDR logs.

Control No	Description of Controls	Test Performed	Results of Testing
		• Inspected the firewall configuration to determine whether traffic to the corporate servers and network was blocked unless specifically whitelisted.	
7.11	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 exceptions noted.
7.12	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 HighRadius 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 exceptions noted.
7.13	User access review for standard and privileged users having access to AD &	• Inquired of the IMS team and Cloud Engineering team managers regarding the quarterly user access review performed.	No exceptions noted.

Control No	Description of Controls	Test Performed	Results of Testing
	LDAP are performed by IMS and Cloud Engineering teams on a quarterly basis.	• 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.	
7.14	Cyber Security – Operations team performs penetration testing on the HighRadius network and servers, and 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 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 exceptions noted.
7.15	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.	No exceptions noted.

Control No	Description of Controls	Test Performed	Results of Testing
		• 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.	
7.16	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 exceptions noted.
7.17	Security patches are tested and updated on Windows workstations through Microsoft Intune on monthly basis.	• 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 windows patch updates to determine whether security patches were updated.	No exceptions noted.

Control No	Description of Controls	Test Performed	Results of Testing
7.18	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 environments. **Management response:** The Cloud Engineering team manages the patching process. 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.

Control No	Description of Controls	Test Performed	Results of Testing
			Action taken: Subsequently, in Q3, the pending patches were deployed.
7.19	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 exceptions noted.
7.20	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 exceptions noted.
7.21	Cyber Security 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	• Inquired of the Cyber Security 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 team.	No exceptions noted.

Control No	Description of Controls	Test Performed	Results of Testing
	of non-compliance from analysis are tracked to closure.	• 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.	
7.22	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 exceptions noted.
7.23	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 exceptions noted.

Control No	Description of Controls	Test Performed	Results of Testing
7.24	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 exceptions noted.
7.25	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 exceptions noted.
7.26	Background checks for identity, criminal, education, and employment verification are conducted for new employees as per the defined procedures. Also, address, 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.	No exceptions noted.

Control No	Description of Controls	Test Performed	Results of Testing
		• 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.	
7.27	Security incidents are registered with the Cyber Security - Operations team using the MangeEngine-Genie 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 MangeEngine-Genie ticketing tool, ticket details and Security incident e-mails to determine whether the security incidents were registered and tracked through the MangeEngine-Genie ticketing tool or by e-mails.	No exceptions noted.

Complementary User Entity Controls	• 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.
Conclusion	Based on the tests of operating effectiveness described above, the controls were operating with sufficient effectiveness to achieve this control objective.

APPENDIX: LIST OF ABBREVIATIONS

Abbreviation	Expanded Form
AD	Active Directory
ATP	Advanced Threat Protection
AWS	Amazon Web Services
BCP	Business Continuity Plan
BGV	Background Verification Checks
CASB	Cloud Access Security Broker
CCM	Cloud Configuration Management
CCTV	Closed Circuit Television
CD-ROM	Compact Disk – Read Only Memory
CR	Change Request
DoS	Denial-of-Service
DDoS	Distributed Denial-of-Service
DLP	Data Loss Prevention
DR	Disaster Recovery
EIPP	Electronic Invoice Presentment and Payment
ERP	Enterprise Resource Planning
HR	Human Resources
HTTPS	Hypertext Transfer Protocol Secure
IMS	Infrastructure Management System
ISMS	Information Security Management System

Abbreviation	Expanded Form
ISO	International Standards Organization
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MD	Managing Director
NDA	Non-Disclosure Agreements
OS	Operating System
POC	Point of Contact
RCA	Root Cause Analysis
SFTP	Secure File Transfer Protocol
SLA	Service Level Agreement
SOW	Statement of Work
TLS	Transport Layer Security
UAT	User Acceptance Testing
UPS	Uninterrupted Power Supply
USB	Universal Serial Bus
VAPT	Vulnerability Assessment and Penetration Testing
XDR	Extended Detection and Response