KPMG Assurance and Consulting Services LLP
KRM Tower, Ground Floor,
No. 1, Harrington Road, Chetpet,
Chennai – 600 031, India.
Tel: +91 44 3914 5000
Fax: +91 44 3914 5999

INDEPENDENT SERVICE AUDITOR'S REPORT

To

The Board of Directors

Ramco Systems Limited

Scope

We have examined Ramco Systems Limited's (hereafter referred to as "Ramco" or "Service Organization") description of its system in Section 3 for providing payroll processing services and supporting general operating environment for processing user entities' transactions from its facility located at Chennai, India, throughout the period 1 October 2023 to 30 September 2024, ("description") and the suitability of 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 "Ramco's Assertion" ("assertion"). The controls and control objectives included in the description are those that the management of Ramco believes are likely to be relevant to the user entities' internal controls over financial reporting, and the description does not include those aspects of the system that are not likely to be relevant to user entities' internal controls over financial reporting.

Ramco uses Microsoft Corporation for providing cloud backup 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 Ramco and excludes the control objectives and related controls of the subservice organization(s). The description also indicates that certain control objectives specified by Ramco can be achieved only if complementary subservice organization controls assumed in the design of Ramco's controls are suitably designed and operating effectively, along with the related controls at Ramco. Our examination did not extend to controls of the subservice organization(s) 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 Ramco's controls are suitably designed and operating effectively, along with related controls at Ramco. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design and operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

In section 2, Ramco has provided an assertion about the fairness of presentation of the description and suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description. Ramco is responsible for preparing the description and assertion, including the completeness, accuracy and method of presentation of the description and the 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 October 2023 to 30 September 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 service organization's system and the suitability of the design and operating effectiveness of the 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 the 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 International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants (including International Independence Standards) (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional behaviour. The firm applies International Standard on Quality Management 1, which requires the firm to design, implement and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

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 particular 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 presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of Test of Controls

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

Opinion

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

a) the description fairly presents Ramco's system for providing payroll processing services and supporting general operating environment that was designed and implemented throughout the period 1 October 2023 to 30 September 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 1 October 2023 to 30 September 2024, and subservice organization(s) and user entities applied the complementary user entity controls assumed in the design of Ramco's controls throughout the period 1 October 2023 to 30 September 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 October 2023 to 30 September 2024, if complementary subservice organization and user entity controls, assumed in the design of Ramco's controls operated effectively throughout the period 1 October 2023 to 30 September 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 Ramco, user entities of Ramco's system during some or all of the period 1 October

2023 to 30 September 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

Date: 23rd December 2024

SECTION 2

RAMCO’S ASSERTION

RAMCO’S ASSERTION[1]

We have prepared the description of Ramco Systems Limited’s (hereafter referred to as “Ramco”) System for providing Payroll Processing services and supporting general operating environment for processing user entities’ transactions from its facility located at Chennai, India throughout the period 1 October 2023 to 30 September 2024 (‘description’) for user entities of the system during some or all of the period 1 October 2023 to 30 September 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 of the system themselves, when assessing the risks of material misstatements of user entities’ financial statements.

Ramco uses Microsoft Corporation for providing cloud backup services 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 Ramco and excludes the control objectives and related controls of the subservice organization(s). The description also indicates that certain control objectives specified by Ramco can be achieved only if complementary subservice organization controls assumed in the design of Ramco’s controls are suitably designed and operating effectively, along with the related controls at Ramco. Our examination did not extend to controls of the subservice organization(s).

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 Ramco's controls are suitably designed and operating effectively, along with related controls at Ramco. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design and operating effectiveness of such complementary user entity controls.

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

a) The description fairly presents Ramco’s System made available to user entities during some or all of the period 1 October 2023 to 30 September 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 type 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

[1] The service organization’s “assertion” is equivalent to the service organization’s “statement” as defined under ISAE 3402.

assumed in the design of the service organization’s controls;

- 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 the Ramco’s system during the period covered by the descriptions;

iii. does not omit or distort information relevant to the scope of Ramco’s system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities and their user auditors and may not, therefore, include every aspect of Ramco’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 operated effectively throughout the period 1 October 2023 to 30 September 2024 to achieve those control objectives if subservice organization(s) and user entities applied the complementary controls assumed in the design of Ramco’s controls throughout the period 1 October 2023 to 30 September 2024. The criteria used in making this assertion were that:

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

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

RAMCO'S DESCRIPTION OF THE SYSTEM

Introduction and Scope of the Report

This section includes control objectives and description of underlying controls at Ramco Systems Limited (hereafter referred to as “Ramco” or “service organization”), pertaining to the payroll processing and general operating environment supporting payroll processing service provided to its customers (hereafter referred to as “Clients” or “user entities”) from its facility located at No. 64, Sardar Patel Road, Taramani, Chennai, India throughout the period 1 October 2023 to 30 September 2024.

This description features the payroll processing service provided by Ramco and focuses on control objectives, as they may be relevant to Ramco’s clients’ internal controls over financial reporting.

The coverage of control objectives in this report is across the following areas of payroll processing and general operating environment supporting payroll processing:

- Payroll Processing:
    - User entity onboarding
    - Payroll Input Operations
    - Processing Operations
    - Output Operations
    - Income Tax Filing Process
    - Audit Trail
- General IT Environment:
    - Information Security Framework
    - Change Management
    - Logical Access
    - Backup and Restoration Management
    - Network Security
    - Physical Access
    - Environmental Security
    - Recruitment, Training and Separation

All other services offered by Ramco from its facility located in Chennai are excluded from the scope of this report. This report focuses only on significant processes and controls that are common for the user entities serviced by Ramco. Any unique user entity situation is outside the scope of this report.

Overview of the Organization and Services offered by the Organization

Ramco Systems is a cloud enterprise software company focused on providing multi-tenant enterprise software to corporates in the area of Global Payroll & HR, Enterprise Resource Planning (ERP) & Logistics Platform covering TMS (Travel Management System), WMS (Warehouse Management system), HMS (Hub Management System), Billing and Ramco Aviation Solution. Ramco Systems is part of the Ramco Group. Headquartered in Chennai (India), the company has 30 offices spread across India, USA, Canada, Europe, Australia, Middle East, South Africa and APAC. Globally, Ramco has over 2000000 users from more than 1000+ customer organizations.

Ramco provides various Information Technology (IT) consulting and outsourcing services including software product development/support services and payroll processing services. Powered by ONE unified platform across 50+ countries, digital payroll managed services leverage emerging technologies including RPA, AI, Machine Learning and advanced analytics to help businesses with scalability, security, and productivity enhancements across global operations. Ramco has in-house ERP & Logistics Platform which are delivered to its clients as a SaaS (Software as a Service) offering. The product line Magna goes through an annual SOC 2 examination on the suitability of the design and operating effectiveness of controls relating to the SaaS offering and the supporting general operating environment.

Ramco has adopted the ISO 27001:2022 that provides a process-based approach for design, implementation, improvement, and maintenance of Information Security Management System (ISMS) across the organization including the BPO function. Further, Ramco has adopted the ISO 20000-1:2018 Service Management Standard (SMS) that provides a process-based approach for design, transition, delivery, and improvement of services that fulfill service requirements across the organization. Ramco is ISO 9001:2015 certified and as part of that requirement has implemented a Quality Management System (QMS) within the company which includes Business Process Outsourcing (BPO). Ramco has also been assessed for CMMI for Dev V 2.0 Maturity Level 3 standard.

System Overview

The Global Payroll and HR enterprise suite of Ramco is used for providing Human Resources (HR) related services to its customers.

- Competency driven HR processes
- Business rule-driven administrative and payroll processes
- Workflow management
- Non-Cost-to-Company (CTC) payroll components

The payroll processing services are offered using the Ramco e.Application (3X) and the Ramco Enterprise Series application (Magna and 4X) which are a part of the Global Payroll and HR enterprise suite. Ramco's payroll processing services manage the transactional functions of user entities' payroll function.

Ramco operates a defined system to provide Payroll Processing services to its user entities. This system consists of multiple components including 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 assists in consistent implementation of the same. The governance structure establishes a structure for operating the System and assists in demonstrating management commitment towards the same. Support functions such as Quality Management Group (QMG), Human Resources (HR), Administration and Infrastructure Management Group (IMG), Learning and development (L&D) are established in order to support the service delivery.

Ramco has defined processes for information systems, including change management, logical access, backup and restoration management, physical access administration, environmental security, recruitment and training to support the Payroll Processing services provided to the user entities. Multiple application systems including Ramco e.Application, Ramco Enterprise Series application, rTrack, rTask, Microsoft Outlook e-mail application are used by Ramco to support the service delivery.

The system includes the following functional control elements of Ramco to support client service delivery:

- Information Technology
- Infrastructure Management
- Recruitment and Training
- Human Resource Management
- Change Management
- Administration and Facility Management
- Quality Management

A representation of Ramco's System supporting the delivery of payroll processing services is illustrated as under:

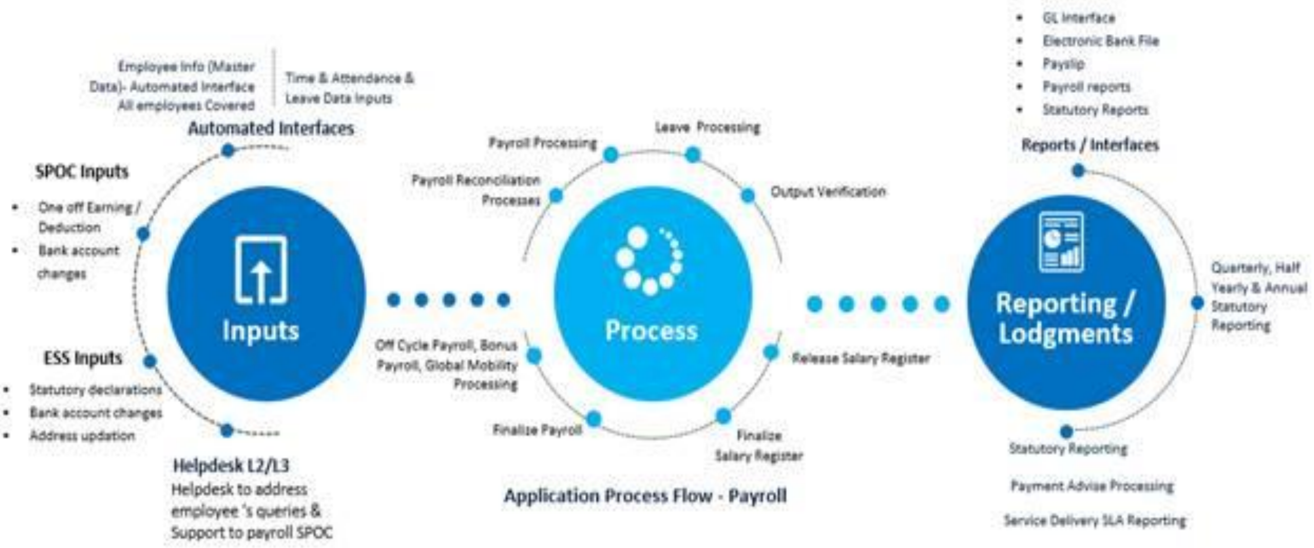
Employee Info (Master Data)- Automated Interface All employees Covered
Time & Attendance & Leave Data Inputs
Automated Interfaces
SPOC Inputs
One off Earning / Deduction
Bank account changes
ESS Inputs
Statutory declarations
Bank account changes
Address updation
Helpdesk L2/L3
Helpdesk to address employee 's queries & Support to payroll SPOC
Inputs
Payroll Processing
Leave Processing
Payroll Reconciliation Processes
Output Verification
Process
Off Cycle Payroll, Bonus Payroll, Global Mobility Processing
Release Salary Register
Finalize Payroll
Finalize Salary Register
Application Process Flow - Payroll
GL Interface
Electronic Bank File
Payslip
Payroll reports
Statutory Reports
Reports / Interfaces
Reporting / Lodgments
Quarterly, Half Yearly & Annual Statutory Reporting
Statutory Reporting
Payment Advise Processing
Service Delivery SLA Reporting

Figure 1: Ramco's Representation of System

Control Environment

Ramco's control environment encompasses Management's overall control consciousness, awareness, attitude and external influences that affects management's adherence to specific internal controls. The following is a description of the key functional elements of the corporate control environment:

- Organizational Structure
- Information Security
- Logical Access Policies and Procedures
- Physical Security Policies and Procedures
- Assignment of Authority and Responsibility
- Management Oversight

Organization Structure

Ramco has established an organizational structure to plan, execute, control, and monitor entity-wide objectives. The key areas of authority and responsibility are defined, and appropriate lines of reporting are established. The organization structure has set a tone to help facilitate the communication of important business information.

The verticals of Ramco are as under:

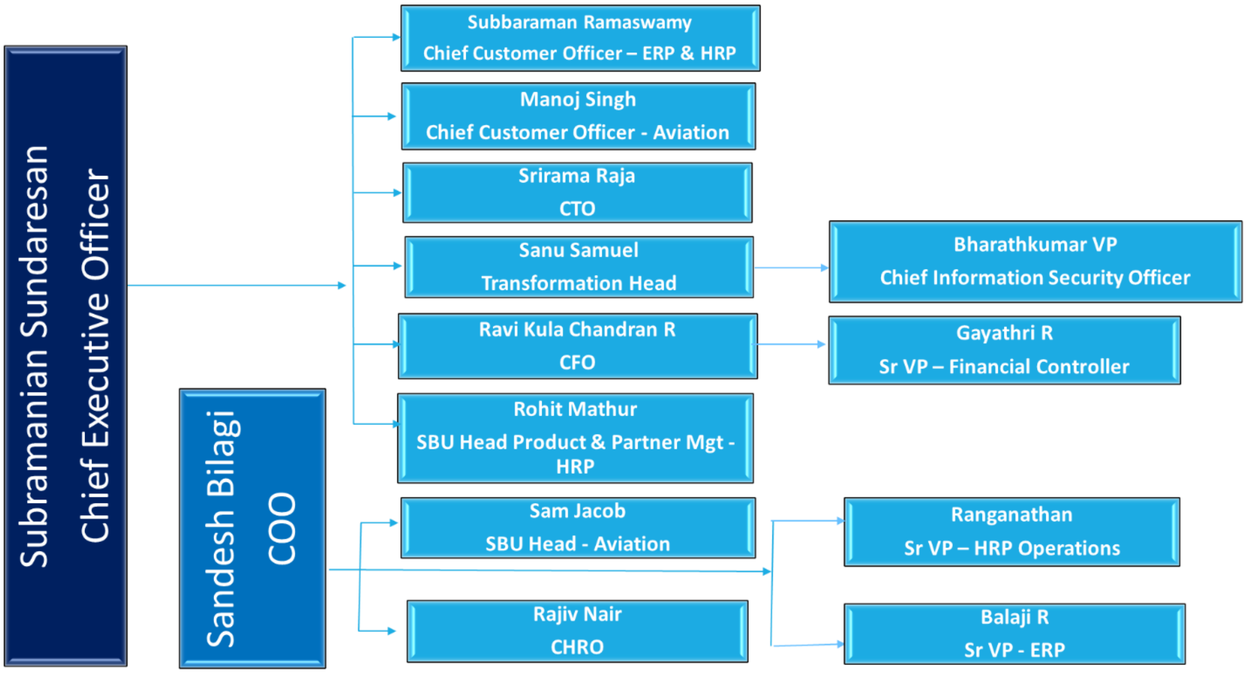

Figure 2: Ramco's Corporate Structure

Ramco's delivery organization structure is broadly classified into business units (verticals) and service lines. Business units (also called as delivery units) have projects executed in respective domains and are responsible for continually improving business performance. Each service line is responsible for delivery of services and growth of business. Business Enabling Units (BEU) consists of support functions including QMG, HR, Finance, Administration, which support service lines and delivery units to perform functions effectively. The verticals of Ramco's Business Unit are identified in the above Organization chart.

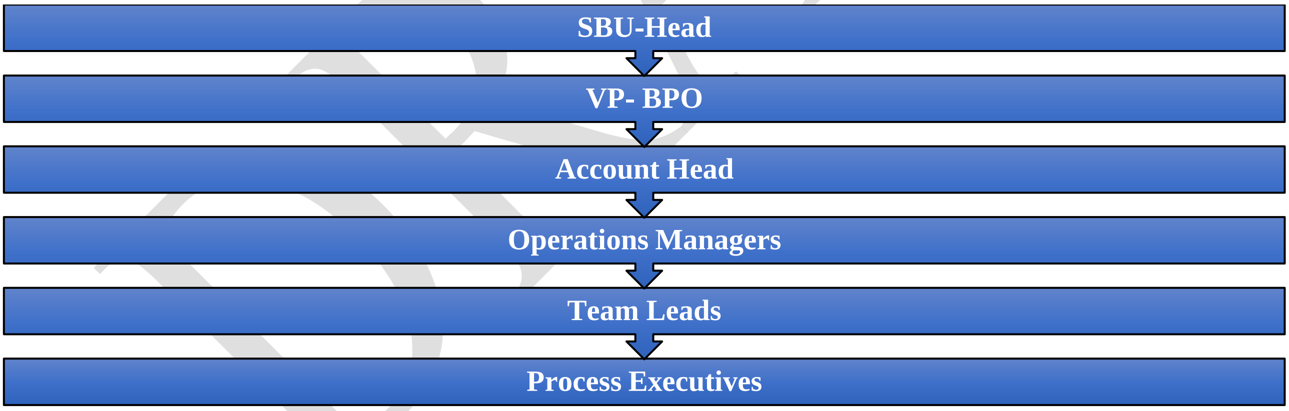

Figure 3: Ramco's BPO Operations Structure

The Strategic Business Unit (SBU) Head – Global Payroll and HR is responsible for the overall BPO function at Ramco. Head of BPO Reports to SBU Head - Human Capital Management (HCM) . The Account Heads, reporting to the Head of BPO, are responsible for the BPO operations and are assisted by Operations Managers.

Information security

As part of the ISO 27001 initiative, Ramco has developed an Information Security Management System (ISMS). The ISMS is a systematic approach to manage sensitive organization information so that it remains secure. It encompasses people, processes, and IT systems. The ISMS is a part of the overall management system, based on a business risk approach to establish, implement, operate, monitor, review, maintain and improve information security.

Logical Access Policies and Procedures

Employee access to the Ramco Active Directory (AD), e-mail and applications is authenticated through password in compliance with the defined password policy.

Ramco employees are granted access to Ramco's AD using Employee Self Service (ESS) portal, after unique ID is created by the HR team in the HRSS application. User IDs of resigned / terminated Ramco employees on the Ramco's AD are revoked based on status update of the employee by the HR team in the ESS portal, based on approval from the Operations Manager / Account Head, BPO[2]. In the event of changes to the job responsibilities, access to specific user entity data is granted / revoked based on authorization from the Account Head / Operations Manager - BPO. Access to payroll applications, for employees who leave the BPO Operations team, is revoked by the BPO Technical Team Leader on receipt of e-mail from the HR / Operations Manager within one day from the last working day of the employee.

Physical Security Policies and Procedures

Physical access to Ramco facility and BPO work area is granted by the HR personnel and provisioned by the Administration team based on the Request for ID card form from the HR personnel on the date of joining of the employee. Access to the BPO work area is restricted through electronic access cards and the list of personnel having access to the BPO work area is reviewed by the Account Head/ VP- BPO, on a monthly basis. Access to the data center is restricted to authorized members of the IMG team based on approvals received from the IMG Head and a review of the list of personnel authorized to access the data center is conducted on a monthly basis.

Assignment of Authority and Responsibility

Following are the roles and responsibilities of key personnel within Ramco BPO delivery structure:

Roles	Responsibilities
SBU Head	• Manages the P & L of the business unit, reviewing day-to-day metrices, problem-solving of the managerial team & their functionaries to meet the required service levels, standards and service targets, to develop the team to ensure delivery of a consistently superior customer experience by highly knowledgeable and customer-focused leaders • Acts as the communication conduit between BPO Management and the Organization leadership • Offers creative solutions, which will enable the unit to evolve consistently & deliver profitability on a quarter-by-quarter basis • Advocates / promotes organization change related to organization mission • Supports motivation of employees in unit products/programs and operations • Ensures staff and management team have sufficient and up to date information • Looks to the future for change opportunities • Interfaces between Management and employees • Formulates policies and planning recommendations to the Management/Executive team • Decides or guides courses of action in operations by staff • Oversee design, delivery and quality of programs and services • Oversee operations of unit

[2] Confirmation mail gets triggered to IMG and QMG teams upon revocation of access to Active Directory for resigned / terminated employees in Ramco.

Roles	Responsibilities
	• Implements plans • Manages financial and physical resources • People Management, including all people related issues, as well as staff development • Managing the Operating Leaders, adherence to timely launch schedules across various geos • Recommendations for process development based on customer feedback and analysis of the same • Reporting metrics at a unit level and improving customer feedback consistently • Recruiting a team to build the unit to a global scale • Ensures the unit is appropriately organized and staffed and to have the authority to hire and terminate staff as necessary to enable it to achieve the approved strategy • Assess the principal risks of the Unit and to ensure that these risks are being monitored and managed • Ensures effective internal controls and management information systems are in place • Ensures that the unit has appropriate systems to enable it to conduct its activities both lawfully and ethically • Ensures that the unit maintains high standards of corporate citizenship and social responsibility wherever it does business • Communicates effectively with management team, employees, Government authorities, other stakeholders • Monitor the unit's daily operations, as well as to supervise the undertakings of each of its operational units as well as the discharge of duties of the unit's employees in all areas
VP – BPO	• Reports to the Head of BPO Business unit • Leads the APAC and International payroll operations ensuring accurate and timely processing, in accordance with Company policies and local tax and labor regulations. • Manage, coach, and develop the Global Payroll Operations team • Ensures all monthly, quarterly, and annual filings and year-end statements are issued as per local legislation • Build and maintain a relationship with key stakeholders within the client organization and internal stakeholders to ensure optimization of end-to-end payroll input and output processes • Ensures proper processing and reporting of salary, equity, bonuses, and benefits • Assists team with managing relationships with our global and/or regional payroll providers • Manages preparation of relevant management quarterly business reviews, KPIs

Roles	Responsibilities
	(Key Performance Indicators), and payroll metrics • Optimizes standard procedures for payroll processing, ensuring strong internal controls and segregation of duties • Ensures best practices for regular audits of earnings, payroll taxes, and annual reporting are performed and are effective to avoid any potential errors • Provides subject matter expertise for cross-functional projects impacting payroll operations • Partners closely with Head of BPO business unit to execute roadmap initiatives focused on processes within payroll operations • Governs and maintains internal controls in accordance General Data Protection Regulation requirements • Ensures policies and procedure manuals are up to date and maintained by payroll personnel • Leads weekly staff meetings, conducts regular employee one-on-one sessions, and annual reviews • Addresses any performance management issues with employees
Account Head	• Approves the user entity specific Process Books • Approval of change request forms and change impact analysis • Authorizes the provision of access to payroll applications • Reviews list of personnel having access to payroll applications • Reviews physical access to the BPO work area
Operations Manager	• Provides operational guidance to BPO Operations teams • Authorizes for provision of access to payroll applications • Reviews and approves the draft payroll register and variance report • Approves the final payroll register • Approves the output for statutory compliance
Team Leader	• Signs off the migration checklist • Approves the reimbursement slips • Approves the payroll and reimbursement upload files • Performs period closure activity on payroll applications
Process Executive	• Prepares the reimbursement slips • Prepares the payroll and reimbursement upload files • Prepares the output for statutory compliance • Communicates with the authorized user entity personnel regarding any clarifications on input data

Management Oversight

Management is responsible for the day-to-day operations of the organization and is committed to providing quality, accurate and timely service to its user entities. Employees follow workflow practices and internal control procedures in order to achieve the highest standards of client satisfaction.

The management oversees and guides the organization and its business. The basic responsibility of the management is to exercise business judgment to act in what will be reasonably in the best interests of the organization. The management also considers the organization's ethical behavior and the interests of the organization clients, employees and communities in which it functions.

Risk Assessment

Ramco has a defined Risk management Policy that outlines the possible risks in the context of Ramco's business objectives. It also provides a suitable strategy to manage these risks by applying the controls as required. Broadly, Ramco's Risk management Policy attempts to identify critical business risks and places significant emphasis on information security as well as process risks. The policy also proposes a strategy to manage these by applying appropriate controls.

Business Risk

Business risk at Ramco is classified into Business Process Changes, Product Changes/ Obsolescence and Human Resources and Statutory changes.

Ramco has deployed its in-house Enterprise Resource Planning solutions, Ramco e.Application and Ramco Enterprise Series application, for payroll processing services offered to user entities. Ramco manages the features of the applications used for outsourcing operations which enables them to adapt to business process changes of the user entities.

The Product Group maintains a Product roadmap for Ramco and is also responsible for research on emerging technologies. Further, the Product Group works on automating mundane manual activities as part of the continuous improvement process. The employees of Ramco undergo periodic training programs to enhance their technical skills. The activities of the Product Group are reviewed by the senior management on a periodic basis. These measures help in reducing the business risks related to technology changes / obsolescence.

With an increasing demand for skilled resources and high rates of attrition in the BPO industry, employee turnover has been identified as another key business risk. To counter this, the company has adopted a series of measures to retain their talent:

- Appraisal systems and Rewards / Recognition program
- Key performance areas for Managers include talent classification, employee retention and team building
- Dedicated Training team, with an objective to create, maintain and enhance technical skills of employees

Further, Ramco maintains an individual skills matrix and sets specific key result areas for each of its employees in order to identify and acquire the latest skills, as a part of the company's performance management process.

In order to comply with the current regulations including local laws, Data protection regulations and global compliance requirements. Ramco has a 'Payroll Bureau' team to monitor the regulatory/ Statutory changes happening globally which could have an impact on the product. As and when there is an amendment/ addition, the same is notified to the clients and a concurrence is taken before rolling it out. The Payroll Bureau in turn communicates to the Product team for updating the same in the product. Product upgrades due to changes in regulatory compliance is part of the support services provided by Ramco.

Information Security Risk

In order to protect Ramco's information systems, the company has devised an information security policy to identify, document, and mitigate threats. There is also a cross-functional and empowered Information Security Forum (ISF) that guides in protecting the confidentiality, integrity, and availability of the company's information assets. Ramco's Information Security policy covers the vital information assets of the company including computing resources, network systems, data handled by the systems, facilities, and restricted areas. Periodic risk assessment identifies the threats that can compromise the confidentiality, integrity, and availability of Ramco's assets. Some of the measures adopted under this policy include:

- Housing of IT facilities supporting critical or sensitive business activities in secure areas
- Protection of company equipment from environmental hazards, to prevent loss, damage or compromise of assets and interruption to business activities
- Immediate reporting of unscrupulous incidents observed or suspected to the Chief Information Security Officer (CISO)
- Formal disciplinary action against employees who commit security breaches

Ramco has also adopted other controls including signing of Non-Disclosure Agreements (NDA) by employees and segregation of duties to deter employees from compromising the interests of Ramco.

Monitoring Activities

Internal Audit

Ramco has defined procedures for its internal quality audits. Internal audit is closely monitored by the Management. Ramco has a Quality Management Group which is responsible for the implementation of Quality Assurance (QA) activities across projects / support groups. QMG is an independent group and is not a part of any delivery unit. The management representative of QMG reports to Head – Global Project Management Office (GPMO)/ Senior Vice President - Head of Transformation[3].

The Ramco BPO Operations team is assisted by a QA team and the responsibilities of QA team include the following:

- To verify the activities of every operational process based on defined checklists;
- To track the status of the various activities done by the Operations team against the monthly Payroll Calendar.
- To validate the deliverables of each operational process; and
- To define / modify any process based on business requirement.

QMG conducts an internal assessment of services delivered to the user entities on a regular basis. The Audit team is independent of the function being audited and is provided training to carry out the audit procedures. Broadly, internal audits are performed to review the internal controls, processes and procedures followed by every department. ISO 9001:2015, ISO 27001:2022, ISO 20000-1:2018 and CMMI for Dev v2.0 ML3 serve as reference standards for these internal audits.

To facilitate the internal audit, an internal audit schedule is prepared and circulated to the Project teams every month. The non-conformities identified are discussed with the auditee and are tracked to closure as per the agreed action points. The audit data and the process improvement suggestions are presented to the senior management every month and the corrective and preventive actions are planned accordingly.

Internal Operational Review for BPO

Ramco has designed a framework to evaluate the health of the active BPO projects in the company. Ramco’s BPO QA team performs a monthly internal operational review to identify and monitor any non-conformance and for tracking errors in payroll processing. The team also reviews the payroll process from an information security standpoint to assess any deviations to the information security related controls implemented in the payroll process. Any deviations identified, are recorded and tracked to closure by the BPO QA team.

Information and Communication

Internal Communication

Ramco uses different modes of communication including e-mail and intranet to communicate important information with its employees on a timely basis.

Circulars / mailers are one of the important channels of internal communication at Ramco. Every quarter, the VP - BPO addresses the employees and provides them a detailed business update for the past quarter. Crucial announcements are

[3] QMG team reports to Senior Vice President – Head of Transformation from 1 October 2023.

communicated to employees by corporate mailers sent by the Marketing team.

Ramco's intranet is another important medium for employee communication to know the current policies and procedures. It also serves as an information management system and supports e-learning. The portal is also used by individual departments to make important announcements such as release of a new policy and any other organization-wide initiatives. Apart from these, Ramco also uses e-mail and the company newsletter to facilitate information flow within the company.

External Communication

External communication occurs through the Ramco website. The responsibility for maintaining this website lies with the Corporate Governance Group which is part of the Support Services group. This group is also responsible for any announcement to the Press or other external media.

Media relations involve managing message development and media relationship building strategies and programs. It involves providing support in planning and executing Ramco's corporate public relations, media and analyst strategies and managing daily activities with Public Relation agencies across geographies. It involves working with the rest of the Corporate Marketing team, as well as senior executives, thought leaders, subject matter experts and external Public Relations agency to produce media pitches, press releases, speaking session abstracts and by-lined articles for business and trade publications.

Communication to clients is handled by the senior management on critical information pertaining to the relationship with the client or with regards to Ramco's public news or announcements. Periodic project status updates are provided to the clients whenever requested. The frequency of such updates and the mechanism for communication are agreed upon at the project inception stage. There are multiple channels for user entity communication such as e-mails, newsletters and web portals for periodic reporting to user entities on operations and Management Information Systems (MIS) reports as agreed with user entities. The Account Head at Ramco is responsible for interacting with the user entities.

Key Application Systems

The following tools are used by Ramco BPO Operations team to support the Payroll processing services provided to its customers[4].

Name of the Tool	Description
Ramco e.Application (3X)	Ramco e.Application is a Ramco proprietary payroll application used by the BPO team for performing payroll, reimbursement, and income tax processing activities. The Ramco e.Application is configured to process payroll, reimbursement and income tax data based on the requirements provided by each user entity. Key validations are built into the application to reduce input data processing errors.
Ramco Enterprise Series application (Magna and 4X)	Magna and 4X applications are Ramco proprietary applications used for performing payroll, reimbursement and income tax processing activities. Aside from the user entity-specific configurations, the Ramco Enterprise Series includes an Employee Self Service (ESS) interface available for the user entities to upload payroll data and view pay slips.
rTrack Application	rTrack is a ticketing application used for logging service requests, changes and incidents at Ramco. rTrack application is also used for raising backup restoration requests by BPO team.
rTask Application[5]	rTask is an in-house ticketing application used for logging service requests, changes and incidents at Ramco by IMG team.
Veris	Veris is a third-party application deployed at Ramco used for recording details of visitors and provide visitor badges as well as to provide temporary badges for new joiners to Ramco.

[4] GITC testing of the supporting applications including rTrack, rTask, Siemens Solution, Microsoft Outlook, Ramco Geek and Veris have not been covered as part of this report.

[5] rTask application has been introduced from February 2024 for IMG related requests.

Name of the Tool	Description
Ramco Geek	Ramco Geek is an in-house facial recognition application deployed at Ramco used for management of Physical access into Ramco facility.
Siemens Solution	Siemens Solutions are access management systems deployed at Ramco used for management of physical access to the BPO delivery center and other sensitive work areas.
Ramco Onboarding	Ramco Onboarding is an in-house application used by new joiners to upload relevant documents and acknowledge Code of conduct and Non-disclosure agreements.
Human Resource Self Service (HRSS)	HRSS application is a part of the Human Resource Management System (HRMS), which is used for creation and deletion of employees in the HRMS.
Microsoft Outlook	Microsoft Outlook software is used for e-mail communications at Ramco.
Azure Cloud	Azure cloud is used for storing the backup data from the corporate and production servers.

Description of Services

Business Process Services

Payroll Process Overview

Payroll processing including reimbursement processing for user entities is performed as per the process outlined in the 'Payroll Process Book' (also referred to as Payroll Operations document) and the 'Reimbursement Process' documents for the user entities.

User Entity Onboarding

BPO Processing team is responsible for the onboarding of the user entities and is also responsible for the creation of the Payroll Process Book. The requirements of the user entities are captured in the Payroll Process Book which outlines the system parameters in the application, the deliverables, expected service levels, statutory and regulatory compliance requirements to be adhered for payroll processing. The Payroll Process Book is approved by the Account Head and Head of BPO Operations and is shared with authorized personnel from the user entity for validation.

Payroll Input Operations

The 'Payroll Process Book' document provides guidance to the BPO Processing team on the payroll input processing. A Payroll Calendar, aligned with the user entity's payroll processing period, outlines the schedule of activities to be performed. The Payroll Calendar is communicated between the BPO Operations team (Operations Manager) and authorized user entity personnel on a monthly basis or yearly basis prior to the start of the processing period as defined in the process book. Adherence to the Payroll Calendar timelines is tracked using a payroll tracker by the BPO team during the payroll processing period[6].

Input files for payroll processing are received from the authorized user entity personnel through agreed mode of communication (e-mails / SFTP) as defined in process book prior to processing the payroll. Payroll input includes data pertaining to variable pay components, changes to the reimbursement cycle, Full and Final settlement (F&F), changes to basic payroll data or additional inputs during the processing period, investment proofs and leave data. For the user entities who have subscribed to the services of Ramco Enterprise Series application, access to the Employee Self Service (ESS) portal is provided for uploading compensation and reimbursement related inputs where user entities provide inputs through hard copies for processing reimbursements and income tax proofs. The inputs are serially numbered period wise and consolidated in a spreadsheet prior to uploading in the payroll processing application. Payroll applications are configured to restrict uploading of

[6] Frequency of communication of the payroll calendar is as per the Payroll Process Book.

erroneous data records like invalid employee number, blank input data, invalid input dates[7].

Payroll Processing Operations

The ‘Payroll Process Book’ document provides guidance to the Processing team on payroll processing. Payroll is processed in the payroll applications by the Process Executives. Payroll applications are configured to prevent payroll processing until payroll readiness check is complete. The payroll readiness check includes the following key validations:

- Payment method has been defined for the employees
- Previous payroll processing period has been authorized[8].

A reconciliation of the payroll input and the output file is performed by the Quality Assurance (QA) team on a monthly basis and errors, if any, are communicated to the Process Executives for correction. Upon processing of payroll input within the payroll applications, a draft payroll register with details of payroll and reimbursement processed and a variance report showing the variances between the outputs of current month and previous month are generated. The draft payroll register along with the payroll variances report are reviewed against user entity input data and approved by the Operations Manager prior to dispatch to the user entities through the agreed mode of communication[9].

Payroll Output Operations

The ‘Payroll Process Book’ document provides guidance to the Payroll Processing team on the payroll output process. The draft payroll registers and variance report are dispatched to the authorized user entity personnel for validation. Changes, if any, are communicated by the authorized user entity personnel[10]. The Payroll Register is finalized based on the confirmation received from the user entities over the draft versions.

The Operations Manager approves final payroll register and variance report prior to dispatch to authorized user entity personnel. The pay slips are generated based on the final payroll register and dispatched to the user entity through the agreed mode of communication as per the timelines defined in the Payroll Calendar as applicable[10].

The statutory reports for statutory compliance, requested by the user entities based on a defined Statutory Compliance checklist, which includes verification of accuracy of statutory deductions is prepared by the Compliance team. The output for statutory compliance is approved by the Account Head / Operations Manager prior to dispatch to the user entity and / or filing with the regulatory body based on a defined checklist[11]. The Payroll application is configured to restrict any processing after payroll period closure, Payroll period closure is performed in the application by the BPO team leader based on the Payroll Calendar / intimation from the user entity.

Income Tax Filing Operations

The ‘BPO Year-end Process’ document provides guidance to the Processing team on the activities pertaining to income tax filing. A calendar for the income tax processing and filing is communicated between the BPO Operations team and the authorized user entity personnel prior to the commencement of income tax processing[12]. The cut off dates for the various income tax filling related activities are defined in the calendar. The Processing team prepares status trackers to monitor the progress of activities as per the cut off dates mentioned in the calendar. Proofs for income tax related claims received from the authorized user entity personnel and the acknowledgement of receipts sent to the authorized user entity personnel are only through the agreed mode of communication as defined in the process book.

The following key validation checks are performed, as appropriate for the countries, during the upload of data related to income tax, into payroll applications:

- Blank ‘Employee Number’ field
- Blank ‘Input Date’ field

[7] Not applicable for MAGNA application, since upload of data is performed by Ramco for user entities.
[8] This process is not applicable for clients using 4X application.
[9] Draft payroll register is not applicable to user entities which do not have additional input procedures included as a part of their payroll calendar.
[10] Not applicable for MAGNA and 4X applications as the pay slips are authorized immediately after payroll.
[11] Statutory compliance processing is performed for those user entities for whom it is defined in the respective process book.
[12] Income tax processing is performed for those user entities for whom it is defined in the respective process book.

- Duplicate entries

The income tax slips are downloaded from the payroll applications and are distributed to the employees of the user entities as per the agreed mode of communication.

Audit Trail[13]

Audit trail is enabled within the payroll application, configured to capture the changes, made to the payroll and reimbursement data through application front-end and through the database tables. There exists audit trail configuration in the payroll application for the transactions processed by the user entity. Audit trail is configured using Change Data Capture (CDC) feature and Trigger methodology enabled in the database server of the payroll application. CDC and Trigger methodology is enabled to capture the changes (insert, update, and delete) made to the database tables[14].

Access to audit trail configuration is restricted to BPO Technical team. Access to audit trail configuration is provided based on the approval from BPO Business Head. Database administrators do not have access to front end of the payroll application and cannot make any changes to the audit trail data. Cloud Infrastructure Service (CIS) team do not have access to change the audit trail data through front-end of payroll application or directly through the database.

A batch job is implemented to enable logging of audit trail data. Failure to audit trail logs are notified to Ramco BPO Technical team through an e-mail alert and failures identified are tracked to closure. Audit trail logs are retained for a minimum of eight years by the Ramco BPO Technical team[15]. Privileged-level access to audit trail configuration within the payroll application is restricted to authorized personnel from Ramco BPO Technical team. Shared or generic accounts with access to privileged tasks or functions to the audit trail configuration within the payroll application are restricted to authorized personnel from Ramco BPO Technical team.

Change requests to the Audit trail configuration are raised in the rTrack application. The change requests are implemented by the Base Product team and approved by the Base Product Quality Assurance (QA) team prior to migrating into the production environment.

General Information Technology Controls

General controls consist of development and change to application systems (and related components such as databases, and network), and management of physical access, logical access, environmental controls, human resources and training. These are described in detail below.

Information Security Framework

The QMG team of Ramco has defined an ISMS policy and ISMS Manual, which is reviewed and approved by the CISO on an annual basis. The policy is made available to the Ramco employees through the intranet portal (MyRamco).

The management has created a framework for managing information security activities by:

- Establishing information security policy and procedures
- Establishing different teams at the organization level for managing information security activities
- Providing sufficient resources to develop, implement, operate and maintain the ISMS

Security groups formed at the organization level are responsible for various security activities. The Information Security Organization consists of a Management Information Security Forum, a dedicated Information Security team, Incident Response team, IT System Administrators, IT Security Coordinators and the Business Continuity team.

Information security management awareness programs are conducted to increase user awareness through various channels including trainings, e-mails, e-learning portal, posters, and team meetings. Security awareness is also spread through password protected screen savers defined by the IMG team for Ramco employees. Information security policy and procedure documents are hosted on the intranet portal and are accessible to the employees for their reference.

[13] Audit Trail was enabled in the payroll applications from January 2024. Audit Trail controls are applicable for Indian customers.

[14] CDC feature is used to capture Audit trail for user entities using MAGNA and 4X application. Trigger methodology is used to capture Audit trail for user entities using 3X application.

[15] Audit trail logs were retained from the date of enablement till the audit period.

Any changes to the security practices or occurrence of incidents are communicated to the employees through Security awareness e-mails sent by the CISO.

Change Management

The ‘Change Management Guideline’ document provides guidance on the process of managing changes to the payroll applications and database. Change requests to the payroll application and database are raised in rTrack application with a unique change request number. The Change request is approved by the Account Head / Operations Manager / Head of BPO Operations. For changes, an impact analysis is carried out by the Technical Support team based on outcome of the impact analysis, risk of implementation is analyzed and approved by the Technical Manager. Test cases and the expected test results are documented by the Process Executive. Technical team tests the changes in the test environment and the actual test results are approved by the Technical Manager prior to implementation in the production environment. Access to migrate changes to the production environment is restricted to the authorized members of the Technical Support team as defined in the Software Configuration Management Plan. User Acceptance Testing is performed by the Process Executive and approved by the Operations Manager for the changes implemented.

Logical Access

Ramco has defined ‘Logical Access Control Process’ document which defines process for granting access to Ramco’s AD and the policy is reviewed and approved by CISO on an annual basis.

User access to the payroll applications is managed as per process defined in the ‘Technical Support’ document. Access to the payroll applications initiated through rTrack / e-Mail communication and access to Payroll application is controlled through a unique user ID and password assigned to the BPO team members based on an approval from the Operations Manager / Account Head. In the event of changes to the job responsibilities, access to specific user entity data is granted / revoked based on authorization from the Account Head / Operations Manager - BPO. In the event of changes to the job responsibilities, access to specific user entity data is granted / revoked based on authorization from the Operations Manager / Account Head. The users are authenticated to the Ramco’s AD and database based on the following password parameters outlined in the ‘Password management guideline’ policy which is reviewed and approved by CISO on an annual basis[16].

- Minimum password length is set to eight characters
- Password complexity is enabled to include alphanumeric and special characters
- Maximum unsuccessful login attempts prior to being locked out is three
- Maximum number of passwords remembered is five
- Maximum number of login failures for account lockout is three
- Minimum number of minutes for screensaver to enable is five.

List of personnel having access to the payroll applications is reviewed on a quarterly basis by the Account Head / VP BPO to identify and revoke any access that is no longer required.

Users who are provided with access to the payroll application are initially granted access to Ramco’s AD using ESS ('Employee Self Service') portal, after unique ID is created by the HR team in the HRSS application. User IDs of resigned / terminated Ramco employees on the Ramco’s AD are revoked based on status update of the employee by the HR team in the ESS portal, based on approval from the Operations Manager/Account Head, BPO[17].

Administrative rights on the workstations are disabled by default on the workstations in Ramco BPO Operations. AD password policies and account lockout policies are defined and enforced through the Ramco’s AD. In case of any exception, approval from Operations Manager is obtained. Guest / anonymous accounts are disabled in the Ramco’s AD and workstations in the BPO processing area by the IMG team. CD-ROM drives and USBs are disabled by default on the workstations in Ramco BPO work area and access is granted by the IMG team based on the exception request raised in the rTrack application and approved by the Account Head.

[16] The password parameters in the Ramco e.Application are configured as specified by the user entity. Authentication for payroll application and database are performed through AD.

[17] Confirmation mail gets triggered to IMG and QMG teams upon revocation of access to Active Directory for resigned/terminated employees in Ramco.

Backup and Restoration Management

Procedures for Back up, Retention and Restoration are defined and documented in the Backup and Restoration process document, which is prepared by the QMG team and approved by the CISO on an annual basis. The payroll data stored in production server is fully backed up on a daily basis. The backup jobs are monitored for successful completion by the IMG; and failure, if any, are recorded and tracked to closure as a security incident by the IMG team. The backup tapes are labeled as per the defined convention and a record of the same is maintained in the tape inventory by the IMG team. The backup tape is stored in a storage vault and access is restricted to only the members of the IMG team. On a weekly basis, backup tapes are moved to an offsite location (The Ramco Cements Limited, Howrah's corporate center, No. 98 A, Dr. RK Salai, Mylapore, Chennai - 4) by authorized personnel from the IMG team. The tape movement is verified at the origin and destination points by the IMG team member and the details are recorded in a Tape movement form.

On a semi-annual basis, the Restoration test for data backup is carried out by the IMG team through tickets raised on rTrack / rTask application or e-mail communication and the test results are validated by the Technical Team Leader for BPO Operations.

Network Security

A specific Virtual Local Area Network ('VLAN') is assigned for the BPO network in Ramco and access is restricted to Ramco BPO operations in the VLAN segment. Access to internet is restricted by IMG team for Ramco BPO employees through Websense / Zscaler content filter[18]. Access to websites other than the sites configured in the firewall in content filter is provided by the IMG team based on approval from the Account Head / VP BPO through the request raised in rTrack / rTask application. Antivirus software is activated / updated on workstations at the time of logging-in. Antivirus software / database is updated when the software vendor issues a new release, through centralized ePO Server and is configured to receive real time signature ('DAT') updates. Ramco IMG team monitors the antivirus server console on a real time basis to check whether workstations are updated with latest released definition. On a daily basis, monitoring reports along with the percentage of compliance are generated and sent to the Desktop team and the Head of IMG. Incoming and outgoing e-mail messages and attachments are scanned at the mail server level and gateway level for spam and virus. On an annual basis, Vulnerability Assessment and Penetration Testing ('VAPT') on Ramco network is conducted by an external vendor and the results are documented.

Physical Access Administration

Ramco has defined and documented a Physical and Environmental Security Policy, which is approved by the CISO on an annual basis. The Physical and Environmental Security Policy is made available to the Ramco employees through the intranet portal. Physical access to Ramco facility and BPO work area is monitored by Security Guards round the clock for restricting unauthorized access. Entry and exit details of the vendors / visitors to Ramco facility are recorded via Visitor Log register by the Security team. Veris application is used for recording details of visitors such as date of visit, contact, person to meet, and purpose of their visit and details of electronic devices (laptop, USB devices) carried by them and to and provide visitor badges as well as to provide temporary badges for new joiners to Ramco. Physical access to Ramco facility and BPO work area is granted by the HR personnel and provisioned by the Administration team based on the Request for ID card form from the HR personnel on the date of joining of the employee. Physical access to the Ramco facility and BPO work area is revoked by the Administration team on the LWD of the employee after submission of access card and post the same, sign-off is provided on the 'Clearance Automation' in the ESS ('Employee Self Service') portal. Access to Ramco facility for employees is monitored through Ramco Geek application, an in-house developed application that provides access to Ramco facility based on facial-recognition mechanism. Closed Circuit Television ('CCTV') Cameras are in place at entry points in the Ramco facility and BPO process premises and are monitored by Security Guards. CCTV footage is retained for a period of 45 days. CCTV incidents are recorded by the Security guard and reviewed by Head of Admin at the time of incident. Physical Access to BPO work area is controlled through implementation of a proximity card reader at the entry / exit to BPO work area.

List of personnel having access to BPO work area is reviewed by the Account Head / VP BPO on a monthly basis and unauthorized access, if any, are identified and revoked by the HR, and de-provisioned by the Administration team. The entry / exit to the data center is monitored through CCTV camera. The CCTV footage is retained for a period of 45 days. Access to the data center is controlled through a proximity card and biometric fingerprint reader.

[18] Zscaler application is in use for internet access restriction and content filtering from 1 October 2023.

Access to the data center is restricted to authorized members of the IMG based on approvals received from the IMG Head. Review of personnel authorized to access the data center is conducted on a monthly basis by the IMG Head and any unauthorized access is revoked as part of the same. The entry / exit of visitors and vendors to the data center is recorded in a visitor register and signed by an IMG team member, who is also required to accompany the visitor inside the data center.

Environmental Security

The environmental controls for the Ramco premises including the data center and the BPO work area are designed and managed as outlined in the 'Physical and Environment Security' document. Smoke detectors, temperature monitoring devices, gas-based fire suppression system, and fire extinguishers, are installed for protection against environmental hazards including fire, dust, power, excessive heat and humidity. The floor layouts highlighting the presence of fire safety equipment and the emergency exit passages have been displayed at the floors. The data center hosting the payroll applications (includes servers and the networking components) is equipped with raised flooring and false ceiling.

Annual Maintenance Contracts (AMC) for the equipment including fire extinguishers, smoke detectors, fire alarms and lifts are maintained, and the equipment are tested at periodic intervals (Monthly for Fire Extinguishers, Fire alarms, and Uninterruptible Power Supply, and Quarterly basis for Diesel Generators) by the respective vendors as per the AMC. Preventive maintenance reports are maintained and reviewed against the maintenance schedule by the Administration team. Power backup through UPS and diesel generator sets has been implemented considering the power requirements for the facility in case of non-availability of primary power supply. Assets for fire safety and power protection including UPS and diesel generators are under Annual Maintenance Contracts (AMC) for support from the vendors in case of any system failure / issues. A preventive maintenance is conducted as per the agreed maintenance schedule by the vendors to facilitate the data center to remain functional and operational during an emergency.

Fire safety drill is conducted by the Emergency Rescue team at Ramco facility on an annual basis. The temperature and humidity levels inside the data center are monitored and recorded by the electrician once every two hours against the threshold values in the 'Temperature Monitoring' register. In case of any exception to the threshold, an incident is logged with the vendors for support.

Recruitment, Training and Separation

As part of QMS, Ramco has published HR processes. HR specific Policies are defined and documented by the Specialist-HR Shared Services and approved by the Senior Manager / Chief Human Resources Officer. The HR policies and procedures are made available to the employees through the intranet portal. The Recruitment function of the Human Resource (HR) department is responsible for the initial screening and evaluation of job applicants in accordance with Ramco's policies and procedures. At the time of hiring a resource, the Project Manager sends a request with the job description and requirement to the HR. The request raised for new hires is approved by the CHRO. Additionally, the Resource requirements are also discussed in the semi-annual BU-HR meetings for new and replacement resources and approval is obtained from CHRO/ BU Head for these requests.

Resources are hired to Ramco BPO process following a criteria-based interview and approval from the respective Project Manager. Post which the Talent Acquisition team raise a request in rTrack application to initiate the Onboarding process. Once the offer letter is released, Background Verification (BGV) is initiated and completed with criminal and employment checks within 180 days of joining[19]. Exceptions if any are reported to the Chief Human Resource Officer on a monthly basis. Background and reference checks are conducted for the candidates by a Third-Party Service Provider. Background verification is not mandatory for temporary employees or project interns. For lateral hires, background verification including educational qualifications, work experience, reference checks and address verification is carried out by the Third-Party Service Provider. For campus hires, only passport copies or a photocopy of the application for passport is verified at the time of joining Ramco and Background Verification is not mandatory. Exceptions with respect to Background Verification process, if any, are tracked in the metrics/tracker maintained by HR team and placed in a secured share point and is reported to the Chief Human Resource Officer on a monthly basis. For third party hires, declaration note from the concerned agency is obtained prior to the employee on-boarding. Client specific background check is performed as per the contractual agreement with the Client.

New joiners are required to sign an NDA, Code of Business Conduct and Ethics, and an undertaking of acceptance to adhere

[19] BGV is conducted only for lateral and contractual hires. For project interns and regularized employees, BGV is not conducted.

to the information security policies and procedures on the Onboarding portal at the time of joining the BPO Operations. New joiners to Ramco are mandated to go through an Organizational Induction Training covering the details on functioning of different internal teams in Ramco[20]. New joiners are educated on Information security practices as a part of joining formalities via Ramco Academy portal and assessment is completed within 90 days of joining[21]. A Mandatory induction program is conducted by the HR for new joiners to Ramco on the date of joining[22]. The training records are reviewed and uploaded in the Ramco ERP (Ramco Hub) Repository by the Ramco Training team member. Exceptions to the trainings, if any, are reported to the respective Business Unit Heads on a periodic basis and followed up on until completion.

On an annual basis, a refresher program and ISMS assessment is conducted for employees, which covers broad aspects of information security and awareness.

At the time of voluntary separation of a resource, an exit request is initiated by the employee through the ESS ('Employee Self Service') portal based on approval by the Resource Manager. Ramco employees leaving the organization are required to get an online 'Clearance Automation' (No Dues) from the respective Department Heads, based on the e-mail trigger from the HRSS application. For regular (includes lateral and campus) hires, the Ramco HR team conducts an exit discussion with the employee.

[20] Regularized employees take up the information security practices training when they are onboarded as project trainees.
[21] Not applicable for Project trainees and Third-party resources.
[22] Regularized employees take up the information security practices training when they are onboarded as project trainees.

Control Activities

Control Objectives and Related Controls

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 related controls are included in Section 4, they are, nevertheless, an integral part of Ramco's description of controls.

Complementary User Entity Controls

In the design of its controls, Ramco has envisaged certain controls to be exercised by the user entities. These controls are listed in Section 4 for each of the control objective under the heading "Complementary User Entity Controls". The responsibility for design, implementation, and operating effectiveness of these controls rests with the user entities. This information has been provided to the user entities and their auditors to be taken into consideration when making assessments of control risk for the user entities[23].

Although, the Complementary User Entity Controls are included in Section 4, they do not form part of scope of the report.

Complementary Subservice Organization Controls

In the design of its controls, Ramco has envisaged certain controls to be exercised by subservice organization – Microsoft Corporation to maintain cloud back up of the payroll servers. The responsibility for design, implementation and operating effectiveness of these controls rests with the subservice organization. This information has been provided to the user entities and their auditors to be taken into consideration when making assessments of control risk for the user entities.

Although we have listed the subservice organization controls below, these complementary subservice controls do not form part of the scope of the report. The list of the complementary subservice organization controls listed below do not represent a comprehensive set of all the controls that should be employed by the subservice organization.

- Subservice organization is responsible for granting, revoking, managing and reviewing physical access to the data centers.
- Subservice organization is responsible for monitoring physical access points to data centers using Closed Circuit Television Camera (CCTV).
- Subservice organization is responsible for installing physical access points to data centers with electronic access control devices.
- Subservice organization is responsible for establishing and managing environmental safeguards related controls for the servers hosted within the Azure environment.

[23] The nature of operation of complementary user entity controls varies from one user entity to another.

SECTION 4

CONTROL OBJECTIVES, RELATED CONTROLS AND TESTS OF OPERATING EFFECTIVENESS

Payroll Processing – User Entity Onboarding

Control Objective: 1	*Controls provide reasonable assurance that the payroll processing system parameters in the payroll applications are established in accordance with specifications provided by the user entities.*

Control Number	Description of Controls	Test Performed	Results of Testing
1.01	For each new user entity, the BPO Processing team prepares a Payroll Process Book that defines payroll process specifications, including system parameters, based on the inputs received from the user entity. The Payroll Process Book is approved by the Account Head and Head of BPO Operations and is shared with authorized personnel from the user entity for validation.	• Inquired of the Senior Manager – BPO Operations, regarding the process of preparing the Process Book that defines the payroll process specifications, including system parameters, based on the inputs received from the new user entity. • For the user entities onboarded during the audit period, inspected the approval from the Account Head and Head of BPO to determine whether the Payroll Process Books capturing payroll process specifications, including system parameters were prepared and approved by the Account Head. • For the user entities onboarded during the audit period, inspected the e-mail communication, containing the Payroll Process Book sent to the authorized user entity personnel to determine whether the Payroll Process Books were communicated to the authorized user entity personnel for validation. • For the user entities onboarded during the audit period, inspected the e-mail communication, containing the Payroll Process Book, to determine whether the validation was done by the user entity and acknowledgement for the process book was obtained.	No relevant exceptions noted.

Complementary User Entity Controls	• The user entity is responsible for providing inputs for the Process Book, validating and approving the Payroll Process Book.

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

Payroll Processing – Payroll Input Operations

Control Objective: 2	*Controls provide reasonable assurance that payroll inputs are validated for errors prior to processing.*

Control Number	Description of Controls	Test Performed	Results of Testing
2.01	A Payroll Calendar is communicated between the BPO Operations team (Operations Manager) and the authorized user entity personnel on a monthly or yearly basis prior to the start of the processing period as defined in the process book. Adherence to the Payroll Calendar timelines is tracked using a payroll tracker by the BPO team during the payroll processing period[6].	• Inquired of the Senior Manager – BPO Operations, regarding the process of communication of Payroll Calendar between the authorized user entity personnel and BPO Operations team and tracking of payroll progress using the payroll tracker. • For a selection of user entities, months and year, inspected the e-mail communications to determine whether the Payroll Calendar was communicated between the authorized user entity personnel on a periodic basis prior to the start of payroll processing period. • For a selection of user entities and months, inspected the payroll tracker to determine whether adherence to the Payroll Calendar timelines was tracked by the BPO team during the payroll processing period.	No relevant exceptions noted.
2.02	Input files are received from the authorized user entity personnel through agreed mode of communication (e-mails / SFTP) as defined in process book prior to processing the payroll.	• Inquired of the Senior Manager – BPO Operations, regarding the process of receiving the input files from the authorized user entity personnel as per the agreed mode of communication prior to processing the payroll. • For a selection of user entities and months, inspected the 'Payroll Process Book' to determine whether the mode of communication was defined, documented and agreed with the user entity. • For a selection of user entities and months, inspected the e-mails / SFTP path for the input files to determine whether the input files were received from the authorized user entity personnel as per the agreed mode of communication as defined in process book prior to processing the payroll.	No relevant exceptions noted.
2.03	Payroll applications are configured to restrict uploading of erroneous data records	• Inquired of the Senior Manager – BPO Operations, regarding the application controls configured on Ramco payroll	No relevant exceptions noted.

Control Number	Description of Controls	Test Performed	Results of Testing
	including invalid employee number, blank input data, invalid input dates[7].	applications to prevent upload of data records until the errors are rectified. • Inspected the 'Payroll Process Book' document to determine whether the process for configuring the payroll applications to not allow the upload of data records until the errors specified were rectified was defined and documented. • Inspected the validation configuration in the payroll application to determine whether the applications were configured to prevent upload of data records until the errors were rectified.	

Complementary User Entity Controls	• The user entity is responsible for sharing the payroll calendar if agreed in the Payroll Process Book. • The user entity is responsible for providing complete and accurate input for payroll processing as per the agreed format. • The user entity is responsible for providing input data on a timely basis as per the agreed deadlines in the monthly Payroll Calendar. • The user entity is responsible for validation of payroll data where ESS interface for upload of data on Ramco Enterprise Series application has been deployed based on user entity specific requirement.

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

Payroll Processing Operations

Control Objective: 3	*Controls provide reasonable assurance that payroll data, reimbursement data and Full and Final settlement is processed completely and accurately.*

Control Number	Description of Controls	Test Performed	Results of Testing
3.01	Payroll applications are configured to prevent payroll processing until payroll readiness check is complete. The payroll readiness check includes the following key validations: • Payment method has been defined for the employees; and • Previous payroll processing period has been authorized[8].	• Inquired of the Senior Manager – BPO Operations, regarding the key validations included in the payroll readiness check prior to payroll processing. • Inspected the 'Payroll Process Book' document to determine whether the process to perform payroll readiness check prior to payroll processing and the key validations performed as a part of the payroll readiness check were defined and documented. • Inspected the output of payroll processing run without performing the payroll readiness check to determine whether the application terminated the payroll process run before readiness check and whether the following key validations were included as a part of the payroll readiness check: - Payment method was defined for the employees; and - Previous payroll processing period had been authorized.	No relevant exceptions noted.
3.02	A reconciliation of the payroll input file and the output file is performed on a monthly basis by the Quality Assurance (QA) team. Errors identified, if any, are communicated to the Process Executives for correction.	• Inquired of the Senior Manager – BPO Operations, regarding the process of reconciliation of the payroll input file with the output file by the Quality Assurance team. • Inspected the 'Payroll Process Book' document to determine whether the process of reconciling the input file with the payroll output file was defined and documented. • For a selection of user entities and months, inspected the e-mail communications from the QA team to the Payroll Processing team to determine whether the payroll input file was reconciled with the output file.	No relevant exceptions noted. *Note: We were informed that there were no discrepancies identified during the QA reconciliation, during the audit period.*

Control Number	Description of Controls	Test Performed	Results of Testing
3.03	The draft payroll register along with the payroll variance report are reviewed against user entity input data and approved by the Operations Manager prior to dispatch to the user entities through the agreed mode of communication[9].	• Inquired of the Senior Manager – BPO Operations, regarding the process of reviewing the draft payroll register and variance report prior to dispatch to the user entity. • Inspected the 'Payroll Process Book' document to determine whether the process of review and approval of the draft payroll and variance report prior to dispatch to the user entity through the agreed mode of communication was defined and documented. • For a selection of user entities and months, inspected the e-mail communication of the draft payroll register and the payroll variance report to determine whether the documents were reviewed and approved by the Operations Manager prior to dispatch to the user entity through the agreed mode of communication.	No relevant exceptions noted.

Complementary User Entity Controls	• The user entity is responsible for providing complete and accurate inputs for payroll processing as per the agreed format.

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

Payroll Output Operations

Control Objective: 4	*Controls provide reasonable assurance that the final payroll registers are authorized by the user entity and pay slips are distributed on a timely basis.*

Control Number	Description of Controls	Test Performed	Results of Testing
4.01	The draft payroll register and variance report are dispatched to the authorized user entity personnel for validation. Changes, if any, are communicated by authorized user entity personnel[10].	• Inquired of the Senior Manager – BPO Operations, regarding the process of dispatching the draft payroll register and variance report to the authorized user entity personnel for validation and the communication of changes identified by the authorized user entity personnel. • Inspected the 'Payroll Process Book' document to determine whether the process of dispatching the draft payroll register and variance report to the authorized user entity personnel for validation and the process of communication of changes identified by the authorized user entity personnel was defined and documented. • For a selection of user entities and months, inspected the e-mail communication of the draft payroll register and variance report to determine whether the documents were dispatched to the authorized user entity personnel for validation.	No relevant exceptions noted.
4.02	The Operations Manager approves final payroll registers and variance reports prior to dispatch to authorized user entity personnel.	• Inquired of the Senior Manager – BPO Operations, regarding the process of approving the final payroll register and variance reports prior to dispatch to the authorized user entity personnel. • Inspected the 'Payroll Process Book' document to determine whether the process of approving the final payroll register and reports prior to dispatch to authorized user entity personnel was defined and documented. • For a selection of user entities and months, inspected the e-mail communication to determine whether the final payroll register and variance reports were approved by the Operations Manager prior to dispatch to the	No relevant exceptions noted.

Control Number	Description of Controls	Test Performed	Results of Testing
		authorized user entity personnel.	
4.03	The pay slips are generated based on the final payroll register and dispatched to the user entity through the agreed mode of communication as per the timelines defined in the Payroll Calendar[11].	• Inquired of the Senior Manager – BPO Operations, regarding the process of generating and dispatching pay slips to the user entity based on the mode of communication agreed with the user entity as per the timelines defined in the Payroll Calendar. • For a selection of user entities, inspected the Payroll Process Book to determine whether the process of generating and distributing pay slips to the user entity was defined and documented. • For a selection of user entities and months, inspected the payroll tracker and the e-mail communications to the user entity to determine whether pay slips were dispatched to the user entities as per the timelines defined in the Payroll Calendar.	No relevant exceptions noted.
4.04	The Compliance team prepares the output for statutory compliance which is approved by the Account Head/Operations Manager prior to dispatch to the user entity and / or filing with the regulatory body based on a defined checklist[12].	• Inquired of the Senior Manager – BPO Operations, regarding the process of preparation and approval of output for statutory compliance prior to dispatch to the user entity and / or filing with the regulatory body based on a defined checklist. • Inspected the 'Payroll Process Book' document to determine whether the process of preparation and approval of output for statutory compliance prior to dispatch to the user entity and / or filing with the regulatory body was defined and documented. • For a selection of user entities and months, inspected the statutory compliance checklists and e-mail communications to determine whether the output for statutory compliance was approved by the Account Head/ Operations Manager prior to dispatch to user entity and/or filing with the regulatory body.	No relevant exceptions noted.

Control Number	Description of Controls	Test Performed	Results of Testing
4.05	The Payroll application is configured to restrict any processing after payroll period closure is performed in the application by the BPO team leader based on the Payroll Calendar / intimation from the user entity.	• Inquired of the Senior Manager – BPO Operations, regarding the closure of the payroll processing period after receiving user entity approval on the final payroll register / based on the schedule defined in the Payroll Calendar. • Inspected the ‘Payroll Process Book’ document to determine whether the process of closure of payroll processing period by the BPO Team Leader was defined and documented. • Inspected the configuration in the payroll application to determine whether the applications were configured to prevent payroll processing after the closure of payroll period. • For a selection of user entities and payroll cycles, inspected the e-mail communications from the user entity / the Payroll Calendar to determine whether the payroll process period was closed after receiving user entity approval on the final payroll register / based on the schedule defined in the Payroll Calendar. • For a selection of user entities and payroll cycles, performed negative testing to determine whether the payroll application restricted the processing after the payroll period closure.	No relevant exceptions noted.

Complementary User Entity Controls	• The user entity is responsible for authorization to close the payroll period on a timely basis. • The user entity is responsible for validating the draft and final payroll registers and communicating changes, if any.

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

Income Tax filing process

Control Objective: 5	*Controls provide reasonable assurance that income tax computation is performed accurately.*

Control Number	Description of Controls	Test Performed	Results of Testing
5.01	A calendar for the income tax processing and filing is communicated between the BPO Operations team and the authorized user entity personnel prior to the commencement of income tax processing[13].	• Inquired of the Senior Manager – BPO Operations, regarding the communication of the income tax processing and filing calendar between the BPO Operations team and the authorized user entity personnel and tracking of progress of tax processing and filing activities using the calendar. • Inspected the 'BPO Year-end process' document to determine whether the process of communication of a calendar for tax processing and filing between the BPO Operations team and authorized user entity personnel and tracking of progress of tax processing and filing activities using the calendar was defined and documented. • For a selection of user entities, inspected the e-mail communication between the BPO Operations team and the authorized user entity personnel to determine whether the calendar for income tax processing and filing was communicated prior to the commencement of income tax processing and that detailed activity and timelines for the processing period were defined and documented in the same.	No relevant exceptions noted.
5.02	Proofs for income tax related claims received from the authorized user entity personnel and the acknowledgement of receipts sent to the authorized user entity personnel are only through the agreed mode of communication as defined in the process book.	• Inquired of the Senior Manager – BPO Operations, regarding the process of receiving and acknowledging proofs for income tax related claims from the user entity. • Inspected the 'Payroll Process Book' document to determine whether the process of receiving and acknowledging proofs for income tax related claims from the user entity was defined and documented. • For a selection of user entities, inspected the input files received from the user entities through e-mail / SFTP to determine whether the input files were received only through the	No relevant exceptions noted.

Control Number	Description of Controls	Test Performed	Results of Testing
		mode of communication agreed with the user entities. - For a selection of user entities, inspected e-mail communications from the BPO Process team to the authorized user entity personnel to determine whether the receipt of income tax claims related proofs was communicated as per the agreed mode of communication.	
5.03	The following key validation checks are performed, as appropriate for the countries, during the upload of data related to income tax, into payroll applications: - Blank 'Employee Number' field; - Blank 'Input Date' field; - Duplicate entries;	- Inquired of the Senior Manager – BPO Operations, regarding the key validations configured within the payroll applications during the upload of income tax related data into payroll applications. - Inspected the 'Payroll Process Book' document to determine whether the key validations configured within the payroll applications during the upload of income tax related data into payroll applications were defined and documented. - Inspected the configuration of the key validations (Blank 'Employee Number' field, Blank 'Input Date' field and Duplicate entries) performed by the payroll applications and the income tax checklist to determine whether the key validations were configured in the payroll applications.	No relevant exceptions noted.
5.04	The income tax slips are downloaded from the payroll applications and are distributed to the employees of the user entities as per the agreed mode of communication.	- Inquired of the Senior Manager – BPO Operations, regarding the process of downloading and distributing the income tax slips to the employees based on the agreed mode of communication with the user entity. - Inspected the 'Payroll Process Book' document to determine whether the process of downloading and distributing the income tax slips to the employees of the user entities based on the agreed mode of communication was defined and documented. - Inspected the income tax slips shared with user entities through e-mail / ESS portal to determine whether the income tax slips downloaded from the payroll applications were distributed to the employees of the user entities as per the agreed mode of	No relevant exceptions noted.

Control Number	Description of Controls	Test Performed	Results of Testing
		communication.	

Complementary User Entity Controls	• The user entity is responsible for sharing the income tax calendar if agreed in the Payroll Process Book • The user entity is responsible for providing the proofs for income tax related claims.

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

Audit Trail[14]

Control Objective: 6	*Controls provide reasonable assurance that the in-scope payroll applications and database are configured to capture audit trail in accordance with the specifications provided by the user entity.*

Control Number	Description of Controls	Test Performed	Results of Testing
6.01	There exists audit trail configuration in the payroll application for the transactions processed for by the user entity.	• Inquired of the Director – BPO Operations, regarding the process of configuring audit trail within payroll application and database for the transactions processed by the user entity. • For a selection of user entities, inspected the audit trail configuration to determine whether the audit trail was configured in the payroll application for the transactions processed by the user entity.	No relevant exceptions noted. .
6.02	Access to audit trail configuration is restricted to BPO Technical team. Access to audit trail configuration is provided based on the approval from BPO Business Head.	• Inquired of the Director – BPO Operations, regarding the process of granting access to audit trail configuration by the BPO Business Head. • Inspected the list of users having access to audit trail configuration to determine whether the access to audit trail configuration was restricted to BPO Technical team. • For a selection of users servicing the user entities, whose access to audit trail configuration was granted during the audit period, inspected the approval emails to determine whether the access to audit trail configuration was granted based on the approval from BPO Business Head.	No relevant exceptions noted.
6.03	Failure to audit trail logs are notified to Ramco BPO Technical team through an e-mail alert and failures identified are tracked to closure.	• Inquired of the Director – BPO Operations, regarding the process of notification of audit trail logs failures to Ramco BPO Technical team. • Inspected the audit trail failure configuration from the payroll application to determine whether the failure to audit trail logs was notified to Ramco BPO Technical team through an e-mail alert.	No relevant exceptions noted. *Note: It was noted that there were no failure requests raised to the audit trail logs in rTrack application during the audit period.*

Control Number	Description of Controls	Test Performed	Results of Testing
6.04	Audit trail logs are retained for a minimum of eight years by the Ramco BPO Technical team[16].	• Inquired of the Director – BPO Operations, regarding the process of retaining audit trail logs by Ramco BPO Technical team. • For a selection of user entities, inspected the audit trail logs to determine whether the audit trail logs were retained for a minimum of eight years by the Ramco BPO Technical team.	No relevant exceptions noted.
6.05	Privileged-level access to audit trail configuration within the payroll application is restricted to authorized personnel from Ramco BPO Technical team.	• Inquired of the Director – BPO Operations, regarding the process of restricting privileged-level access to audit trail configuration within the payroll application to authorized personnel from Ramco BPO Technical team. • Inspected the list of users having privileged-level access to audit trail configuration within the payroll application to determine whether the access was restricted to authorized personnel from Ramco BPO Technical team.	No relevant exceptions noted.
6.06	Shared or generic accounts with access to privileged tasks or functions to the audit trail configuration within the payroll application are restricted to authorized personnel from Ramco BPO Technical team.	• Inquired of the Director – BPO Operations, regarding the process of restricting shared or generic accounts to authorized personnel within the payroll application from Ramco BPO Technical team.	No relevant exceptions noted. *Note: It was noted that there were no shared or generic accounts who had access to audit trail configuration during the audit period.*
6.07	The changes to audit trail configuration are approved by the Base Product Quality Assurance (QA) team prior to migrating into the production environment.	• Inquired of the Director – BPO Operations, regarding the process of approving changes to audit trail configuration. • Inspected the 'Change Management Guideline' document to determine whether the process for raising change requests to audit trail configuration was defined and documented.	No relevant exceptions noted. *Note: It was noted that there were no change requests raised in rTrack application to audit trail configuration during the audit period.*

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

Information Systems Administration – Information Security Framework

Control Objective: 7	*Controls provide reasonable assurance that IS policies and procedures are documented, approved, and communicated.*

Control Number	Description of Controls	Test Performed	Results of Testing
7.01	Ramco QMG team has defined an ISMS policy and ISMS Manual, which is reviewed and approved by the CISO on an annual basis. The policy is made available to Ramco employees through the intranet portal (MyRamco).	• Inquired of the QMG Deputy Manager, regarding the process for Information Security management and whether the ISMS policy and manual were reviewed and approved by the CISO on an annual basis and available to Ramco employees through the intranet portal (MyRamco). • Inspected the 'ISMS Policy' and 'ISMS Manual' document to determine whether the process for Information Security management was defined and documented and whether the process was reviewed and approved by the CISO on an annual basis. • For a selection of employees, inspected the intranet portal to determine whether the policy was made available to Ramco employees through the intranet portal (MyRamco).	No relevant exceptions noted.
7.02	Security awareness is spread through password protected screen savers defined by the IMG team for Ramco employees.	• Inquired of the QMG Deputy Manager, regarding the process of Security awareness for Ramco employees. • Inspected the 'Screensaver settings' in Ramco Group policy to determine whether security awareness was spread through password protected screen savers defined by the IMG team for Ramco employees. • For a selection of workstations, inspected the group policy settings to determine whether security awareness was spread through password protected screen savers defined by the IMG team for Ramco employees.	No relevant exceptions noted.

Control Number	Description of Controls	Test Performed	Results of Testing
7.03	Information security policy and procedure documents are hosted on the intranet portal and are accessible to the employees for their reference.	• Inquired of the QMG Deputy Manager, regarding the process of documenting Information security policy and procedures and whether these documents were hosted on the intranet portal and were accessible to the employees for their reference. • For a selection of employees, inspected the Information Security policy and procedure documents in the intranet portal to determine whether these documents were hosted on the intranet portal and were accessible to the employees for their reference.	No relevant exceptions noted.
7.04	Any changes to the security practices or occurrence of incidents are communicated to the employees through Security awareness e-mails sent by the CISO.	• Inquired of the CISO, regarding the process of sending Security awareness e-mail to Ramco employees. • Inspected the security awareness e-mail communication to determine whether e-mails on security awareness are communicated to the employees by the CISO.	No relevant exceptions noted. *Note: We were informed that there were no changes in security practices or occurrence of incidents raised in the rTrack application during the audit period.*

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

Information Systems Administration – Change Management

Control Objective: 8	*Controls provide reasonable assurance that changes to the payroll applications and database are approved, tested and authorized prior to implementation.*

Control Number	Description of Controls	Test Performed	Results of Testing
8.01	Change requests are raised through rTrack application having a unique change request number. The change request is approved by the Account Head / Operations Manager / Head of BPO Operations.	• Inquired of the Senior Manager – BPO Operations, regarding the process for raising changes to the payroll applications. • Inspected the ‘Change Management Guideline’ document to determine whether the process for raising change requests was defined and documented. • For the changes to the payroll applications, inspected the change request tickets from rTrack application to determine whether the tickets were having a unique change request number. Further, inspected the change request ticket to determine whether the requests were approved by the Account Head / Operations Manager / Head of BPO Operations prior to development.	No relevant exceptions noted.
8.02	For changes, an impact analysis is carried out by the Technical Support team based on outcome of the impact analysis, risk of implementation is analyzed and approved by the Technical Manager.	• Inquired of the Senior Manager – BPO Operations, regarding the process of performing an impact analysis for change requests. • Inspected the ‘Change Management Guideline’ document to determine whether the process for performing an impact analysis for the changes was defined and documented. • For the changes to the payroll applications, inspected the change request tickets to determine whether an impact analysis was carried out by the Technical Support team and the risk of implementation is analyzed and approved by the Technical Manager.	No relevant exceptions noted.

Control Number	Description of Controls	Test Performed	Results of Testing
8.03	Test cases and expected test results are documented by the Process Executive. Technical team tests the changes in the test environment and the actual test results are approved by the Technical Manager prior to implementation in the production environment.	• Inquired of the Senior Manager – BPO Operations, regarding the process of documenting test cases, expected test results for changes and obtaining approval for the actual test results by the Technical Manager prior to implementation in the production environment. • Inspected the 'Change Management Guideline' document to determine whether the process of documenting test cases, expected test results and approval of actual test results from the Technical Manager prior to implementation in the production environment was defined and documented. • For the changes to the payroll applications, inspected the test cases and expected test results to determine whether they were documented by the Process Executive. Further, inspected the test documents to determine whether the actual test results were approved by the Technical Manager prior to implementation in the production environment.	No relevant exceptions noted.
8.04	Access to migrate changes to the production environment is restricted to the authorized members of the Technical Support team as defined in the Software Configuration Management Plan.	• Inquired of the BPO Technical Support Team Leader, regarding the process of restricting the access to migrate changes to the production environment to authorized members of the Technical Support team. • Inspected the 'Software Configuration Management Plan' document to determine whether the process of providing access to migrate changes to the production environment was defined and documented. • Inspected the list of users with access to the production environment of the payroll applications and their defined roles in the application to determine whether the access to migrate changes to the production environment was restricted to authorized members of the Technical Support team.	No relevant exceptions noted.

Control Number	Description of Controls	Test Performed	Results of Testing
8.05	User Acceptance Testing is performed by the Process Executive and approved by the Operations Manager for the changes implemented.	• Inquired of the BPO Technical Support Team Leader, regarding the process of performing User Acceptance Testing for the changes implemented. • Inspected the 'Software Configuration Management Plan' document to determine whether the process of performing User Acceptance Testing for the changes implemented was defined and documented. • For changes to the payroll applications, inspected the testing documentation to determine whether User Acceptance Testing was performed by the Process Executive and approved by the Operations Manager for the changes implemented.	No relevant exceptions noted.

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

Information Systems Administration – Logical access

Control Objective: 9	*Controls provide reasonable assurance that logical access to payroll applications (Ramco e.Application and Ramco Enterprise Series application) is restricted to authorized personnel[24].*

Control Number	Description of Controls	Test Performed	Results of Testing
9.01	Access to the payroll applications is initiated through rTrack / e-Mail communication and access to Payroll application is controlled through a unique user ID and password assigned to the BPO team members based on an approval from the Operations Manager / Account Head.	• Inquired of the Senior Manager – BPO Operations, regarding the process of providing access to the payroll applications. • Inspected the 'Technical Support' document to determine whether the process for creation of access with a unique user ID and password to the payroll applications was defined and documented. • For a selection of new joiners, to the BPO Operations during the period with access to the payroll applications, inspected the rTrack / e-Mail communication to determine whether access to the payroll application module was defined; and whether the requests were approved by the Operations Manager / Account Head.	No relevant exceptions noted.
9.02	In the event of changes to the job responsibilities, access to specific user entity data is granted / revoked based on authorization from the Operations Manager / Account Head.	• Inquired of the Senior Manager – BPO Operations, regarding the process of granting and revoking access to the payroll application in the event of change of job responsibilities. • Inspected the 'Technical Support' document to determine whether the process for granting / revoking access to specific user entity data in the event of change in job responsibilities was defined and documented.	No relevant exceptions noted. *Note: We were informed that there were no changes to job responsibilities during the audit period.*
9.03	Password parameters in AD and database are configured as below[17]: • Minimum password length is set to eight characters • Password complexity is enabled to include alphanumeric and special characters	• Inquired of the BPO Technical Manager, regarding the password parameters configured on the payroll applications. • Inspected the 'Technical Support' document to determine whether the password parameters for the payroll applications were defined and documented. • Inspected the password settings of the Ramco's AD and database to determine whether the password settings were	No relevant exceptions noted.

[24] MAGNA and 4X applications.

Control Number	Description of Controls	Test Performed	Results of Testing
	• Maximum unsuccessful login attempts prior to being locked out is three • Maximum number of passwords remembered is five • Maximum number of login failures for account lockout is three • Minimum number of minutes for screensaver to enable is five.	configured in line with the policy.	
9.04	Access to payroll applications, for employees who leave the BPO Operations team, is revoked by the BPO Technical Team Leader on receipt of e-mail from the HR / Operations Manager within one day from the last working day of the employee.	• Inquired of the Senior Manager – BPO Operations, regarding the process of revoking the access rights of employees leaving the BPO Operations team. • Inspected the 'Technical Support' document to determine whether the process for revoking the access rights of employees leaving the BPO Operations team was defined and documented. • For a selection of employees with access to payroll applications, who had left the BPO Operations team during the period, inspected the e-mail communications from the HR/ Operations Manager to determine whether the access rights were revoked within one day from the last working day of the employee. • Further, inspected the user access list of the payroll applications to determine whether the user IDs of the employees who left the BPO Operations team were revoked within one day from the last working day of the employee.	**Exceptions noted**. It was noted that for five out of 13 leavers, access to the payroll application was revoked with a delay of one to 76 days. However, inspected the last login date from the payroll application and the activity logs noted that the leavers had not logged in the application after their last working day. ***Management response:*** Payroll application has not been accessed by the exited employees after their last working day. This ensures that there has been no unauthorized access to sensitive / confidential information.
9.05	List of personnel having access to the payroll applications is reviewed on a quarterly basis by the Account Head / VP BPO to identify and revoke any access that is no longer required.	• Inquired of the Senior Manager – BPO Operations, regarding the process of reviewing user access rights on the payroll applications. • Inspected the 'Technical Support' document to determine whether the process for review of access to payroll application on a quarterly	No relevant exceptions noted.

Control Number	Description of Controls	Test Performed	Results of Testing
		basis was defined and documented. • For a selection of quarters, inspected the access review reports to determine whether accesses to the payroll applications were reviewed by the Account Head / VP BPO to identify and revoke access that was no longer required.	
9.06	Ramco employees are granted access to Ramco's AD using ESS ('Employee Self Service') portal, after unique ID is created by the HR team in the HRSS application.	• Inquired of the Manager – IMG team, regarding ID creation process on the Ramco's AD. • Inspected the 'Logical Access Control Process' document to determine whether the process for granting access to Ramco's AD was defined and documented. • For a selection of new joiners, to the BPO Operations, inspected the access request notification e-mail/ e-mail communication from HR/ asset allocation date to determine whether Ramco employees were granted access to Ramco's AD using ESS ('Employee Self Service') portal, after unique ID was created by the HR team in the HRSS application.	No relevant exceptions noted.
9.07	User IDs of resigned / terminated Ramco employees on the Ramco's AD are revoked based on status update of the employee by the HR team in the ESS portal, based on approval from the Operations Manager/ Account Head, BPO[18].	• Inquired of the Manager – IMG team, regarding the ID deletion process in the Ramco's AD. • Inspected the 'Logical Access Control Process' document to determine whether the process for revoking access to Ramco's AD was defined and documented. • For a selection of leavers from Ramco BPO during the audit period, inspected access revocation notification e-mail to determine whether user IDs of resigned / terminated Ramco employees on the Ramco's AD were revoked based on status update of the employee by the HR team in the ESS Portal, based on approval from the Operations Manager/ Account Head, BPO.	No relevant exceptions noted.
9.08	Administrative rights on the workstations are disabled by default on the workstations in Ramco BPO Operations work	• Inquired of the Manager – IMG team, regarding the administrative rights on the workstations.	No relevant exceptions noted. *Note: It was noted that there were no*

Control Number	Description of Controls	Test Performed	Results of Testing
	area. In case of any exception, approval from Operations Manager is obtained.	- For a selection of workstations in the BPO work area, inspected the administrative rights on the workstations to determine whether the administrative privileges were disabled in the workstations in Ramco BPO Operations.	*exception requests raised in the rTrack application for enabling administrative access during the audit period.*
9.09	AD password policies and account lockout policies are defined and enforced through the Ramco's AD.	- Inquired of the Manager – IMG team, regarding the AD password policies and account lockout policies. - Inspected the 'Password management guideline' policy to determine whether the password policies were defined and whether the policy was reviewed and approved by the CISO on an annual basis. - For a selection of workstations in the BPO work area, inspected the password settings to determine whether the AD password policies and account lockout policies were defined and enforced through the Ramco's AD.	No relevant exceptions noted.
9.10	Guest / anonymous accounts are disabled in the Ramco's AD and workstations in the BPO processing area by the IMG team.	- Inquired of the Manager – IMG team, regarding disabling the guest and anonymous accounts on Ramco's AD. - For a selection of workstations in the BPO work area, inspected the Active Directory guest and anonymous account status to determine whether the guest and anonymous accounts were disabled on the Ramco's AD.	No relevant exceptions noted. *Note: It was noted that there were no exception requests raised in the rTrack application for enabling Guest / anonymous accounts during the audit period.*
9.11	CD-ROM drives and USBs are disabled by default on the workstations in Ramco BPO work area and access is granted by the IMG team based on the exception request raised in the rTrack application and approved by the Account Head.	- Inquired of the Manager – IMG team, regarding disabling CD- ROM drives and USBs by default on the workstations in Ramco BPO work area. - For a selection of workstations in the BPO work area, inspected the external media policy to determine whether CD-ROM drives and USBs were disabled by default on the workstations in Ramco BPO work area. - For a selection of workstations in the BPO work area with USB enabled, inspected the	No relevant exceptions noted.

Control Number	Description of Controls	Test Performed	Results of Testing
		rTrack request to determine whether the access to USB and CD-ROM rights were given based on the exception request raised in the rTrack and was approved by the Account Head.	

Complementary User Entity Controls	• The user entity is responsible for the configuration of the password rules in ESS portal, as applicable. • The user entity is responsible for access provisioning and de-provisioning for its employees wherever ESS website has been implemented.

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

Information Systems Administration – Back-up and restoration management

Control Objective: 10	*Controls provide reasonable assurance that payroll data is backed up and tested for restoration periodically.*

Control Number	Description of Controls	Test Performed	Results of Testing
10.01	Procedures for Backup, Retention and Restoration are defined and documented in the Backup and Restoration process document, which is prepared by the QMG team and approved by the CISO on an annual basis.	• Inquired of the Manager – IMG team, regarding the policy and procedure document which consist of the process for Backup, Retention, and Restoration. • Inspected the Backup policy and procedure document to determine whether the procedures for Backup, Retention, and Restoration were documented by the QMG team and approved by Ramco's CISO on an annual basis.	No relevant exceptions noted.
10.02	The payroll data stored in production server is fully backed up on a daily basis. The backup jobs are monitored for successful completion by the IMG; and failure, if any, are recorded and tracked to closure as a security incident by the IMG team.	• Inquired of the Manager – IMG team, regarding the process of monitoring the backup job for the backup of the payroll data stored in the production server. • Inspected the 'Backup Archival and Storage' procedure document to determine whether the process for daily backup of user entity data stored on the production server was defined and documented. • Inspected the 'Backup Schedule Configuration' to determine whether the payroll data stored in production server was fully backed up on a daily basis. • For a selection of days, inspected the automated e-mail generated from the backup application upon completion of backup to determine whether the user entity data stored in the production server were backed up on a daily basis. • For a selection of days where backup failure occurred, inspected the Risk Control Assessment (RCA) Document to determine whether the failure was recorded and tracked to closure as a security incident by the IMG team.	No relevant exceptions noted.
10.03	The backup tapes are moved to an offsite location on a weekly basis.	• Inquired of the Manager, IMG team, regarding the process of moving the backup	No relevant exceptions noted.

Control Number	Description of Controls	Test Performed	Results of Testing
	The backup tapes are accessible to authorized personnel within the IMG team.	tapes to an offsite storage location. • Inspected the 'Backup Archival and Storage' procedure document to determine whether it defined and documented the process of offsite storage of backup tapes. • For a selection of weeks, inspected the Tape Movement Register to determine whether the backup tapes were moved to the offsite storage location as per the backup schedule defined.	
10.04	Restoration test for data backup is carried out on a semi-annual basis through tickets raised on rTrack / rTask application or e-mail communication and the testing results are validated by the Technical Team Leader for the BPO Operations.	• Inquired of the IMG Manager, regarding the process of restoring the data in the backup tape on an annual basis. • Inspected the 'Backup Archival and Storage' procedure document to determine whether the process for restoration of backup was defined and documented. • Inspected the tickets raised on rTrack / rTask application or e-mail communication to determine whether the restoration of backed up data was performed on a semi-annual basis and the testing results are validated by the Technical Team Leader for the BPO Operations.	No relevant exceptions noted.

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

Information Systems Administration - Network Security

Control Objective: 11	*Controls provide reasonable assurance that access to Ramco's network is restricted to authorized users.*

Control Number	Description of Controls	Test Performed	Results of Testing
11.01	A specific Virtual Local Area Network ('VLAN') is assigned for the BPO network in Ramco and access is restricted to the Ramco BPO operations in the VLAN segment.	• Inquired of the Manager - IMG team, regarding the process of VLAN segregation for the BPO network in Ramco and whether access was restricted to the Ramco BPO employees in the VLAN segment. • Inspected the VLAN configuration for Ramco BPO to determine whether a specific Virtual Local Area Network ('VLAN') was assigned for the BPO network in Ramco. • Inspected the access control list to determine whether access is restricted to the Ramco BPO employees in the VLAN segment.	No relevant exceptions noted.
11.02	Access to internet is restricted by IMG team for Ramco BPO employees through Websense / Zscaler content filter[19]. Access to websites other than the sites configured in the firewall in content filter is provided by the IMG team based on approval from the Account Head/ VP -BPO through the request raised in rTrack / rTask application.	• Inquired of the Manager - IMG team, regarding the process of access restriction for the Ramco BPO employees through Websense / Zscaler content filter and access to websites other than the sites configured in the firewall. • Inspected the Websense / Zscaler content filter configuration to determine whether access to internet was restricted by the IMG team for the Ramco BPO employees through Websense / Zscaler content filter. • For the population of request raised in rTrack / rTask application during the audit period, inspected the ticket details to determine whether the access to websites other than the sites configured in the firewall in the content filter was provided by the IMG team based on the approval obtained from the Account Head/ VP -BPO.	No relevant exceptions noted.
11.03	Antivirus software is activated / updated on workstations at the time of logging-in. Antivirus software / database is updated when the software vendor issues a new release, through centralized ePO Server and is configured to	• Inquired of the Manager - IMG team, regarding the process of activating / updating workstations at the time of logging in and whether antivirus software / database was updated when the software vendor issues a new release, through centralized ePO Server and was configured to receive real time	No relevant exceptions noted.

Control Number	Description of Controls	Test Performed	Results of Testing
	receive real time signature ('DAT') updates.	signature ('DAT') updates. • Inspected the antivirus configuration screenshot to determine whether it was configured to receive real time signature ('DAT') updates. • For a selection of workstations in the BPO work area, inspected the Antivirus patch update date and version to determine whether antivirus software / database was updated when the software vendor issued a new release, through centralized ePO Server.	
11.04	The Ramco IMG team monitors the antivirus server console on a real time basis to check whether workstations are updated with latest released definition. On a daily basis, monitoring reports along with the percentage of compliance are generated and sent to the Desktop team and the Head of IMG.	• Inquired of the Manager - IMG team, regarding the process of monitoring the antivirus server console. • Inspected the 'antivirus server console' to determine whether the Ramco IMG team monitors the antivirus server console on a real time basis to check whether workstations were updated with latest released definition. • For a selection of dates, inspected the antivirus monitoring reports to determine whether on a daily basis, monitoring reports along with the percentage of compliance were generated and sent to the Desktop team and the Head of IMG.	No relevant exceptions noted. *Note: It was noted from rTrack application that there were no incidents for antivirus compliance failure during the audit period.*
11.05	Incoming and outgoing e-mails messages and attachments are scanned at the mail server level and gateway level for spam and virus.	• Inquired of the IMG Manager - IT Infrastructure Management team, regarding the implementation of e-mail scanning at the mail server level and gateway level for spam and virus. • Inspected Ramco's network diagram to determine whether the Incoming and outgoing e-mail messages and attachments were scanned at the mail server level and gateway level for spam and virus. • Inspected Ramco's e-mail scanning configuration to determine whether the Incoming and outgoing e-mail messages and attachments were scanned at the mail server level and gateway level for spam and virus.	No relevant exceptions noted.
11.06	On an annual basis, Vulnerability Assessment and Penetration Testing ('VAPT') on Ramco	• Inquired of the CISO, regarding VAPT tests performed on Ramco's network by an	No relevant exceptions noted.

Control Number	Description of Controls	Test Performed	Results of Testing
	network is conducted by an external vendor and the results are documented.	external vendor. • Inspected the report related to the VAPT review conducted during the audit period to determine whether the VAPT was conducted on Ramco's network on an annual basis by the external vendor and the results were documented.	

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

Information Systems Administration - Physical Access

Control Objective: 12	*Controls provide reasonable assurance that physical access to Ramco facility, BPO work area, and the data center is restricted to authorized personnel and monitored for detecting unauthorized access.*

Control Number	Description of Controls	Test Performed	Results of Testing
12.01	Ramco QMG team has defined and documented a Physical and Environmental Security Policy, which is approved by the CISO on an annual basis. The Physical and Environmental Security Policy is made available to the Ramco employees through the intranet portal.	• Inquired of the QMG Deputy Manager, regarding the Physical and Environmental Security Policy / Procedure which consists of the process for controlling physical access to the Ramco facility and data center. • Inspected the 'Physical and Environmental Security Policy' document to determine whether Ramco QMG team had defined and documented a Physical Security Policy, which was approved by the CISO on an Annual basis. • Inspected the intranet portal to determine whether the Physical and Environmental Security Policy was made available to the Ramco employees through the intranet portal.	No relevant exceptions noted.
12.02	Physical access to Ramco facility and BPO work area is monitored by Security Guards round the clock for restricting unauthorized access.	• Inquired of the Head of Administration, regarding the process of monitoring the premises round the clock. • Inspected the 'Physical and Environmental Security Policy' document to determine whether the process of manning the premises round the clock was defined and documented. • Performed a physical walkthrough of Ramco facility and BPO work area to determine whether access to Ramco facility and BPO work area was monitored by Security guards for restricting unauthorized access. • For a selection of dates and shifts, inspected the attendance register of the security personnel to determine whether the entrance and exit of Ramco facility and BPO work area was monitored round the clock for restricting unauthorized access.	No relevant exceptions noted.

Control Number	Description of Controls	Test Performed	Results of Testing
12.03	Entry and exit details of the vendors / visitors to Ramco facility are recorded via Visitor Log register by the Security team. Vendors / Visitors entering the facility are issued a visitors' badge and a visitor slip that captures the date, contact, person to meet, and purpose of their visit. Electronic devices (laptop, USB devices) are declared at the entrance of Ramco facility.	• Inquired of the Head of Administration, regarding the process of recording entry and exit details of vendors / visitors to Ramco facility. • For a selection of dates, inspected the 'Visitor badge' and 'Visitor slip' to determine whether vendors/ visitors entering the facility were issued a visitors' badge and a visitor slip that captures the date, contact, person to meet, and purpose of their visit. • Inspected the 'Laptop declaration register' to determine whether electronic devices (laptop, USB devices) were declared at the entrance of Ramco facility.	No relevant exceptions noted.
12.04	Physical access to Ramco facility and BPO work area is granted by the HR personnel and provisioned by the Administration team based on the Request for ID card form from the HR personnel on the date of joining of the employee.	• Inquired of the Head of Administration, regarding the process of granting access to the BPO work area to the new joiners to the BPO Operations team. • Inspected the 'Physical and Environment Security' document to determine whether the process for granting access cards to new joiners to the BPO Operations team was defined and documented. • For a selection of new joiners to the BPO Operations, inspected the access request forms to determine whether physical access to Ramco facility and BPO work area was granted based on the Request for ID card form by the HR personnel on the date of joining of the employee.	No relevant exceptions noted.
12.05	Physical access to the Ramco facility and BPO work area is revoked by the Administration team on the Last Working Day of the employee after submission of access card and sign-off is provided on the 'Clearance Automation' in the ESS ('Employee Self Service') portal.	• Inquired of the HR Manager, regarding the process of revoking physical access to the BPO work area for leavers on the last day of employment as part of the exit formalities. • Inspected the 'Physical and Environment Security' document to determine whether the process of deactivation of access to BPO work area for employees leaving the company was defined and documented. • For a selection of resigned employees in the BPO Operations, inspected the e-mail notification for deactivation of access, received by the HR Manager from the HRSS	No relevant exceptions noted.

Control Number	Description of Controls	Test Performed	Results of Testing
		application. • For a selection of resigned employees in the BPO Operations, inspected the access control system records to determine whether access was revoked on the last working day of the employee.	
12.06	Closed Circuit Television ('CCTV') Cameras are in place at entry points in the Ramco facility and BPO process premises and are monitored by the Security Guard. The CCTV footage is retained for a period of 45 days.	• Inquired of the Head of Administration, regarding the process of monitoring access to the Ramco facility and BPO process premises. • Inspected the 'Physical and Environment Security' document to determine whether the process of monitoring access to Ramco facility and BPO process premises was defined and documented. • Performed a physical walkthrough of the Ramco facility and BPO process premises to determine whether CCTV cameras were installed at the entry / exit points. • Performed a physical walkthrough of the BMS room to determine whether the entry / exit to the Ramco facility and BPO process premises were monitored through a CCTV camera. • Inspected the CCTV footage stored by the BMS team to determine whether the footage was maintained for a period of 45 days.	No relevant exceptions noted.
12.07	Physical Access to the BPO work area is controlled through implementation of a proximity card reader at the entry / exit to the BPO work area.	• Inquired of the Head of Administration, regarding the process of restricting access to the BPO work area through proximity card reader. • Inspected the 'Physical and Environment Security' document to determine whether it defines the process for controlling access to the BPO work area through electronic proximity card was defined and documented. • Performed a physical walkthrough of the BPO work area to determine whether access to the BPO work area was controlled through a proximity card reader.	No relevant exceptions noted.

Control Number	Description of Controls	Test Performed	Results of Testing
12.08	List of personnel having access to the BPO work area is reviewed by the Account Head / VP BPO on a monthly basis and unauthorized access, if any, is identified and revoked by the HR, and de-provisioned by the Administration team.	• Inquired of the Head of Administration, regarding the process of review of access to the BPO work area on a weekly basis. • Inspected the 'Physical and Environment Security' document to determine whether the process for review of access to the BPO work area by the Account Head / VP BPO was defined and documented. • For a selection of months and weeks, inspected the access review report for the BPO work area to determine whether it was reviewed by the Account Head / VP BPO and unauthorized access, if any, was identified and revoked.	No relevant exceptions noted.
12.09	The entry / exit to the data center is monitored through CCTV camera. The CCTV footage is retained for a period of 45 days.	• Inquired of the Head of Administration, regarding the process of monitoring access to the data center. • Inspected the 'Physical and Environment Security' document to determine whether the process of monitoring access to data center was defined and documented. • Performed a physical walkthrough of the data center to determine whether CCTV cameras were installed at the entry / exit points. • Inspected the CCTV footage stored by the BMS team to determine whether the footage was maintained for a period of 45 days.	No relevant exceptions noted.
12.10	Access to the data center is controlled through a proximity card and biometric fingerprint reader.	• Inquired of the IMG Head, regarding the process of controlling access to data center. • Performed a physical walkthrough of the data center to determine whether the access to the data center was controlled through a proximity card and biometric fingerprint reader.	No relevant exceptions noted.

Control Number	Description of Controls	Test Performed	Results of Testing
12.11	Access to the data center is restricted to authorized members of the IMG based on approvals received from the IMG Head.	• Inquired of the IMG Head, regarding the process of restricting access to the data center. • Inspected the 'Physical and Environment Security' document to determine whether the process of restricting access to the data center was defined and documented. • Inspected the list of users having access to the data center to determine whether access to the data center was restricted to authorized members of the IMG.	No relevant exceptions noted.
12.12	Review of personnel authorized to access the data center is conducted on a monthly basis by the IMG Head and any unauthorized access is revoked as part of the same.	• Inquired of the IMG Head, regarding the process of reviewing the access to the data center. • Inspected the 'Physical and Environment Security' document to determine whether the process of reviewing the access to the data center was defined and documented. • For a selection of months, inspected the access review reports to determine whether the access rights to the data center were reviewed by the IMG Head and any unauthorized access was revoked as part of the review.	No relevant exceptions noted.
12.13	The entry / exit of visitors and vendors to data center is recorded in a visitor register and signed by an IMG team member, who is also required to accompany the visitor inside the data center.	• Inquired of the Head of Administration, regarding the process of granting access to data center for visitors and vendors. • Inspected the 'Physical and Environment Security' document to determine whether the process of granting access to data center for visitors and vendors was defined and documented. • Performed a physical walkthrough of the premises to determine whether visitors and vendors were provided access to the data center by an authorized IMG team member having access to the data center. • For a selection of days, inspected the visitor register maintained at the data center to determine whether the name of the visitor, purpose of visit, time of visit and the name of	No relevant exceptions noted.

Control Number	Description of Controls	Test Performed	Results of Testing
		IMG team member accompanying the visitor were recorded.	

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

Information Systems Administration - Environmental Security

Control Objective: 13	*Controls provide reasonable assurance that the facility including the data center and BPO work area are protected from environmental damage.*

Control Number	Description of Controls	Test Performed	Results of Testing
13.01	Smoke detectors, temperature monitoring devices, gas-based fire suppression system, and fire extinguishers, are installed for protection against environmental hazards such as fire, dust, power, excessive heat and humidity.	• Inquired of the Head of Administration, regarding the process of installing equipment for protection against environmental hazards. • Performed a physical walkthrough of the Ramco facility and data center to determine whether smoke detectors, temperature monitoring devices, gas-based fire suppression system, and fire extinguishers, were installed for protection against environmental hazards such as fire, dust, power, excessive heat and humidity.	No relevant exceptions noted.
13.02	Servers and network components are housed in the data center having raised floor and false ceiling.	• Inquired of the Head of Administration, regarding the installation of server and network components on the raised floor within the data center. • Performed a physical walkthrough of the Ramco facility and data center to determine whether servers and network components were housed in the data center having raised floor and false ceiling.	No relevant exceptions noted.
13.03	An Annual Maintenance Contract (AMC) for the equipment including fire extinguishers, smoke detectors, fire alarms and lifts are maintained, and the equipment are tested at periodic intervals by the respective vendors as per the AMC. Preventive maintenance reports are maintained and reviewed against the maintenance schedule by the Administration team.	• Inquired of the Head of Administration, regarding the AMC for equipment like fire extinguishers, smoke detectors, fire alarms and lifts, and whether preventive maintenance was performed for the equipment and reports were maintained and reviewed against the maintenance schedule by the Administration team. • Inspected the 'AMC' for equipment including fire extinguishers, smoke detectors, fire alarms and lifts to determine whether the equipment were maintained and were tested at periodic intervals by the respective vendors as per the AMC. • For a selection of quarters/months, inspected the preventive maintenance report to determine whether the maintenance of the equipment including fire extinguishers,	No relevant exceptions noted.

Control Number	Description of Controls	Test Performed	Results of Testing
		smoke detectors, fire alarms and lifts were performed in periodic intervals by the respective vendors as per the AMC and reviewed against the maintenance schedule by the Administration team.	
13.04	Power backup is provided through Uninterruptible Power Supply (UPS) and diesel generator sets to the facility.	• Inquired of the Head of Administration, regarding the availability of UPS and Generators to support the Ramco facility and data center for continuous operation of hardware equipment in the event of a component or power failure. • Performed a physical walkthrough of the Ramco facility and data center to determine whether it was supported by UPS and diesel generator sets for continuous operation of hardware equipment in the event of a component or power failure.	No relevant exceptions noted.
13.05	The UPS, and diesel generators are covered under AMC and a preventive maintenance is performed as per the preventive maintenance schedule.	• Inquired of the Head of Administration, regarding the AMC for UPS and diesel generators and whether preventive maintenance was performed for the equipment and reports were maintained and reviewed against the maintenance schedule by the Administration team. • Inspected the 'AMC' for UPS and diesel generators to determine whether they were maintained and the tested at periodic intervals by the respective vendors as per the AMC. • For a selection of quarters/months, inspected the preventive maintenance report to determine whether the maintenance of UPS and Diesel generators were performed in periodic intervals by the respective vendors as per the AMC and reviewed against the maintenance schedule by the Administration team.	No relevant exceptions noted.
13.06	Fire safety drill is conducted by the Emergency Rescue team at Ramco facility on an annual basis.	• Inquired of the Head of Administration regarding the fire safety drill conducted by the Emergency Rescue team at Ramco facility. • Inspected the 'Fire drill report' to determine whether Fire safety drill was conducted by the Emergency Rescue team at Ramco	No relevant exceptions noted.

Control Number	Description of Controls	Test Performed	Results of Testing
		facility annually.	
13.07	Suitable temperature and humidity levels are maintained within the data center and the readings are monitored by the electrician once every two hours. In case of any exception to the threshold, an incident is logged with the vendors for support.	• Inquired of the Head of Administration, regarding the process of monitoring temperature and humidity levels within the data center. • Inspected the 'Physical and Environment Security' document to determine whether the process of monitoring temperature and humidity levels within the data center was defined and documented. • Performed a physical walkthrough of the premises to determine whether the temperature and humidity monitoring devices were installed in the data center. • For a selection of dates, inspected the 'Temperature Monitoring' register to determine whether the temperature and humidity levels were monitored once every two hours by the electrician.	No relevant exceptions noted. *Note: We were informed that there were no incidents logged with the vendor due to exceptions related to temperature and humidity threshold during the audit period.*

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

Information Systems Administration - Recruitment, Training and Separation

Control Objective: 14	*Controls provide reasonable assurance that policies and procedures for hiring, and separation of the Ramco BPO employees are adhered.*

Control Number	Description of Controls	Test Performed	Results of Testing
14.01	Ramco HR Policies and procedures are defined and documented by the Specialist-HR Shared Services and approved by the Senior Manager / Chief Human Resources Officer. The HR policies and procedures are made available to the employees through the intranet portal.	• Inquired of the HR Specialist, regarding the documentation of HR policies and procedures and whether these policies were made available to the employees through the intranet portal. • Inspected the 'Recruitment process', 'Separation process', and 'Transfer policy' to determine whether HR policies and procedures were defined and documented by the Specialist-HR Shared Services, reviewed and approved by the Senior Manager / Chief Human Resources Officer. • Inspected the intranet portal to determine whether HR policies and procedures were made available to the employees through the intranet portal.	No relevant exceptions noted.
14.02	At the time of hiring a resource, the Project Manager sends a request with the job description and requirement to the HR. The request is approved by the CHRO.	• Inquired of the HR Specialist, regarding the process of Hiring for new joiners to Ramco. • For a selection of new joiners to the BPO Operations, inspected rTrack request for hire to determine whether the request was sent by the Project Manager with the job description and whether the request was approved by the CHRO.	No relevant exceptions noted.
14.03	Resources are hired to Ramco BPO process following a criteria-based interview and approval from the respective Project Manager. The Talent Acquisition team raises a request in rTrack application to initiate the Onboarding process.	• Inquired of the HR Specialist, regarding the process of interview evaluation prior to onboarding a resource to Ramco BPO. • For a selection of new joiners to Ramco BPO, inspected the 'Interview assessment form' to determine whether resources were hired to Ramco BPO process following a criteria-based interview and approval from the respective Project Manager. • For a selection of new joiners to Ramco BPO, inspected the 'Employee joining report', and 'rTrack request' to determine whether the Talent Acquisition team raise a request in rTrack application to initiate the	No relevant exceptions noted.

Control Number	Description of Controls	Test Performed	Results of Testing
		Onboarding process.	
14.04	Background Verification (BGV) including criminal and employment checks is initiated and completed within 180 days of joining, exceptions, if any, are reported to the Chief Human Resource Officer on a monthly basis[20].	• Inquired of the HR Specialist, regarding the process of background verification of new joiners to Ramco BPO. • For a selection of new joiners to the BPO Operations, inspected the 'Profile confidential report' and 'Employee joining report' to determine whether Background Verification including criminal and employment checks was initiated and completed within 180 days of joining. • For a selection of new joiners to the BPO Operations, inspected the e-mail communication to determine whether the exceptions during the Background Verification process were communicated to the Chief Human Resource Officer on a monthly basis.	No relevant exceptions noted.
14.05	New joiners are required to sign an NDA, Code of Business Conduct and Ethics, and an undertaking of acceptance to adhere to the information security policies and procedures at the time of joining the BPO Operations[21].	• Inquired of the HR Specialist, regarding the process of declaration of NDA, Code of Business Conduct and Ethics, and an acceptance to adhere to the information security policies and procedures at the time of joining the BPO operations. • For a selection of new joiners to the BPO Operations, inspected the 'NDA', 'Code of Conduct declaration' and 'Desktop security agreement' on the on-boarding portal to determine whether new joiners were required to sign an NDA, Code of Business Conduct and Ethics, and an undertaking of acceptance to adhere to the information security policies and procedures at the time of joining the BPO Operations.	No relevant exceptions noted.
14.06	New joiners to Ramco are mandated to go through training on Information security practices as a part of joining formalities and complete the ISMS assessment within 90 days of joining[22]. A Mandatory induction program is conducted by the HR for new joiners to Ramco on the date of joining[23]. Exceptions, if any, are reported to the Business Unit Heads on a periodic basis and	• Inquired of the Training Coordinator, regarding the process of induction training for new joiners to Ramco as a part of joining formalities. • Inspected the 'Organizational Induction deck', and 'HR Induction deck' to determine whether the Organizational induction and HR induction training covered Information security practices as a part of joining formalities for new joiners to Ramco BPO. • For a selection of new joiners to the BPO	No relevant exceptions noted.

Control Number	Description of Controls	Test Performed	Results of Testing
	followed up on until completion.	Operations, inspected the 'Training Schedule' and 'Employee attendance' to determine whether new joiners to Ramco were mandated to go through an Organizational Induction Training covering Information security practices as a part of joining formalities within 90 days of joining, whether Mandatory induction program was conducted by the HR for new joiners to Ramco on the date of joining and whether exceptions were reported to the Business Unit Heads on a periodic basis and tracked to completion.	
14.07	On an annual basis, a refresher program and ISMS assessment is conducted for employees, which covers broad aspects of information security and awareness.	• Inquired of the Training Coordinator, regarding the refresher program and ISMS assessment conducted for employees. • For a selection of employees, inspected the 'Refresher program schedule' and 'ISMS assessment quiz results' to determine whether on an annual basis, a refresher program and ISMS assessment was conducted for employees, which covers broad aspects of information security and awareness.	No relevant exceptions noted.
14.08	Ramco employees leaving the organization are required to get an online 'Clearance Automation' (No Dues) from the respective Department Heads, based on the e-mail trigger from the HRSS application.	• Inquired of the HR Specialist, regarding the process of No Dues Clearance for Ramco employees leaving the organization and regarding the process of exit discussion. • For a selection of leavers from Ramco BPO, inspected the 'ESS Exit management system' and 'Final Settlement advise' to determine whether Ramco employees leaving the organization were required to get an online 'Clearance Automation' (No Dues) from the respective Department Heads, based on the e-mail trigger from the HRSS application.	No relevant exceptions noted.

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

ANNEXURE

List of Abbreviations

S. No	Abbreviations	Expanded Form
1.	AMC	Annual Maintenance Contract
2.	AD	Active Directory
3.	BEU	Business Enabling Units
4.	BGV	Background Verification
5.	BPO	Business Process Outsourcing
6.	CCTV	Closed Circuit Television
7.	CDC	Change Data Capture
8.	CIS	Cloud Infrastructure Services
9.	CISO	Chief Information Security Officer
10.	CTC	Cost to Company
11.	CUEC	Complementary User Entity controls
12.	ERP	Enterprise Resource Planning
13.	ESS	Employee Self Service
14.	F&F	Full and Final settlement
15.	GDPR	General Data Privacy Regulations
16.	HCM	Human Capital Management
17.	HR	Human Resource
18.	HMS	Hub Management System
19.	HRMS	Human Resource Management System
20.	HRSS	Human Resource Self Service
21.	IMG	Infrastructure Management Group
22.	ISMS	Information Security Management System
23.	IT	Information Technology
24.	L&D	Learning and Development
25.	MIS	Management Information Systems
26.	MRO	Maintenance Repair and Overhaul
24.	NDA	Non-Disclosure Agreement
26.	QA	Quality Assurance

S. No	Abbreviations	Expanded Form
27.	QMG	Quality Management Group
28.	SaaS	Software as a Service
29.	SBU	Strategic Business Unit
30.	TMS	Travel Management System
31.	UPS	Uninterruptible Power Supply
32.	VAPT	Vulnerability Assessment and Penetration Testing
33.	VLAN	Virtual Local Area Network
34.	VPN	Virtual Private Network
35.	WMS	Warehouse Management system