SOC 2 TYPE 2



Independent Service Auditor's Report on a Description of a Service Organization's System Relevant to Security, Availability and Confidentiality and the Suitability of the Design and Operating Effectiveness of Controls for the period, July 1, 2025, to June 30, 2026.

TABLE OF CONTENTS

SECTION 1 - INDEPENDENT SERVICE AUDITOR'S REPORT... 3

SECTION 2 - HOTWAX'S ASSERTION 8

SECTION 3 - DESCRIPTION OF THE SYSTEM 10

SECTION 4 - APPLICABLE TRUST SERVICES CRITERIA AND RELATED CONTROL ACTIVITIES... 51

SECTION – 1 INDEPENDENT SERVICE AUDITOR'S REPORT

Precision Assurance
CPA LLC

INDEPENDENT AUDITOR'S REPORT

To
HotWax Software Inc.

Scope

We have examined HotWax Software Inc's ("HotWax" or the "service organization") accompanying description of its "SaaS product-HotWax Commerce" throughout the period 1st July 2025 to 30th June 2026, (the "description"), based on the criteria for a description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria) ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the description throughout the period 1st July 2025 to 30th June 2026, to provide reasonable assurance that HotWax's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability and Confidentiality ("applicable trust services criteria") set forth in TSP section 100, Trust Services Criteria for Security, Availability, Confidentiality, Processing Integrity and Privacy (AICPA, Trust Services Criteria).

HotWax uses AWS for application hosting and data backup, MySQL for data storage, ClickUp for project management and GitHub and GitLab for code repository. The description in Section 3 includes only the controls of HotWax and excludes controls of the various subservice organizations. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at HotWax, to achieve HotWax's service commitments and system requirements based on the applicable trust services criteria. The description presented by HotWax also indicates that certain trust services criteria and the types of complementary subservice organization controls can be met only if the subservice organization's controls, contemplated in the design of HotWax's controls, are suitably designed and operating effectively along with related controls at the service organization. The description does not disclose the actual controls at the subservice organization. Our examination did not extend to controls of various subservice organizations for data center services and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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

HotWax's Responsibility

HotWax has provided the attached assertion, in Section 2, which is based on the criteria identified in management's assertion. HotWax is responsible for (1) preparing the description and assertion; (2) the completeness, accuracy, and method of presentation of both the description and assertion; (3)

Provide the services covered by the description; (4) specifying the controls that meet the applicable trust services criteria and stating them in the description; and (5) designing, implementing, and documenting the controls to meet the applicable trust services criteria.

Service Auditor's Responsibility

Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of controls 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 3000, Assurance Engagements Other Than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria; and
- Evaluating the overall presentation of the description.

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Test of Controls

The specific controls we tested, and the nature, timing, and results of those tests are presented in section 4 of our report titled "Testing Matrices."

Opinion

In our opinion, in all material respects, based on the description criteria identified in HotWax's assertion and the applicable trust services criteria

a. the description fairly presents HotWax's "SaaS product-HotWax Commerce" that were designed and implemented throughout the period 1st July 2025 to 30th June 2026; and
b. the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period 1st July 2025 to 30th June 2026, and if user organization applied the complementary user controls contemplated in the design of HotWax's controls throughout the period 1st July 2025 to 30th June 2026; and
c. the controls tested operated effectively to provide reasonable assurance that the applicable trust service criteria were met throughout the period of 1st July 2025 to 30th June 2026, if the complementary user entity controls referred to in the Scope paragraph of this report were also throughout the period 1st July 2025 to 30th June 2026.

Restricted Use

This report and the description of controls thereof are intended solely for the information and use of HotWax; user entities of HotWax' s services system throughout the period 1st July 2025 to 30th June 2026; and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria; and
- The risks that may threaten the achievement of the service organization's service commitments and system requirements, and how controls address those risks.

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

Precision Assurance CPA LLC

Certified Public Accountants
License No. CF - 0010917
Dover, Delaware.

Date - October 17, 2026

SECTION – 2 HOTWAX'S MANAGEMENT ASSERTION

HOTWAX COMMERCE

MANAGEMENT'S ASSERTION

We have prepared the accompanying description of HotWax Software Private Limited's (hereinafter "HotWax") "SaaS product-HotWax Commerce" system (the "description"), throughout the period 1st July 2025 to 30th June 2026 based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), ("description criteria"). The description is intended to provide report users with information about the SaaS product-HotWax Commerce that may be useful when assessing the risks arising from interactions with HotWax's system, particularly information about system controls that HotWax has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

HotWax uses AWS for application hosting and data backup, MySQL for data storage, ClickUp for project management and GitHub and GitLab for code repository. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at HotWax, to achieve HotWax's service commitments and system requirements based on the applicable trust services criteria. The description presents HotWax controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of HotWax's controls. The description does not disclose the actual controls at the subservice organization.

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

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

a. the description presents HotWax's SaaS product-HotWax Commerce as per the requirement of clients that was designed and implemented throughout the period 1st July 2025 to 30th June 2026, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period 1st July 2025 to 30th June 2026, to provide reasonable assurance that HotWax's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period and if the subservice organizations and if user entities applied the complementary controls assumed in the design of HotWax's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period 1st July 2025 to 30th June 2026, to provide reasonable assurance that HotWax's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of HotWax's controls operated effectively throughout that period.

Authorized Signatory
HotWax Software Private Limited
Date: October 12, 2026



SECTION – 3 DESCRIPTION OF THE SYSTEM

OVERVIEW OF OPERATIONS

Company Background

HotWax Software Inc., incorporated in Delaware, USA, is a product-based company that holds the controlling interest in HotWax Systems Pvt. Ltd.

HotWax Commerce, an omnichannel order management system (OMS), is a proprietary product of HotWax Software Inc. It is offered as a Software-as-a-Service (SaaS) solution to retailers worldwide.

HotWax Systems Pvt. Ltd. provides software development, product enhancement, implementation, and ongoing support services for HotWax Commerce. This includes maintaining the OMS platform, delivering updates, and ensuring service reliability for clients.

The strategic relationship between the two entities allows HotWax Software Inc. to focus on marketing, sales, and global commercial success, while HotWax Systems Pvt. Ltd. is responsible for product development, technical operations, and client services.

Together, HotWax Software Inc. and HotWax Systems Pvt. Ltd. work in alignment to ensure that HotWax Commerce enables retailers to integrate multiple sales channels, streamline order fulfillment, and support improved customer experiences in a secure and reliable manner.

Description of Solutions in HotWax Commerce

Here is summary of the solutions available in HotWax commerce order management system:

Buy Online Pick-Up in Store (BOPIS): The system enhances conversions by displaying store details on the product detail page for convenient pick-up location selection. It also allows customers to place mixed cart orders with pickup and shipping items and provides reserved until date and time for order items.

BOPIS Fulfillment: Store associates can view, manage, and deliver BOPIS orders using the integrated BOPIS fulfillment app within Shopify POS. It facilitates order notifications to customers and re-sending pick-up notifications to prevent order abandonment.

Ship From Store: This service controls unified inventory, shows ETA on the product detail page, and reduces shipping costs through strategic order routing based on inventory availability and customer proximity. It also expedites last-mile delivery, handles exception cases efficiently, optimizes order picking, and toggles store inventory for online sales.

Pre-Order Management: HotWax commerce offers pre-order management services, increasing speed-to-market, avoiding markdowns, and automating pre-order fulfillment while balancing inventory allocation between stores and online channels.

Store Inventory Management: The system facilitates inbound shipment receiving and verification, maintains accurate inventory count, and enables seamless inventory updates to eCommerce platforms, ensuring up-to- date inventory counts.

Use of Subservice Organization

HotWax Systems Pvt. Ltd. uses:-

- Amazon Web Services (AWS) for hosting and monitoring applications.
- ClickUp (app.clickup.com) application for task and incident management.
- Github (github.com) and GitLab for code repository on public and private repositories.
- Open-source projects from Apache Software foundation(www.apache.org) like Apache OFBiz, Apache NIFI, Moqui, Apache Solr etc.

Principal Service Commitments and System Requirements

HotWax Systems Pvt. Ltd delivers HotWax commerce OMS in SaaS (software-as-a-service) model to retailers . Delivery includes setting up HotWax commerce, customizing it if needed, testing it and getting acceptance from retailers. Once HotWax commerce OMS is in production, HotWax Systems Pvt. Ltd. also maintains and oversees the functioning of the software so that retailers can use it uninterruptedly as per the retailer's requirements.
The unscheduled downtime for the application is designed to be minimal, and a system is in place such that the support team is able to inform / seek approval for scheduled downtime so that the business needs of the customer are not affected.

Security principles are such that the proper authentication and authorization are necessary to access as well as modify any data or to request the change of state of an application.

In addition, there is a monitoring system in place to detect any spikes in use, slowness of the system or availability. Monitoring of these is necessary to maintain the committed service levels.

Components of the System:

Infrastructure

Primary infrastructure utilized by HotWax Systems Pvt. Ltd. includes the following:

Primary Infrastructure		
Hardware	Type	Purpose
Amazon AWS Cloud Platform	Cloud Computing platform	AWS (Amazon Web Services) is a cloud computing platform provided by Amazon. It includes a mixture of infrastructure-as-a-service (IaaS), platform-as-a- service (PaaS) and packaged software-as-a-service (SaaS) offerings. AWS offers tools such as compute power, database storage and content delivery services. We deploy and host all HC OMS application on AWS platform

Below are the AWS services and resources that HotWax Systems applications use for deploying .

1. VPC (Virtual Private Cloud): AWS network in which we will deploy our services, in Infra setup we created two private zones and two public zones, In public zones, we have GitLab Runner, ALB and NAT Gateway.

2. Code Commit: It is a managed Git repository provided by AWS

3. CodePipeline: It is used to trigger CI/C

4. CodeBuild: It is used to build docker image and push to ECR

5. CodeDeploy: It is used to update the ECS cluster

6. ALB (Application Load Balancer): ALB forward end user traffic to ECS cluster where HC docker images are deployed.

7. AWS Nat Gateway: It is a highly available AWS managed service that makes it easy to connect to the internet from instances within a private subnet in an AWS VPC.

8. ECR (Elastic Container Registry): HC docker image and Solr image will be stored here.

9. ECS (Elastic Container Service): It is a managed cluster of Amazon EC2 instances that allow you to easily manage and deploy docker containers and run applications.

10. Auto Scaling: It will be used to auto scale ECS HC containers based on CPU threshold.

11. EFS (Elastic File System): Elastic File Storage will be used to store images, user upload, Solr data etc. and keep them centralized for all the ECS containers.

12. EC2 (Amazon Elastic Compute Cloud): It is used by ECS clusters to deploy containers.

13. RDS (Relational Database Service): It is a MySQL database hosted in a multi zone; it means it will create a slave instance in another zone for failover.

14. WAF : Integrated with oms-lb to filter web traffic.

15. Inspector: Used to scan the OS and ECR images for account.

16. EKS: Deploying all instances on it.

Software
Primary software used to provide includes the following:

Primary Software	
Software	Purpose
Docker	Provides containers for running all microservices. Works like virtualization but virtualizes services instead of operating systems.
GitLab	Code commit repository on GitLab

Software	Purpose
MySQL Workbench	Workbench to access MYSQL databases
Intellij idea	Development IDE
OpenVpn Client	To access private zone servers on AWs
Grafana	Tool to display the log metrics in a graphical way.
Amazon CloudWatch	For application and infrastructure monitoring.
Kubernetes	Open-source container orchestration engine for automating deployment, scaling, and management of containerized applications.
EC2	Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable compute capacity in the cloud.
VPC	A virtual private cloud (VPC) is a secure, isolated private cloud hosted within a public cloud.
API gateway	Amazon API gateway is an AWS service for creating, publishing, maintaining, monitoring, and securing REST, HTTP, and websocket APIs at any scale.

People

The staff for can be classified into the following departments:

- The Board: Oversees the organizational direction and decides the strategy for the product and technology
- Support Services: Human resources, IT & Admin. They assist the organization in ensuring that the delivery activities are smooth
- R&D: HotWax Systems Pvt. Ltd. continuously performs research and proof of concept activities to improve the HotWax Systems Pvt. Ltd. Order management system platform to take it to the next level
- Product Development: The software development team that adds features to the product and fixes issues
- Implementation Team: Implements the solution for a new customer, and helps in testing upgrades for an existing customer, also configures and customizes the customer based on the need
- Support Team: 24x7 support for any customer issues, which can range from a query to an unavailability issue
- DevOps team: Responsible for maintaining the system and ensuring uptime and performance
- Product Management: Maintains and owns the product road map, and functionally directs the product development team
- Sales / Pre-Sales and Marketing: Scouting for new opportunities, lead generation, product demos, filling up RFPs
- IT Team: Responsible for maintaining local hardware, network and server infrastructure ensuring each user get smooth services.

Data

The data used by the HC OMS, is as follows:

Customer Data from Ecom Portal : HC OMS (HotWax Commerce Order Management System) fetches customer's name, shipping address, phone and email along with sales order data placed on Ecom portal (Shopify). OMS does not fetch and use any kind of private data like CC data, SSN, bank account details, etc.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the HotWax Systems Pvt. Ltd. policies and procedures that define how services should be delivered. These are located on the company's intranet and can be accessed by any HotWax Systems Pvt. Ltd. team member.

Physical Security

Physical protection shall be achieved by creating several physical barriers around HotWax Systems Pvt. Ltd.'s premises and information processing facilities. Each barrier shall establish a security perimeter, creating a defense in depth strategy and eliminating a single point of failure.

Logical Access

Logical Access controls shall be deployed with the principle of 'deny all unless explicitly permitted' to protect information from unauthorized access. Customers ,third party vendors, service providers, shall be provided access to HotWax Systems Pvt. Ltd.'s information assets only on presenting business needs and signing contractual agreements.

Access to this network is protected by user id and password-based access.

For the internal office networks, there is access control via user id and password to various resources. During the hiring and termination process, HR follows the access activation and deactivation procedure.

Computer Operations – Backups

This procedure applies to all individuals who access, use, and control HotWax Systems Pvt. Ltd.'s owned resources. This includes but is not limited to HotWax Systems Pvt. Ltd.'s employees, contractors, consultants, and other workers including all personnel affiliated to external organization with access to HotWax Systems Pvt. Ltd.'s network.

Head of Departments / Business Units shall clearly identify the data to be backup, minimum backup frequency and archival rules for the respective asset. The IT department is responsible for the implementation of the backup plan for the servers.

There is a limited number of people within the organization who have the ability to download or restore a particular backup.

Computer Operations – Availability

The cloud-based computing infrastructure provided by AWS has a certain reliability which is leveraged for providing the services to our customers.

Availability may still be hampered by spikes in usage or performance issues. For that purpose, a high availability cluster spanning multiple nodes and managed by Kubernetes is created so that the system is available despite such situations.

Change Control

This policy establishes standard procedure for managing change requests in an agile and efficient manner, in an effort to drastically minimize the risk and impact a change which can have on the business operations of the company.

The change management process begins with the creation of a change request within the company's selected technology platform. It ends with the satisfactory implementation of the change and communication of the result of that change to all interested parties. Further reporting shall be a part of entire process, at every step

Change management is a continuous improvement within the IT systems of the company and it generally including the following steps :

1. Prioritize and respond to the change proposals
2. Conduct cost benefit analysis of the proposed changes
3. Assessment of risk associated with the changes
4. Change implementation and monitoring
5. Continuous reporting

Data Communications

Firewalls are in place to ensure that there is no unauthorized access of organization's resources. The firewalls have monitoring logs, and they are reviewed on a periodic basis.

In addition, remote access is made available via VPN for a restricted set of users for a specified time. This set of user access is also reviewed on a periodic basis.

Boundaries of the System

The scope of this report covers the implementation, delivery, and maintenance of the HotWax commerce order management system applications hosted on AWS, carried out at the Indore, India facilities.

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

Control Environment

Integrity and Ethical Values

Integrity and ethical values, while they are not something that can be enforced via policy documents, can be promoted by creating an environment and culture that makes it easier to have integrity and be ethical than not. Employees undergo training related to expected standards of behavior and ethics, they are also asked to go through policy documents related to ethics and integrity during their orientation.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook
- Background checks are performed for employees as a component of the hiring process.

Commitment to Competence

An annual performance appraisal is held for all employees, which is based on a points system.

The employees are incentivized to improve their skills and be more productive. Pay revisions and compensation improvements and promotions are linked to the performance appraisal.

Specific control activities that the service organization has implemented in this area are described below:

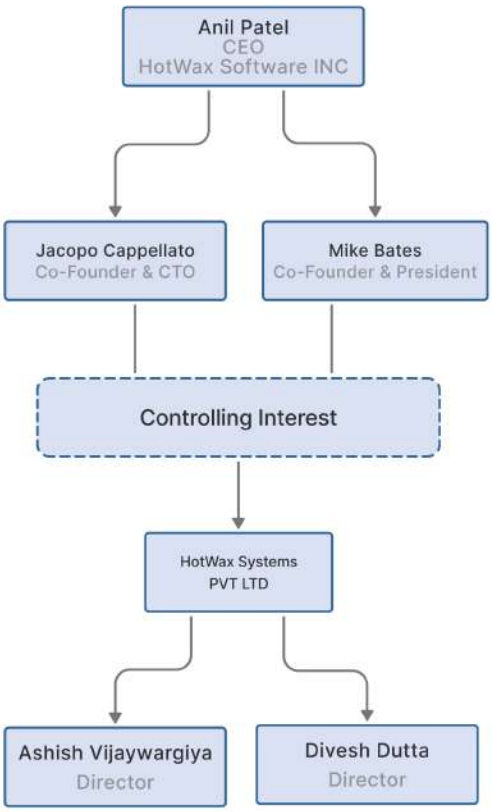
- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements
- Training is provided to maintain the skill level of personnel in certain positions

Management's Philosophy and Operating Style
Management philosophy for the organization is based on the premise that focusing on the customer's long- term needs rather than providing short term solutions is a more beneficial policy in the long run.

In addition, management believes that the changing regulatory environment as well as improvements in technology provide business opportunities, so it is important to stay up to date on these, they must be looked at as opportunities rather than problems.

Specific control activities that the service organization has implemented in this area are described below:
- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole.

Organizational Structure and Assignment of Authority and Responsibility



The goal of the organization is to have lean and agile teams. However, every team member is part of a formal hierarchy that rolls up to the CEO.

While employees and multiple teams may collaborate informally to get things done faster, in case of conflicts or deciding how something new would be handled, the formal hierarchy is used as the basis for coming to conclusions.

It is also ensured that collaborative work does not mean sharing of confidential data or credentials that must not be shared with unauthorized persons.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility
- Organizational charts are communicated to employees and updated as needed

Human Resources Policies and Practices

The human resource department under the direction of the board and CXOs directs the policies and procedures such that there is:

- Delivery excellence
- An environment where merit and performance are valued
- People feel part of something bigger than them
- A high-performance work ethic

There are policies that dictate induction of new joiners, exit and termination policies as well as promotions that lead to achieving the goals listed above.

Risk Assessment Process

HotWax Systems Pvt. Ltd.'s assessment process identifies and manages risks that could potentially affect HotWax Systems Pvt. Ltd.'s ability to provide reliable services to their customers. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. HotWax Systems Pvt. Ltd. identifies the underlying sources of risk, measures the impact to organization, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by HotWax Systems Pvt. Ltd., and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk - changes in the environment and critical staff
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance - legal and regulatory changes

HotWax Systems Pvt. Ltd. has established an internal team responsible for identifying risks to the entity and monitoring the operation of the firm's internal controls. HotWax Systems Pvt. Ltd. attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management.

Integration with Risk Assessment

The environment in which the system operates, along with the commitments, agreements, and responsibilities of HotWax Systems Pvt. Ltd.'s order management system, creates risks that could prevent the criteria from being met. HotWax Systems Pvt. Ltd. mitigates these risks by implementing appropriately designed controls to provide reasonable assurance that the criteria are satisfied. Since each system and its operating environment are unique, the combination of risks and the necessary controls will also be unique. As part of the system's design and operation, HotWax Systems Pvt. Ltd.'s management identifies the specific risks that could prevent the criteria from being met and determines the controls required to address those risks.

Information and Communications Systems

It is important for the customer and internal stakeholders to be aware of the changes to be made to the production systems as well as the reasons for that. The same applies to communications after the changes have been made or rolled back.

Similarly, a new initiative taken internally to add product features or to improve the systems in any other

way needs to be communicated to the team and responsibilities need to be assigned. That requires a robust and efficient mode of communication that is also secure.

Various degrees and means of communication are required for interaction with prospects, live customers and employees.

In addition, it is required to keep track of the communications as well as what actions have been taken to achieve the goals.

For that purpose, we use, in addition to email, Google Chat as well as ClickUp for the purpose of tracking and accountability.

ClickUp is also used for productivity measurements and time tracking.

Monitoring Controls

Being a cloud-based system, the monitoring is via logs, which may be application logs as well as access logs.

A dedicated support team monitors all the production systems 24x7 and keeps an eye out for anomalies.

The support team also receives issues raised by the customer and attempts to correlate the customer's findings with the corresponding logs, thereby pre-empting a customer report by taking corrective action even before it is reported by them.

Log monitoring is also used to pass on valuable information to the development teams to solve issues that cannot be simulated in a development environment.

On-Going Monitoring

HotWax Systems Pvt. Ltd.'s management conducts quality assurance monitoring on a regular basis and additional training is provided based upon the results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in HotWax Systems Pvt. Ltd.'s operations help to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of HotWax Systems Pvt. Ltd.'s personnel.

Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Applicable Trust Service Criteria and Related Controls

The security, availability and confidentiality trust services categories and HotWax Systems Pvt. Ltd.'s related controls are included in section 4 of this report, "Independent Service Auditor's Description of Tests of Controls and Results".

HotWax Systems Pvt. Ltd. has determined that Processing Integrity and Privacy trust services Categories are not relevant to the system.

Subservice Organizations

This report does not include the subservice organization services as mentioned earlier in the report.

Subservice Description of Services

The data center hosting services provided by AWS are monitored by management; however, they have not been included in the scope of this review.

Complementary Subservice Organization Controls

HotWax Systems Pvt. Ltd.'s services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to HotWax Systems Pvt. Ltd.'s services to be solely achieved by HotWax Systems Pvt. Ltd. control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of HotWax Systems Pvt. Ltd.

Work From Home

HotWax Systems Pvt. Ltd. is committed to work-life balance and to exploring flexible work practices with the employees. The purpose of this policy is to outline the policy guidelines and eligibility requirements and other aspects regarding work from home.

Work from home during normal scenarios: Employees must ensure their manager agrees and approves their work from home arrangements. Certain roles, due to the nature of their job, are not possible to perform away from the office and hence they require physical presence in the office.

Employees approved for the work from home facility are expected to maintain normal productivity and performance. They must not carry out and undertake non-work-related activities during their working hours. Work from home facility is not an opportunity to perform household duties, care for children or other dependents, or attend to other personal business. Employees should liaise with their manager about their patterns of work and days in the office and will be responsible for keeping their manager and team informed about the status of their work. It is the employee's responsibility to ensure they have a suitable remote work area available and ensure a safe and healthy work environment. They must ensure that they have the proper IT systems and technology to perform their job duties from a remote location without impacting productivity.

Employees working remotely will be dealing with HotWax Systems Pvt. Ltd. and customer confidential and personal data, so reasonable steps must be taken to ensure that such data is treated with adequate regard to data protection, confidentiality and security measures. Employees must ensure that the access to the information is obtained through a secure ID. HotWax Systems Pvt. Ltd.'s IT team has put in place an infrastructure to facilitate working remotely and IT person can be contacted if there are any specific issues related to access or IT security.

No third parties, including family members, should be permitted to access HotWax Systems Pvt. Ltd.'s computer or customer documents.

All other respective employment policies and practices apply to employees while working from home, irrespective of work location or schedule arrangement.

Kindly note that the company reserves the right to withdraw work from home approval at any time, with or without reason.

Work from home during extraordinary circumstances: When a large number of employees are forced to work from home for unforeseen reasons and extraordinary circumstances such as lockdowns due to any reasons (epidemic, pandemic, social unrest), or even based on the business requirements, they are notified by the HR

department. It is important to follow all the directives and guidelines issued from time to time by the Company as well as local civic authorities, State and Central Government. The safety, security and well-being of self and colleagues is to be ensured at all costs.

Complementary User Entity Controls (CUEC)

The controls at HotWax relating to the system for revenue management services controls relevant to security, availability, confidentiality (applicable 'Trust Services Criteria') provided to user entities by HotWax cover only a portion of the overall internal control structure of user entities. The control criteria cannot be achieved without taking into consideration the operating effectiveness of controls at the user entities as well. Therefore, the user entity's internal control structure must be evaluated in conjunction with HotWax's control policies and procedures summarized in Section 4 of this report.

This section highlights those internal control structure responsibilities that HotWax believes should be present at user entities, and which HotWax has considered in developing its control structure policies and the procedures described in this report. In order to rely on the control structure policies and procedures reported herein, user entities and their auditors must evaluate user entities' internal control structure to determine if the Complementary User Entity Controls (CUECs) mentioned below or similar procedures are in place and operating effectively.

The CUECs mentioned below are as explained and provided by HotWax management. These controls address the interface and communication between user entities and HotWax and are not intended to be a complete listing of the controls related to the security, availability, processing integrity and confidentiality criteria of user entities.

Contractual Arrangements

- User organizations are responsible for understanding and complying with their contractual obligations to HotWax such as providing input information, review and approval of processed output and releasing any instructions.

Other Controls

- User organizations are responsible for ensuring end customer privacy.
- User organizations are responsible for their network security policy and access management for their networks, application & data.
- User organizations are responsible for working with HotWax to jointly establish service levels and revise the same based on changes in business conditions.
- User organizations are responsible for developing their own disaster recovery and business continuity plans that address their ability to access or utilize HotWax services.
- User organizations are responsible for notifying HotWax of changes made to technical or administrative contact information in a timely manner.
- User organizations are responsible for understanding and defining data storage requirements.
- User organizations are responsible for notifying HotWax of any regulatory issues that may affect the services provided by HotWax.

Security (Common Criteria) 1.1: COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.

Control Number	Control Activity Description
CA-10	A Master Service Agreement ('MSA') is signed between HotWax and the client covering the service offerings, responsibilities, security, availability, and confidentiality commitments of HotWax and the client.
CA-39	The policies are made available to HotWax associates via email. Security awareness is spread amongst the associates through emails sent by corporate announcements.
CA-44	For campus hires and lateral hires, background verification is carried out by the third- party service provider and the results are reviewed by HR Team.
CA-45	HR policies are in place to determine that violations of code of conduct, Non-Disclosure agreement and other confidential matters are subject to disciplinary action and sanctions based on investigation performed in timely manner.
CA-46	HotWax associates are required to sign the 'NDA' document which includes clauses for maintaining confidentiality of information obtained, intellectual property rights of HotWax, termination of employment on breach of NDA amongst others on or before the day of joining.
CA-69	Third party service providers sign a non-disclosure agreement with HotWax before commencement of services

Common Criteria 1.2: COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

Control Number	Control Activity Description
Not applicable. HotWax does not have a Board of Directors.	

Common Criteria 1.3: COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

Control Number	Control Activity Description
CA-01	HotWax has defined and documented a 'Change Management Procedure' that includes the following matters: a. Assigning responsibility and accountability for system changes and maintenance b. Testing, evaluating, and authorizing system components before implementation.
CA-03	HotWax has defined and documented a 'Security Incident Management Procedure that includes the following matters: a. Addressing how complaints and requests relating to security issues are resolved b. Identifying and mitigating security breaches and other incidents c. Providing for the handling of exceptions and situations not specifically addressed in its system security policy
CA-04	HotWax has defined and documented an 'Information Classification Procedure' that includes the following matters: a. Classifying data based on its criticality and sensitivity and that classify is used

	to define protection requirements, access rights and access restrictions, and retention and destruction requirements b. Preventing unauthorized access
CA-05	HotWax has defined and documented a 'Risk Assessment and Treatment procedure' that includes the following matters: a. Assessing risks on a periodic basis b. Providing for the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.
CA-08	HotWax has defined and documented an 'Access Control Policy' that includes the following matters: a. Identifying and documenting the security requirements of authorized users b. Preventing unauthorized access c. Adding new users, modifying the access levels of existing users, and removing users who no longer need access d. Assigning responsibility and accountability for system security e. Identifying and mitigating security breaches and other incidents f. Providing training and other resources to support its system security policies.
CA-14	The organization chart for HotWax is maintained by the HR Team and reviewed on a need basis.
CA-36	HotWax has defined 'Information Security Policy' documented and reviewed by the management. The policy includes the following aspects: Risk Management, Access Controls, Personnel Security, Asset Management, Physical Security, Business Continuity, Information Transfer.
CA-38	Physical and Environmental Security Policy is defined and documented by the admin team and approved by chief information officer
CA-41	HotWax has defined job descriptions specifying the responsibilities and academic and professional requirements for key job positions which are reviewed by the management on a need basis.
CA-42	HotWax maintains clearly defined personnel structures with appropriate reporting lines and oversight roles.

Common Criteria 1.4: COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

Control Number	Control Activity Description
CA-35	HotWax associates are made aware of their security commitments by means of annual security training and assessment covering security principles awareness, roles and responsibilities, information protection methods and security lapses.
CA-40	An annual performance evaluation process is in place covering KPI's, values, behavior, training needs and career aspiration.
CA-41	HotWax has defined job descriptions specifying the responsibilities and academic and professional requirements for key job positions which are reviewed by the management on a need basis.
CA-44	For campus hires and lateral hires, background verification is carried out by the third- party Service Provider and the results are reviewed by HR Team.
CA-46	HotWax associates are required to sign the 'NDA' document which includes clauses for maintaining confidentiality of information obtained, intellectual property rights of HotWax, termination of employment on breach of NDA amongst others on or before the day of joining.

Common Criteria 1.5: COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Control Number	Controls Activity Description
CA-01	HotWax has defined and documented a 'Change Management Procedure' that includes the following matters: a.Assigning responsibility and accountability for system changes and maintenance b. Testing, evaluating, and authorizing system components before implementation.
CA-03	HotWax has defined and documented a 'Security Incident Management Procedure' that includes the following matters: a. Addressing how complaints and requests relating to security issues are resolved b. Identifying and mitigating security breaches and other incidents c. Providing for the handling of exceptions and situations not specifically addressed in its system security policies.
CA-04	HotWax has defined and documented an 'Information Classification Procedure' that includes the following matters: a. Classifying data based on its criticality and sensitivity and that classify is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements b. Preventing unauthorized access
CA-05	HotWax has defined and documented a 'Risk Assessment and Treatment procedure' that includes the following matters: a. Assessing risks on a periodic basis b. Providing for the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.
CA-06	HotWax has defined and documented a 'Business continuity Framework' that includes the following matters: a. Recovering and continuing service in accordance with documented customer commitments or other agreements. b. Monitoring system capacity to achieve customer commitments or other agreements regarding availability
CA-08	HotWax has defined and documented an 'Access Control Policy' that includes the following matters: a. Identifying and documenting the security requirements of authorized users b. Preventing unauthorized access c. Adding new users, modifying the access levels of existing users, and removing users who no longer need access d. Assigning responsibility and accountability for system security e. Identifying and mitigating security breaches and other incidents f. Providing for training and other resources to support its system security policies.

CA-36	HotWax has defined 'Information Security Policy' documented and reviewed by the management. The policy includes the following aspects: Risk Management, Access Controls, Personnel Security, Asset Management, Physical Security, Business Continuity, Information Transfer.
CA-38	Physical and Environmental Security Policy is defined and documented by the admin team and approved by chief information officer
CA-41	HotWax has defined job descriptions specifying the responsibilities and academic and professional requirements for key job positions which is reviewed by the management on need basis.
CA-45	HR Policies are in place to determine that violations of code of conduct, non-disclosure agreement and other confidential matters are subject to disciplinary action and sanctions based on investigation performed in timely manner.
CA-46	HotWax associates are required to sign the 'NDA' document which includes clauses for maintaining confidentiality of information obtained, intellectual property rights of HotWax, termination of employment on breach of NDA amongst others on or before the day of joining.

Common Criteria 2.1: COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.

Control Number	Control Activity Description
CA-01	HotWax has defined and documented a 'Change Management Procedure' that includes the following matters: a. Assigning responsibility and accountability for system changes and maintenance b. Testing, evaluating, and authorizing system components before implementation.
CA-03	HotWax has defined and documented a 'Security Incident Management Procedure' that includes the following matters: a. Addressing how complaints and requests relating to security issues are resolved b. Identifying and mitigating security breaches and other incidents c. Providing for the handling of exceptions and situations not specifically addressed in its system security policies.
CA-04	HotWax has defined and documented an 'Information Classification Procedure' that includes the following matters: a. Classifying data based on its criticality and sensitivity and that classify is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements b. Preventing unauthorized access
CA-05	HotWax has defined and documented a 'Risk Assessment and Treatment procedure' that includes the following matters: a. Assessing risks on a periodic basis b. Providing for the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.
CA-29	On an annual basis, HotWax's IT team performs a risk assessment for HotWax to identify the risk factors considering the changes in the system environment.
CA-32	On an annual basis, Penetration Testing is conducted by the external vendors on HotWax network and corrective actions are taken and tracked by the IT team.
CA-35	HotWax associates are made aware of their security commitments by means of annual

	security training and assessment covering security principles awareness, roles and responsibilities, information protection methods and security lapses.
CA-36	HotWax has defined 'Information Security Policy' documented and reviewed by the management. The policy includes the following aspects: Risk Management, Access Controls, Personnel Security, Asset Management, Physical Security, Business Continuity, Information Transfer.
CA-38	Physical and Environmental Security Policy is defined and documented by the admin team and approved by chief information officer
CA-39	HotWax associates via email. Security awareness is spread amongst the associates through emails sent by corporate announcements.
CA-46	HotWax associates are required to sign the 'NDA' document which includes clauses for maintaining confidentiality of information obtained, intellectual property rights of HotWax, termination of employment on breach of NDA amongst others on or before the day of joining.
CA-61	On a weekly basis, patches and version upgrades are implemented in workstations through antivirus by infrastructure team.

Common Criteria 2.2: COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

Control Number	Control Activity Description
CA-01	HotWax has defined and documented a 'Change Management Procedure' that includes the following matters: a. Assigning responsibility and accountability for system changes and maintenance b. Testing, evaluating, and authorizing system components before implementation.
CA-04	HotWax has defined and documented a 'Information Classification Procedure' that includes the following matters: a. Classifying data based on its criticality and sensitivity and that classify is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements b. Preventing unauthorized access CA-09 Changes in HotWax management hierarchy and system of internal control are documented.
CA-14	Organization chart for HotWax is maintained by the HR Team and reviewed on need basis.
CA-15	Request for granting logical access to the HotWax associates to the network is sent by the respective HR Executive to the IT Team through E-mail.
CA-27	HotWax HR department has established a process to report, track and resolve potential occurrence of breach of code of business conduct and other concerns.
CA-28	HotWax HR department communicates changes to confidentiality commitments through the employee code of conduct and Disciplinary Policy and Procedure.
CA-35	HotWax associates are made aware of their security commitments by means of annual security training and assessment covering security principles awareness, roles and responsibilities, information protection methods and security lapses.
CA-36	HotWax has defined 'Information Security Policy' documented and reviewed by the management. The policy includes the following aspects: Risk Management, Access Controls, Personnel Security, Asset Management, Physical Security, Business Continuity, Information Transfer.
CA-38	Physical and Environmental Security Policy is defined and documented by the admin team and approved by chief information officer
CA-39	HotWax associates via email. Security awareness is spread amongst the associates through emails sent by corporate announcements.
CA-43	HotWax's security commitments to associates and required security obligations are communicated to associates during the induction program.
CA-46	HotWax associates are required to sign the 'NDA' document which includes clauses for maintaining confidentiality of information obtained, intellectual property rights of HotWax, termination of employment on breach of NDA amongst others on or before the day of joining.
CA-61	On weekly basis, patches and version upgrades are implemented in workstations through antivirus by infrastructure team.
CA-64	The IT team informs the associate about changes that may affect system security by means of an Email alert.

Common Criteria 2.3: COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.

Control Number	Control Activity Description
CA-10	A Master Service Agreement ('MSA') is signed between HotWax and the Client covering the service offerings, responsibilities, security, availability, and confidentiality commitments of HotWax and the client.
CA-11	HotWax communicates its commitment to security as a top priority for its customers via MSA.
CA-13	MSA defines security, availability, and confidentiality commitments along with responsibilities of HotWax and the client.
CA-28	HotWax HR department communicates changes to confidentiality commitments through the employee code of conduct and Disciplinary Policy and Procedure.
CA-31	HotWax's security commitments (including security obligations, terms, conditions, and responsibilities) are documented, along with the responsibilities of external users, in newly onboarded third party contracts and non-disclosure agreements.
CA-41	HotWax has defined job descriptions specifying the responsibilities and academic and professional requirements for key job positions which is reviewed by the management on need basis.
CA-68	Master Service Agreements (MSAs) between HotWax and vendors are incorporated to include: • Scope of business relationship and services offered • Information security requirements • Timely notification of a security incident to customers • Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification) • Expiration of the business relationship and treatment of customer data impacted
CA-70	The MSA with the client contain clauses relating to confidentiality with respect to the services performed.

Common Criteria 3.1: COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

Control Number	Control Activity Description
CA-05	HotWax has defined and documented a 'Risk Assessment and Treatment procedure' that includes the following matters: a. Assessing risks on a periodic basis b. Providing for the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.
CA-06	HotWax has defined and documented a 'Business continuity Framework' that includes the following matters: a. Recovering and continuing service in accordance with documented customer commitments or other agreements. b. Monitoring system capacity to achieve customer commitments or other agreements regarding availability

CA-25	BCP plan defining the roles and responsibilities and identifying the critical information technology application programs, operating systems, personnel, data files, and periods needed to ensure high availability and system reliability is defined by HotWax.
CA-29	On an annual basis, HotWax's IT team performs a risk assessment for HotWax to identify the risk factors considering the changes in the system environment.
CA-36	HotWax has defined 'Information Security Policy' documented and reviewed by the management. The policy includes the following aspects: Risk Management, Access Controls, Personnel Security, Asset Management, Physical Security, Business Continuity, Information Transfer.
CA-38	Physical and Environmental Security Policy is defined and documented by the Physical Security Team and approved by the VP - Physical Security Team.
CA-67	HotWax enters into agreements with third party vendors covering the scope of services and confidentiality clauses. The vendor agreements, including any security, availability, and confidentiality commitments, are reviewed by HotWax management during the procurement process.

Common Criteria 3.2: COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

Control Number	Controls Activity Description
CA-03	HotWax has defined and documented a 'Security Incident Management Procedure' that includes the following matters: a. Addressing how complaints and requests relating to security issues are resolved b. Identifying and mitigating security breaches and other incidents c. Providing for the handling of exceptions and situations not specifically addressed in its system security policies.
CA-04	HotWax has defined and documented a 'Information Classification Procedure' that includes the following matters: a. Classifying data based on its criticality and sensitivity and that classify is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements b. Preventing unauthorized access
CA-05	HotWax has defined and documented a 'Risk Assessment and Treatment procedure' that includes the following matters: a. Assessing risks on a periodic basis b. Providing for the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.
CA-06	HotWax has defined and documented a 'Business continuity Framework' that includes the following matters: a. Recovering and continuing service in accordance with documented customer commitments or other agreements. b. Monitoring system capacity to achieve customer commitments or other agreements regarding availability
CA-08	HotWax has defined and documented a 'Access Control Policy' that includes the following matters: a. Identifying and documenting the security requirements of authorized users b. Preventing unauthorized access c. Adding new users, modifying the access levels of existing users, and removing users who no

	longer need access d. Assigning responsibility and accountability for system security e. Identifying and mitigating security breaches and other incidents f. Providing for training and other resources to support its system security policies.
CA-25	BCP plan defines the roles and responsibilities and identifying the critical information technology application programs, operating systems, personnel, data files, and periods needed to ensure high availability and system reliability is defined by HotWax.
CA-26	Upon notification of security incidents via manage engine tool by the HotWax associates, the IT Team follows-up with the relevant departments / individuals for RCA, preventive action and corrective action and the security incident tickets are resolved as per the procedure mentioned in the 'Security Incident Reporting & Handling Procedure' document.
CA-29	On an annual basis, HotWax's IT team performs a risk assessment for HotWax to identify the risk factors considering the changes in the system environment.
CA-32	On an annual basis, Penetration Testing is conducted by the external vendors on HotWax network and corrective actions are taken and tracked by the IT team.
CA-36	HotWax has defined 'Information Security Policy' documented and reviewed by the management. The policy includes the following aspects: Risk Management, Access Controls, Personnel Security, Asset Management, Physical Security, Business Continuity, Information Transfer.
CA-37	HotWax IT Security team has a documented Security Incident Management Procedure for handling security incident and the same is approved by the management.
CA-38	Physical and Environmental Security Policy is defined and documented by the admin team and approved by chief information officer

Common Criteria 3.3: COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.

Control Number	Control Activity Description
CA-03	HotWax has defined and documented a 'Security Incident Management Procedure' that includes the following matters: a. Addressing how complaints and requests relating to security issues are resolved b. Identifying and mitigating security breaches and other incidents c. Providing for the handling of exceptions and situations not specifically addressed in its system security policies.
CA-04	HotWax has defined and documented a 'Information Classification Procedure' that includes the following matters: a. Classifying data based on its criticality and sensitivity and that classify is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements b. Preventing unauthorized access

CA-05	HotWax has defined and documented a 'Risk Assessment and Treatment procedure' that includes the following matters: a. Assessing risks on a periodic basis b. Providing for the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.
CA-08	HotWax has defined and documented a 'Access Control Policy' that includes the following matters: a. Identifying and documenting the security requirements of authorized users b. Preventing unauthorized access c. Adding new users, modifying the access levels of existing users, and removing users who no longer need access d. Assigning responsibility and accountability for system security e. Identifying and mitigating security breaches and other incidents f. Providing for training and other resources to support its system security policies.
CA-29	On an annual basis, HotWax's IT team performs a risk assessment for HotWax to identify the risk factors considering the changes in the system environment.
CA-32	On an annual basis, Penetration Testing is conducted by the external vendors on HotWax network and corrective actions are taken and tracked by the IT team.
CA-36	HotWax has defined 'Information Security Policy' documented and reviewed by the management. The policy includes the following aspects: Risk Management, Access Controls, Personnel Security, Asset Management, Physical Security, Business Continuity, Information Transfer.
CA-37	HotWax IT Security team has a documented Security Incident Management Procedure for handling security incident and the same is approved by the management.
CA-38	Physical and Environmental Security Policy is defined and documented by the admin team and approved by chief information officer c concerns raising channels mentioned in procedure document for verbal, in writing or through email address are mentioned in procedure document.
CA-46	HotWax associates are required to sign the 'NDA' document which includes clauses for maintaining confidentiality of information obtained, intellectual property rights of HotWax, termination of employment on breach of NDA amongst others on or before the day of joining.

Common Criteria 3.4: COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.

Control Number	Control Activity Description
CA-09	Changes in HotWax management hierarchy and system of internal control are documented.

Common Criteria 4.1: COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

Control Number	Control Activity Description
CA-01	HotWax has defined and documented a 'Change Management Procedure' that includes the following matters: a. Assigning responsibility and accountability for system changes and maintenance. b. Testing, evaluating, and authorizing system components before implementation.
CA-03	HotWax has defined and documented a 'Security Incident Management Procedure' that includes the following matters: c. Addressing how complaints and requests relating to security issues are resolved d. Identifying and mitigating security breaches and other incidents e. Providing for the handling of exceptions and situations not specifically addressed in its system security policies.
CA-04	HotWax has defined and documented a 'Information Classification Procedure' that includes the following matters: a. Classifying data based on its criticality and sensitivity and that classify is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements b. Preventing unauthorized access
CA-05	HotWax has defined and documented a 'Risk Assessment and Treatment procedure' that includes the following matters: a. Assessing risks on a periodic basis b. Providing for the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.
CA-08	HotWax has defined and documented a 'Access Control Policy' that includes the following matters: a. Identifying and documenting the security requirements of authorized users b. Preventing unauthorized access c. Adding new users, modifying the access levels of existing users, and removing users who no longer need access d. Assigning responsibility and accountability for system security e. Identifying and mitigating security breaches and other incidents f. Providing for training and other resources to support its system security policies.
CA-26	Upon notification of security incidents via manage engine tool by the HotWax associates, the IT Team follows-up with the relevant departments / individuals for RCA, preventive action and corrective action and the security incident tickets are resolved as per the procedure mentioned in the 'Security Incident Reporting & Handling Procedure' document.
CA-29	On an annual basis, HotWax's IT team performs a risk assessment for HotWax to identify the risk factors considering the changes in the system environment.
CA-32	On an annual basis, Penetration Testing is conducted by the external vendors on HotWax network and corrective actions are taken and tracked by the IT team.
CA-36	HotWax has defined 'Information Security Policy' documented and reviewed by the management. The policy includes the following aspects: Risk Management,

	Access Controls, Personnel Security, Asset Management, Physical Security, Business Continuity, Information Transfer.
CA-37	HotWax IT Security team has a documented Security Incident Management Procedure for handling security incident and the same is approved by the management.
CA-38	Physical and Environmental Security Policy is defined and documented by the admin team and approved by chief information officer
CA-39	The policies are made available to HotWax associates via email. Security awareness is spread amongst the associates through emails sent by corporate announcements.
CA-40	An annual performance evaluation process is in place covering KPI's, values, behavior, training needs and career aspiration.
CA-53	Antivirus server is configured to update last released definition file from antivirus vendor.
CA-61	On weekly basis, patches and version upgrades are implemented in workstations through antivirus by infrastructure team.
CA-65	The IT team monitors the antivirus server console to check whether workstations are updated with latest released definition.

Common Criteria 4.2: COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Control Number	Control Activity Description
CA-25	BCP plan defines the roles and responsibilities and identifying the critical information technology application programs, operating systems, personnel, data files, and periods needed to ensure high availability and system reliability is defined by HotWax.
CA-61	On weekly basis, patches and version upgrades are implemented in workstations through antivirus by infrastructure team.
CA-65	The IT team monitors the antivirus server console to check whether workstations are updated with latest released definition.

Common Criteria 5.1: COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

Control Number	Control Activity Description
CA-01	HotWax has defined and documented a 'Change Management Procedure' that includes the following matters: a. Assigning responsibility and accountability for system changes and maintenance a. Testing, evaluating, and authorizing system components before implementation.
CA-03	HotWax has defined and documented a 'Security Incident Management Procedure' that includes the following matters: b. Addressing how complaints and requests relating to security issues are resolved c. Identifying and mitigating security breaches and other incidents d. Providing for the handling of exceptions and situations not specifically addressed in its system security policies.
CA-04	HotWax has defined and documented a 'Information Classification Procedure' that includes the following matters: a. Classifying data based on its criticality and sensitivity and that classify is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements b. Preventing unauthorized access
CA-05	HotWax has defined and documented a 'Risk Assessment and Treatment procedure' that includes the following matters: a. Assessing risks on a periodic basis b. Providing for the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.
CA-06	HotWax has defined and documented a 'Business continuity Framework' that includes the following matters: a. Recovering and continuing service in accordance with documented customer commitments or other agreements. b. Monitoring system capacity to achieve customer commitments or other agreements regarding availability
CA-08	HotWax has defined and documented a 'Access Control Policy' that includes the following matters: a. Identifying and documenting the security requirements of authorized users b. Preventing unauthorized access c. Adding new users, modifying the access levels of existing users, and removing users who no longer need access d. Assigning responsibility and accountability for system security e. Identifying and mitigating security breaches and other incidents f. Providing for training and other resources to support its system security policies.
CA-25	BCP plan defines the roles and responsibilities and identifying the critical information technology application programs, operating systems, personnel, data files, and periods needed to ensure high availability and system reliability is defined by HotWax.

CA-29	On an annual basis, HotWax's IT team performs a risk assessment for HotWax to identify the risk factors considering the changes in the system environment.
CA-32	On an annual basis, Penetration Testing is conducted by the external vendors on HotWax network and corrective actions are taken and tracked by the IT team.
CA-34	Firewalls are used in the perimeter of the core network to block traffic unless specifically configured to permit.
CA-36	HotWax has defined 'Information Security Policy' documented and reviewed by the management. The policy includes the following aspects: Risk Management, Access Controls, Personnel Security, Asset Management, Physical Security, Business Continuity, Information Transfer.
CA-37	HotWax IT Security team has a documented Security Incident Management Procedure for handling security incident and the same is approved by the management.
CA-38	Physical and Environmental Security Policy is defined and documented by the admin team and approved by chief information officer
CA-39	The policies are made available to HotWax associates via email. Security awareness is spread amongst the associates through emails sent by corporate announcements.
CA-53	Antivirus server is configured to update last released definition file from antivirus vendor.
CA-61	On weekly basis, patches and version upgrades are implemented in workstations through antivirus by infrastructure team.
CA-63	Access control mechanisms are configured over the network devices such as firewall.
CA-65	The IT team monitors the antivirus server console to check whether workstations are updated with the latest released definition.

Common Criteria 5.2: COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.

Control Number	Control Activity Description
CA-06	HotWax has defined and documented a 'Business Continuity Framework' that includes the following matters: a. Recovering and continuing service in accordance with documented customer commitments or other agreements. b. Monitoring system capacity to achieve customer commitments or other agreements regarding availability
CA-15	Request for granting logical access to the HotWax associates to the network is sent by the respective HR Executive to the IT Team through E-mail.
CA-16	The Associate Manager-HR communicates the 'End Date' of the HotWax Associate through E-mail for revoking the logical access of the HotWax associate from the network.
CA-25	BCP plan defines the roles and responsibilities and identifying the critical information technology application programs, operating systems, personnel, data files, and periods needed to ensure high availability and system reliability is defined by HotWax.
CA-29	On an annual basis, HotWax's IT team performs a risk assessment for HotWax to identify the risk factors considering the changes in the system environment.

CA-34	Firewalls are used in the perimeter of the core network to block traffic unless specifically configured to permit.
CA-39	HotWax associates via email. Security awareness is spread amongst the associates through emails sent by corporate announcements.
CA-49	User IDs of resigned / terminated HotWax associates on HotWax domain controller are revoked from LTab based on the request raised by the HR team, within one working day from the associate's LWD.
CA-50	Access to the internet is restricted by the IT team for HotWax associates through the content filter. Access to websites other than the sites configured in the content filter is provided by the IT security team.
CA-53	Antivirus server is configured to update last released definition file from antivirus vendor.
CA-55	CD-ROM drives and USBs are disabled on the workstations by default and access is granted by the IT team based on the exception request raised in the manage engine Tool that is approved by the respective department head.
CA-59	Network devices are in place (Firewall, Switch and Router) for protecting HotWax network from unauthorized access.
CA-60	Network diagram detailing the network devices such as firewalls and switches to prevent unauthorized access is maintained for each location by the IT Team and is approved by the IT Head.
CA-61	On weekly basis, patches and version upgrades are implemented in workstations through antivirus by infrastructure team.
CA-65	The IT team monitors the antivirus server console to check whether workstations are updated with latest released definition.

Common Criteria 5.3: COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

Control Number	Control Activity Description
CA-01	HotWax has defined and documented a 'Change Management Procedure' that includes the following matters: a. Assigning responsibility and accountability for system changes and maintenance b. Testing, evaluating, and authorizing system components before implementation.
CA-03	HotWax has defined and documented a 'Security Incident Management Procedure' that includes the following matters: a. Addressing how complaints and requests relating to security issues are resolved b. Identifying and mitigating security breaches and other incidents c. Providing for the handling of exceptions and situations not specifically addressed in its system security policies.
CA-04	HotWax has defined and documented a 'Information Classification Procedure' that includes the following matters: a. Classifying data based on its criticality and sensitivity and that classify is used to define protection requirements, access rights and access restrictions, and

	retention and destruction requirements b. Preventing unauthorized access.
CA-05	HotWax has defined and documented a 'Risk Assessment and Treatment procedure' that includes the following matters: a. Assessing risks on a periodic basis b. Providing for the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.
CA-07	HotWax HR has defined and documented HR Policies which are approved by the management. The HR Policies is available to HotWax associates through 'HotWax intranet portal'.
CA-08	HotWax has defined and documented a 'Access Control Policy' that includes the following matters: a. Identifying and documenting the security requirements of authorized users b. Preventing unauthorized access c. Adding new users, modifying the access levels of existing users, and removing users who no longer need access d. Assigning responsibility and accountability for system security e. Identifying and mitigating security breaches and other incidents f. Providing for training and other resources to support its system security policies.
CA-14	Organization chart for HotWax is maintained by the HR Team and reviewed on need basis.
CA-26	Upon notification of security incidents via manage engine tool by the HotWax associates, the IT Team follows-up with the relevant departments / individuals for RCA, preventive action and corrective action and the security incident tickets are resolved as per the procedure mentioned in the 'Security Incident Reporting & Handling Procedure' document.
CA-29	On an annual basis, HotWax's IT team performs a risk assessment for HotWax to identify the risk factors considering the changes in the system environment.
CA-35	HotWax associates are made aware of their security commitments by means of annual security training and assessment covering security principles awareness, roles and responsibilities, information protection methods and security lapses.
CA-36	HotWax has defined 'Information Security Policy' documented and reviewed by the management. The policy includes the following aspects: Risk Management, Access Controls, Personnel Security, Asset Management, Physical Security, Business Continuity, Information Transfer.
CA-37	HotWax IT security team has a documented Security Incident Management Procedure for handling security incident and the same is approved by the management.
CA-38	Physical and Environmental Security Policy is defined and documented by the admin team and approved by chief information officer
CA-39	The policies are made available to HotWax associates via email. Security awareness is spread amongst the associates through emails sent by corporate announcements.
CA-46	HotWax associates are required to sign the 'NDA' document which includes clauses for maintaining confidentiality of information obtained, intellectual property rights of HotWax, termination of employment on breach of NDA amongst others on or before the day of joining.

Common Criteria 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

Control Number	Control Activity Description
CA-04	HotWax has defined and documented a 'Information Classification Procedure' that includes the following matters: a. Classifying data based on its criticality and sensitivity and that classify is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements b. Preventing unauthorized access
CA-12	Audit policies are enabled by the IT team on HotWax domain controller.
CA-15	Request for granting logical access to the HotWax associates to the network is sent by the respective HR Executive to the IT Team through E-mail.
CA-16	The associate manager-HR communicates the 'End Date' of the HotWax Associate through E-mail for revoking the logical access of the HotWax Associate from the network.
CA-32	On an annual basis, Penetration Testing is conducted by the external vendors on HotWax network and corrective actions are taken and tracked by the IT team.
CA-34	Firewalls are used in the perimeter of the core network to block traffic unless specifically configured to permit.
CA-36	HotWax has defined 'Information Security Policy' documented and reviewed by the management. The policy includes the following aspects: Risk Management, Access Controls, Personnel Security, Asset Management, Physical Security, Business Continuity, Information Transfer.
CA-39	HotWax associates via email. Security awareness is spread amongst the associates through emails sent by corporate announcements.
CA-49	User IDs of resigned / terminated HotWax associates on HotWax domain controller are revoked from LTab based on the request raised by the HR team, within one working day from the associate's LWD.
CA-50	Access to the internet is restricted by the IT team for HotWax associates through the content filter. Access to websites other than the sites configured in the content filter is provided by the IT Security team.
CA-55	CD-ROM drives and USBs are disabled on the workstations by default and access is granted by the IT team based on the exception request raised in the manage engine tool that is approved by the respective department head.
CA-57	Domain user's password policies, account lockout policies and screensaver time-out settings are defined and enforced through HotWax domain controller.
CA-59	Network devices are in place (Firewall, Switch and Router) for protecting HotWax network from unauthorized access.
CA-60	Network diagram detailing the network devices such as firewalls and switches to prevent unauthorized access is maintained for each location by the IT Team and is approved by the IT Head.
CA-61	On weekly basis, patches and version upgrades are implemented in workstations through antivirus by infrastructure team.
CA-63	Access control mechanism is configured over the network devices such as firewall.

Common Criteria 6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

Control Number	Control Activity Description
CA-10	A Master Service Agreement ('MSA') is signed between HotWax and the client covering the service offerings, responsibilities, security, availability, and confidentiality commitments of HotWax and the client.
CA-15	Request for granting logical access to the HotWax associates to the network is sent by the respective HR Executive to the IT Team through E-mail.
CA-16	The associate manager-HR communicates the 'End Date' of the HotWax associate through E-mail for revoking the logical access of the HotWax associate from the network.
CA-36	HotWax has defined 'Information Security Policy' documented and reviewed by the management. The policy includes the following aspects: Risk Management, Access Controls, Personnel Security, Asset Management, Physical Security, Business Continuity, Information Transfer.
CA-37	HotWax IT security team has a documented Security Incident Management Procedure for handling security incident and the same is approved by the management.
CA-38	Physical and Environmental Security Policy is defined and documented by the admin team and approved by chief information officer
CA-49	User IDs of resigned / terminated HotWax associates on HotWax domain controller are revoked from LTab based on the request raised by the HR team, within one working day from the associate's LWD.
CA-50	Access to the internet is restricted by the IT team for HotWax associates through the content filter. Access to websites other than the sites configured in the content filter is provided by the IT security team.
CA-56	HotWax has defined a 'Media Disposal Procedure' that includes the following matters: • Disposal guidelines for electronic-based media • Disposal guidelines for paper-based media
CA-57	Domain user's password policies, account lockout policies and screensaver time-out settings are defined and enforced through HotWax domain controller.
CA-59	Network devices are in place (Firewall, Switch and Router) for protecting HotWax network from unauthorized access.
CA-63	Access control mechanism is configured over the network devices such as firewall.

Common Criteria 6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, considering the concepts of least privilege and segregation of duties, to meet the entity's objectives.

Control Number	Control Activity Description
CA-15	Request for granting logical access to the HotWax associates to the network is sent by the respective HR executive to the IT Team through E-mail.
CA-16	The associate manager-HR communicates the 'End Date' of the HotWax associate through E-mail for revoking the logical access of the HotWax associate from the network.
CA-34	Firewalls are used in the perimeter of the core network to block traffic unless specifically configured to permit.
CA-49	User IDs of resigned / terminated HotWax associates on HotWax domain controller are revoked from LTab based on the request raised by the HR team, within one working day from the associate's LWD.
CA-50	Access to the internet is restricted by the IT team for HotWax associates through the content filter. Access to websites other than the sites configured in the content filter is provided by the IT security team.
CA-55	CD-ROM drives and USBs are disabled on the workstations by default and access is granted by the IT team based on the exception request raised in the manage engine tool that is approved by the respective department head
CA-57	Domain user's password policies, account lockout policies and screensaver time-out settings are defined and enforced through HotWax domain controller.
CA-60	Network diagram detailing the network devices such as firewalls and switches to prevent unauthorized access is maintained for each location by the IT Team and is approved by the IT Head.

Common Criteria 6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

Control Number	Control Activity Description
CA-17	The business continuity framework includes backup and restoration procedures for restoration of system operations.
CA-18	CCTV cameras are in place at entry points in HotWax facility. Events are recorded and retained in the system.
CA-19	Entry and exit details of the vendors / visitors to HotWax facility are recorded via visitors register.
CA-20	As per the AMC, preventive maintenance is performed for equipment like fire extinguishers, smoke detectors, air conditioners, UPS, and diesel generators.
CA-21	Physical access of the resigned/ terminated HotWax associates is revoked by the facilities manager based on a revocation request sent by the HotWax HR on the last working day of the associate.
CA-22	Physical access to HotWax onboarded associates is granted by the facilities manager

	based on the request raised by the HR through email.
CA-23	Physical access to HotWax facilities is monitored by the security guards for restricting unauthorized access.
CA-24	Proximity card-based access control system with anti-pass back system is installed in HotWax facility.
CA-52	Smoke / fire detection, suppression systems, temperature and humidity monitoring devices, UPS and diesel generators are installed for protection against environmental hazards such as fire, dust, power, excessive heat, and humidity.
CA-66	On an annual basis, Fire safety drill is conducted by the emergency rescue team at HotWax facility

Common Criteria 6.5: The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.

Control Number	Control Activity Description
CA-21	Physical access of the resigned/ terminated HotWax associates is revoked by the facilities manager based on revocation request sent by the HotWax HR on the last working day of the associate.
CA-49	User IDs of resigned / terminated HotWax associates on HotWax domain controller are revoked from LTab based on the request raised by the HR team, within one working day from the associate's LWD.
CA-56	HotWax has defined a 'Media Disposal Procedure' that includes the following matters: • Disposal guidelines for electronic-based media • Disposal guidelines for paper-based media

Common Criteria 6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

Control Number	Control Activity Description
CA-04	HotWax has defined and documented a 'Information Classification Procedure' that includes the following matters: a. Classifying data based on its criticality and sensitivity and that classify is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements b. Preventing unauthorized access
CA-16	The associate manager-HR communicates the 'End Date' of the HotWax associate through E-mail for revoking the logical access of the HotWax associate from the network.
CA-34	Firewalls are used in the perimeter of the core network to block traffic unless specifically configured to permit.
CA-36	HotWax has defined 'Information Security Policy' documented and reviewed by the management. The policy includes the following aspects: Risk Management, Access Controls, Personnel Security, Asset Management, Physical Security, Business Continuity, Information Transfer.
CA-38	Physical and Environmental Security Policy is defined and documented by the admin team and approved by chief information officer
CA-39	HotWax associates via email. Security awareness is spread amongst the associates through emails sent by corporate announcements.
CA-46	HotWax associates are required to sign the 'NDA' document which includes clauses

	for maintaining confidentiality of information obtained, intellectual property rights of HotWax, termination of employment on breach of NDA amongst others on or before the day of joining.
CA-49	User IDs of resigned / terminated HotWax associates on HotWax domain controller are revoked from LTab based on the request raised by the HR team, within one working day from the associate's LWD.
CA-50	Access to the internet is restricted by the IT team for HotWax associates through the content filter. Access to websites other than the sites configured in the content filter is provided by the IT security team.
CA-53	Antivirus server is configured to update last released definition file from antivirus vendor.
CA-55	CD-ROM drives and USBs are disabled on the workstations by default and access is granted by the IT team based on the exception request raised in the manage engine tool that is approved by the respective department head.
CA-57	Domain user's password policies, account lockout policies and screensaver time-out settings are defined and enforced through HotWax domain controller.
CA-59	Network devices are in place (Firewall, Switch and Router) for protecting HotWax network from unauthorized access.
CA-60	Network diagram detailing the network devices such as firewalls and switches to prevent unauthorized access is maintained for each location by the IT Team and is approved by the IT Head.
CA-63	Access control mechanism is configured over the network devices such as firewall.

Common Criteria 6.7: The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.

Control Number	Control Activity Description
CA-16	The associate manager-HR communicates the 'End Date' of the HotWax associate through E-mail for revoking the logical access of the HotWax associate from the network.
CA-17	The business continuity framework includes backup and restoration procedures for restoration of system operations.
CA-34	Firewalls are used in the perimeter of the core network to block traffic unless specifically configured to permit
CA -36	HotWax has defined 'Information Security Policy' documented and reviewed by the management. The policy includes the following aspects: Risk Management, Access Controls, Personnel Security, Asset Management, Physical Security, Business Continuity, Information Transfer.
CA-38	Physical and Environmental Security Policy is defined and documented by the admin team and approved by chief information officer
CA-50	Access to the internet is restricted by the IT team for HotWax associates through the content filter. Access to websites other than the sites configured in the content filter is provided by the IT security team.
CA-55	CD-ROM drives and USBs are disabled on the workstations by default and access is granted by the IT team based on the exception request raised in the manage engine tool that is approved by the respective department head.
CA-56	HotWax has defined a 'Media Disposal Procedure' that includes the following matters: • Disposal guidelines for electronic-based media

	• Disposal guidelines for paper-based media
CA-57	Domain user's password policies, account lockout policies and screensaver time-out settings are defined and enforced through HotWax domain controller.
CA-59	Network devices are in place (Firewall, Switch and Router) for protecting HotWax network from unauthorized access.

Common Criteria 6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

Control Number	Control Activity Description
CA-15	Request for granting logical access to the HotWax associates to the network is sent by the respective HR executive to the IT team through E-mail.
CA-16	The associate manager-HR communicates the 'End Date' of the HotWax associate through E-mail for revoking the logical access of the HotWax associate from the network.
CA-32	On an annual basis, Penetration Testing is conducted by the external vendors on HotWax network and corrective actions are taken and tracked by the IT team.
CA-34	Firewalls are used in the perimeter of the core network to block traffic unless specifically configured to permit.
CA-50	Access to the internet is restricted by the IT team for HotWax associates through the content filter. Access to websites other than the sites configured in the content filter is provided by the IT security team.
CA-53	Antivirus server is configured to update last released definition file from antivirus vendor.
CA-55	CD-ROM drives and USBs are disabled on the workstations by default and access is granted by the IT team based on the exception request raised in the manage engine tool that is approved by the respective department head.
CA-59	Network devices are in place (Firewall, Switch and Router) for protecting HotWax network from unauthorized access.
CA-60	Network diagram detailing the network devices such as firewalls and switches to prevent unauthorized access is maintained for each location by the IT Team and is approved by the IT Head.
CA-61	On weekly basis, patches and version upgrades are implemented in workstations through antivirus by infrastructure team.
CA-63	Access control mechanism is configured over the network devices such as firewall.
CA-65	The IT team monitors the antivirus server console to check whether workstations are updated with latest released definition.

Common Criteria 7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.

Control Number	Control Activity Description
CA-53	Antivirus server is configured to update last released definition file from antivirus vendor.
CA-63	Access control mechanism is configured over the network devices such as firewall.
CA-65	The IT team monitors the antivirus server console to check whether workstations are updated with latest released definition.

Common Criteria 7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.

Control Number	Control Activity Description
CA-03	HotWax has defined and documented a 'Security Incident Management Procedure' that includes the following matters: a. Addressing how complaints and requests relating to security issues are resolved b. Identifying and mitigating security breaches and other incidents c. Providing for the handling of exceptions and situations not specifically addressed in its system security policies.
CA-17	The business continuity Framework includes backup and restoration procedures for restoration of system operations.
CA-19	Entry and exit details of the vendors / visitors to HotWax facility are recorded via visitors register.
CA-20	As per the AMC, preventive maintenance is performed for equipment like fire extinguishers, smoke detectors, air conditioners, UPS, and diesel generators.
CA-52	Smoke / fire detection, suppression systems, temperature and humidity monitoring devices, UPS and diesel generators are installed for protection against environmental hazards such as fire, dust, power, excessive heat, and humidity.
CA-53	Antivirus server is configured to update last released definition file from antivirus vendor.
CA-55	CD-ROM drives and USBs are disabled on the workstations by default and access is granted by the IT team based on the exception request raised in the manage engine tool that is approved by the respective department head.
CA-59	Network devices are in place (Firewall, Switch and Router) for protecting HotWax network from unauthorized access.
CA-63	Access control mechanism is configured over the network devices such as firewall.
CA-65	The IT team monitors the antivirus server console to check whether workstations are updated with latest released definition.
CA-66	On an annual basis, fire safety drill is conducted by the emergency rescue team at HotWax facility.

Common Criteria 7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

Control Number	Control Activity Description
CA-03	HotWax has defined and documented a 'Security Incident Management Procedure' that includes the following matters: a. Addressing how complaints and requests relating to security issues are resolved b. Identifying and mitigating security breaches and other incidents c. Providing for the handling of exceptions and situations not specifically addressed in its system security policies.
CA-32	On an annual basis, Penetration Testing is conducted by the external vendors on HotWax network and corrective actions are taken and tracked by the IT team.
CA-47	The process for informing HotWax IT Team about possible security breaches and other incidents and escalation of the same is and is also intimated as part of the induction program.
CA-65	The IT team monitors the antivirus server console to check whether workstations are updated with latest released definition.

Common Criteria 7.4: The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.

Control Number	Control Activity Description
CA-03	HotWax has defined and documented a 'Security Incident Management Procedure' that includes the following matters: a. Addressing how complaints and requests relating to security issues are resolved b. Identifying and mitigating security breaches and other incidents c. Providing for the handling of exceptions and situations not specifically addressed in its system security policies.
CA-08	HotWax has defined and documented a 'Access Control Policy' that includes the following matters: a. Identifying and documenting the security requirements of authorized users b. Preventing unauthorized access c. Adding new users, modifying the access levels of existing users, and removing users who no longer need access d. Assigning responsibility and accountability for system security e. Identifying and mitigating security breaches and other incidents f. Providing for training and other resources to support its system security policies.
CA-26	Upon notification of security incidents via manage engine tool by the HotWax associates, the IT Team follows-up with the relevant departments / individuals for RCA, preventive action and corrective action and the Security incident tickets are resolved as per the procedure mentioned in the 'Security Incident Reporting & Handling Procedure' document.
CA-32	On an annual basis, Penetration Testing is conducted by the external vendors on HotWax network and corrective actions are taken and tracked by the IT team.
CA-37	HotWax IT Security team has a documented Security Incident Management Procedure for handling security incident and the same is approved by the management.
CA-47	The process for informing HotWax IT Team about possible security breaches and other incidents and escalation of the same is and is also intimated as part of the induction program.

Common Criteria 7.5: The entity identifies, develops, and implements activities to recover from identified security incidents.

Control Number	Control Activity Description
CA-03	HotWax has defined and documented a 'Security Incident Management Procedure' that includes the following matters: a. Addressing how complaints and requests relating to security issues are resolved b. Identifying and mitigating security breaches and other incidents c. Providing for the handling of exceptions and situations not specifically addressed in its system security policies.
CA-25	BCP plan defines the roles and responsibilities and identifying the critical information technology application programs, operating systems, personnel, data files, and periods needed to ensure high availability and system reliability is defined by HotWax.
CA-32	On an annual basis, Penetration Testing is conducted by the external vendors on HotWax network and corrective actions are taken and tracked by the IT team.
CA-47	The process for informing HotWax IT Team about possible security breaches and other incidents and escalation of the same is and is also intimated as part of the induction program.

Common Criteria 8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

Control Number	Control Activity Description
CA-01	HotWax has defined and documented a 'Change Management Procedure' that includes the following matters: a. Assigning responsibility and accountability for system changes and maintenance b. Testing, evaluating, and authorizing system components before implementation.
CA-29	On an annual basis, HotWax's IT team performs a risk assessment for HotWax to identify the risk factors considering the changes in the system environment.
CA-32	On an annual basis, Penetration Testing is conducted by the external vendors on HotWax network and corrective actions are taken and tracked by the IT team.
CA-51	Acquisition and implementation of new IT Systems are performed as per the change management procedure.
CA-58	Emergency changes to HotWax Information System are logged using the manage engine tool and resolved as per the change management procedure.
CA-61	On weekly basis, patches and version upgrades are implemented in workstations through Antivirus by infrastructure team.
CA-65	The IT team monitors the antivirus server console to check whether workstations are updated with latest released definition.
CA-113	Change requests are logged in the 'JIRA' ticketing tool maintained by the product manager

Common Criteria 9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.

Control Number	Control Activity Description
CA-17	The business continuity framework includes backup and restoration procedures for restoration of system operations.
CA-25	BCP plan defines the roles and responsibilities and identifying the critical information technology application programs, operating systems, personnel, data files, and periods needed to ensure high availability and system reliability is defined by HotWax.
CA-29	On an annual basis, HotWax's IT team performs a risk assessment for HotWax to identify the risk factors considering the changes in the system environment.

Common Criteria 9.2: The entity assesses and manages risks associated with vendors and business partners.

Control Number	Control Activity Description
CA-31	HotWax's security commitments (including security obligations, terms, conditions, and responsibilities) are documented, along with the responsibilities of external users, in newly onboarded third party contracts and non-disclosure agreements.
CA-67	HotWax enters into agreements with third party vendors covering the scope of services and confidentiality clauses. The vendor agreements, including any security, availability, and confidentiality commitments, are reviewed by HotWax management during the procurement process.
CA-68	Master Service Agreements (MSAs) between HotWax and vendors are incorporated to include: a. Scope of business relationship and services offered b. Information security requirements c. Timely notification of a security incident to customers d. Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification) e. Expiration of the business relationship and treatment of customer data impacted
CA-69	Third party service providers sign a Non-Disclosure agreement with HotWax before commencement of services.

Availability 1.1: The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.

Control Number	Control Activity Description
CA-25	BCP plan defines the roles and responsibilities and identifying the critical information technology application programs, operating systems, personnel, data files, and periods needed to ensure high availability and system reliability is defined by HotWax.

Availability 1.2: The entity authorizes, designs, develops, or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.

Control Number	Control Activity Description
CA-17	The business continuity framework includes backup and restoration procedures for restoration of system operations.
CA-20	As per the AMC, preventive maintenance is performed for equipment like fire extinguishers, smoke detectors, air conditioners, UPS, and diesel generators.
CA-25	BCP's plan defining the roles and responsibilities and identifying the critical information technology application programs, operating systems, personnel, data files, and periods needed to ensure high availability and system reliability is defined by HotWax.
CA-54	Backup file copies are stored in an alternate location on periodic basis.
CA-66	On an annual basis, fire safety drill is conducted by the emergency rescue team at HotWax facility

Availability 1.3: The entity tests recovery plan procedures supporting system recovery to meet its objectives.

Control Number	Control Activity Description
CA-06	HotWax has defined and documented a 'Business continuity Framework' that includes the following matters: a. Recovering and continuing service in accordance with documented customer commitments or other agreements. b. Monitoring system capacity to achieve customer commitments or other agreements regarding availability
CA-17	The business continuity framework includes backup and restoration procedures for restoration of system operations.
CA-25	BCP plan defines the roles and responsibilities and identifying the critical information technology application programs, operating systems, personnel, data files, and periods needed to ensure high availability and system reliability is defined by HotWax.

Confidentiality 1.1: The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality

Control Number	Control Activity Description
CA-02	HotWax established written policies related to retention periods for the confidential information.
CA-04	HotWax has defined and documented an 'Information Classification Procedure' that includes the following matters: a. Classifying data based on its criticality and sensitivity and that classify is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements b. Preventing unauthorized access
CA-55	CD-ROM drives and USBs are disabled on the workstations by default and access is granted by the IT team based on the exception request raised in the manage engine tool that is approved by the respective department head.
CA-62	System change requests are evaluated to determine the potential effect of the change on security, availability, processing integrity, and system requirements as part of the change management process.

Confidentiality 1.2: The entity disposes of confidential information to meet the entity's objectives related to confidentiality.

Control Number	Control Activity Description
CA-04	HotWax has defined and documented an 'Information Classification Procedure' that includes the following matters: a. Classifying data based on its criticality and sensitivity and that classify is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements b. Preventing unauthorized access

SECTION – 4 TRUST SERVICES CRITERIA AND HOTWAX CONTROL

#	Control Activity	Trust Services Criteria mapping	Tests Performed	CUEC/ CSOC	Results of Tests
CA-01	HotWax has defined and documented a Change Management Procedure that includes the following: a. Assigning responsibility and accountability for system changes and maintenance. b. Testing, evaluating, and authorizing system components before implementation.	CC 1.3 CC 1.5 CC 2.1 CC 2.2 CC 4.1 CC 5.1 CC 5.3 CC 8.1	Inspected the 'Change Management Procedure' document for the following aspects: Policy Version-V3 Contents of the Document to ascertain whether HotWax had defined a 'Change Management Procedure' that includes the following matters: a. Assigning responsibility and accountability for system changes and maintenance. b. Testing, evaluating, and authorizing system components before implementation.	None	No exceptions noted
CA-02	HotWax has established written policies related to retention periods for the confidential information.	C 1.1	Inspected the Data Retention Policy and Data Registration for aspects Policy Version – V2' and 'Contents of the Document' to ascertain whether HotWax had established written policies related to retention periods for the confidential information.	None	No exceptions noted.

#	Control Activity	Trust Services Criteria mapping	Tests Performed	CUEC / CSOC	Results of Tests
CA-03	HotWax has defined and documented a Security Incident Management Procedure that includes the following: a. Addressing how complaints and requests related to security issues are resolved. b. Identifying and mitigating security breaches and other incidents. c. Providing procedures for handling exceptions and situations not specifically addressed in its system security policies.	CC 1.3 CC 1.5 CC 2.1 CC 3.2 CC 3.3 CC 4.1 CC 5.1 CC 5.3 CC 7.2 CC 7.3 CC 7.4 CC 7.5	Inspected the 'Security Incident Management Procedure' document for the following aspects: Policy Version-V02 Contents of the Document to ascertain whether HotWax had defined and documented a 'Security Incident Management Procedure' that includes the following matters: a. Addressing how complaints and requests relating to security issues are resolved. b. Identifying and mitigating security breaches and other incidents. c. Providing for the handling of exceptions and situations not specifically addressed in the system security policies.	None	No exceptions noted

CA-04	HotWax has defined and documented an Information Classification Procedure that includes the following: a. Classifying data based on its criticality and sensitivity, and using that classification to define protection requirements access	**CC 1.3** **CC 1.5** **CC 2.1** **CC 2.2** **CC 3.2** **CC 3.3** **CC 4.1** **CC 5.1** **CC 5.3** **CC 6.1** **CC 6.6** **C 1.1** **C 1.2**	Inspected the 'Data Classification Policy' document for the following aspects: Policy Version-V2.0 Contents of the Document to ascertain whether HotWax had defined an 'Information	None	No exceptions noted.

#	Control Activity	Trust Services Criteria mapping	Tests Performed	CUEC/ CSOC	Results of Tests
	rights and restrictions, as well as retention and destruction requirements. b. Preventing unauthorized access.		Classification Procedure' that includes the following matters a. Classifying data based on its criticality and sensitivity and ensuring the classification is used to define protection requirements, access rights and restrictions, and retention and destruction requirements. b. Preventing unauthorized access.	None	No exceptions noted.
CA-05	HotWax has defined and documented an Information Classification Procedure that includes the following: a. Classifying data based on its criticality and sensitivity, and using that classification to define protection requirements, access rights and restrictions, as well as retention and destruction requirements. b. Preventing unauthorized access.	CC 1.3 CC 1.5 CC 2.1 CC 3.1 CC 3.2 CC 3.3 CC 4.1 CC 5.1 CC 5.3	Inspected the 'Risk Assessment and Treatment Procedure' for aspects as Policy Version–V03 and 'Contents of the Document' to ascertain whether HotWax has defined and documented a Risk Assessment and Treatment Procedure that includes the following matters: a. Assessing risks on a periodic basis. b. Ensuring identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.	None	No exceptions noted.

#	Control Activity	Trust Services Criteria mapping	Tests Performed	CUEC/ CSOC	Results of Tests
CA-06	HotWax has defined and documented a Business Continuity Framework that includes the following: a. Recovering and continuing service in accordance with documented customer commitments or other agreements. b. Monitoring system capacity to ensure achievement of customer commitments or other agreements regarding availability.	CC 1.5 CC 3.1 CC 3.2 CC 5.1 CC 5.2 A 1.3	Inspected the 'Business Continuity Plan' for aspects as Policy Version – V01 and 'Contents of the Document' to ascertain whether HotWax has defined a Business Continuity Plan that includes the following matters: a. Procedures for recovering and continuing services in accordance with documented customer commitments or other agreements. b. Monitoring system capacity to ensure the achievement of customer commitments or other agreements regarding availability.	None	No exceptions noted.
CA-07	HotWax HR has defined and documented HR Policies which are approved by the management. The HR Policies is available to HotWax associates through 'HotWax Intranet portal'.	CC 5.3	Inspected the 'Human Resource Information Security Manual' for aspects as Policy Version-V2.0 and 'Contents of the Document' to ascertain whether HotWax HR had defined and documented HR policies which were approved by the management.	None	No exceptions noted.

#	Control Activity	Trust Services Criteria mapping	Tests Performed	CUEC/ CSOC	Results of Tests
CA-08	HotWax has defined and documented an Access Control Policy that includes the following: a. Identifying and documenting the security requirements of authorized users. b. Preventing unauthorized access. c. Adding new users, modifying the access levels of existing users, and removing users who no longer need access. d. Assigning responsibility and accountability for system security. e. Identifying and mitigating security breaches and other incidents f. Providing training and other resources to support its system security policies.	CC 1.3 CC 1.5 CC 2.1 CC 2.2 CC 3.2 CC 3.3 CC 4.1 CC 5.1 CC 5.3 CC 7.4	Inspected the 'Access Control Policy' document for the following aspects: Policy Version: 2.0 Contents of the Document to ascertain whether HotWax had defined an 'Access Control Policy' that includes the following matters: a. Identifying and documenting the security requirements of authorized users. b. Preventing unauthorized access. c. Adding new users, modifying access levels of existing users, and removing users who no longer need access. d. Assigning responsibility and accountability for system security. e. Identifying and mitigating security breaches and other incidents. f. Providing training and other resources to support system security policies.	None	No exception noted

#	Control Activity	Trust Services Criteria mapping	Tests Performed	CUEC/ CSOC	Results of Tests
CA-09	Changes in HotWax management hierarchy and system of internal control are documented.	CC 2.2 CC 3.4	Inspected the organization chart to determine that the changes in HotWax management hierarchy and system of internal control are documented.	None	No exceptions noted.
CA-10	A Master Service Agreement ('MSA') is signed between HotWax and the Client covering the service offerings, responsibilities, security, availability, and confidentiality commitments of HotWax and the Client.	CC 1.1 CC 2.3 CC 6.2	Inspected a sample of Master Service Agreements for aspects such as 'scope of services', 'date of effectiveness of MSA' and 'validity of agreement' to ascertain whether a Master Service Agreement ('MSA') was signed between HotWax, and the clients covered the service offerings, responsibilities, security, availability, and confidentiality commitments of HotWax and the Client.	None	No exceptions noted.
CA-11	HotWax communicates its commitment to security as a top priority for its customers via MSA.	CC 2.3	Inspected the Master Service Agreement for aspects such as 'scope of services', 'date of effectiveness of MSA', 'validity of agreement' and 'security commitments' to ascertain whether to ascertain whether HotWax communicated its commitment to security as a top priority for its customers via MSA.	None	No exceptions noted.

CA-12	Audit policies are enabled by the IT team on HotWax Domain Controller.	CC 6.1	Inspected the Windows Domain Controller Policy for aspects such as 'Audit Policy Settings' to ascertain whether audit policies were enabled by the IT Team on the HotWax Windows Domain Controller. Inspected the audit policies for sample workstations for aspects such as 'Associate ID', 'Associate name', and 'Audit policies enabled status' to ascertain whether the Audit policies were enabled by the IT Team on the HotWax Windows Domain Controller.	None	No exceptions noted.

#	Control Activity	Trust Services Criteria mapping	Tests Performed	CUEC / CSOC	Results of Tests
CA-13	MSA defines security, availability, and confidentiality commitments along with responsibilities of HotWax and the Client.	CC 2.3	Inspected the Master Service Agreement for aspects such as 'scope of services', 'date of effectiveness of MSA', 'validity of agreement', 'sign-off details of the clients' and 'sign-off details of HotWax' to ascertain whether MSA defined security and confidentiality commitments along with responsibilities of HotWax and the client.	None	No exceptions noted.
CA-14	Organization Chart for HotWax is maintained by the HR Team and reviewed on need basis.	CC 1.3 CC 2.2 CC 5.3	Inspected the Organization Chart to ascertain whether organization chart for HotWax was maintained by the HR Team and reviewed on need basis.	None	No exceptions noted.
CA-15	Request for granting logical access to the HotWax associates to the 'network is sent by the respective HR Executive to the IT Team through E-mail.	CC 2.2 CC 5.2 CC 6.1 CC 6.2 CC 6.3 CC 6.8	Inspected the email communications for aspects such as 'Associate name', 'Date of Joining', 'Created by', 'requested on' and 'Logical access grant date' for sample HotWax on boarding associates to ascertain whether request for granting logical access to the HotWax associates to network was sent by the respective HR Executive to the IT Team through E-mail.	None	No exceptions noted.
CA-16	The Associate Manager-HR communicates the 'End Date' of the HotWax Associate through E- mail for revoking the logical access of the HotWax Associate from the network.	CC 5.2 CC 6.1 CC 6.2 CC 6.3 CC 6.6 CC 6.7 CC 6.8	Inspected email requests for the aspects such as 'Associate Name', 'Last Working Date of off-boarding associate', 'Date of access revocation', 'Email Sent by', 'Email sent on' for sample HotWax Off- boarded associates to ascertain whether The Associate Manager-HR communicated the 'End Date' of the HotWax Associate through E-mail for revoking the logical access of the HotWax Associate from the network.	None	No exceptions noted.

CA-17	The Business continuity Framework includes backup and restoration procedures for restoration of system operations.	CC 6.4 CC 6.7 CC 7.2 CC 9.1 A 1.2 A 1.3	Inspected the Backup and Recovery Policy' for aspects as Policy Version-V2.0 and 'Contents of the Document' to ascertain whether the Business continuity Framework included backup and restoration procedures for restoration of system operations.	None	No exceptions noted.

#	Control Activity	Trust Services Criteria mapping	Tests Performed	CUEC/ CSOC	Results of Tests
CA-18	CCTV Cameras are in place at entry points in HotWax facility. Events are recorded and retained in the system.	CC6.4	Observed the HotWax facility to ascertain whether CCTV Cameras were in place at entry points in HotWax facility and were recorded and retained in the system.	None	No exceptions noted.
CA-19	Entry and exit details of the vendors / visitors to HotWax facility are recorded via Visitors register.	CC 6.4 CC 7.2	Inspected the Visitor Register for aspects such as 'Location', 'Visitor/ Vendor Name', 'Date', 'In time', 'Out time' and 'for sample dates to ascertain whether entry and exit details of the vendors / visitors to HotWax facility were recorded via Visitors register.	None	No exceptions noted.
CA-20	As per the AMC, preventive maintenance is performed for equipment like fire extinguishers, smoke detectors, air conditioners, UPS, and diesel generators.	CC 6.4 CC 7.2 A 1.2	Not applicable as necessary checks and maintenance is done by the inhouse team of HotWax.	None	Not applicable.
CA-21	Physical access of the resigned/ terminated HotWax associates is revoked by the Facilities Manager based on revocation request sent by the HotWax HR on the Last Working Day of the associate.	CC 6.4 CC 6.5	Inspected the email communication for aspects such as 'associate name', 'last working date of the associates', 'request raised date', 'access revoked date', 'sender of Email' and 'recipient of Email' for sample off boarded associates to ascertain whether physical access of the resigned/ terminated HotWax associates were revoked by the Facilities Manager based on revocation request sent by the HotWax HR on the Last Working Day of the associate.	None	No exceptions noted.

#	Control Activity	Trust Services Criteria mapping	Tests Performed	CUEC/ CSOC	Results of Tests
CA-22	Physical access to HotWax onboarded associates is granted by the Facilities Manager based on the request raised by the HR through email.	CC 6.4	Inspected the email communications and Physical Access tool for aspects such as 'Associate name', 'Date of Joining HotWax', 'created by', 'requested on', 'physical access grant date', 'sender of Email' and 'recipient of Email' for sample HotWax on boarding associates to ascertain whether Physical access to HotWax onboarded associates were granted by the Facilities Manager based on the request raised by the HR through email.	None	No exceptions noted.
CA-23	Physical access to HotWax facilities is monitored by the Security Guards for restricting unauthorized access.	CC 6.4	Observed the HotWax facilities for aspects such as 'availability of Security Guards' to ascertain whether the physical access to the HotWax facilities was monitored by the Security Guards for restricting unauthorized access.	None	No exceptions noted.
CA-24	Proximity card-based access control system with anti-pass back system is installed in HotWax Facility.	CC 6.4	Observed the HotWax facility and inspected the proximity card reader configurations for aspects such as 'Anti-pass back enabled' to ascertain whether the proximity card-based access control system with anti-pass back feature was installed in HotWax facility.	None	No exceptions noted.
CA-25	BCP plan defines the roles and responsibilities and identifying the critical information technology application	CC 3.1 CC 3.2 CC 4.2 CC 5.1 CC 5.2	Inspected the Business Continuity Plan for aspects such as 'Prepared and Issued by-MR (ISMS) Operations and 'Contents of Plan' to ascertain whether a	None	No exceptions noted.

#	Control Activity	Trust Services Criteria mapping	Tests Performed	CUEC/ CSOC	Results of Tests
	programs, operating systems, personnel, data files, and periods needed to ensure high availability and system reliability is defined by HotWax.	CC 7.5 CC 9.1 A 1.1 A 1.2 A 1.3	BCP plan defined the roles and responsibilities and identified the critical information technology application programs, operating systems, personnel, data files, and periods needed to ensure high availability and system reliability was defined by the HotWax.	None	No exceptions noted.
CA-26	Upon notification of security incidents via manage engine tool by the HotWax associates, the IT Team follows-up with the relevant departments / individuals for RCA, preventive action and corrective action and the Security incident tickets are resolved as per the procedure mentioned in the 'Security Incident Reporting & Handling Procedure' document.	CC 3.2 CC 4.1 CC 5.3 CC 7.4	Inspected the Security Incident Reporting & Handling Procedure document for aspects such as to ascertain whether upon notification of security incidents via manage engine tool by the HotWax associates, the IT Team follows- up with the relevant departments / individuals for RCA, preventive action and corrective action and the Security incident tickets were resolved as per the procedure mentioned in the 'Security Incident Reporting & Handling Procedure' document.	None	No exceptions noted.

#	Control Activity	Trust Services Criteria mapping	Tests Performed	CUEC/ CSOC	Results of Tests
CA-27	HotWax HR department has established a process to report, track and resolve potential occurrence of breach of Code of Business Conduct and other concerns.	CC 2.2	Inspected the Disciplinary Process for to ascertain whether HotWax HR department had established a process to report, track and resolve potential occurrence of breach of Code of Business Conduct and other concerns.	None	No exceptions noted.
CA-28	HotWax HR department communicates changes to confidentiality commitments through the employee Code of Conduct and Disciplinary Policy and Procedure.	CC 2.2 CC 2.3	Inspected the Disciplinary Policy Process and availability of policy in Intranet portal to ascertain whether HotWax HR department communicated changes to confidentiality commitments through Disciplinary Process.	None	No exceptions noted.
CA-29	On an annual basis, HotWax's IT team performs a risk assessment for HotWax to identify the risk factors considering the changes in the system environment.	CC 2.1 CC 3.1 CC 3.2 CC 3.3 CC 4.1 CC 5.1 CC 5.2 CC 5.3 CC 8.1 CC 9.1	Inspected the Risk Assessment tracker to ascertain whether on an annual basis, HotWax's Corporate Security team performed a risk assessment for HotWax to identify the risk factors considering the changes in the system environment.	None	No exceptions noted.

#	Control Activity	Trust Services Criteria mapping	Tests Performed	CUEC/ CSOC	Results of Tests
CA-31	HotWax's security commitments (including security obligations, terms, conditions, and responsibilities) are documented, along with the responsibilities of external users, in newly onboarded third party contracts and non- disclosure agreements.	CC 2.3 CC 9.2	Inspected the NDA signed by the third parties in a sample MSA for aspects such as 'Third party name', 'Scope of service', 'security obligations', 'responsibilities' to ascertain whether HotWax's security commitments (including security obligations, terms, conditions, and responsibilities) were documented, along with the responsibilities of external users, in newly onboarded third party contracts and non- disclosure agreements.	None	No exceptions noted.
CA-32	On an annual basis, Penetration Testing is conducted by the external vendor.	CC 2.1 CC 3.2 CC 3.3 CC 4.1 CC 5.1 CC 6.1 CC 6.8 CC 7.3 CC 7.4 CC 7.5 CC 8.1	Inspected the Penetration Testing Report. Testing was conducted by the external vendors on HotWax OMS.	None	No exceptions noted.

#	Control Activity	Trust Services Criteria mapping	Tests Performed	CUEC/ CSOC	Results of Tests
CA-34	Firewalls are used in the perimeter of the core network to block traffic unless specifically configured to permit.	CC 5.1 CC 5.2 CC 6.1 CC 6.3 CC 6.6 CC 6.7 CC 6.8	Inspected the network diagram of HotWax for aspects as 'Version Number-V2.0 and 'firewall configuration details' to ascertain whether the firewalls were used in the perimeter of the core network to block traffic unless specifically configured to permit.	None	No exceptions noted.
CA-35	HotWax associates are made aware of their security commitments by means of annual security training and assessment covering security principles awareness, roles and responsibilities, information protection methods and security lapses.	CC 1.4 CC 2.1 CC 2.2 CC 5.3	Inspected the training attendance register aspects such as 'Attendance Details' and 'Completion date' for sample associates to ascertain whether HotWax associates were made aware of their security commitments by means of annual security training and assessment covering security principles awareness, roles and responsibilities, information protection methods and security lapses.	None	No exceptions noted.

#	Control Activity	Trust Services Criteria mapping	Tests Performed	CUEC/ CSOC	Results of Tests
CA-36	HotWax has defined 'Information Security Policy' documented and reviewed by the management. The policy includes the following aspects: Risk Management, Access Controls, Personnel Security, Asset Management, Physical Security, Business Continuity, Information Transfer.	CC 1.3 CC 1.5 CC 2.1 CC 2.2 CC 3.1 CC 3.2 CC 3.3 CC 4.1 CC 5.1 CC 5.3 CC 6.1 CC 6.2 CC 6.6 CC 6.7	Inspected the Information Security Policy for aspects such as 'Prepared and Issued by-MR (ISMS) and 'Contents of Plan' to ascertain whether HotWax had defined 'Information Security Policy' documented and reviewed by the management and the policy included the following aspects: Risk Management, Access Controls, Personnel Security, Asset Management, Physical Security, Business Continuity, Information Transfer.	None	No exceptions noted.
CA-37	HotWax IT Security team has a documented Security Incident Management Procedure for handling security incident and the same is approved by the management.	CC 3.2 CC 3.3 CC 4.1 CC 5.1 CC 5.3 CC 6.2 CC 7.4	Inspected the Security Incident Management Procedure document for aspects as Policy Version – 02' and 'Contents of the Document' to ascertain whether HotWax IT Security team had a documented Security Incident Management Procedure for handling security incident and the same was approved by the management.	None	No exceptions noted.

#	Control Activity	Trust Services Criteria mapping	Tests Performed	CUEC/ CSOC	Results of Tests
CA-38	Physical and Environmental Security Policy is defined and documented by the Physical Security Team and approved by the VP - Physical Security Team.	CC 1.3 CC 1.5 CC 2.1 CC 2.2 CC 3.1 CC 3.2 CC 3.3 CC 4.1 CC 5.1 CC 5.3 CC 6.2 CC 6.6 CC 6.7	Inspected the Physical and Environmental Security Policy document for to ascertain whether physical Security Policy was defined and documented by the Physical Security Team and approved by the VP - Physical Security Team.	None	No exceptions noted.
CA-39	The policies are made available to HotWax associates via email. Security awareness is spread amongst the associates through emails sent by Corporate Announcements.	CC 1.1 CC 2.1 CC 2.2 CC 4.1 CC 5.1 CC 5.2 CC 5.3 CC 6.1 CC 6.6	Inspected a sample email for aspects such as 'associate name', 'availability of security policy in the email for sample associates' in the HotWax to ascertain whether the policies were made available to the HotWax associates through emails. Inspected the email communication for aspects such as ‘subject of Email communication’, ‘sender of email’, ‘recipient of email’ and ‘date of Email communication’ for sample months to ascertain whether Security awareness was spread amongst the associates through emails sent by Corporate Announcements.	None	No exceptions noted.

#	Control Activity	Trust Services Criteria mapping	Tests Performed	CUEC/ CSOC	Results of Tests
CA-40	An annual performance evaluation process is in place covering KPI's, values, behavior, training needs and career aspiration.	CC 1.4 CC 4.1	Inspected the annual performance evaluation document for a few sample employees to ascertain whether an annual performance evaluation process was in place covering KPI's, values, behavior, training needs and carrier aspiration.	None	No exceptions noted.
CA-41	HotWax has defined job descriptions specifying the responsibilities and academic and professional requirements for key job positions which is reviewed by the management on need basis.	CC 1.3 CC 1.4 CC 1.5 CC 2.3	Inspected the job detail overview and role to ascertain whether HotWax had defined job descriptions specifying the responsibilities and academic and professional requirements for key job positions which was reviewed by Team Lead on needed basis.	None	No exceptions noted.
CA-42	HotWax maintains clearly defined personnel structures with appropriate reporting lines and oversight roles.	CC 1.3	Inspected the Organization Chart ascertain whether HotWax maintained clearly defined personnel structures with appropriate reporting lines and oversight roles.	None	No exceptions noted.
CA-43	HotWax's security commitments to associates and required security obligations are communicated to the associates during the induction program.	CC 2.2	Inquired with the HR Manager to determine that HotWax's security commitments to associates and required security obligations are communicated to the associates during the induction program.	None	No exceptions noted.
CA-44	For campus hires and lateral hires, background verification is carried out by the Third-Party Service Provider, and the results are reviewed by HR.	CC 1.1 CC 1.4	Not applicable as HotWax does not performs the background checks on their employees.	None	Not applicable.

#	Control Activity	Trust Services Criteria mapping	Tests Performed	CUEC/ CSOC	Results of Tests
CA-45	HR Policies are in place to determine that violations of Code of Conduct, Non-Disclosure agreement and other confidential matters are subject to disciplinary action and sanctions based on investigation performed in timely manner.	CC 1.1 CC 1.5	Inspected various HR policies for aspects such as 'prepared by', 'reviewed by', 'approved by', 'version history' and 'contents of the document' to ascertain whether HR Policies were in place to determine that violations of Code of Conduct, Non-Disclosure agreement and other confidential matters were subject to disciplinary action and sanctions based on investigation performed in timely manner.	None	No exceptions noted.
CA-46	HotWax associates are required to sign the 'NDA' document which includes clauses for maintaining confidentiality of information obtained, intellectual property rights of HotWax, termination of employment on breach of NDA amongst others on or before the day of joining.	CC 1.1 CC 1.4 CC 1.5 CC 2.1 CC 2.2 CC 3.3 CC 5.3 CC 6.6	Inspected the NDA for aspects such as 'Contents of NDA', 'associate name', 'Date of Joining HotWax', 'signature details' and 'date of signature' for sample on boarded associates to ascertain whether HotWax associates were required to sign the 'NDA' document which included clauses for maintaining confidentiality of information obtained, intellectual property rights of HotWax, termination of employment on breach of NDA amongst others on or before the day of joining.	None	No exceptions noted.
CA-47	The process for informing HotWax IT Team about possible security breaches and other incidents and escalation of the same is and is also intimated as part of the induction program.	CC 7.3 CC 7.4 CC 7.5	Inspected the 'Security Incident Management Procedure' document for aspects as Policy Version – 02' and 'Contents of the Document' to ascertain whether the process for informing the HotWax Helpdesk Team about possible security breaches and other incidents and escalation of the same was shared via email.	None	No exceptions noted.

CA-49	User IDs of resigned / terminated HotWax associates on HotWax Domain Controller are revoked from LTab based on the request raised by the HR team, within one working day from the Associate's LWD.	CC 5.2 CC 6.1 CC 6.2 CC 6.3 CC 6.5 CC 6.6	Inspected Email communication and LTab for aspects such as 'Email Sent by', 'Email sent on', 'Associate ID', 'Associate Name', 'Date of revocation' and 'last working date in HotWax' for sample off-boarded associate to ascertain whether the user IDs of resigned/ terminated HotWax associates on HotWax Domain Controller were revoked from the LTab based on the request raised by the HR Team, within one working day from the Associate's LWD.	None	No exceptions noted.
CA-50	Access to the internet is restricted by the IT team for HotWax associates through the content filter. Access to websites other than the sites configured in the content filter is provided by the IT Security team.	CC 5.2 CC 6.1 CC 6.2 CC 6.3 CC 6.6 CC 6.7 CC 6.8	Inspected the configuration settings in Firewall including blocked and permitted websites details to ascertain whether access to internet was restricted by the IT Team for HotWax associates.	None	No exceptions noted.
CA-51	Acquisition and Implementation of new IT Systems are performed as per the change management procedure.	CC 8.1	Inspected the 'Change Management Procedure' document for aspects as Policy Version-V3 and 'Table of Contents of the procedure document' to ascertain whether Acquisition and Implementation of new IT Systems were performed.	None	No exceptions noted.

#	Control Activity	Trust Services Criteria mapping	Tests Performed	CUEC/ CSOC	Results of Tests
CA-52	Diesel generators, AC and Fire Extinguisher are installed for protection against environmental hazards such as fire, power, excessive heat, and humidity.	CC 6.4 CC 7.2	Observed HotWax facilities during site walkthrough to ascertain whether diesel generators, AC and Fire Extinguisher are installed for protection against environmental hazards such as fire, power, excessive heat, and humidity.	None	No exceptions noted
CA-53	Antivirus server is configured to update last released definition file from antivirus vendor.	CC 4.1 CC 5.1 CC 5.2 CC 6.6 CC 6.8 CC 7.1 CC 7.2	Inspected the antivirus configuration in Sentinel One for aspects such as 'Push configuration', 'Pull configuration' and 'Antivirus version number' to ascertain whether Antivirus server was configured to update last released definition file from antivirus vendor.	None	No exceptions noted.
CA-54	Backup file copied are stored in an alternate location on periodic basis.	A 1.2	Inspected the backup tool configuration (AWS) for aspects such as 'backup settings configured', 'backup frequency', 'location' and backup logs for sample dates for aspects such as 'Back up location' and 'Back up Result' to ascertain whether backup file copied were stored in an alternate location on periodic basis	None	No exceptions noted.
CA-55	CD-ROM drives and USBs are disabled on the workstations by default and access is granted by the IT team based on the exception request raised in the manage engine tool that is approved by the respective Department Head.	CC 5.2 CC 6.1 CC 6.3 CC 6.6 CC 6.7 CC 6.8 CC 7.2 C 1.1	Not applicable. HotWax does not disable CD-ROM drives and USBs as they work on Opensource (OFBIZ).	None	Not applicable.

#	Control Activity	Trust Services Criteria mapping	Tests Performed	CUEC/ CSOC	Results of Tests
CA-56	HotWax has defined a 'Media Disposal Procedure' that includes the following matters: • Disposal Guidelines for Electronic-Based Media • Disposal Guidelines for Paper- Based Media	CC 6.2 CC 6.5 CC 6.7	Inspected the Media Disposal Procedure document for aspects as Policy Version V-2.0. HotWax has the internal practice to dispose of their data.	None	No exceptions noted.
CA-57	Domain User's password policies, account lockout policies and screensaver time-out settings are defined and enforced through HotWax Domain Controller.	CC 6.1 CC 6.2 CC 6.3 CC 6.6 CC 6.7	Inspected the Password policy document for aspects as Policy Version-V3 and 'Table of Contents of the procedure document' to ascertain whether the Domain User's password policies, account lockout policies and Screen saver time-out settings were defined.	None	No exceptions noted.
CA-58	Emergency changes to HotWax Information System are logged using the manage engine tool and resolved as per the change management procedure.	CC 8.1	Inquired with the IT Manager to ascertain that the emergency changes to HotWax Information System are logged using the manage engine tool and resolved as per the change management procedure.	None	No exceptions noted.
CA-59	Network device is in place (Firewall) for protecting HotWax network from unauthorized access.	CC 5.2 CC 6.1 CC 6.2 CC 6.6 CC 6.7 CC 6.8 CC 7.2	Inspected the configuration settings of the Firewall to ascertain whether network device is in place (Firewall) for protecting HotWax network from unauthorized access.	None	No exceptions noted.

#	Control Activity	Trust Services Criteria mapping	Tests Performed	CUEC / CSOC	Results of Tests
CA-60	Network diagram detailing the network devices such as firewalls and switches to prevent unauthorized access is maintained for each location by the IT Team and is approved by the IT Head.	CC 5.2 CC 6.1 CC 6.3 CC 6.6 CC 6.8	Inspected the network diagram for aspects as 'Version Number-V2.0 and 'firewall configuration details' to ascertain whether Network diagram detailing the network devices such as firewalls and switches to prevent unauthorized access was maintained for each location by the IT Team and was approved by the IT Head.	None	No exceptions noted.
CA-61	On weekly basis, Patches and version upgrades are implemented in workstations through Antivirus by Infrastructure team.	CC 2.1 CC 2.2 CC 4.1 CC 4.2 CC 5.1 CC 5.2 CC 6.1 CC 6.8 CC 8.1	Inspected the Patch configuration of AWS to ascertain whether patches and version upgrades were implemented in workstations through AWS by Infrastructure team.	None	No exceptions noted.
CA-62	System change requests are evaluated to determine the potential effect of the change on security, availability, processing integrity, and system requirements as part of the change management process.	C 1.1	Inspected the sample system change requests in JIRA tool (ClickUp) to ascertain whether system change requests were evaluated to determine the potential effect of the change on security, availability, processing integrity, and system requirements as part of the change management process.	None	No exceptions noted.
CA-63	Access control mechanism is configured over the network devices such as firewall.	CC 5.1 CC 6.1 CC 6.2 CC 6.6 CC 6.8 CC 7.1 CC 7.2	Inspected the firewall configurations to ascertain whether Access control mechanism was configured over the network devices such as firewall.	None	No exceptions noted.

#	Control Activity	Trust Services Criteria mapping	Tests Performed	CUEC / CSOC	Results of Tests
CA-64	The IT Team informs the associate about changes that may affect system security by means of an Email alert.	CC 2.2	Inspected the email communication sent for aspects such as 'Date of Email', 'Email sent by', 'Email addressed to' and 'Contents of the Email' for sample alerts to ascertain whether the IT Team informed the associate about changes that may affect system security by means of an email alert.	None	No exceptions noted.
CA-65	The IT team monitors the antivirus server console to check whether workstations are updated with the latest released definition.	CC 4.1 CC 4.2 CC 5.1 CC 5.2 CC 6.8 CC 7.1 CC 7.2 CC 7.3 CC 8.1	Inspected from the Sentinel One Antivirus configurations for aspects such as 'AV Version Number', 'Pull configuration', 'Push Configuration', 'scheduling of PULL' and scheduling of PUSH' and inspected the Sentinel One Endpoint Security Tool Antivirus Version to ascertain whether workstations were updated with latest released definition.	None	No exceptions noted.
CA-66	On an annual basis, Fire safety drill is conducted by the Emergency Rescue Team at HotWax facility.	CC 6.4 CC 7.2 A 1.2	Not applicable as HotWax conducts the fire safety drill on a need basis. Last fire drill was conducted in 2018.	None	Not applicable.
CA-67	HotWax enters into agreements with third party vendors covering the scope of services and confidentiality clauses.	CC 3.1 CC 9.2	Inspected the Master Service Agreement (MSA) for aspects such as 'agreement date', 'signature details of HotWax and vendor', 'date of signature of HotWax and vendor', 'scope of service', 'agreement period', 'confidentiality clause' and	None	No exceptions noted.

#	Control Activity	Trust Services Criteria mapping	Tests Performed	CUEC / CSOC	Results of Tests
			and 'availability and security clause' to ascertain whether HotWax enters into agreements with third party vendors covering the scope of services and confidentiality clauses and the vendor agreements, included any security, availability, and confidentiality commitments, were reviewed by HotWax management during the procurement process.		
CA-68	Master Service Agreements (MSAs) between HotWax and vendors are incorporated to include: • Scope of business relationship and services offered • Information security requirements • Timely notification of a security incident to customers • Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification)	CC 2.3 CC 9.2	Inspected the MSA entered by HotWax with third party vendors for aspects such as 'Third party vendor', 'agreement date', 'signatory details of HotWax', 'signatory details of the vendor', 'contents of the agreement', 'agreement period', 'extensions, if any', to ascertain whether Master Service Agreements (MSA's) between HotWax and vendors were incorporated to include: • Scope of business relationship and services offered • Information security requirements • Timely notification of a security incident to customers • Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification)	None	No exceptions noted

#	Control Activity	Trust Services Criteria mapping	Tests Performed	CUEC / CSOC	Results of Tests
	• Expiration of the business relationship and treatment of customer data impacted		• Expiration of the business relationship and treatment of customer data impacted and 'availability and security clause' to ascertain whether HotWax enters into agreements with third party vendors covering the scope of services and confidentiality clauses and the vendor agreements, included any security, availability, and confidentiality commitments, were reviewed by HotWax management during the procurement process.	None	No exceptions noted
CA-69	Third Party Service providers sign a Non-Disclosure Agreement with HotWax before commencement of services.	CC 1.1 CC 9.2	Inspected NDA signed by third-party service providers in a sample MSA for aspects such as 'availability of NDA', 'signed by', 'signed on' and 'contents of the document' to ascertain whether the Third-Party Service providers signed a Non- Disclosure Agreement with HotWax before commencement of services.	None	No exceptions noted
CA-70	The MSA with the Client contain clauses relating to confidentiality with respect to the services performed.	CC 2.3	Inspected the Master Service Agreement for aspects such as 'scope of services', 'date of effectiveness of MSA', 'validity of agreement', 'confidentiality clause', 'sign-off details of the clients' and 'sign-off details of HotWax' to ascertain whether the MSA with the client contained clauses relating to confidentiality with respect to the services performed.	None	No exceptions noted

End of The Report