

Proprietary & Confidential



Abacus & Emburse Spend System

SOC 2

Report on Emburse, Inc.'s

System and Organization Controls

Relevant to Security, Availability, and Confidentiality



Integrated SOC 2 Type 2 Report Prepared in Accordance with the AICPA Attestation Standards and IAASB ISAE No. 3000 (Revised) Standards

JANUARY 1, 2022 TO SEPTEMBER 30, 2022



Table of Contents

	Independent Service Auditor's Report								
I.	Em	nburse, Inc	:.'s Assertion	5					
II.	En	Emburse, Inc.'s Description of Its Abacus & Emburse Spend System							
	A.	Services Pr	rovided	6					
	B.	Principal So	ervice Commitments and System Requirements	7					
	C.	Componen	ts of the System Used to Provide the Services	8					
		1. Infrastru	ucture	8					
		2. Softwar	e	8					
		3. People		9					
		4. Data		10					
		5. Process	ses and Procedures	10					
	D.		spects of the Control Environment, Risk Assessment Process, and Communication, and Monitoring	11					
		1. Control	Environment	11					
		2. Risk As	sessment Process	18					
		0.	tion and Communication	18					
		4. Monitor	ing Controls	19					
	E.	Trust Servi	ces Categories, Criteria, and Related Controls	20					
	F.	Compleme	ntary Subservice Organization Controls	20					
	G.	Complemen	ntary User Entity Controls	21					
۷.		ust Service ntrols	Services Categories, Criteria, Related Controls, and Tests of rols						
	A.	Applicable	Trust Services Criteria	24					
		Common Criteria							
		CC1.0	Common Criteria Related to Control Environment	24					
			Common Criteria Related to Communication and Information	27					
			Common Criteria Related to Risk Assessment	30					
			Common Criteria Related to Monitoring Activities	33					
			Common Criteria Related to Control Activities Common Criteria Related to Logical and Physical Access Controls	35 39					
			Common Criteria Related to System Operations	43					
			Common Criteria Related to Change Management	49					
			Common Criteria Related to Risk Mitigation	50					
		Availability		51					
		Confidential	ity	52					
	B.	Description	n of Test of Controls and Results	53					
٧.			ation Provided by Emburse That Is Not Covered by the						
	Se A.		tor's Report nt's Response to Identified Testing Exceptions	82 82					
	Α.	Manageme	in a response to identified resulty Exceptions	02					



I. Independent Service Auditor's Report

Emburse, Inc. 320 Cumberland Avenue Portland, ME 04101

To the Management of Emburse, Inc.:

Scope

We have examined Emburse, Inc.'s (Emburse) accompanying description of its system in Section III titled "Emburse, Inc.'s Description of Its Abacus & Emburse Spend System" throughout the period January 1, 2022 to September 30, 2022 (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 January 1, 2022 to September 30, 2022, to provide reasonable assurance that Emburse's service commitments and system requirements were achieved based on the trust services criteria for Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

The information included in Section V titled "Other Information Provided by Emburse That Is Not Covered by the Service Auditor's Report" is presented by Emburse management to provide additional information and is not a part of Emburse's description. Information about Emburse's management responses to identified testing exceptions has not been subjected to the procedures applied in the examination of the description and of the suitability of the design and operating effectiveness of the controls to achieve Emburse's service commitments and system requirements based on the applicable trust services criteria, and accordingly, we express no opinion on it.

Emburse uses Amazon Web Services for cloud hosting services (subservice organization). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Emburse, to achieve Emburse's service commitments and system requirements based on the applicable trust services criteria. The description presents Emburse's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Emburse's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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



Service Organization's Responsibilities

Emburse is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Emburse's service commitments and system requirements were achieved. Emburse has provided the accompanying assertion in Section II titled "Emburse, Inc.'s Assertion" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Emburse is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of the 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 in accordance with International Standard on Assurance Engagements (ISAE) 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board (IAASB). 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 Emburse'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 the 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 the 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
- Evaluating the overall presentation of the description

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



Service Auditor's Independence and Quality Control

We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

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 Tests of Controls

The specific controls we tested and the nature, timing, and results of our tests are listed in Section IV of this report titled "Trust Services Categories, Criteria, Related Controls, and Tests of Controls."

Opinion

In our opinion, in all material respects:

- the description presents Emburse's Abacus & Emburse Spend System that was designed and implemented throughout the period January 1, 2022 to September 30, 2022, in accordance with the description criteria.
- the controls stated in the description were suitably designed throughout the period January 1, 2022 to September 30, 2022 to provide reasonable assurance that Emburse's service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Emburse's controls throughout that period.
- the controls stated in the description operated effectively throughout the period January 1, 2022 to September 30, 2022 to provide reasonable assurance that Emburse'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 Emburse's controls operated effectively throughout that period.



Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of Emburse, user entities of Emburse's Abacus & Emburse Spend System during some or all of the period January 1, 2022 to September 30, 2022, business partners of Emburse subject to risks arising from interactions with the Abacus & Emburse Spend System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, 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 complementary subservice organization 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
- 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.

Moss ADAMS LLP

San Francisco, California December 22, 2022





II. Emburse, Inc.'s Assertion

We have prepared the accompanying description of Emburse, Inc.'s (Emburse) Abacus & Emburse Spend System in Section III titled "Emburse, Inc.'s Description of Its Abacus & Emburse Spend System" throughout the period January 1, 2022 to September 30, 2022 (description) based on the criteria for a description of a service organization's system in DC Section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria) (description criteria). The description is intended to provide report users with information about the Abacus & Emburse Spend System that may be useful when assessing the risks arising from interactions with Emburse's Abacus & Emburse Spend System, particularly information about system controls that Emburse 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, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

Emburse uses Amazon Web Services for cloud hosting services (subservice organization). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Emburse, to achieve Emburse's service commitments and system requirements based on the applicable trust services criteria. The description presents Emburse's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Emburse'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 Emburse, to achieve Emburse's service commitments and system requirements based on the applicable trust services criteria. The description presents Emburse's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Emburse's controls.

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

- the description presents Emburse's Abacus & Emburse Spend System that was designed and implemented throughout the period January 1, 2022 to September 30, 2022, in accordance with the description criteria.
- the controls stated in the description were suitably designed throughout the period January 1, 2022 to September 30, 2022 to provide reasonable assurance that the Emburse service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively throughout the period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Emburse's controls throughout that period.
- the controls stated in the description operated effectively throughout the period January 1, 2022 to September 30, 2022 to provide reasonable assurance that Emburse'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 Emburse's controls operated effectively throughout that period.



III. Emburse, Inc.'s Description of Its Abacus & Emburse Spend System

A. Services Provided

COMPANY OVERVIEW

Abacus Labs, Inc. (Abacus) and Emburse Spend (collectively the Company) are wholly-owned subsidiaries of Emburse, Inc. (Emburse). Emburse is a modern spend management company that revolutionizes the way organizations manage expenses, process invoices, and make payments. Emburse's offerings are tailored to meet the unique business needs of specific industries and company sizes are trusted by nine million users in 120 countries.

OVERVIEW OF THE ABACUS & EMBURSE SPEND SYSTEM

The Abacus & Emburse Spend Systems are cloud software as a service (SaaS) applications designed for automated expense creation, custom approval workflows, expense policy controls, employee reimbursements, and continuous accounting synchronization. The Abacus & Emburse Spend subscription software service allows employees to submit expenses by recording receipts at the time of transaction. Once approved, Abacus & Emburse Spend sends reimbursement directly to the employee's bank account. Managers can review and approve expenses from a mobile device or a computer at the office.

Key features include:

- Replacing expense reporting with real time expense system
- Integrating direct deposit for fast reimbursement
- Setting multilevel expense approvals
- Creating and setting rules for the organization's expense policy
- Tracking and managing expenses with real time reporting
- Synchronizing with accounting software for quick reconciliation
- Tracking, managing, and reconciling corporate credit cards

The software offers direct finance and account integration with QuickBooks, Desktop, Xero, NetSuite, and Intacct accounting software to manage online finance and accounting solutions for expense reimbursement. Businesses can also export a comma separated value (CSV) file to import to any accounting platform.

The software syncs with the accounting system each night. Once the chart of accounts is set up within the software, the application reconciles transactions automatically. The same is true for reconciling corporate credit cards. The software pulls transactions from many banks, including Chase, Bank of America, and American Express.

Customers can invite collaborators from inside and outside of the corporate structure, such as bookkeepers and accountants. The software creates a full audit trail by tracking each update to every expense. The software can manage Internal Revenue Service compliance for seven-year receipt keeping. In addition, all data is fully portable through either CSV or Portable Document Format (PDF).



Employees and managers sign up, download the account, and enter their corporate and personal bank accounts and credit cards. Individuals enter expenses in real time, take a photo of a receipt, select the merchant, and add notes. Emburse also suggests nearby merchants to save employee time and automatically categorizes the expense based on the merchant.

Customers can customize the software by forming groups, setting multiple approval levels, and assigning managerial roles. Customers can organize in more depth with custom categories, tags, and expense rules, and control cash flow using the application to:

- Set rules for expense policies
- Create custom reports with deep search and apply bulk actions
- Set payments not to start until they are fully approved
- Track all debits and credits

Abacus & Emburse Spend serve U.S. businesses through synchronization with any number of U.S. banks. They also provide services for organizations whose employees live and work abroad. For these customers, overseas employees can be set up for payments in other currencies.

SCOPE OF THE DESCRIPTION

This description of the Abacus & Emburse Spend System addresses only Abacus & Emburse Spend's cloud SaaS applications provided to its user entities and excludes other services provided by Emburse. The description does not include other Emburse or third-party service offerings which may access or provide functionality to the Abacus & Emburse Spend System through secure application programming interfaces (APIs).

B. Principal Service Commitments and System Requirements

Emburse designs its process and procedures to meet its objectives for its Abacus & Emburse Spend System. Those objectives are based on the service commitments that Emburse makes to user entities, the laws and regulations that govern the provision of the Abacus & Emburse Spend System, and the operational and compliance requirements that Emburse has established for the services. Abacus & Emburse Spend System is subject to the security and privacy requirements of the Payment Card Industry Data Security Standard (PCI DSS), as well as the privacy security laws and regulations in the jurisdictions in which Emburse operates.

Security, availability, and confidentiality commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements as in the description of the service offering provided online. Security, availability, and confidentiality commitments are standardized and include, but are not limited to, the following:

Security principles with the fundamental designs of the Abacus & Emburse Spend System are
designed to permit system users to access the information they need based on their roles in the
system while restricting them from accessing information not needed for their roles.



- Use of encryption technologies to protect customer data both at rest and in transit.
- Maintaining a business continuity plan that includes a recovery strategy, recovery procedures, client notification procedures, and a commitment to test the business continuity plan as often as required to reasonably prepare for a successful recovery in the time allotted in the event an actual recovery is required.

Emburse establishes operations requirements that support the achievement of security, availability, and confidentiality commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated via Abacus & Emburse Spend's System policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the System.

C. Components of the System Used to Provide the Services

1. Infrastructure

HARDWARE

Abacus & Emburse Spend uses the following major equipment components:

- AWS Elastic Compute Cloud (EC2) Servers running Ubuntu Linux
- Firewall: Web Application Firewall (WAF)
- Intrusion Detection: Threat Stack
- Storage: Amazon Elastic Block Store (EBS) and Simple Storage Service (S3) Storage

2. Software

The significant application programs and IT system software that support application programs (e.g., operating systems, middleware, and utilities) include:

Software and Systems	Description
Systems/Network Monitoring	All computing systems, including server, networking, security, application, and database platforms, are monitored through Threat Stack, Instana, Logz.io, and other technical methods.
Ticketing and Workflow Management	Service desk ticketing and workflow management, including software development lifecycle (SDLC), are managed through GitHub, Zendesk and Jira.
Project Management	Abacus & Emburse Spend uses a cloud version of GitHub and Jira to plan, track, and manage its core application-related software development activities.



Software and Systems	Description
Vulnerability Management	Abacus & Emburse Spend uses Tenable (Nessus) to perform internal vulnerability scans. For external application scanning, Abacus & Emburse Spend uses a third-party service.
AWS Identity Access Manager (IAM)	Abacus & Emburse Spend's administrator team uses AWS's IAM product to configure and administer the group policies for Abacus & Emburse Spend users. The administrator team uses IAM tools to manage user memberships and all other entitlements across the Company. These tools allow the creation, deletion, and specific entitlement designation of individual users and groups.
Multi-Factor Authentication	Abacus & Emburse Spend uses Okta to facilitate multi-factor authentication for accounts accessing privileged information sensitive information.
Backup Tools	Abacus & Emburse Spend uses AWS cloud snapshots as a method to backup all server infrastructure.
Building and Office Access	Abacus & Emburse Spend uses smart readers to restrict physical access to the Emburse offices.
Database Administration	Abacus & Emburse Spend use RDS command line tools for database management.
Logging	Abacus & Emburse Spend uses Logz.io to collect application logs from all production systems.

3. People

Emburse is organized in the following functional areas:

- Accounting and Finance Responsible for the oversight of accounting and finance activities.
- Human Resources (HR) Responsible for acquiring, developing, and retaining staff and oversight for Company-provided benefits.
- Product Management Responsible for defining product features, system integrations, and compliance.
- Sales and Marketing Responsible for the generation of revenue from sales activities, marketing, marketing automation, professional services, and major accounts management.
- System Operations Responsible for server and network configurations and responsible for performance monitoring and the enforcement of hardening standards.
- Engineering Responsible for defining software development processes and assuring that they are being observed.
- *Testing/QA Personnel* Responsible for the development, maintenance, and testing of the software, production operations, and customer support.



4. Data

Emburse provides controls at each level of data storage, access, and transfer. Emburse has established training programs for privacy and information security to support data confidentiality. All employees are required to complete these training programs annually. All product feature launches that include new collection, processing, or sharing of user data are required to go through an internal design review process. Emburse has also established incident response processes to report and handle events related to confidentiality. Emburse establishes agreements, including non-disclosure agreements, for preserving confidentiality of information and software exchange with external parties.

At AWS, when a storage device has reached the end of its useful life, these procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. All decommissioned hardware is sanitized and physically destroyed in accordance with industry-standard practices.

5. Processes and Procedures

Emburse has developed the following policies, standards, and procedures to guide activities undertaken by personnel responsible for operating the platform:

- Information Security Policy
- Security Awareness Guideline
- **Network Security Policy**
- **Business Continuity Plan**
- Information Security Disaster Recovery Plan
- Security Incident Response Plan
- Third Party Risk Management Policy
- Change Control procedure
- Secure Application Development Policy
- **New Hire and Termination Procedures**



D. Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring

1. Control Environment

The control environment begins at the highest level of Emburse. Executive and senior management play important roles in Emburse's tone from the top, and their direct leadership is an integral part of the integrity and ethics, which are part of the corporate culture. The control environment is embodied by the organization's awareness of the need for controls and the emphasis given to the appropriate controls through management's actions supported by its policies, procedures, and organizational structure. The management team is responsible for setting the strategic direction of the Company. The management team meets regularly to monitor Company progress. Additionally, Emburse has established an Information Security Committee to oversee data security-related issues.

ORGANIZATION

Management has the primary responsibility to develop, maintain, and document adequate internal and compliance controls, and provides oversight to Emburse's operations. A documented management organizational structure exists that depicts levels of reporting and accountability. Management is responsible for directing and controlling the Company's operations, including establishment and communication of Company policies and procedures.

The key individuals responsible for the daily operations include the following positions:

- Chief Technology Officer (CTO)
- Vice President (VP) of Engineering
- Chief Product Officer
- Chief Information Security Officer (CISO)
- Vice President (VP), Systems Operations
- Chief Operating Officer (COO)

The following operational positions report to the Chief Executive Officer (CEO) or CTO:

- CTO Responsibilities include setting the direction for the technical architecture, coding standards, and scalability of the system. The CTO is also responsible for information security for production operations.
- VP of Engineering Directs the activities of software development. This individual is responsible for defining software development processes and assuring that they are being observed. Oversees product development efforts.
- CISO Responsible for Emburse's compliance efforts, manages the annual Risk Assessment process, and develops and enforces the information security policy.
- VP of Operations Oversees the server and network configurations and is responsible for performance monitoring and the enforcement of hardening standards.



PERSONNEL PRACTICES

Personnel policies and procedures are documented in the Emburse Employee Handbook and communicated to employees. Employee job descriptions include position summaries and describe major duties and responsibilities. They are developed by the department managers as part of the recruiting process. Human Resources (HR) reviews job descriptions on a periodic basis and updates them as the operational needs of the Company change.

NEW EMPLOYEE ONBOARDING PROCESS

Emburse performs employment background screening for employee candidates through a thirdparty service. Background checks are performed on prospective employees, and the results are provided to administrative support personnel. The administrative support personnel review the results of the background check and will not extend an offer to or will rescind an offer from employee candidates who have committed a felony. Reference checks are performed in most cases, but may not be necessary in certain circumstances, such as when the candidate has worked with Emburse employees in the past. Results of background checks are noted on the new hire checklist.

Management establishes skills through continued training of its security, availability, and confidentiality commitments. Employees are required to attend annual IT Security Awareness trainings that cover Emburse's security awareness policy, users' incident reporting responsibilities, as well as confidentiality topics such as critical information classification. Management monitors compliance to confirm employees have met their training requirements. Management also performs ongoing social engineering exercises by sending a phishing email. All employees or contractors who click on or respond to the phishing email are required to complete a phishing remedial training.

The employee signs an Employee Invention Assignment and Confidentiality Agreement, which is retained on file. Additionally, contractors sign a standard agreement that contains a Confidentiality Agreement and Intellectual Property Assignment Agreement.

Emburse maintains multiple levels of system access based upon employee roles and responsibilities. System access is approved by an employee's manager and reflects organizational structure.

Employees are cross-trained, where practical, to allow sufficient backup in the event of unexpected illness, termination, resignation, or promotion.

TERMINATION PROCESS

Employee profiles and access rights are deactivated or disabled from the system within 24 business hours. A termination checklist is completed by HR to verify that Emburse's assets are collected from the terminated employee and a help desk ticket is created to initiate access removal from Emburse's systems. Access lists are reviewed at least guarterly to ensure that only current employees are in the active user lists.



SEGREGATION OF DUTIES

Duties are segregated among Abacus & Emburse Spend functional areas.

SUPPORT TEAM

- Are organizationally independent of other Abacus & Emburse Spend functional areas.
- Do not have implementation duties; however, they may from time to time assist the configuration team with changes to rules, templates, and scripts.
- The support team includes a production support engineer. That role has responsibility for both engineering and support tasks and has special access to both functions.
- Do not have development responsibilities.
- Do not have administrative duties.

IMPLEMENTATION PERSONNEL

- Are organizationally independent of other Abacus & Emburse Spend functional areas.
- Do not have development responsibilities.
- Do not have duties as support and quality assurance (QA) personnel.
- Do not have administrative duties.
- Do not have access to production source code. However, the rules, scripts, and templates that they develop are stored in the source control systems.

ENGINEERING PERSONNEL

- Are organizationally independent of other Abacus & Emburse Spend functional areas.
- Do not have implementation duties, although they may assist implementation when special skills are required.
- Do not have administrative duties.
- Do not have duties as support personnel but may be called on from time to time to assist in troubleshooting activities.

SYSTEMS ADMINISTRATORS

- Are organizationally independent of other Abacus & Emburse Spend functional areas.
- Do not have implementation duties, although they may assist implementation when special skills are required.
- Do not have administrative duties.

ADMINISTRATIVE PERSONNEL

- Are organizationally independent of other Abacus & Emburse Spend functional areas.
- Do not have implementation duties.
- Do not have duties as support and QA personnel.
- Do not have development responsibilities.
- Do not have access to production source code.



SECURITY MANAGEMENT

Emburse has a dedicated Information Security team responsible for management of Information Security throughout the organization. The Information Security team holds positions on the Information Security Committee and maintains security credentials. They are further responsible for developing, maintaining, and enforcing the Company's information security policies. The Information Security Policy is reviewed annually by the CISO, the legal department, and Policy Review Board and is approved by the Information Security Committee.

To maintain system security, the Information Security team monitors known incidents, available patches, and vulnerability assessment testing results to ensure timely resolution and to reflect any necessary policies and procedures changes. Such changes can include a reclassification of data, a reassessment of risk, a change in incident response plans, and modification of the technical standards.

SECURITY POLICIES

Emburse has developed policies, standards, and procedures to guide activities undertaken by personnel responsible for operating the platform. All employees are required to annually sign and acknowledge their review of the Company's information security policies.

SERVER AND NETWORK INFRASTRUCTURE

Abacus & Emburse Spend implements high availability and redundant solutions wherever possible, leveraging appropriate Amazon AWS technologies. Abacus & Emburse Spend maintains a network diagram depicting the production infrastructure.

All external points of connectivity utilize best practice hardening and configuration.

HELP DESK SYSTEM

Abacus & Emburse Spend maintains a help desk system, Zendesk, to monitor and track potential customer problems. Zendesk ticketing system is used to review, prioritize, and respond to problems. Customer and operational issues are identified, responded to within a period of two business days, and documented within a help desk ticket.

VULNERABILITY ASSESSMENTS AND PENETRATION TESTING

Emburse performs weekly internal vulnerability scans and weekly external vulnerability scans on the production network. The vulnerability scans identify security risks that may affect the application, firewall, and operating system configurations.

Emburse contracts a third-party vendor to perform annual penetration testing on the production network. Penetration testing is used to identify higher-risk vulnerabilities that may be difficult to detect with automated network or application vulnerability scanning software. Both the vulnerability scans and the penetration testing are reviewed by the CISO and remediated if needed.

BACKUP AND FAILOVER OPERATIONS

Critical data in the core Abacus & Emburse Spend Systems is replicated between independent data centers in the appropriate region.



BUSINESS CONTINUITY AND DISASTER RECOVERY

Emburse maintains a detailed business continuity plan to help the Company prepare for and respond to disruptive events. On an annual basis the Information Security team conducts annual simulation scenarios to test the effectiveness of the plan. The Information Security team reassesses the business continuity plan and updates as needed based on the results.

Critical systems are backed up to the cloud, protecting the data from localized incidents and disasters. All backups are then mirrored in separate AWS availability zones. The entire backup and recovery process is fully tested annually.

INCIDENT MANAGEMENT

Emburse has established and regularly tests its Incident Response procedures. Operations personnel follow defined protocols for evaluating reported events. Security-related events are assigned to the security group for evaluation. Operations and security personnel follow defined protocols for resolving and escalating reported events. Customer and operational issues are identified, are responded to within a period of two business days, and documented within a help desk ticket. On a monthly basis, the Information Security Committee convenes to discuss Emburse's security profile and discuss security events and threats (e.g., incidents or problems).

DATA TRANSMISSIONS

Emburse uses industry standard encryption techniques to protect user authentication information and the corresponding communication session transmitted over the internet or other public networks. Transmission-level Secure Sockets Layer (SSL) security is implemented when information is being transmitted over public networks.

Clients using the web-based products connect to the web servers using secure hypertext transport (HTTPS). HTTPS assures that all client data is transmitted using SSL (TLS 1.2) that generates a 256-bit certificate using a 2048-bit key. Abacus & Emburse Spend maintains Secure Server ID Certificates from a recognized certification authority on the servers that web-product clients access.

ENCRYPTION

Emburse uses Amazon RDS encryption services to encrypt the Amazon RDS database instances. Data that is encrypted at rest includes the underlying storage for database instances, and its automated backups, read replicas, and snapshots. Emburse's Amazon RDS encrypted database instances use the industry standard AES-256 encryption algorithm.

ACCESS

OVERVIEW

Security policies and procedures have been documented and communicated to Emburse employees. Emburse uses Light Directory Access Protocol (LDAP) services to enforce password and role-based security for users that log into the production systems. Company systems are segregated into multiple domains to provide for the logical separation between sensitive customer data and Company data.



Separate subnets are maintained for internal systems (including development and staging) and the production systems that support customer data. The networks and subnets are physically separated by network devices, including firewalls to separate the non-production systems from the Abacus & Emburse Spend production systems. AWS security groups are in place to segregate the Web front end, application layer, and database layer as an additional defensive measure.

PASSWORD POLICY

The Emburse user-level password policy includes the following requirements:

- Passwords are at least 16 characters in length.
- Passwords are changed every 12 months.
- Passwords contain complexity elements (i.e., uppercase characters, lowercase characters, numbers, special characters).

Access by Emburse employees is permitted only through multi-factor authentication (MFA).

LOGICAL ACCESS

Logical access to the Abacus & Emburse Spend application database and stored procedures within the production environment is granted solely to authorized personnel. Emburse uses LDAP services to enforce password and role-based security for users that log into the production systems.

User accounts are reviewed monthly by management to verify appropriateness. The results from these reviews are documented and maintained.

All system activity, including audit logs, are transferred to a third-party service (Threat Stack), where they are available read-only for data forensic investigation and incident response. Network access control settings are maintained by internal system administrator personnel.

SYSTEMS DEVELOPMENT AND MAINTENANCE

INFRASTRUCTURE CHANGES

Emburse has implemented change control procedures to ensure that Emburse is tracking changes to systems and workstations including software releases and software vulnerability patching in information systems. Change control procedures are necessary to establish adequate testing and recovery plans. Change management processes include properly authorizing, testing, approving, implementing, documenting, and maintaining system applications and security patches.

APPLICATION CHANGES

Application changes are major functional changes to the user-facing application, which may also include changes in the backend process requirements. Application changes include changes to the business logic or user interface of the Abacus & Emburse Spend service and are executed by changing the source code run in the production environment.



Application changes proceed through deployments. A deployment can include significant functional improvements, significant additions, correction of larger functional defects, minor functional improvements, less significant additions, and corrections of smaller functional defects found in the service. Deployments can happen multiple times a day and are not scheduled.

APPLICATION CHANGE INITIATION

The development of items in deployments is governed by the application development process, which is internally published to the Company. Application changes are initially input into the change management ticketing system in instances when a request is received from a customer for an enhancement, a defect is identified within the software, or there is an internal request to upgrade, modify, or introduce new functionality to the software application. Once the design and technical specifications have been identified, the change ticket gets passed to the Product Manager or Engineering Manager for review. An authorized approver reviews the specifications and approves application changes within the ticketing system.

APPLICATION CHANGE DEVELOPMENT

Once the authorized manager has approved the change requirements, the development process begins. Developers work in the development environment until the development process is completed. Once the development process is completed, the changes are reviewed, and the application is compiled and loaded onto the staging environment for testing purposes.

APPLICATION TESTING

The developers communicate to the team that development is complete, and the application change is ready for testing. Developers test the change in the staging environment. The successful completion of testing indicates the approval to migrate the change to the production environment. Abacus & Emburse Spend also uses automated tools to validate code against known vulnerabilities and standards.

MIGRATION TO PRODUCTION

After successful testing is completed, the change is ready to migrate to the production environment. The Engineering team performs the migration to the production environment.

POSTPRODUCTION TESTING

When the change has been migrated to the production environment, checks are performed to make certain the change was functioning as intended within the production environment for enhancements. Postproduction testing is completed for application changes, and the results of the testing are documented on the change ticket.

CONFIDENTIALITY

Emburse maintains formal written policies over data confidentiality. Upon employment, employees sign a nondisclosure form stating that no confidential or proprietary data from Emburse or its customers is to be communicated outside the organization.

Confidential information, as defined in agreements with customers, is protected during the system design, development, testing, implementation, and change processes in accordance with confidentiality commitments and requirements.



As noted above, a role-based security process has been defined. Access to data is restricted to authorized personnel through access control software. System access is approved by an employee's manager and captured in a ticket reflecting the employee's place in the organizational structure.

Emburse obtains confidentiality commitments, which are consistent with its confidentiality requirements, from vendors and other third parties whose products and services comprise part of the system or who may have access to confidential information. Changes to confidentiality commitments and requirements are communicated to internal and external users, vendors, and other third parties whose products and services are included in the system.

In accordance with its customer agreements, customer data is retained unless the customer instructs Emburse to destroy its data. Upon termination of a customer relationship with Emburse, the cancellation process is initiated, and customers may submit a notice of data cancellation. Data is disposed of using secure data disposal methods.

2. Risk Assessment Process

Emburse's management routinely assesses internal and external risks to maintain service operations and, as necessary, address future identified risks. During the risk assessment and management process, risk management personnel identify changes to business objectives, commitments and requirements, internal operations, and external factors that threaten the achievement of business objectives and update the potential threats to system objectives. Application development and product development processes are in place that allow system changes to effectively address known risk factors.

Emburse's Security Policy also requires the Company to conduct a comprehensive risk assessment of its information assets every year and whenever there is significant change in the Company's use of information technology. The CISO has primary responsibility for the risk assessment process.

The Risk Assessment Team evaluates risk management practices of the Company's information assets, assesses the impact of the most relevant threats to these information assets and Emburse's related security, availability, and confidentiality commitments and requirements, and identifies mitigation strategies for these risks. The CISO performs an initial ranking of the effect of threats on the security, availability, and confidentiality of information assets, the likelihood of occurrence, and the overall impact. This process results in a risk level rating, which is then adjusted based on the team members' comments and review of the initial analysis.

3. Information and Communication

Emburse has a documented description of its Abacus & Emburse Spend that details the relevant system components and design of the system. The description is made available to authorized internal users via system and training materials on the Company's intranet, and to external users on the Company's public website.



Policy and procedure documents for significant processes are published and available to Emburse personnel on the organization's intranet. These include responsibilities for reporting operational failures, incidents, system problems, concerns, and user complaints. Annually, employees are required to acknowledge the Information Security Policy. Emburse has also communicated to external users the incident reporting process via the Privacy Policy as described on the customer-facing website.

4. Monitoring Controls

Emburse employs a combination of ongoing and periodic monitoring activities to monitor that controls are functioning effectively and that risks are appropriately mitigated.

ONGOING MONITORING

Organizational goals are set by the Emburse management team and shared with employees and business units. Policies and procedures are routinely updated to reflect the most effective operating principles and practices.

Emburse monitors its technical operations to manage the availability and performance of its Webbased application and the application's security, as well as reporting any changes to the production environment and backups performed. Emburse monitors its application operations and customer service functions using automated tools while maintaining the status of such functions through an internal and external help desk ticketing system. Automated alerts of critical events are sent to an alerting system, and a root cause analysis ticket is created to record when issues are detected and track their remediation.

On a quarterly basis, the Information Security Committee convenes to discuss Emburse's security profile, security events, and threats, including any identified incidents or problems. Anti-virus software is installed on applicable servers and workstations. Management maintains formal policy and procedures over anti-virus updates and configuration. Machines have endpoint protection installed and are continuously monitored.

MONITORING OF THE SUBSERVICE ORGANIZATION

Emburse uses the subservice organizations described herein to provide cloud hosting services.

Emburse Management receives and reviews the compliance attestations of each subservice organization on an annual basis. In addition, through its daily operational activities, Emburse Management monitors the services performed by the subservice organizations to ensure that operations and controls expected to be implemented at the subservice organizations are functioning effectively.



SYSTEM MONITORING

Instana monitoring software is used to monitor the performance and uptime of production systems. If a performance threshold previously configured is exceeded, Instana is configured to send an automatic alert to the systems operations staff. Upon notification of the alert, systems operations staff members research the issues. The alert may result in a routine sysadmin action or in the creation of a ticket if a configuration change is required. Informational alerts may be cleared with no action taken. Root-cause analysis procedures are followed to document the cause, impact, and resolution. Tickets are closed upon the completion of the incident.

On a weekly basis, Abacus & Emburse Spend hosts a Site Availability Meeting with a summary of the previous week's incidents and technical anomalies. The meeting is composed of application, infrastructure, and network subject matter experts. Incidents and defects are discussed, along with their associated root causes. Tickets are created to address any findings that may have arisen from the meeting, and reviews are conducted of the previous week's fixes as well.

E. Trust Services Categories, Criteria, and Related Controls

Although the applicable trust services categories, criteria, and related controls are presented in Section IV of this report titled "Trust Services Categories, Criteria, Related Controls, and Tests of Controls", they are an integral part of Emburse's system description throughout the period January 1, 2022 to September 30, 2022.

F. Complementary Subservice Organization Controls

Emburse's controls related to the Abacus & Emburse Spend System cover only a portion of overall internal control for each user entity of Emburse. It is not feasible for the criteria related to the Abacus & Emburse Spend System to be achieved solely by Emburse. Therefore, each user entity's internal controls must be evaluated in conjunction with Emburse's controls and the related tests and results described in Section IV of this report, taking into account the types of controls expected to be implemented by the subservice organization as described below.

Cor	nplementary Subservice Organization Controls	Related Criteria
1	AWS is responsible for controlling access, logging and monitoring of the systems and underlying infrastructure.	> CC6.1
2	AWS is responsible for deactivating or disabling users' system access upon termination.	> CC6.2 and CC6.3
3	AWS is responsible for ensuring that data center access for their employees, contractors, vendors, and customers is added only for authorized individuals, removed when no longer required and reviewed on a periodic basis.	> CC6.4
4	AWS is responsible for implementing processes to ensure that hardware for all systems and underlying infrastructure is disposed in a secure fashion.	> CC6.5
5	AWS is responsible for implementing a detailed incident response plan for all systems and underlying infrastructure.	> CC7.1



Cor	nplementary Subservice Organization Controls	Re	Related Criteria		
6	AWS is responsible for ensuring that change management process is developed to ensure that changes for all systems and underlying infrastructure are authorized, developed, documented, tested, approved, and implemented in accordance with the policies.	>	CC8.1		
7	AWS is responsible for ensuring that business recovery and continuity procedures are in place and tested regularly for all systems and underlying infrastructure.	>	CC9.1, CC9.2, and A1.3		
8	AWS is responsible for ensuring that processes are in place to identify risks relevant to the subservice organization's infrastructure and supporting systems, evaluate risk and communicate them to management, and perform timely remediation activities.	>	CC9.2		
9	AWS is responsible for ensuring that a detailed vendor management program exists to assess and manage risks associated with vendors and business partners.	>	CC9.2		

G. Complementary User Entity Controls

Emburse's Abacus & Emburse Spend System was designed under the assumption that certain controls would be implemented by the user entities for whom it provides its Abacus & Emburse Spend System. In these situations, the application of specific controls at these user entities is necessary to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

This section describes additional controls that should be in operation at the user entities to complement the controls at Emburse. User auditors should consider whether the following controls have been placed in operation by the user entity.

Each user entity must evaluate its own internal control structure to determine if the identified user entity controls are in place.

Cor	nplementary User Entity Controls	Related Criteria
1	User entities are responsible for communicating the responsibilities of using the Abacus & Emburse Spend System including legal and regulatory requirements to users.	➤ CC2.3
2	User entities are responsible for setting up and maintaining security privileges for their own data in adherence to their own security policies.	> CC6.1 and CC6.2
3	User entities are responsible for the safekeeping of the user ID and password for accessing their accounts via the website	> CC6.1
4	User entities are responsible for configuring and verifying that strong password security is enforced.	> CC6.1
5	User entities are responsible for user entities are responsible for ensuring that physical access to sensitive locations is restricted to authorized personnel.	> CC6.4



Cor	nplementary User Entity Controls	Related Criteria		
6	User entities are responsible for ensuring that the transmission, movement, and removal of information from the Company's network and its assets is restricted to authorized users and processes and is protected during transmission, movement, or removal.	>	CC6.8	
7	User entities are responsible for communicating relevant security, availability, and confidentiality issues and incidents to the Company through identified channels.	>	CC7.3	



IV. Trust Services Categories, Criteria, Related Controls, and Tests of Controls

This integrated SOC 2 Type 2 Report was prepared in accordance with the AICPA attestation standards and in accordance with the International Standard on Assurance Engagements (ISAE) 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board (IAASB), and has been performed to examine the suitability of the design and operating effectiveness of controls to meet the criteria for the Security, Availability, and Confidentiality categories set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria) throughout the period January 1, 2022 to September 30, 2022.

The trust services categories for the Security, Availability, and Confidentiality criteria and related controls specified by Emburse are presented in Section IV of this report.



A. Applicable Trust Services Criteria

Common Criteria

CC1.0	Common Criteria Related to Control Environment						
	Trust Services Criteria	Emburse #	Controls Specified by Emburse	Test Results			
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	POL.03	Emburse policies and procedures are reviewed annually, or as needed, by upper management or their designees, including by the CISO where required, for consistency with the organization's risk management strategy and updated as necessary for changes in the strategy.	No exceptions noted.			
		HR.01	Emburse has documented the Code of Conduct, which includes ethical standards.				
		HR.02	The Emburse Code of Conduct Standard is documented and provides guidance to Emburse personnel on any disciplinary action that will be followed for non-compliance.				
		HR.03	Human Resources provide separate communication channels, including anonymous channels, for internal personnel to communicate concerns and complaints.				
		HR.04	Emburse performs annual performance evaluations, which are tracked within the Company's performance review software.				
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	OVS.01	The Board of Directors consists of a majority of independent members to maintain independence from Emburse management. Meetings occur on a quarterly basis.	No exceptions noted.			
		OVS.02	Upper management holds monthly security meetings to monitor and manage departments' progress or lack thereof as it relates to their achievement of the departments' responsibilities.				
		RM.02	Emburse's Information Security Committee meets quarterly to provide oversight for the organization's processes and commitments, review the results of the risk assessment, and evaluate any security or confidentiality-related incidents.				



	Trust Services Criteria	Emburse #	Controls Specified by Emburse	Test Results
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	HR.08	An organization chart is documented that outlines the reporting lines of Emburse employees.	No exceptions noted.
		POL.04	Emburse's Chief Information Security Officer (CISO) and Information Security Committee are responsible for establishing, maintaining, and enforcing the overall security policies and procedures, including incident response and vendor risk assessment policy.	
		OVS.02	Upper management holds monthly security meetings to monitor and manage departments' progress or lack thereof as it relates to their achievement of the departments' responsibilities.	
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	HR.05	Emburse conducts skill assessments on candidates to assess their ability to complete job responsibilities.	No exceptions noted.
		HR.06	Where permitted by applicable law, prior to employment, personnel undergo background screening including verification against regulatory screening databases.	
		HR.07	Employees are required to read and sign an acknowledgement that they will abide by the Code of Conduct standards defined in the Employee Handbook upon hire.	
		TRAIN.01	Emburse has a security awareness training program that includes annual security awareness training and simulated phishing campaigns to improve security knowledge and awareness and to model appropriate security behaviors.	



CC1.0	Common Criteria Related to Control Environment						
	Trust Services Criteria	Emburse #	Controls Specified by Emburse	Test Results			
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	POL.04	Emburse's Chief Information Security Officer (CISO) and Information Security Committee are responsible for establishing, maintaining, and enforcing the overall security policies and procedures, including incident response and vendor risk assessment policy.	No exceptions noted.			
		HR.07	Employees are required to read and sign an acknowledgement that they will abide by the Code of Conduct standards defined in the Employee Handbook upon hire.				
		HR.04	Emburse performs annual performance evaluations, which are tracked within the Company's performance review software.				



	Trust Services Criteria	Emburse #	Controls Specified by Emburse	Test Results
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	LEG.01	The Emburse legal team maintains a repository of contract terms and commitments. Emburse's contracts administrator is responsible for changes to contractual terms and commitments.	No exceptions noted.
		RM.03	A documented risk assessment and Risk Treatment Methodology is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	
		RM.01	A company-wide risk assessment is performed annually by the security team, to identify risks arising from external and internal sources. Risks, including fraud risks, are tracked in a risk assessment table which documents mitigation strategies, remediation plans and assigned owners.	
		RM.02	Emburse's Information Security Committee meets quarterly to provide oversight for the organization's processes and commitments, review the results of the risk assessment, and evaluate any security or confidentiality-related incidents.	
		MON.03	Internal control assessments are performed on an annual basis and communicated during the Information Security Committee meeting.	



CC2.0	Common Criteria Related to Com			
	Trust Services Criteria	Emburse #	Controls Specified by Emburse	Test Results
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning	POL.01	Policy and procedure documents relating to significant processes are available to Emburse personnel on the organization's intranet. Annually, employees and contractors are required to acknowledge the Information Security Policy.	No exceptions noted.
	of internal control.	TXN.01	Emburse has a documented description of its Expense Management System that details relevant system components and design of the system. The description is made available to authorized internal users via system and on Emburse's intranet, and to external users on Emburse public websites.	
		INC.01	Incident response policies and procedures, which include responsibility and processes for reporting operational failures, incidents, system problems, concerns and user complaints, are published and available to internal users via the intranet.	
		INC.02	Internal and external users are informed of relevant incidents in a timely manner and advised of corrective measures to be taken on their part.	



CC2.0	Common Criteria Related to Com	munication an	d Information	
	Trust Services Criteria	Emburse #	Controls Specified by Emburse	Test Results
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal	LEG.03	Emburse's security and confidentiality commitments are established and documented within agreements, defining service provider terms, conditions, and responsibilities.	No exceptions noted.
	control.	TXN.01	Emburse has a documented description of its Expense Management System that details relevant system components and design of the system. The description is made available to authorized internal users via system and on Emburse's intranet, and to external users on Emburse public websites.	
		SUP.05	Emburse customer-facing website includes a Support page with a customer support form and links to assist customers with reporting any operational failures, incidents, problems, concerns, and complaints.	
		in a t	Internal and external users are informed of relevant incidents in a timely manner and advised of corrective measures to be taken on their part.	



CC3.0	Common Criteria Related to Risk	Assessment		
	Trust Services Criteria	Emburse #	Controls Specified by Emburse	Test Results
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	RM.03	A documented risk assessment and Risk Treatment Methodology is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
		RM.01	A company-wide risk assessment is performed annually by the security team, to identify risks arising from external and internal sources. Risks, including fraud risks, are tracked in a risk assessment table which documents mitigation strategies, remediation plans and assigned owners.	
		provide oversight for the organization's proces commitments, review the results of the risk as:	Emburse's Information Security Committee meets quarterly to provide oversight for the organization's processes and commitments, review the results of the risk assessment, and evaluate any security or confidentiality-related incidents.	
		VULN.01	During quarterly Information Security Committee meetings, management assesses the scope and frequency of vulnerability assessments, including penetration testing and vulnerability scanning.	
	management initiates corrective action vulnerabilities. Results and recomme	External penetration tests are conducted annually and management initiates corrective actions for identified vulnerabilities. Results and recommendations from these assessments for improvement are reported to management, which initiates corrective actions.		
		VULN.03 Internal and external vulnerability scans are performed a least quarterly.	Internal and external vulnerability scans are performed at least quarterly.	
		TPRM.01	Service providers are subject to review as part of the vendor risk assessment process. Attestations and certifications are obtained and evaluated on an annual basis.	
		MON.03	Internal control assessments are performed on an annual basis and communicated during the Information Security Committee meeting.	



CC3.0	Common Criteria Related to Risk	Common Criteria Related to Risk Assessment				
	Trust Services Criteria	Emburse #	Controls Specified by Emburse	Test Results		
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	RM.01	A company-wide risk assessment is performed annually by the security team, to identify risks arising from external and internal sources. Risks, including fraud risks, are tracked in a risk assessment table which documents mitigation strategies, remediation plans and assigned owners.	No exceptions noted.		
		RM.02	Emburse's Information Security Committee meets quarterly to provide oversight for the organization's processes and commitments, review the results of the risk assessment, and evaluate any security or confidentiality-related incidents.			
		VULN.03	Internal and external vulnerability scans are performed at least quarterly.			
		VULN.02	External penetration tests are conducted annually and management initiates corrective actions for identified vulnerabilities. Results and recommendations from these assessments for improvement are reported to management, which initiates corrective actions.			
		VULN.01	During quarterly Information Security Committee meetings, management assesses the scope and frequency of vulnerability assessments, including penetration testing and vulnerability scanning.			
		TPRM.01	Service providers are subject to review as part of the vendor risk assessment process. Attestations and certifications are obtained and evaluated on an annual basis.			
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	RM.01	A company-wide risk assessment is performed annually by the security team, to identify risks arising from external and internal sources. Risks, including fraud risks, are tracked in a risk assessment table which documents mitigation strategies, remediation plans and assigned owners.	No exceptions noted.		



CC3.0	Common Criteria Related to Risk	Assessment		
	Trust Services Criteria	Emburse #	Controls Specified by Emburse	Test Results
CC3.4	changes that could significantly impact the system of internal control. the security team, to identify risk internal sources. Risks, includin risk assessment table which do remediation plans and assigned VULN.03 Internal and external vulnerabilit least quarterly. VULN.02 External penetration tests are comanagement initiates corrective vulnerabilities. Results and recognises assessments for improvement as	RM.01	A company-wide risk assessment is performed annually by the security team, to identify risks arising from external and internal sources. Risks, including fraud risks, are tracked in a risk assessment table which documents mitigation strategies, remediation plans and assigned owners.	No exceptions noted.
		VULN.03	Internal and external vulnerability scans are performed at least quarterly.	
		External penetration tests are conducted annually and management initiates corrective actions for identified vulnerabilities. Results and recommendations from these assessments for improvement are reported to management, which initiates corrective actions.		
		VULN.01	During quarterly Information Security Committee meetings, management assesses the scope and frequency of vulnerability assessments, including penetration testing and vulnerability scanning.	
	MON.04 MON.05 MON.02	TPRM.01	Service providers are subject to review as part of the vendor risk assessment process. Attestations and certifications are obtained and evaluated on an annual basis.	_
		MON.04	Monitoring tools are used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	
		MON.05	The monitoring solutions send messages to the operations center. Where escalation is required, the team opens an incident ticket, which is followed through to resolution.	
		MON.02	A cloud infrastructure monitoring tool is utilized to monitor cloud infrastructure availability and performance and generates alerts when specific predefined thresholds are met.	



	Trust Services Criteria	Emburse #	Controls Specified by Emburse	Test Results
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	MON.04	Monitoring tools are used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	No exceptions noted.
		MON.05	The monitoring solutions send messages to the operations center. Where escalation is required, the team opens an incident ticket, which is followed through to resolution.	
		VULN.03	Internal and external vulnerability scans are performed at least quarterly.	
		VULN.02	External penetration tests are conducted annually and management initiates corrective actions for identified vulnerabilities. Results and recommendations from these assessments for improvement are reported to management, which initiates corrective actions.	
		VULN.01	During quarterly Information Security Committee meetings, management assesses the scope and frequency of vulnerability assessments, including penetration testing and vulnerability scanning.	
		VULN.04	Anti-malware technology is installed on assets placed into production and end points.	
		MON.02	A cloud infrastructure monitoring tool is utilized to monitor cloud infrastructure availability and performance and generates alerts when specific predefined thresholds are met.	



	Trust Services Criteria	Emburse #	Controls Specified by Emburse	Test Results
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	VULN.01	During quarterly Information Security Committee meetings, management assesses the scope and frequency of vulnerability assessments, including penetration testing and vulnerability scanning.	No exceptions noted.
		RM.02	Emburse's Information Security Committee meets quarterly to provide oversight for the organization's processes and commitments, review the results of the risk assessment, and evaluate any security or confidentiality-related incidents.	
		VULN.02	External penetration tests are conducted annually and management initiates corrective actions for identified vulnerabilities. Results and recommendations from these assessments for improvement are reported to management, which initiates corrective actions.	
		RM.01	A company-wide risk assessment is performed annually by the security team, to identify risks arising from external and internal sources. Risks, including fraud risks, are tracked in a risk assessment table which documents mitigation strategies, remediation plans and assigned owners.	
		INC.02	Internal and external users are informed of relevant incidents in a timely manner and advised of corrective measures to be taken on their part.	



CC5.0	Common Criteria Related to Cont	rol Activities		
	Trust Services Criteria	Emburse #	Controls Specified by Emburse	Test Results
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	OPS.01	A VPC is in place and configured to secure the perimeter of the environment. VPC access, configurations, and security events are logged through AWS CloudTrail. Administrative access privileges to the VPC are limited to operations personnel.	No exceptions noted.
		OPS.02	End user and server workload network traffic is segmented to support isolation.	
		MON.04	Monitoring tools are used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	
		MON.05	The monitoring solutions send messages to the operations center. Where escalation is required, the team opens an incident ticket, which is followed through to resolution.	
		VULN.03	Internal and external vulnerability scans are performed at least quarterly.	
		VULN.02	External penetration tests are conducted annually and management initiates corrective actions for identified vulnerabilities. Results and recommendations from these assessments for improvement are reported to management, which initiates corrective actions.	
		AM.09	A role-based security process has been defined with an access control system that is required to use roles when possible.	
		AM.01	Users are assigned a password to access Emburse systems. Passwords must be configured in accordance with the Emburse Password Policy.	
		MON.02	A cloud infrastructure monitoring tool is utilized to monitor cloud infrastructure availability and performance and generates alerts when specific predefined thresholds are met.	



CC5.0	Common Criteria Related to Cont	rol Activities		
	Trust Services Criteria	Emburse #	Controls Specified by Emburse	Test Results
general control activities ove technology to support the		AM.02	Infrastructure components and software are configured to require unique usernames and passwords. Privileged access requires multi-factor authentication.	No exceptions noted.
	achievement of objectives.	AM.10	Logical access to the administration console and database is restricted to application and database administrators.	
		ENC.01	Databases housing sensitive customer data are encrypted at rest.	
		AM.08	Remote access to Emburse systems requires multi-factor authentication to VPN to the Emburse network along with employee's authentication credentials.	
		ENC.02	Encryption keys used by integrated services are encrypted themselves with a unique master key.	
		ENC.04	HTTPS, TLS 1.2, and VPN encryption technologies are deployed for transmission of confidential or sensitive information over public networks.	



CC5.0	Common Criteria Related to Cont	rol Activities		
	Trust Services Criteria	Emburse #	Controls Specified by Emburse	Test Results
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	POL.04	Emburse's Chief Information Security Officer (CISO) and Information Security Committee are responsible for establishing, maintaining, and enforcing the overall security policies and procedures, including incident response and vendor risk assessment policy.	No exceptions noted.
		POL.01	Policy and procedure documents relating to significant processes are available to Emburse personnel on the organization's intranet. Annually, employees and contractors are required to acknowledge the Information Security Policy.	
		AM.01	Users are assigned a password to access Emburse systems. Passwords must be configured in accordance with the Emburse Password Policy.	
		TXN.02	Emburse maintains a transaction flow diagram that demonstrates how sensitive data moves throughout the organization.	
		CM.01	Formally documented change management procedures are in place to govern the implementation, modification and maintenance of production systems and address security, confidentiality, and availability requirements.	
		INC.01	Incident response policies and procedures, which include responsibility and processes for reporting operational failures, incidents, system problems, concerns and user complaints, are published and available to internal users via the intranet.	
		INC.03	Annual testing of the incident response plan is performed to ensure the incident response procedures are up-to-date and effective. When updating the incident response plan, lessons learned from incident testing are used to implement changes to reflect effective procedures when handling incidents.	
		CONF.01	A Data Classification Policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	



CC5.0	Common Criteria Related to Control Activities			
	Trust Services Criteria	Emburse #	Controls Specified by Emburse	Test Results
		CONF.02	Confidential or personal information involved in business processes, systems, and third-party involvement is identified and tracked.	
		CONF.03	Documented data retention and disposal policies and procedures are in place to guide personnel in retention and disposal of confidential information.	
		MON.01	Documented procedures are in place to direct personnel in monitoring the system performance and availability.	



	Trust Services Criteria	Emburse #	Controls Specified by Emburse	Test Results
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.	The entity implements logical access security software, infrastructure, and architectures over protected	POL.02	Formal information security policies are available on the intranet and provide procedures on security of user accounts, user authentication, and monitoring.	
	from security events to meet the	AM.09	A role-based security process has been defined with an access control system that is required to use roles when possible.	
		AM.01	Users are assigned a password to access Emburse systems. Passwords must be configured in accordance with the Emburse Password Policy.	
		AM.02	Infrastructure components and software are configured to require unique usernames and passwords. Privileged access requires multi-factor authentication.	
	AM.06	Privileged access to sensitive resources is restricted to individuals in DevOps, Site Reliability Engineering (SRE), and Technical Support roles.		
		AM.10	Logical access to the administration console and database is restricted to application and database administrators.	
		OPS.01	A VPC is in place and configured to secure the perimeter of the environment. VPC access, configurations, and security events are logged through AWS CloudTrail. Administrative access privileges to the VPC are limited to operations personnel.	



	Trust Services Criteria	Emburse #	Controls Specified by Emburse	Test Results
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new	AM.03	For all users, to obtain system access, a request must be submitted in the ticketing system by HR or the employee's manager.	AM.04: Logical access for two of 10 randomly selected terminated contractors was
	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	AM.04	Upon notification of employee end date, a termination ticket is created in the ticketing system by HR personnel. Terminated user access is removed within 24 business hours of termination.	not removed within 24 business hours of termination.
	when user access is no longer authorized.	AM.11	Only IT personnel are permitted to create or modify user access and user access privileges.	
		AM.05	On a quarterly basis, the IT and operations teams conduct a review of all personnel with access to system resources.	
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles,	AM.04	Upon notification of employee end date, a termination ticket is created in the ticketing system by HR personnel. Terminated user access is removed within 24 business hours of termination.	AM.04: Logical access for two of 10 randomly selected terminated contractors was not removed within 24
	responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	AM.05	On a quarterly basis, the IT and operations teams conduct a review of all personnel with access to system resources.	business hours of termination.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	TPRM.01	Service providers are subject to review as part of the vendor risk assessment process. Attestations and certifications are obtained and evaluated on an annual basis.	No exceptions noted.



	Trust Services Criteria	Emburse #	Controls Specified by Emburse	Test Results
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or	CONF.04	Emburse has established policies to protect against unauthorized and willful acquisition, use, or disposal of assets.	No exceptions noted.
	recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	CONF.05	Computer drives are securely destroyed using third-party data destruction service providers. Certificates of destruction are retained.	
security measures to protect ag	The entity implements logical access security measures to protect against threats from sources outside its	AM.06	Privileged access to sensitive resources is restricted to individuals in DevOps, Site Reliability Engineering (SRE), and Technical Support roles.	No exceptions noted.
	system boundaries.	AM.08	Remote access to Emburse systems requires multi-factor authentication to VPN to the Emburse network along with employee's authentication credentials.	
		ENC.01	Databases housing sensitive customer data are encrypted at rest.	
		ENC.02	Encryption keys used by integrated services are encrypted themselves with a unique master key.	
		VULN.04	Anti-malware technology is installed on assets placed into production and end points.	
		AM.05	On a quarterly basis, the IT and operations teams conduct a review of all personnel with access to system resources.	



CC6.0	Common Criteria Related to Logic	cal and Physic	cal Access Controls	
	Trust Services Criteria	Emburse #	Controls Specified by Emburse	Test Results
CC6.7	The entity restricts the transmission, movement, and removal of	ENC.02	Encryption keys used by integrated services are encrypted themselves with a unique master key.	No exceptions noted.
	information to authorized internal and external users and processes and protects it during transmission, movement, or removal to meet the entity's objectives.	ENC.01	Databases housing sensitive customer data are encrypted at rest.	
		ENC.04	HTTPS, TLS 1.2, and VPN encryption technologies are deployed for transmission of confidential or sensitive information over public networks.	
			Computer drives are securely destroyed using third-party data destruction service providers. Certificates of destruction are retained.	
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	VULN.04	Anti-malware technology is installed on assets placed into production and end points.	No exceptions noted.



	Trust Services Criteria	Emburse #	Controls Specified by Emburse	Test Results
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to	MON.04	Monitoring tools are used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	No exceptions noted.
	configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	MON.05	The monitoring solutions send messages to the operations center. Where escalation is required, the team opens an incident ticket, which is followed through to resolution.	
		VULN.03	Internal and external vulnerability scans are performed at least quarterly.	
		VULN.02	External penetration tests are conducted annually and management initiates corrective actions for identified vulnerabilities. Results and recommendations from these assessments for improvement are reported to management, which initiates corrective actions.	
		VULN.01	During quarterly Information Security Committee meetings, management assesses the scope and frequency of vulnerability assessments, including penetration testing and vulnerability scanning.	
		MON.02	A cloud infrastructure monitoring tool is utilized to monitor cloud infrastructure availability and performance and generates alerts when specific predefined thresholds are met.	



CC7.0	Common Criteria Related to Syst	em Operations	5	
	Trust Services Criteria	Emburse #	Controls Specified by Emburse	Test Results
CC7.2	The entity monitors system components and the operation of those components for anomalies that	MON.02	A cloud infrastructure monitoring tool is utilized to monitor cloud infrastructure availability and performance and generates alerts when specific predefined thresholds are met.	No exceptions noted.
	are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed	VULN.03	Internal and external vulnerability scans are performed at least quarterly.	
	to determine whether they represent security events.	VULN.02	External penetration tests are conducted annually and management initiates corrective actions for identified vulnerabilities. Results and recommendations from these assessments for improvement are reported to management, which initiates corrective actions.	
		VULN.04	Anti-malware technology is installed on assets placed into production and end points.	



	Common Criteria Related to Systematics Trust Services Criteria	Emburse #	Controls Specified by Emburse	Test Results
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.	to determine whether they could or have resulted in a failure of the entity to meet its objectives (security	INC.01	Incident response policies and procedures, which include responsibility and processes for reporting operational failures, incidents, system problems, concerns and user complaints, are published and available to internal users via the intranet.	No exceptions noted.
	INC.03	Annual testing of the incident response plan is performed to ensure the incident response procedures are up-to-date and effective. When updating the incident response plan, lessons learned from incident testing are used to implement changes to reflect effective procedures when handling incidents.		
		INC.04	All incidents related to the security of the system are logged, tracked, and communicated to affected parties by management until resolved.	
		INC.05	After an incident has been confirmed, specific personnel are engaged in the containment process to reduce the magnitude of the incident.	
			As part of the forensic investigation, the Incident Response Team determines whether sensitive information was used or disclosed.	
		INC.07	The Incident Response team classifies reported incidents based on their perceived severity and impact on the organization. The classification is used to determine response procedures.	
		INC.09	The Information Security Team periodically provides a report to upper management of relevant security-related activities and incidents. Management monitors for completion of corrective action plans.	
		INC.08	For high severity incidents, a root cause analysis is prepared and reviewed by management. Based on the root cause analysis, change requests are prepared and the entity's risk management process and relevant risk management data is updated to reflect the planned incident and problem resolution, as needed.	



	Trust Services Criteria	Emburse #	Controls Specified by Emburse	Test Results
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to	INC.04	All incidents related to the security of the system are logged, tracked, and communicated to affected parties by management until resolved.	No exceptions noted.
	understand, contain, remediate, and communicate security incidents, as appropriate.	INC.05	After an incident has been confirmed, specific personnel are engaged in the containment process to reduce the magnitude of the incident.	
		INC.06	As part of the forensic investigation, the Incident Response Team determines whether sensitive information was used or disclosed.	
		INC.07	The Incident Response team classifies reported incidents based on their perceived severity and impact on the organization. The classification is used to determine response procedures.	
		INC.09	The Information Security Team periodically provides a report to upper management of relevant security-related activities and incidents. Management monitors for completion of corrective action plans.	
		INC.08	For high severity incidents, a root cause analysis is prepared and reviewed by management. Based on the root cause analysis, change requests are prepared and the entity's risk management process and relevant risk management data is updated to reflect the planned incident and problem resolution, as needed.	
		INC.02	Internal and external users are informed of relevant incidents in a timely manner and advised of corrective measures to be taken on their part.	



	Trust Services Criteria	Emburse #	Controls Specified by Emburse	Test Results
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	MON.07	Management evaluates the Business Continuity Plan for any needed additional tools and resources to achieve business objectives including contingency plans for assignments of responsibility important for internal control.	No exceptions noted.
		INC.01	Incident response policies and procedures, which include responsibility and processes for reporting operational failures, incidents, system problems, concerns and user complaints, are published and available to internal users via the intranet.	
		INC.03	Annual testing of the incident response plan is performed to ensure the incident response procedures are up-to-date and effective. When updating the incident response plan, lessons learned from incident testing are used to implement changes to reflect effective procedures when handling incidents.	
		INC.04	All incidents related to the security of the system are logged, tracked, and communicated to affected parties by management until resolved.	
		INC.05	After an incident has been confirmed, specific personnel are engaged in the containment process to reduce the magnitude of the incident.	
		INC.06	As part of the forensic investigation, the Incident Response Team determines whether sensitive information was used or disclosed.	
		INC.07	The Incident Response team classifies reported incidents based on their perceived severity and impact on the organization. The classification is used to determine response procedures.	
		INC.09	The Information Security Team periodically provides a report to upper management of relevant security-related activities and incidents. Management monitors for completion of corrective action plans.	



CC7.0	Common Criteria Related to System Operations					
	Trust Services Criteria	Emburse #	Controls Specified by Emburse	Test Results		
		INC.08	For high severity incidents, a root cause analysis is prepared and reviewed by management. Based on the root cause analysis, change requests are prepared and the entity's risk management process and relevant risk management data is updated to reflect the planned incident and problem resolution, as needed.			



	Trust Services Criteria	Emburse #	Controls Specified by Emburse	Test Results
CC8.1	develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	CM.01	Formally documented change management procedures are in place to govern the implementation, modification and maintenance of production systems and address security, confidentiality, and availability requirements.	No exceptions noted.
		CM.07	Source code management tools are utilized and access is restricted to appropriate personnel.	
		CM.04	Production environments are segregated from development and test environments.	
		CM.02	Emburse requires all changes to be documented in the ticketing application and tracked from initiation through deployment and validation. Code reviews are completed at the time of the merge.	
		CM.03	System and regression testing is required prior to approval, and is performed by product teams using approved test plans and test data. Deviations from planned results are analyzed and submitted to the developer for remediation.	
		CM.06	The ability to approve system changes is restricted to the Software Engineering Team and DevOps.	



	Trust Services Criteria	Emburse #	Controls Specified by Emburse	Test Results
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from business disruption.	BP.1	Backup snapshots are created for production database clusters.	No exceptions noted.
		MON.07	Management evaluates the Business Continuity Plan for any needed additional tools and resources to achieve business objectives including contingency plans for assignments of responsibility important for internal control.	
		RM.04	The risk management program includes the use of insurance to minimize the financial impact of any loss events.	
		TPRM.02	The Company's Information Security Team is responsible for assessing and monitoring risk and compliance status of vendors and business partners.	
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	TPRM.01	Service providers are subject to review as part of the vendor risk assessment process. Attestations and certifications are obtained and evaluated on an annual basis.	No exceptions noted.
		TPRM.02	The Company's Information Security Team is responsible for assessing and monitoring risk and compliance status of vendors and business partners.	
		LEG.05	Emburse's requirements with respect to security, availability, and confidentiality, and availability of information are included within vendor agreements, defining terms, conditions, and responsibilities.	
		RM.04	The risk management program includes the use of insurance to minimize the financial impact of any loss events.	



Availability

A.0	Additional Criteria for Availability					
	Trust Services Criteria	Emburse #	Controls Specified by Emburse	Test Results		
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system	MON.04	Monitoring tools are used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	No exceptions noted.		
	components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	MON.02	A cloud infrastructure monitoring tool is utilized to monitor cloud infrastructure availability and performance and generates alerts when specific predefined thresholds are met.			
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	BP.1	Backup snapshots are created for production database clusters.	No exceptions noted.		
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	MON.07	Management evaluates the Business Continuity Plan for any needed additional tools and resources to achieve business objectives including contingency plans for assignments of responsibility important for internal control.	No exceptions noted.		
		INC.05	After an incident has been confirmed, specific personnel are engaged in the containment process to reduce the magnitude of the incident.			



Confidentiality

C.0	Additional Criteria for Confidentiality					
	Trust Services Criteria	Emburse #	Controls Specified by Emburse	Test Results		
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to	CONF.01	A Data Classification Policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	No exceptions noted.		
	confidentiality.	CONF.02	Confidential or personal information involved in business processes, systems, and third-party involvement is identified and tracked.			
		CONF.03	Documented data retention and disposal policies and procedures are in place to guide personnel in retention and disposal of confidential information.			
		TPRM.02	The Company's Information Security Team is responsible for assessing and monitoring risk and compliance status of vendors and business partners.			
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	CONF.01	A Data Classification Policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	No exceptions noted.		
		CONF.02	Confidential or personal information involved in business processes, systems, and third-party involvement is identified and tracked.			
		CONF.03	Documented data retention and disposal policies and procedures are in place to guide personnel in retention and disposal of confidential information.			
		CONF.04	Emburse has established policies to protect against unauthorized and willful acquisition, use, or disposal of assets.			
		CONF.05	Computer drives are securely destroyed using third-party data destruction service providers. Certificates of destruction are retained.			



B. Description of Test of Controls and Results

Test procedures performed in connection with determining the operating effectiveness of controls detailed here in Section IV are described below:

Test Procedure		Description
Inquiry	>	Inquiry of appropriate personnel and corroboration with management.
Observation	>	Observation of the application, performance, or existence of the control.
Inspection	>	Inspection of documents and reports indicating performance of the control.
Reperformance	>	Reperformance of the control.

In addition, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.



Emburse #	Controls Specified by Emburse	Tests Performed by Moss Adams LLP	Test Results
AM.01	Users are assigned a password to access Emburse systems. Passwords must be configured in accordance with the Emburse Password Policy.	Inquired of the Senior Manager, Information Technology about the user access noting that users were assigned a password to access Emburse systems. Also noted that passwords must be configured in accordance with the Emburse Password Policy.	No exceptions noted.
		Inspected the Emburse Password Policy noting that the Emburse Password Policy defined the password requirements to access Emburse systems.	No exceptions noted.
		Inspected the password policies for Okta and AWS application noting that passwords to Emburse systems were configured in accordance with the Emburse Password Policy. Also noted that customers were able to establish their own password configurations.	No exceptions noted.
		Inspected the password configurations for the Abacus & Emburse Spend application noting that passwords were required.	No exceptions noted.



Emburse #	Controls Specified by Emburse	Tests Performed by Moss Adams LLP	Test Results
AM.02	Infrastructure components and software are configured to require unique usernames and passwords. Privileged access requires multi-factor authentication.	Inquired of the Senior Manager, Information Technology about authentication requirements noting that infrastructure components and software were configured to require unique usernames and passwords. Also noted that privileged access required multi-factor authentication.	No exceptions noted.
		Inspected the system-generated user lists for the in-scope systems noting that users were assigned unique usernames.	No exceptions noted.
		Inspected the password policies for Okta and AWS noting that passwords to Emburse systems were configured in accordance with the Emburse Password Policy.	No exceptions noted.
		Inspected the password policies to the domain, and AWS noting that infrastructure components and software were configured to require passwords.	No exceptions noted.
		Observed remote access to the Emburse environment with the Senior Manager, Information Technology noting that remote access to Emburse systems required multi-factor authentication to VPN to the Emburse network along with the employee's authentication credentials.	No exceptions noted.
AM.03	For all users, to obtain system access, a request must be submitted in the ticketing system by HR or the employee's manager.	Inquired of the Senior Manager, Information Technology noting that for all users, to obtain system access, a request was submitted in the ticket system by HR or the employee's manager.	No exceptions noted.
		Inspected access tickets for randomly selected new employees and contractors provisioned during the examination period noting that tickets were submitted by HR or the employee's manager and access was provisioned as requested.	No exceptions noted.



Emburse #	Controls Specified by Emburse	Tests Performed by Moss Adams LLP	Test Results
AM.04	Upon notification of employee end date, a termination ticket is created in the ticketing system by HR personnel. Terminated user access is removed within 24 business hours of termination.	Inquired of the Senior Manager, Information Technology about the termination process noting that upon notification of employee end date, a termination ticket was created in the ticketing system by HR personnel. Also noted that terminated user access was removed within 24 business hours of termination.	No exceptions noted.
		Inspected tickets and evidence of access removal for terminated employees and contractors during the examination period noting that upon notification of employee end date, a termination ticket was created in the ticketing system by HR personnel. Also noted that terminated user access was removed within 24 business hours of termination.	Logical access for two of 10 randomly selected terminated contractors was not removed within 24 business hours of termination. See Section V - Other Information Provided by Emburse That Is Not Covered by the Service Auditor's Report for management response to
			the noted exception.
AM.05	On a quarterly basis, the IT and operations teams conduct a review of all personnel with access to system resources.	Inquired of the Senior Information Security Manager about user access reviews noting that on a quarterly basis, the IT and operations teams conducted a review of all personnel with access to system resources.	No exceptions noted.
		Inspected user access reviews for randomly selected quarters during the examination period noting that on a quarterly basis, the IT and operations teams conducted a review of all personnel with access to system resources.	No exceptions noted.
AM.06	Privileged access to sensitive resources is restricted to individuals in DevOps, Site Reliability Engineering (SRE), and Technical Support roles.	Inquired of the Principal Solutions Architect and the DevSecOps Engineer II about privileged access noting that privileged access to sensitive resources was restricted to individuals in DevOps, SRE, and Technical Support roles.	No exceptions noted.
		Inspected a system-generated report of users with access to AWS noting that privileged access to sensitive resources was restricted to individuals in DevOps, SRE, and Technical Support roles.	No exceptions noted.



Emburse #	Controls Specified by Emburse	Tests Performed by Moss Adams LLP	Test Results
AM.08	Remote access to Emburse systems requires multi-factor authentication to VPN to the Emburse network along with employee's authentication credentials.	Inquired of the Senior Manager, Information Technology about VPN multi-factor authentication noting that remote access to Emburse systems required multi-factor authentication to VPN to the Emburse network along with the employee's authentication credentials.	No exceptions noted.
		Observed remote access to the Emburse environment with the Senior Manager, Information Technology noting that remote access to Emburse systems required multi-factor authentication to VPN to the Emburse network along with the employee's authentication credentials.	No exceptions noted.
AM.09	A role-based security process has been defined with an access control system that is required to use roles when possible.	Inquired of the Senior Manager, Information Technology about role-based security noting that a role-based security process had been defined with an access control system that is required to use roles when possible.	No exceptions noted.
		Inspected the user listings for the in-scope systems noting that a role-based security process had been defined with an access control system that was required to use roles when possible.	No exceptions noted.
AM.10	Logical access to the administration console and database is restricted to application and database administrators.	Inquired of the DevSecOps Engineer III about access to the administration console and database noting that logical access to the administration console and database was restricted to application and database administrators.	No exceptions noted.
		Inspected the list of users with logical access to the administration console and database noting that logical access to the administration console and database was restricted to application and database administrators	No exceptions noted.
AM.11	Only IT personnel are permitted to create or modify user access and user access privileges.	Inquired of the Senior Manager, Information Technology about creating and modifying users' access noting that only IT personnel were permitted to create or modify user access and user access privileges.	No exceptions noted.
		Inspected the listing of Okta administrative users noting that only IT personnel were permitted to create or modify user access and user access privileges.	No exceptions noted.



Emburse #	Controls Specified by Emburse	Tests Performed by Moss Adams LLP	Test Results
BP.1	Backup snapshots are created for production database clusters.	Inquired of the DevSecOps Engineer III about backup snapshots for the production database clusters noting that backup snapshots were created for production database clusters.	No exceptions noted.
		Inspected the AWS backup configuration settings noting that backup snapshots were created for production database clusters.	No exceptions noted.
CM.01	Formally documented change management procedures are in place to govern the implementation, modification and maintenance of production systems and address security, confidentiality, and availability requirements.	Inquired of the Senior Manager, Software Engineering about change management procedures noting that formally documented change management procedures were in place to govern the implementation, modification and maintenance of production systems and address security, confidentiality, and availability requirements.	No exceptions noted.
		Inspected the change management procedures noting that formally documented change management procedures were in place to govern the implementation, modification and maintenance of production systems and address security, confidentiality, and availability requirements.	No exceptions noted.
CM.02	Emburse requires all changes to be documented in the ticketing application and tracked from initiation through deployment and validation. Code reviews are completed at the time of the merge.	Inquired of the Staff Engineer about change documentation noting that Emburse required all changes to be documented in the ticketing application and tracked from initiation through deployment and validation. Also noted that code reviews were completed at the time of the merge.	No exceptions noted.
		Inspected changes and associated tickets for randomly selected changes completed during the examination period noting that Emburse required all changes to be documented in the ticketing application and tracked from initiation through deployment and validation. Also noted that code reviews were completed at the time of the merge.	No exceptions noted.



Emburse #	Controls Specified by Emburse	Tests Performed by Moss Adams LLP	Test Results
CM.03	System and regression testing is required prior to approval, and is performed by product teams using approved test plans and test data. Deviations from planned results are analyzed and submitted to the developer for remediation.	Inquired of the Staff Engineer about system and regression testing noting that system and regression testing was required prior to approval, and was performed by product teams using approved test plans and test data. Also noted that deviations from planned results were analyzed and submitted to the developer for remediation.	No exceptions noted.
		Inspected changes and associated tickets for randomly selected changes completed during the examination period noting that system and regression testing was required prior to approval, and was performed by product teams using approved test plans and test data. Also noted that deviations from planned results were analyzed and submitted to the developer for remediation.	No exceptions noted.
CM.04	Production environments are segregated from development and test environments.	Inquired of the Staff Engineer about segregated environments noting that production environments were segregated from development and test environments.	No exceptions noted.
		Inspected AWS VPC configurations noting that production environments were segregated from development and test environments.	No exceptions noted.
CM.06	The ability to approve system changes is restricted to the Software Engineering Team and DevOps.	Inquired of the Staff Engineer about the ability to approve changes noting that the ability to approve system changes was restricted to the Software Engineering Team and DevOps.	No exceptions noted.
		Inspected users with the ability to approve system changes noting that the ability to approve system changes was restricted to the Software Engineering Team and DevOps.	No exceptions noted.
CM.07	Source code management tools are utilized and access is restricted to appropriate personnel.	Inquired of the Staff Engineer about access to the source code management tools noting that source code management tools were utilized and access was restricted to appropriate personnel.	No exceptions noted.
		Inspected lists of users with access to the source code management tools noting that source code management tools were utilized and access was restricted to appropriate personnel.	No exceptions noted.



Emburse #	Controls Specified by Emburse	Tests Performed by Moss Adams LLP	Test Results
CONF.01	A Data Classification Policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inquired of the CISO about the Data Classification Policy noting that a Data Classification Policy was in place to help ensure that confidential data was properly secured and restricted to authorized personnel.	No exceptions noted.
		Inspected the Data Classification Policy noting that a Data Classification Policy was in place to help ensure that confidential data was properly secured and restricted to authorized personnel.	No exceptions noted.
CONF.02	Confidential or personal information involved in business processes, systems, and third-party involvement is identified and tracked.	Inquired of the CISO about identifying and classifying confidential or personal information noting that confidential or personal information involved in business processes, systems, and third-party involvement was identified and tracked.	No exceptions noted.
		Inspected Emburse's tracking of data classification included as part of the system noting that confidential or personal information involved in business processes, systems, and third-party involvement was identified, classified based on severity, and tracked.	No exceptions noted.
CONF.03	Documented data retention and disposal policies and procedures are in place to guide personnel in retention and disposal of confidential information.	Inquired of the Compliance Manager about data retention and disposal policies and procedures noting that documented data retention and disposal policies and procedures were in place to guide personnel in retention and disposal of confidential information. Also noted there were no requests received to delete customer data during the examination period.	No exceptions noted.
		Inspected Emburse's Data Retention Policy noting that a policy was in place providing guidance for the company retention and disposal processes for confidential information.	No exceptions noted.
		Inspected database records for randomly selected customers during the examination period noting that expense data was retained since go live date.	No exceptions noted.

60



Emburse #	Controls Specified by Emburse	Tests Performed by Moss Adams LLP	Test Results
CONF.04	Emburse has established policies to protect against unauthorized and willful acquisition, use, or disposal of assets.	Inquired of the CISO about policies to protect against unauthorized and willful acquisition, use, or disposal of assets noting that Emburse had established policies to protect against unauthorized and willful acquisition, use, or disposal of assets.	No exceptions noted.
		Inspected the Access Management Policy noting that Emburse had established policies to protect against unauthorized and willful acquisition, use, or disposal of assets.	No exceptions noted.
CONF.05	Computer drives are securely destroyed using third-party data destruction service providers. Certificates of destruction are retained.	Inquired of the Senior Manager, Information Technology about asset disposal noting that computer drives were securely destroyed using third-party data destruction service providers. Noted that certificates of destruction were retained. Also noted that there were no hardware disposals during the examination period.	No exceptions noted.
ENC.01	Databases housing sensitive customer data are encrypted at rest.	Inquired of the Principal Solutions Architect and the DevSecOps Engineer III about encryption at rest noting that databases housing sensitive customer data were encrypted at rest.	No exceptions noted.
		Inspected the Cryptography Encryption Policy noting that policies existed to provide guidance for the data classification types and encryption processes.	No exceptions noted.
		Inspected the database encryption settings noting that databases housing sensitive customer data were encrypted at rest.	No exceptions noted.
ENC.02	Encryption keys used by integrated services are encrypted themselves with a unique master key.	Inquired of the Principal Solutions Architect and the DevSecOps Engineer III about encryption key management noting that encryption keys used by integrated services were encrypted themselves with a unique master key.	No exceptions noted.
		Inspected encryption keys used by integrated services noting that encryption keys used by integrated services were encrypted themselves with a unique master key.	No exceptions noted.



Emburse #	Controls Specified by Emburse	Tests Performed by Moss Adams LLP	Test Results
ENC.04	HTTPS, TLS 1.2, and VPN encryption technologies are deployed for transmission of confidential or sensitive information over public networks.	Inquired of the DevSecOps Engineer III about transmission and encryptions of confidential data noting that HTTPS, TLS 1.2, and VPN encryption technologies were deployed for transmission of confidential or sensitive information over public networks.	No exceptions noted.
		Observed the encryption settings noting that HTTPS, TLS 1.2, and VPN encryption technologies were deployed for transmission of confidential or sensitive information over public networks.	No exceptions noted.
HR.01	Emburse has documented the Code of Conduct, which includes ethical standards.	Inquired of the Senior HR Generalist about the Code of Conduct noting that Emburse had documented the Code of Conduct, which included ethical standards.	No exceptions noted.
		Inspected the Code of Conduct noting that Emburse had documented the Code of Conduct, which included ethical standards.	No exceptions noted.
HR.02	The Emburse Code of Conduct Standard is documented and provides guidance to Emburse personnel on any disciplinary action that will be followed for noncompliance.	Inquired of the Senior HR Generalist about personnel compliance noting that the Emburse Code of Conduct Standard was documented and provided guidance to Emburse personnel on any disciplinary action that would be followed for noncompliance.	No exceptions noted.
		Inspected the Emburse Code of Conduct Standard noting that the Emburse Code of Conduct Standard was documented and provided guidance to Emburse personnel on any disciplinary action that would be followed for non-compliance.	No exceptions noted.
HR.03	Human Resources provide separate communication channels, including anonymous channels, for internal personnel to communicate concerns and complaints.	Inquired of the Senior HR Generalist about communication channels noting that Human Resources provided separate communication channels, including anonymous channels, for internal personnel to communicate concerns and complaints.	No exceptions noted.
		Inspected the anonymous reporting tool noting that Human Resources provided separate communication channels, including anonymous channels, for internal personnel to communicate concerns and complaints.	No exceptions noted.



Emburse #	Controls Specified by Emburse	Tests Performed by Moss Adams LLP	Test Results
HR.04	Emburse performs annual performance evaluations, which are tracked within the Company's performance review software.	Inquired of the Senior HR Generalist about annual performance evaluations noting that Emburse performed annual performance evaluations, which were tracked within the Company's performance review software.	No exceptions noted.
		Inspected the annual performance evaluations for randomly selected current employees during the examination period noting that Emburse performed annual performance evaluations, which were tracked within the Company's performance review software.	No exceptions noted.
HR.05	Emburse conducts skill assessments on candidates to assess their ability to complete job responsibilities.	Inquired of the Senior HR Generalist about skill assessments noting that Emburse conducted skill assessments on candidates to assess their ability to complete job responsibilities.	No exceptions noted.
		Inspected skill assessments for randomly selected new employees onboarded during the examination period noting that Emburse conducted skill assessments on candidates to assess their ability to complete job responsibilities.	No exceptions noted.
HR.06	Where permitted by applicable law, prior to employment, personnel undergo background screening including verification against regulatory screening databases.	Inquired of the Senior HR Generalist about background checks noting that where permitted by applicable law, prior to employment, personnel underwent background screening including verification against regulatory screening databases.	No exceptions noted.
		Inspected background checks for randomly selected new employees onboarded during the examination period noting that where permitted by applicable law, prior to employment, personnel underwent background screening including verification against regulatory screening databases.	No exceptions noted.



Emburse #	Controls Specified by Emburse	Tests Performed by Moss Adams LLP	Test Results
HR.07	Employees are required to read and sign an acknowledgement that they will abide by the Code of Conduct standards defined in the Employee Handbook upon hire.	Inquired of the Senior HR Generalist about the Employee Handbook noting that employees were required to read and sign an acknowledgement that they would abide by the Code of Conduct standards defined in the Employee Handbook upon hire.	No exceptions noted.
		Inspected the Code of Conduct standards noting that employees were required to read and sign an acknowledgement that they would abide by the Code of Conduct standards defined in the Employee Handbook upon hire.	No exceptions noted.
		Inspected Employee Handbook acknowledgement for randomly selected new employees onboarded during the examination period noting that Code of Conduct acknowledgements were completed as part of the onboarding process.	No exceptions noted.
HR.08	An organization chart is documented that outlines the reporting lines of Emburse employees.	Inquired of the Senior HR Generalist about organizational charts noting that an organization chart was documented that outlined the reporting lines of Emburse employees.	No exceptions noted.
		Inspected the Emburse organizational charts noting that an organization chart was documented that outlined the reporting lines of Emburse employees.	No exceptions noted.
INC.01	Incident response policies and procedures, which include responsibility and processes for reporting operational failures, incidents, system problems, concerns and user complaints, are published and available to internal users via the intranet.	Inquired of the CISO and the Compliance Manager about the incident response policies and procedures noting that incident response policies and procedures, which included responsibility and processes for reporting operational failures, incidents, system problems, concerns and user complaints, were published and available to internal users via the intranet.	No exceptions noted.
		Inspected the Security Incident Response Plan noting that incident response policies and procedures, which included responsibility and processes for reporting operational failures, incidents, system problems, concerns and user complaints, were published and available to internal users via the intranet.	No exceptions noted.



Emburse #	Controls Specified by Emburse	Tests Performed by Moss Adams LLP	Test Results
INC.02	Internal and external users are informed of relevant incidents in a timely manner and advised of corrective measures to be taken on their part.	Inquired of the CISO and the Compliance Manager about the incident management process noting that internal and external users were informed of relevant incidents in a timely manner and advised of corrective measures to be taken on their part. Also noted that there were no reported security or confidentiality related incidents relevant to the Abacus & Emburse Spend System during the examination period.	No exceptions noted.
		Inspected the Security Incident Response Plan noting that the plan provided guidance that internal and external users were to be informed of relevant incidents in a timely manner and advised of corrective measures to be taken on their part.	No exceptions noted.
INC.03	Annual testing of the incident response plan is performed to ensure the incident response procedures are up-to-date and effective. When updating the incident response plan, lessons learned from incident testing are used to implement changes to reflect effective procedures when handling incidents.	Inquired of the CISO and the Compliance Manager about incident response plan testing noting that annual testing of the incident response plan was performed to ensure the incident response procedures were up-to-date and effective. Also noted that when updating the incident response plan, lessons learned from incident testing were used to implement changes to reflect effective procedures when handling incidents.	No exceptions noted.
	when handing modelts.	Inspected the annual incident response plan testing completed during the examination period noting that annual testing of the incident response plan was performed to ensure the incident response procedures were up-to-date and effective. Also noted that when updating the incident response plan, lessons learned from incident testing were used to implement changes to reflect effective procedures when handling incidents.	No exceptions noted.



Emburse #	Controls Specified by Emburse	Tests Performed by Moss Adams LLP	Test Results
INC.04	All incidents related to the security of the system are logged, tracked, and communicated to affected parties by management until resolved.	Inquired of the CISO and the Compliance Manager about the incident response process noting that all incidents related to the security of the system were logged, tracked, and communicated to affected parties by management until resolved. Also noted that there were no reported security or confidentiality related incidents relevant to the Abacus & Emburse Spend System during the examination period.	No exceptions noted.
		Inspected the Security Incident Response Plan noting that the plan provided guidance that all incidents related to the security of the system were to be logged, tracked, and communicated to affected parties by management until resolved.	No exceptions noted.
INC.05	After an incident has been confirmed, specific personnel are engaged in the containment process to reduce the magnitude of the incident.	Inquired of the CISO and the Compliance Manager about the incident response process noting that after an incident had been confirmed, specific personnel were engaged in the containment process to reduce the magnitude of the incident. Also noted that there were no reported security or confidentiality related incidents relevant to the Abacus & Emburse Spend System during the examination period.	No exceptions noted.
		Inspected the Security Incident Response Plan noting that the plan provided guidance that after an incident had been confirmed, specific personnel were to be engaged in the containment process to reduce the magnitude of the incident.	No exceptions noted.
INC.06	As part of the forensic investigation, the Incident Response Team determines whether sensitive information was used or disclosed.	Inquired of the CISO and the Compliance Manager about the incident management process noting that as part of the forensic investigation, the Incident Response Team determines whether sensitive information was used or disclosed. Also noted that there were no reported security or confidentiality related incidents relevant to the Abacus & Emburse Spend System during the examination period.	No exceptions noted.
		Inspected the Security Incident Response Plan noting that the plan provided guidance that as part of the forensic investigation, the Incident Response Team determined whether sensitive information was used or disclosed.	No exceptions noted.



Emburse #	Controls Specified by Emburse	Tests Performed by Moss Adams LLP	Test Results
INC.07	The Incident Response team classifies reported incidents based on their perceived severity and impact on the organization. The classification is used to determine response procedures.	Inquired of the CISO and the Compliance Manager about the incident management process noting that the Incident Response Team classified reported incidents based on their perceived severity and impact on the organization. Noted that the classification was used to determine response procedures. Also noted that there were no reported security or confidentiality related incidents relevant to Abacus & Emburse Spend System during the examination period.	No exceptions noted.
		Inspected the Security Incident Response Plan noting that the plan provided guidance that Incident Response Team to classify reported incidents based on their perceived severity and impact on the organization. Also noted that the classification was used to determine response procedures.	No exceptions noted.
INC.08	For high severity incidents, a root cause analysis is prepared and reviewed by management. Based on the root cause analysis, change requests are prepared and the entity's risk management process and relevant risk management data is updated to reflect the planned incident and problem resolution, as needed.	Inquired of the CISO and the Compliance Manager about the incident management process noting that for high severity incidents, a root cause analysis was prepared and reviewed by management. Noted that based on the root cause analysis, change requests were prepared, and the entity's risk management process and relevant risk management data were updated to reflect the planned incident and problem resolution, as needed. Also noted that there were no reported security or confidentiality related incidents relevant to the Abacus & Emburse Spend System during the examination period.	No exceptions noted.
		Inspected the Security Incident Response Plan noting that the plan provided guidance which required for high severity incidents, a root cause analysis was prepared and reviewed by management. Also noted that based on the root cause analysis, change requests were prepared and the entity's risk management process and relevant risk management data were updated to reflect the planned incident and problem resolution, as needed.	No exceptions noted.



Emburse #	Controls Specified by Emburse	Tests Performed by Moss Adams LLP	Test Results
INC.09	The Information Security Team periodically provides a report to upper management of relevant security-related activities and incidents. Management monitors for completion of corrective action plans.	Inquired of the CISO and the Compliance Manager about the incident management process that the Information Security team periodically provided a report to upper management of relevant security-related activities and incidents. Noted that management monitored for completion of corrective action plans. Also noted that there were no reported security or confidentiality related incidents relevant to the Abacus & Emburse Spend System during the examination period.	No exceptions noted.
		Inspected the Security Incident Response Plan noting that the plan provided guidance for the Information Security team to provide reports periodically to upper management of relevant security-related activities and incidents. Also noted that management monitored for completion of corrective action plans.	No exceptions noted.
LEG.01	The Emburse legal team maintains a repository of contract terms and commitments. Emburse's contracts administrator is responsible for changes to contractual terms and commitments.	Inquired of the Senior Contract Administrator about communication and evaluation of contract terms and commitments noting that the Emburse legal team maintained a repository of contract terms and commitments. Also noted that Emburse's contracts administrator was responsible for changes to contractual terms and commitments.	No exceptions noted.
		Inspected the job description for the contract administrator noting that Emburse's contracts administrator was responsible for changes to contractual terms and commitments.	No exceptions noted.
		Inspected the contract repository noting that the legal team maintained a repository of contract terms and commitments.	No exceptions noted.



Emburse #	Controls Specified by Emburse	Tests Performed by Moss Adams LLP	Test Results
LEG.03	Emburse's security and confidentiality commitments are established and documented within agreements, defining service provider terms, conditions, and responsibilities.	Inquired of the Senior Contract Administrator about security and confidentiality commitments noting that Emburse's security and confidentiality commitments were established and documented within agreements, defining service provider terms, conditions, and responsibilities.	No exceptions noted.
		Inspected the signed contract agreements for randomly selected new customers onboarded during the examination period noting that Emburse's security and confidentiality commitments were established and documented within agreements, defining service provider terms, conditions, and responsibilities.	No exceptions noted.
LEG.05	Emburse's requirements with respect to security, availability, and confidentiality, and availability of information are included within vendor agreements, defining terms, conditions, and responsibilities.	Inquired of the Senior Manager, Contracts and the Information Security Coordinator about third party contracts noting that Emburse's requirements with respect to security, availability, and confidentiality, and availability of information were included within vendor agreements, defining terms, conditions, and responsibilities.	No exceptions noted.
		Inspected the third-party contracts and annual due diligence documentation for randomly selected Abacus vendors noting that Emburse's requirements with respect to security, availability, and confidentiality, and availability of information were included within vendor agreements, defining terms, conditions, and responsibilities.	No exceptions noted.
MON.01	Documented procedures are in place to direct personnel in monitoring the system performance and availability.	Inquired of the DevSecOps Engineer II about the documented procedures for monitoring system performance and availability noting that documented procedures were in place to direct personnel in monitoring the system performance and availability.	No exceptions noted.
		Inspected Confluence pages where documented procedures were posted noting that documented procedures were in place to direct personnel in monitoring the system performance and availability.	No exceptions noted.



Emburse #	Controls Specified by Emburse	Tests Performed by Moss Adams LLP	Test Results
MON.02	A cloud infrastructure monitoring tool is utilized to monitor cloud infrastructure availability and performance and generates alerts when specific predefined thresholds are met.	Inquired of the DevSecOps Engineer II and the System Operations Engineer about availability and performance monitoring noting that a cloud infrastructure monitoring tool was utilized to monitor cloud infrastructure availability and performance and generated alerts when specific predefined thresholds were met.	No exceptions noted.
		Inspected the cloud infrastructure monitoring tool and alert logs for alerts that occurred during the examination period noting that a cloud infrastructure monitoring tool was utilized to monitor cloud infrastructure availability and performance and generated alerts when specific predefined thresholds were met. Also noted that alert logs were available for alert logs that occurred during the examination period.	No exceptions noted.
MON.03	Internal control assessments are performed on an annual basis and communicated during the Information Security Committee meeting.	Inquired of the CISO and the Compliance Manger about the internal control assessments noting that internal control assessments were performed on an annual basis and communicated during the Information Security Committee meeting.	No exceptions noted.
		Inspected the internal controls assessment noting that internal control assessments were performed on an annual basis. Also noted that the CISO communicated internal control results and corrective actions during the Information Security Committee meeting.	No exceptions noted.
MON.04	Monitoring tools are used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	Inquired of the Principal Solutions Architect about monitoring noting that monitoring tools were used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	No exceptions noted.
		Inspected the monitoring tools noting that monitoring tools were used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	No exceptions noted.



Emburse #	Controls Specified by Emburse	Tests Performed by Moss Adams LLP	Test Results
MON.05	The monitoring solutions send messages to the operations center. Where escalation is required, the team opens an incident ticket, which is followed through to resolution.	Inquired of the Principal Solutions Architect about incidents requiring escalation noting that the monitoring solution sent messages to the operations center. Also noted that where escalation was required, the team opened an incident ticket, which was followed through to resolution.	No exceptions noted.
		Inspected the monitoring solution configurations and alerts received during the examination period noting the monitoring solution sent messages to the operations center. Noted that where escalation was required, the team opened an incident ticket, which was followed through to resolution. Also noted that alerts were received throughout the examination period.	No exceptions noted.
		Inspected the internal procedure documents and on-call schedule for the Operations team throughout the examination period noting that guidance was available for problem resolution. Also noted that team members were on-call 24x7x365 throughout the examination period.	No exceptions noted.
MON.07	Management evaluates the Business Continuity Plan for any needed additional tools and resources to achieve business objectives including contingency plans for assignments of responsibility important for internal control.	Inquired of the CISO and the Compliance Manager about evaluation of the Business Continuity Plan noting that management evaluated the Business Continuity Plan for any needed additional tools and resources to achieve business objectives including contingency plans for assignments of responsibility important for internal control.	No exceptions noted.
		Inspected the Business Continuity Plan noting that management evaluated the Business Continuity Plan for any needed additional tools and resources to achieve business objectives including contingency plans for assignments of responsibility important for internal control.	No exceptions noted.



Emburse #	Controls Specified by Emburse	Tests Performed by Moss Adams LLP	Test Results
OPS.01	A VPC is in place and configured to secure the perimeter of the environment. VPC access, configurations, and security events are logged through AWS CloudTrail. Administrative access privileges to the VPC are limited to operations personnel.	Inquired of the Site Reliability Engineer II and the Principal Solutions Architect about the VPC and administrative access privileges noting that a VPC was in place and configured to secure the perimeter of the environment. Noted that VPC access, configurations, and security events were logged. Also noted that administrative access privileges to the VPC were limited to operations personnel.	No exceptions noted.
		Observed VPC configurations and results of the network segmentation testing noting that VPC and security groups were configured to secure the perimeter of the environment.	No exceptions noted.
		Inspected the monitoring tools noting that monitoring tools were used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity.	No exceptions noted.
		Inspected the monitoring solution configurations and alerts received during the examination period noting the monitoring solution sent messages to the operations center. Noted that where escalation was required, the team opened an incident ticket, which was followed through to resolution. Also noted that alerts were received throughout the examination period.	No exceptions noted.
		Inspected the system-generated list of users with access to the security groups noting that administrative access to the VPC was limited to operations personnel.	No exceptions noted.
OPS.02	End user and server workload network traffic is segmented to support isolation.	Inquired of the DevSecOps Engineer III about network traffic isolation noting that end user and server workload network traffic was segmented to support isolation.	No exceptions noted.
		Inspected the AWS VPC configurations noting that end user and server workload network traffic was segmented to support isolation.	No exceptions noted.



Emburse #	Controls Specified by Emburse	Tests Performed by Moss Adams LLP	Test Results
OVS.01	The Board of Directors consists of a majority of independent members to maintain independence from Emburse management. Meetings occur on a quarterly basis.	Inquired of the CISO about the Board of Directors noting that the Board of Directors consisted of a majority of independent members to maintain independence from Emburse management. Also noted that meetings occurred on a quarterly basis.	No exceptions noted.
		Inspected the list of Board of Directors members noting that the Board of Directors consisted of a majority of independent members to maintain independence from Emburse management.	No exceptions noted.
		Inspected Board of Director meeting invites for randomly selected quarters during the examination period noting that meetings occurred on a quarterly basis and meeting minutes were retained.	No exceptions noted.
OVS.02	Upper management holds monthly security meetings to monitor and manage departments' progress or lack thereof as it relates to their achievement of the departments' responsibilities.	Inquired of the CISO about the security meetings noting that upper management held monthly security meetings to monitor and manage departments' progress or lack thereof as it related to their achievement of the departments' responsibilities.	No exceptions noted.
	acparation responsibilities.	Inspected security meeting agendas for randomly selected months during the examination period noting that upper management held monthly security meetings to monitor and manage departments' progress or lack thereof as it related to their achievement of the departments' responsibilities.	No exceptions noted.



Emburse #	Controls Specified by Emburse	Tests Performed by Moss Adams LLP	Test Results
POL.01	Policy and procedure documents relating to significant processes are available to Emburse personnel on the organization's intranet. Annually, employees and contractors are required to acknowledge the Information Security Policy.	Inquired of the CISO about policies and procedures noting that policy and procedures documents for significant processes were made available to personnel via Emburse's intranet. Also noted that annually, employees and contractors were required to acknowledge the Information Security Policy.	No exceptions noted.
	miormation Security Folicy.	Inspected policies and procedures documents noting that policy and procedures documents for significant processes were made available to personnel via Emburse's intranet.	No exceptions noted.
		Inspected the records of the annual security awareness training which included Information Security Policy acknowledgement for randomly selected current employees during the examination period noting that security awareness training was completed annually, and the Information Security Policy was acknowledged.	No exceptions noted.
		Inspected the records of the annual security awareness training which included Information Security Policy acknowledgement for randomly selected current contractors during the examination period noting that security awareness training was completed annually, and the Information Security Policy was acknowledged.	No exceptions noted.
POL.02	Formal information security policies are available on the intranet and provide procedures on security of user accounts, user authentication, and monitoring.	Inquired of the Senior Manager, Information Technology about information security policies noting that formal information security policies were available on the intranet and provide procedures on security of user accounts, user authentication, and monitoring.	No exceptions noted.
		Inspected the Access Management Policy and its location on the intranet noting that formal information security policies were available on the intranet and provided procedures on security of user accounts, user authentication, and monitoring.	No exceptions noted.



Emburse #	Controls Specified by Emburse	Tests Performed by Moss Adams LLP	Test Results
POL.03	Emburse policies and procedures are reviewed annually, or as needed, by upper management or their designees, including by the CISO where required, for consistency with the organization's risk management strategy and updated as necessary for changes in the strategy.	Inquired of the CISO about policies and procedures reviews noting that Emburse policies and procedures were reviewed annually, or as needed, by upper management or their designees, including by the CISO where required, for consistency with the organization's risk management strategy and updated as necessary for changes in the strategy. Inspected policies and procedures reviews noting that Emburse policies and procedures were reviewed annually, or as needed, by upper management or their designees, including by the CISO where required, for consistency with the organization's risk management strategy and updated as necessary for changes in the strategy.	No exceptions noted. No exceptions noted.
POL.04	Emburse's Chief Information Security Officer (CISO) and Information Security Committee are responsible for establishing, maintaining, and enforcing the overall security policies and procedures, including incident response and vendor risk assessment policy.	Inquired of the CISO about the CISO and Information Security Committee responsibilities noting that Emburse's CISO and Information Security Committee were responsible for establishing, maintaining, and enforcing the overall security policies and procedures, including incident response and vendor risk assessment policy. Inspected the Information Security Committee Charter noting that Emburse's CISO and Information Security Committee were responsible for establishing, maintaining, and enforcing the overall security policies and procedures, including incident response and vendor risk assessment policy.	No exceptions noted. No exceptions noted.



Emburse #	Controls Specified by Emburse	Tests Performed by Moss Adams LLP	Test Results
RM.01	A company-wide risk assessment is performed annually by the security team, to identify risks arising from external and internal sources. Risks, including fraud risks, are tracked in a risk assessment table which documents mitigation strategies, remediation plans and assigned owners.	Inquired of the CISO about the company-wide risk assessment noting that a company-wide risk assessment was performed annually by the security team, to identify risks arising from external and internal sources. Also noted that risks, including fraud risks, were tracked in a risk assessment table which documented mitigation strategies, remediation plans and assigned owners.	No exceptions noted.
		Inspected the company risk assessment noting that a company- wide risk assessment was performed annually by the security team, to identify risks arising from external and internal sources. Also noted that risks, including fraud risks, were tracked in a risk assessment table which documented mitigation strategies, remediation plans and assigned owners.	No exceptions noted.
RM.02	Emburse's Information Security Committee meets quarterly to provide oversight for the organization's processes and commitments, review the results of the risk assessment, and evaluate any security or confidentiality-related incidents.	Inquired of the CISO and the Compliance Manager about the Information Security Committee quarterly meetings noting that Emburse's Information Security Committee met quarterly to provide oversight for the organization's processes and commitments, review the results of the risk assessment, and evaluate any security or confidentiality-related incidents.	No exceptions noted.
		Inspected Information Security Committee meeting slides for randomly selected quarters during the examination period noting that Emburse's Information Security Committee met quarterly to provide oversight for the organization's processes and commitments, review the results of the risk assessment, and evaluate any security or confidentiality-related incidents.	No exceptions noted.



Emburse #	Controls Specified by Emburse	Tests Performed by Moss Adams LLP	Test Results
RM.03	A documented risk assessment and Risk Treatment Methodology is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inquired of the CISO and the Compliance Manager about the risk assessment and Risk Treatment Methodology noting that a documented risk assessment and Risk Treatment Methodology was in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
		Inspected Emburse's risk assessment noting that a documented risk assessment was in place that included identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
		Inspected Emburse's risk assessment methodology policy noting that a documented Risk Treatment Methodology was in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
RM.04	The risk management program includes the use of insurance to minimize the financial impact of any loss events.	Inquired of the CISO and the Compliance Manager about the risk management program noting that the risk management program included the use of insurance to minimize the financial impact of any loss events.	No exceptions noted.
		Inspected the certificates of liability insurance noting that liabilities policies were in place to minimize the financial impact of any loss events.	No exceptions noted.



Emburse #	Controls Specified by Emburse	Tests Performed by Moss Adams LLP	Test Results
SUP.05	Emburse customer-facing website includes a Support page with a customer support form and links to assist customers with reporting any operational failures, incidents, problems, concerns, and complaints.	Inquired of the Director, Services and the Manager, Site Reliability Engineer about customer support resources noting that the Emburse customer-facing website included a support page with a customer support form and links to assist customers with reporting any operational failures, incidents, problems, concerns, and complaints.	No exceptions noted.
		Inspected the customer-facing website noting that customer responsibilities, which included responsibility for reporting operational failures, incidents, problems, concerns, and complaints, and Emburse contact information, were available on the customer-facing website.	No exceptions noted.
TPRM.01	Service providers are subject to review as part of the vendor risk assessment process. Attestations and certifications are obtained and evaluated on an annual basis.	Inquired of the CISO and the Information Security Coordinator about vendor evaluation process noting that service providers were subject to review as part of the vendor risk assessment process. Also noted that attestations and certifications were obtained and evaluated on an annual basis.	No exceptions noted.
		Inspected annual due diligence completed for randomly selected Abacus vendors during the examination period noting that service providers were subject to review as part of the vendor risk assessment process. Also noted that attestations and certifications were obtained and evaluated on an annual basis.	No exceptions noted.
TPRM.02	The Company's Information Security Team is responsible for assessing and monitoring risk and compliance status of vendors and business partners.	Inquired of the CISO and the Information Security Coordinator about vendors and business partners noting that the Company's Information Security Team was responsible for assessing and monitoring risk and compliance status of vendors and business partners.	No exceptions noted.
		Inspected the Third Party Risk Management Policy noting that policies and procedures defined the company's Information Security Team was responsible for assessing and monitoring risk and compliance status of vendors and business partners.	No exceptions noted.



Emburse #	Controls Specified by Emburse	Tests Performed by Moss Adams LLP	Test Results
TRAIN.01	Emburse has a security awareness training program that includes annual security awareness training and simulated phishing campaigns to improve security knowledge and awareness and to model appropriate security behaviors.	Inquired of the CISO about security awareness training noting that Emburse had a security awareness training program that included annual security awareness training and simulated phishing campaigns to improve security knowledge and awareness and to model appropriate security behaviors.	No exceptions noted.
		Inspected the Security Awareness training materials and phishing campaign results noting that Emburse had a security awareness training program that included annual security awareness training and simulated phishing campaigns to improve security knowledge and awareness and to model appropriate security behaviors.	No exceptions noted.
		Inspected the records of the annual security awareness training which included Information Security Policy acknowledgement for randomly selected current employees during the examination period noting that security awareness training was completed annually, and the Information Security Policy was acknowledged.	No exceptions noted.
		Inspected the records of the annual security awareness training which included Information Security Policy acknowledgement for randomly selected current contractors during the examination period noting that security awareness training was completed annually, and the Information Security Policy was acknowledged.	No exceptions noted.



Emburse #	Controls Specified by Emburse	Tests Performed by Moss Adams LLP	Test Results
TXN.01	Emburse has a documented description of its Expense Management System that details relevant system components and design of the system. The description is made available to authorized internal users via system and on Emburse's intranet, and to external users on Emburse public websites.	Inquired of the Compliance Manager about documented system descriptions noting that Emburse had a documented description of its Expense Management System that detailed relevant system components and design of the system. Also noted that the description was made available to authorized internal users via system and on Emburse's intranet, and to external users on Emburse public websites. Inspected the Company's intranet and public website noting that Emburse had a documented description of its Expense	No exceptions noted. No exceptions noted.
		Management System that detailed relevant system components and design of the system. Also noted that the description was made available to authorized internal users via system and on Emburse's intranet, and to external users on Emburse public websites.	
TXN.02	Emburse maintains a transaction flow diagram that demonstrates how sensitive data moves throughout the organization.	Inquired of the Principal Solutions Architect about transaction flow diagrams noting that Emburse maintained a transaction flow diagram that demonstrated how sensitive data moved throughout the organization.	No exceptions noted.
		Inspected the transaction flow diagram noting that Emburse maintained a transaction flow diagram that demonstrated how sensitive data moved throughout the organization.	No exceptions noted.
VULN.01	During quarterly Information Security Committee meetings, management assesses the scope and frequency of vulnerability assessments, including penetration testing and vulnerability scanning.	Inquired of the IT Security Engineer about Information Security Committee meetings noting that during quarterly Information Security Committee meetings, management assessed the scope and frequency of vulnerability assessments, including penetration testing and vulnerability scanning.	No exceptions noted.
	Joanning.	Inspected quarterly meeting minutes and agendas for randomly selected quarters during the examination period noting that during monthly Information Security Committee meetings, management assessed the scope and frequency of vulnerability assessments, including penetration testing and vulnerability scanning.	No exceptions noted.



Emburse #	Controls Specified by Emburse	Tests Performed by Moss Adams LLP	Test Results
VULN.02	External penetration tests are conducted annually and management initiates corrective actions for identified vulnerabilities. Results and recommendations from these assessments for improvement are reported to management, which initiates corrective actions.	Inquired of the IT Security Engineer about penetration tests noting that external penetration tests were conducted annually and management initiated corrective actions for identified vulnerabilities. Also noted that results and recommendations from these assessments for improvement were reported to management, which initiated corrective actions. Inspected the annual penetration test and supporting tickets for corrective actions noting that external penetration tests were conducted annually and management initiated corrective actions for identified vulnerabilities. Also noted that results and recommendations from these assessments for improvement were reported to management.	No exceptions noted. No exceptions noted.
VULN.03	Internal and external vulnerability scans are performed at least quarterly.	Inquired of the IT Security Engineer about vulnerability scans noting that internal and external vulnerability scans were performed at least quarterly. Inspected internal and external vulnerability scans for randomly selected quarters during the examination period noting that internal and external vulnerability scans were performed at least quarterly. Also noted that the identified vulnerabilities were tracked through resolution.	No exceptions noted. No exceptions noted.
VULN.04	Anti-malware technology is installed on assets placed into production and end points.	Inquired of the Senior Manager, Information Technology and the Principal Solutions Architect about anti-malware software and monitoring of software installations noting that anti-malware technology was installed on the assets placed into production and end points. Inspected the system-generated report from CrowdStrike noting that anti-malware technology was installed on assets placed into production.	No exceptions noted. No exceptions noted.
		Inspected the system-generated report from CrowdStrike for randomly selected current employees during the examination period noting that anti-malware technology was deployed on end points.	No exceptions noted.



V. Other Information Provided by Emburse That Is Not Covered by the Service Auditor's Report

The following information is provided for informational purposes only and has not been subjected to the procedures applied in the examination. Accordingly, Moss Adams expresses no opinion on the following information.

A. Management's Response to Identified Testing Exceptions

Emburse #	Controls Specified by Emburse	Exception Noted by Moss Adams LLP	Emburse Management Response
AM.04	Upon notification of employee end date, a termination ticket is created in the ticketing system by HR personnel. Terminated user access is removed within 24 business hours of termination.	Logical access for two of 10 randomly selected terminated contractors was not removed within 24 business hours of termination.	Access for the two terminated contractors was removed outside of the 24 business hours policy due to managers not timely notifying HR and IT. Once HR and IT were notified access was appropriately removed. Management reviewed these accounts and determined that the accounts were not accessed post-termination date. Management has worked with individual managers and provided training to reinforce the importance of timely notification to HR for terminated contractors to ensure the termination process is completed within 24 hours.

