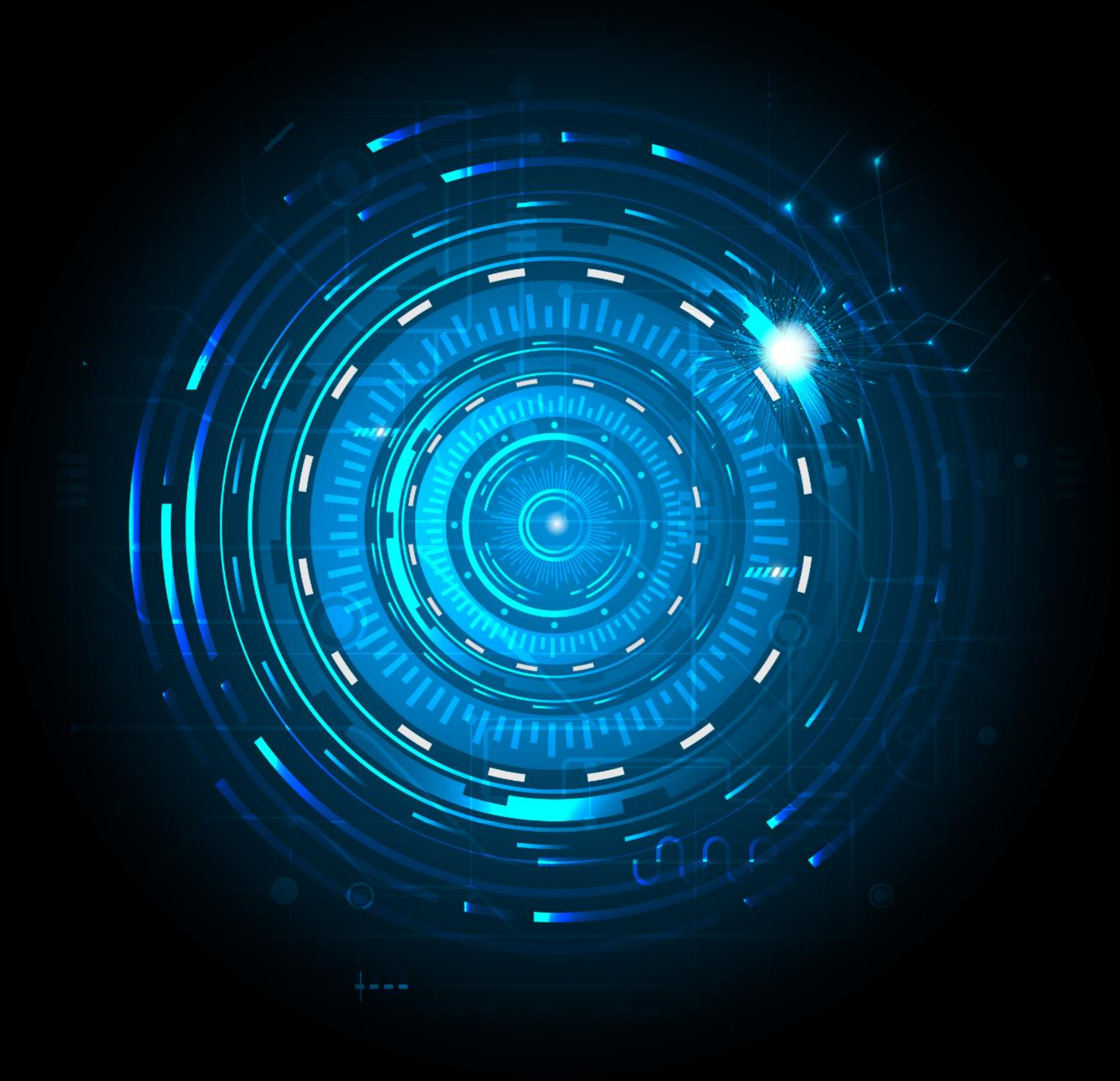
EPAM Systems, Inc.



SOC 2 (ISAE 3000) Type 2

Report for security, availability and confidentiality
on controls placed in operation and
tests of operating effectiveness for the period

May 1, 2025 to October 31, 2025

This page is intentionally left blank

Executive Summary

SOC 2 (ISAE 3000) Type 2

Scope	**Mobitru**
Period of examination	**May 1, 2025 to October 31, 2025**
Applicable Trust Principles	• **Common Criteria (Security)** • **Availability** • **Confidentiality**
Subservice providers	**N/A**
Opinion Result	**Unqualified**
Testing Exceptions	**1**

This report is intended solely for the information and use of the management of EPAM, its clients who have used EPAM's services, and the independent auditors of its clients, and is not intended to be, AND SHOULD NOT BE, USED BY ANYONE OTHER THAN THESE SPECIFIED PARTIES.

Contents

1. Independent Service Auditor’s Report

Independent Service Auditor’s Assurance Report on the Description of Controls, their Design and Operating Effectiveness

To the Board of Directors of EPAM Systems Inc.

Scope

We have examined the attached description of the system of EPAM Systems Inc.’s (NYSE: EPAM) (hereafter ‘EPAM’ or the ’Service Organization’) internal control system relating to Mobitru. We have performed our examination based on the criteria for a description of a service organization’s system set forth in DC Section 200, 2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2® Report (“description criteria”), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period May 1, 2025 to October 31, 2025, to provide reasonable assurance that EPAM’s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality (“applicable trust services criteria”) set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

The information included in Section 5, is presented by management of EPAM to provide additional information and is not a part of the description. Information about additional information provided by EPAM has not been subjected to the procedures applied in the examination of the description and the suitability of the design and operating effectiveness of the controls, to achieve EPAM’s service commitments and system requirements based on the applicable trust services criteria.

EPAM uses Amazon Web Services (“subservice organization”) that is providing corporate IT infrastructure with a professional environment to house EPAM Cloud solutions. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at EPAM, to achieve EPAM’s service commitments and system requirements based on the applicable trust services criteria. The description presents EPAM’s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of EPAM’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 and 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 EPAM, to achieve EPAM's service commitments and system requirements based on the applicable trust services criteria. The description presents EPAM's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of EPAM'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.

EPAM's Responsibilities

EPAM 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 EPAM's service commitments and system requirements were achieved. EPAM has provided the accompanying assertion titled "Assertion by EPAM Systems Inc." (the "assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. EPAM 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. We conducted our engagement in accordance with International Standard on Assurance Engagements 3000, "International Framework for Assurance Engagements and Related Conforming Amendments," issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria, and the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the Service Organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our conclusion.

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

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

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

Our Independence and Quality Control

We have complied with the independence and other ethical requirements of the Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior. The firm applies International Standard on Quality Management 1 and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Limitations of Controls at a Service Organization

The description is prepared to meet the common needs of a broad range of 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 the 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.

Conclusion

In our opinion, in all material respects,

a. The description presents EPAM's internal control system relating to Mobitru application environment that was designed and implemented throughout the May 1, 2025 to October 31, 2025 in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period May 1, 2025 to October 31, 2025, to provide reasonable assurance that EPAM's service commitments and systems requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively throughout that period and the subservice organization and user entities applied the complementary controls assumed in the design of EPAM's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period May 1, 2025 to October 31, 2025, to provide reasonable assurance that EPAM's service commitments and system requirements were achieved based on the applicable trust services criteria and if complementary subservice organization controls and complementary user entity controls assumed in the design of EPAM's controls operated effectively throughout that period.

Intended Users and Purpose

This report , including the description of tests of controls and results thereof in Section 4 is intended solely for the information and use of EPAM, user entities of the system of EPAM during some or all of the period May 1, 2025 to October 31, 2025, business partners of EPAM subject to risks arising from interactions with EPAM's 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 they interact with related controls at the Service Organization to achieve the Service Organization's 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.

Budapest, January 30, 2026

Tamás Horváth

On behalf of

Deloitte Auditing and Consulting Ltd.

2. Assertion by EPAM Systems Inc.

The accompanying description has been prepared for the customers relied on EPAM's Mobitru services and their auditors who have a sufficient understanding to consider the description, along with other information including information about controls operated by customers themselves, when assessing the risks arising from interactions with EPAM's system, particularly information about system controls that EPAM 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 set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy ("applicable trust services criteria").

Assertion of EPAM Systems, Inc.

We have prepared the description of the system in Section 3 of EPAM (the "Service Organization") throughout the period May 1, 2025, to October 31, 2025, (the "period") related to Mobitru service, based on 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 ("description criteria").The description is intended to provide users with information about our system that may be useful when assessing the risks arising from interactions with EPAM's system, particularly information about system controls that EPAM 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 set forth in TSP Section 100, 2017 *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* ("applicable trust services criteria").

EPAM uses Amazon Web Services ("subservice organization") that is providing corporate IT infrastructure with a professional environment to house EPAM Cloud solutions. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at EPAM, to achieve EPAM's service commitments and system requirements based on the applicable trust services criteria. The description presents EPAM's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of EPAM'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 and 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 EPAM, to achieve EPAM's service commitments and system requirements based on the applicable trust services criteria. The description presents EPAM's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of EPAM's controls.

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

a. The description presents EPAM's system that was designed and implemented throughout the period May 1, 2025, to October 31, 2025, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period May 1, 2025, to October 31, 2025, to provide reasonable assurance that EPAM's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and if user entities applied the complementary controls assumed in the design of EPAM's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period May 1, 2025, to October 31, 2025, to provide reasonable assurance that EPAM's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization and user entity controls assumed in the design of EPAM's controls operated effectively throughout that period.

Newtown, January 30, 2026

Jason Peterson, Chief Financial Officer
EPAM Systems Inc.

3. System Description by EPAM Systems Inc.

3.1. TYPES OF SERVICES PROVIDED

3.1.1 Overview of Operations - EPAM Systems Inc.

Since 1993, EPAM Systems, Inc. (NYSE: EPAM) has used its software engineering expertise to become a leading global provider of digital engineering, cloud and AI-enabled transformation services, and a leading business and experience consulting partner for global enterprises and ambitious startups. We address our clients' transformation challenges by fusing EPAM Continuum's integrated strategy, experience and technology consulting with our 30+ years of engineering execution to speed our clients' time to market and drive greater value from their innovations and digital investments.

We leverage AI and GenAI to deliver transformative solutions that accelerate our clients' digital innovation and enhance their competitive edge. Through platforms like EPAM AI/RUN™ and initiatives like DIALX Lab, we integrate advanced AI technologies into tailored business strategies, driving significant industry impact and fostering continuous innovation.

We deliver globally, but engage locally with our expert teams of consultants, architects, designers and engineers, making the future real for our clients, our partners and our people around the world.

We believe the right solutions are the ones that improve people's lives and fuel competitive advantage for our clients across diverse industries. Our thinking comes to life in the experiences, products and platforms we design and bring to market.

Added to the S&P 500 and the Forbes Global 2000 in 2021 and recognized by Glassdoor and Newsweek as Most Loved Workplace, our multidisciplinary teams serve customers across six continents. We are proud to be among the top 15 companies in Information Technology Services in the Fortune 1000 and to be recognized as a leader in the IDC MarketScapes for Worldwide Experience Build Services, Worldwide Experience Design Services and Worldwide Software Engineering Services.

Learn more at www.epam.com and follow us on LinkedIn.

3.1.2 Description of Mobitru

3.1.2.1 Overview

Mobitru is EPAM’s cloud-based application testing and development platform designed to provide secure remote access to real execution environments for software development, quality assurance, automation, and debugging activities.

The platform enables authorized users to interact with and execute manual and automated tests on real mobile devices (iOS and Android) and desktop browser environments through a centralized web interface, APIs, and integrations with development and CI/CD tools. Automated testing is supported through industry-standard automation frameworks, while manual testing is performed through interactive device and browser sessions.

Mobitru supports both Software-as-a-Service (SaaS) and customer-managed (private cloud or on-premises) deployment models, allowing customers to align platform usage with internal security, compliance, and infrastructure requirements.

The platform provides controlled capabilities for executing tests and collecting testing artifacts, including logs, screenshots, videos, and execution metadata generated during testing sessions. Testing may be performed under configurable conditions, such as network configuration, geolocation settings, device sensors, and media inputs, to validate application behaviour across different environments.

Mobitru includes AI-assisted functionality intended to support testing workflows, such as analysis of testing artifacts and generation of supporting testing or development outputs. AI-assisted features are executed through controlled AI execution services (MCP servers) operating within EPAM-managed or customer-managed environments. These services process customer-generated testing data within the boundaries of configured environments, access controls, and audit logging, and do not alter customer application logic or production systems.

Mobitru is designed to support distributed development and quality assurance teams and includes controls for authentication, authorization, session isolation, logging, and operational monitoring. Customer data processed by the platform is limited to application binaries, configuration data, and testing artifacts required to provide the described services.

The Mobitru system is operated in accordance with EPAM’s established security, availability, and confidentiality policies and is subject to ongoing monitoring and control activities as part of EPAM’s SOC 2 Type II compliance program.

3.2. THE PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

The EPAM makes service commitments to its customers and has established system requirements as part of Mobitru application. The EPAM is responsible for its service commitments and system requirements and designing, implementing, and operating effective controls within the system to provide reasonable assurance that service commitments and system requirements are achieved.

Commitments are documented and communicated in the EPAM Ethics and Compliance Library, Privacy Policy, Privacy Notice, Contractual documents, and Service Level Agreements.

The EPAM's principal service commitments include, but are not limited to, the following:

- Security - the EPAM will implement technical and organizational measures to secure EPAM and Customer data complying with relevant laws and regulations.
- Availability - the EPAM will implement technical and organizational measures to ensure ongoing availability, confidentiality, and resilience of Mobitru application.
- Confidentiality - EPAM implements technical and organizational measures to ensure the confidentiality of data. Upon termination of the Service, the EPAM will use commercially reasonable efforts to return or destroy all Confidential Information of the other party.

The EPAM's applicable controls supporting the security, availability, and confidentiality categories and related criteria are the following:

- Control environment;
- Communication and information;
- Risk management and risk mitigation;
- Monitoring activities;
- Control activities;
- System operations;
- Change management.

3.2.1 Control Environment

The EPAM's control environment reflects the position of the management, its Board of Directors, and others concerning the importance of controls and the emphasis given to controls in its policies, procedures, methods, and organizational structure. The key elements of the EPAM's control environment related to software development and maintenance services are as follows:

- Oversight by the Board of Directors;
- Global Operations Office;
- Human Resources Policies and Practices;
- Corporate Internal Audit Function;
- Corporate Internal Verification of Internal Management Systems;
- Audit Committee;
- Process Management;
- Risk Assessment and Business Impact Analysis;
- Monitoring.

3.2.1.1 Oversight by Board of Directors

EPAM's Board of Directors has the ultimate responsibility for overseeing management's execution of the strategy and significant business policies of EPAM. The Board of Directors, which is composed of a majority of independent external directors, meets at least once per quarter to discuss matters pertinent to EPAM's operations.

The Audit Committee of the Board of Directors meets at least quarterly and is responsible for reviewing:

- EPAM's financial results;
- Audit results of the independent external auditors;
- Recommendations identified as a result of internal and external audits;
- Significant areas of potential exposure (e.g. material litigation).

3.2.1.2 Global Operations Office

The Global Operations (GO) division manages internal IT infrastructure, services, and corporate applications. The GO Office includes the following groups:

- Global Service Desk
- Enterprise Services
    - Process Management;
    - Compliance Management;
    - Corporate Security and Resiliency (Physical security and Business Continuity);
    - Data Privacy;
    - Artificial Intelligence.
- IT Services
    - Global IT Services (Enterprise Administration, Network Administration, Datacenter Support, Cloud Support, Telecommunications, License Management, Internal Application Support, Monitoring, Service Management Office);
    - Local IT Services (a.k.a. End-User Services, Remote Support).
- Information Security;
- Internal Applications Development (a.k.a. Digital Platform).

3.2.1.3 Human Resource Policies and Procedures

Controls have been developed covering critical aspects of employment including: hiring; training and skills development; performance appraisals; career advancement; and termination. All new employees are issued an employee packet documenting various procedural and administrative matters, which are then discussed under the new hire orientation program.

Talent Acquisition is primarily responsible for recruiting and evaluating job applicants. Depending on the security clearance required for the job, various levels of background checks are performed for applicants prior to or following their employment with EPAM.

Employee performance appraisals are performed periodically by the direct supervisor. To supplement on-the-job training, a wide range of in-house training programs is offered covering topics such as general leadership, management development, customer service and industry-specific topics.

3.2.1.4 Corporate Internal Audit Function

Internal Auditing is an independent and objective assurance and consulting activity that is guided by a philosophy of adding value to improve risk management and the operations of EPAM. The Corporate Internal Audit (IA) function reports functionally to the Audit Committee of the Board of Directors and administratively to the Chief Financial Officer. The IA function is governed by EPAM's Internal Audit Charter and adherence to The Institute of Internal Auditors' mandatory guidance including the Definition of Internal Auditing, the Code of Ethics, and the International Standards for the Professional Practice of Internal Auditing. IA performs audits based on an annual audit plan using an agile internal audit approach that is approved by the Audit Committee and is designed to bring a systematic and disciplined approach to evaluate and improve the effectiveness of the organization's governance, risk management, and internal control. IA reports the results of audits performed to management and the Audit Committee.

3.2.1.5 Corporate Internal Verification of Internal Management Systems

The Corporate Compliance Assurance Office is an independent group within the Global Operations Office. The Compliance Assurance Office aims to make processes visible to EPAM management by objectively evaluating whether processes are followed and associated work products are in compliance with internal regulations. The group's activity is based on a standard audit process developed by EPAM, which is reviewed annually. For each verification performed, the standard audit process is tailored, if necessary.

3.2.1.6 Audit Committee

The primary functions of the Audit Committee are to assist the Board of Directors in fulfilling its oversight responsibilities with respect to:

- the EPAM's systems of internal controls regarding finance, accounting, legal compliance and ethical behavior;
- the EPAM's auditing, accounting and financial reporting processes generally;
- the EPAM's financial statements and other financial information provided by the company to its stockholders, the public and others; and
- the performance of the EPAM's Corporate Internal Audit Function and independent auditors. Consistent with these functions, the Committee will encourage continuous improvement of, and foster adherence to, the EPAM's policies, procedures and practices at all levels.

3.2.1.7 EPAM's Process Asset Management

Administrative and operational controls for each major functional area are documented in various policies, standards and process descriptions. These descriptions are updated periodically and distributed to appropriate personnel. The Global Operations Office and Compliance Assurance Office prepares and maintains EPAM's Process Assets, which includes the following:

- EPAM's set of standard processes, including the process architectures and process elements.
- Approved life-cycle models.
- Guidelines and criteria for tailoring EPAM's set of standard processes.
- Measurement repository.
- EPAM Ethics and Compliance Library.

3.2.1.8 Risk Assessment and Business Impact Analysis

EPAM recognizes that risk management is a critical component of its operations. To properly manage corporate assets and to serve customers as expected, EPAM has developed a Business Continuity Program and annual security risk assessments of EPAM IT and Engineering Services. This assessment, which is performed by the Director, Security and Compliance, investigates external and internal risks in IT and Engineering Services, and management's ability to focus and mitigates the impact of such risk factors on operations. EPAM has implemented various measures designed to mitigate such risk factors.

The EPAM has developed a Global Business Continuity Plan (BCP) to facilitate the recovery of its critical business functions and critical site operations during a disruption, while minimizing adverse impacts on EPAM's customer satisfaction and revenue. As part of this effort, a Business Impact Analysis (BIA) was conducted across the critical corporate functions.

3.2.1.9 Monitoring

3.2.1.9.1 Operational Monitoring

EPAM IT and Engineering Services management and supervisory personnel monitor the quality of internal control performance as a regular part of their activities. To assist in this monitoring, service managers have implemented a series of management reports that measure the results of the processes involved in providing software development and maintenance services to clients. These include reports on project status and progress tracking, actual system and service availability, and response times compared to established service level goals and standards.

Exceptions in normal or scheduled processing due to hardware, software or procedural problems are logged, reported, and resolved daily. Appropriate levels of management review these reports daily, and action is taken as necessary.

IT and Engineering Services are monitored through daily management meetings and status reports. Escalation procedures are in place to alert management to issues and concerns.

Ongoing risk assessment and feedback from management are used to determine specific internal and external audit activities needed. Management designates personnel to monitor selected projects on an ongoing basis during the design and implementation phases to consider impact on the control environment prior to implementation.

3.2.1.9.2 Internal and External Audit Monitoring

EPAM is subject to a review by internal and external auditors on a periodic basis. Recommendations by both internal and external auditors regarding internal controls are given appropriate consideration.

Involvement of the internal and external audit may include, but is not limited to, gaining an understanding of, and periodic evaluation of the following:

- Management structure
- Systems development and software testing
- Information Security Management System (ISMS)
- Quality Management System (QMS)
- People Management
- Computer operations
- Physical security
- Finance and Accounting

3.2.1.10 Communication

3.2.1.10.1 Employees

EPAM has implemented various methods of communication to ensure employees understand their individual roles, responsibilities and corporate controls and to ensure significant events are communicated in a timely manner. These include:

- Orientation and training programs for new employees and existing employees changing their job function, including trainings on systems relevant to this report. Training courses are updated regularly to cover changes in technology and policy. New employees, as part of the orientation process, read the EPAM policies.
- Newsletters and memorandums summarize significant events and changes to corporate policies and are issued regularly. Time sensitive information is communicated to employees via email.
- Weekly, or as needed, managers also hold staff meetings and one-on-one meetings. These meetings are opportunities for the employee to bring to the management’s attention any questions or exceptions they may have with standard policies.

3.2.1.10.2 Clients

EPAM has implemented various methods of communication to ensure clients understand the roles and responsibilities of EPAM and to ensure events are communicated to clients in a timely manner.

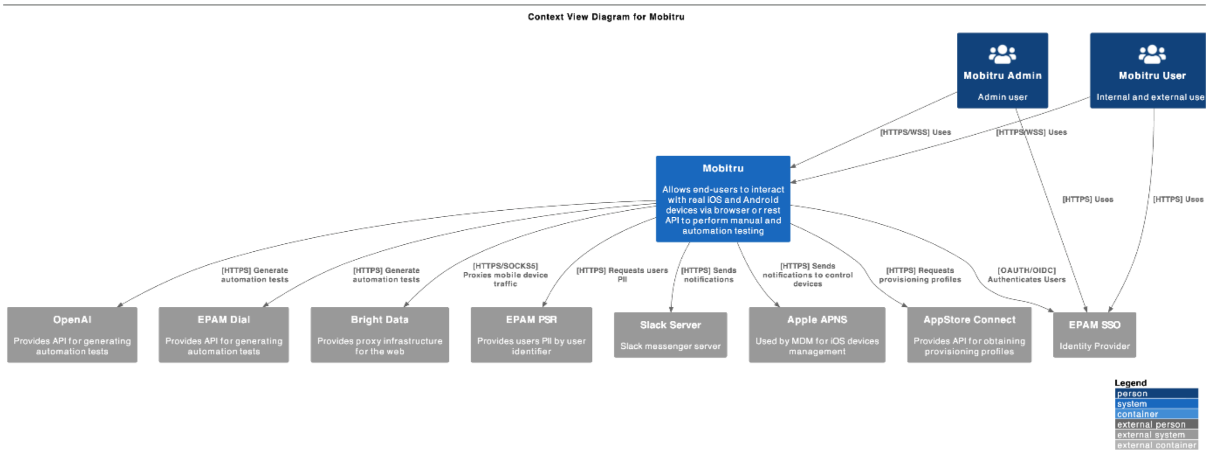
These methods include Account Managers' active participation in user group meetings. The Account Managers maintain contact with the designated client representatives to inform them of new issues and developments.

The particulars for communicating with clients may vary; however, each Account Manager holds meetings to inform clients of any relevant information. In addition, the Account Manager communicates regularly with clients via face-to-face meetings, video conferences, phone, fax, letter and email.

3.3. SYSTEM COMPONENTS

The structure of Mobitru is a combination of the EPAM's infrastructure, software, people, procedures, and data necessary to provide its services and support principal service commitments made to the customers.

The components that directly support the services provided to customers are described in the subsections below.


Context View Diagram for Mobitru
Mobitru Admin
Admin user
Mobitru User
Internal and external use
Mobitru
Allows end-users to interact with real iOS and Android devices via browser or rest API to perform manual and automation testing
[HTTPS/WSS] Uses
[HTTPS/WSS] Uses
[HTTPS] Uses
[HTTPS] Uses
[HTTPS] Generate automation tests
[HTTPS] Generate automation tests
[HTTPS/SOCKS5] Proxies mobile device traffic
[HTTPS] Requests users PII
[HTTPS] Sends notifications
[HTTPS] Sends notifications to control devices
[HTTPS] Requests provisioning profiles
[OAUTH/OIDC] Authenticates Users
OpenAI
Provides API for generating automation tests
EPAM Dial
Provides API for generating automation tests
Bright Data
Provides proxy infrastructure for the web
EPAM PSR
Provides users PII by user identifier
Slack Server
Slack messenger server
Apple APNS
Used by MDM for iOS devices management
AppStore Connect
Provides API for obtaining provisioning profiles
EPAM SSO
Identity Provider
Legend
person
system
container
external person
external system
external container

3.3.1 Mobitru architecture

Core components of the Mobitru architecture are represented in the diagram below.

3.3.2 Infrastructure

Core system components are hosted in dedicated EPAM server rooms located within CIS, EU and US regions. This ensures robust and reliable service delivery. Mobile devices are connected to the machines located in the server rooms through hubs.

To safeguard against any system failures, our backend server infrastructure is equipped with an automatic data backup system. This includes comprehensive backups of databases, various product versions, and dependencies, ensuring a seamless rollback capability if any part of the system encounters issues.

We prioritize security in all server interactions, which are conducted exclusively over HTTPS and TLS protocols. This guarantees the secure handling and storage of user-related information.

Our infrastructure is tailored to align with the current stage of Mobitru development and the specific requirements of each system release.

Mobitru uses the following infrastructure defined by the stage of application development and the system release:

- *Development*. Development servers located in the CIS region, and owned by development teams and are configured in accordance with the EPAM privacy policies and regulator's compliance.
- *Testing.* Servers are hosted in EPAM office in the CIS region are configured in accordance with the EPAM privacy policies and regulator's compliance. Provides version control and configured as production to avoid compatibility issues.
- *Production.* Production machines are hosted in EPAM server rooms located within CIS, EU and US regions. Certain components, such as backups, artifacts registry stored in EPAM server rooms. The production environment is enabled with back-up and restore options that allow for server recovery, data recovery, and service restoration in case of disaster events.

3.3.3 Software

The software consists of the programs and applications that support Mobitru (operating systems, middleware, and utilities). The list of software used to support, build, secure, maintain, and monitor Mobitru includes the following applications and technologies:

- Frontend (API/UI)
  - AngularJS
  - React
- Backend (API)
  - Nginx
  - Fabio
  - NodeJS
  - Golang
  - C++
  - C
- Service To Service communication
  - RabbitMQ
  - ZeroMQ
  - GRPC
  - Protobuf
  - Consul Connect
  - PgBouncer
  - Consul service mesh
- Data Storage
  - PostgreSQL
  - RethinkDB
  - Redis
  - Minio
- Epam self-hosted Gitlab
- Docker, docker-compose
  - Operating SystemsUbuntu 22.04.4 LTS
- Mobile Applications
  - Java
  - Kotlin
  - Objective C
  - Swift
- Service Discovery
  - Consul
- Video Processing
  - FFMPEG
  - LibAV
  - WebRTC
  - Logging and MonitoringLoki
  - Zabbix
  - Grafana

-

3.3.4 People

The EPAM personnel are organized into service teams that develop and maintain the application and the support teams that provide supporting services for system operations. In relation to Mobitru, the following groups can be specified:

The Global teams:

- *The Executive Management* is responsible for defining long-term EPAM goals, overseeing EPAM processes, defining a roadmap for project development and future improvements.
- *The Core IT division* is responsible for maintenance of Active Directory services, authentication rules, and user access, configuring and testing standard images for servers and workstations, configuring and monitoring backups.
- *The IT Security division is* responsible for the protection of the EPAM assets from harmful threats including monitoring of security incidents, vulnerability management, penetration testing, security baseline establishment.
- *The Global Operations Management* is responsible for the EPAM Infrastructure and Systems management, monitoring of availability, integrity, and resilience of the EPAM Infrastructure and Systems. The Global Operations division manages internal IT infrastructure, services, and corporate applications.
- *The People Management* is responsible for recruiting and onboarding new employees, performing appropriate background checks, provisioning appropriate awareness education and pieces of training, training and skills development, performance appraisals, career advancement, and termination.

The Mobitru teams:

- *The Project Management Team is* responsible for project planning, resource provisioning, project processes establishing and tailoring, project performance monitoring and reporting, impediment removal, communication with stakeholders, etc.
- *The Software Development Team* is responsible for new version releases, Service continuous improvement and new features development, bug-fixing, and providing support for issues received from the Success Manager.
- *The Software Testing Team* is responsible for quality assurance, new feature and bug-fixes testing, running automation and smoke tests before releases.
- *The DevOps Team is* responsible for CI/CD configuring and setup, dev environment safety and stability, environment security patching, for production environments operation and availability, monitoring, and releases to production environments.
- *The Success Manager* is responsible for communicating with users and consulting them about Product business logic, usage, and navigation, creating Team accounts and onboarding team members to the platform.

3.3.5 Procedures

Mobitru adheres to the EPAM's Information Security and Privacy Policies which is owned and approved by the Head of Global Operations and Data Privacy Lead. Security principles and controls are documented in the key Information Security Management System (ISMS) and Data Privacy Regulatory, they address:

- Organizational controls
- People controls
- Physical controls
- Technological controls

The EPAM's Integrated Quality Management System is based on the EPAM's Quality Policy and Information Security and Privacy Policy reflecting all applicable requirements of ISO 9001, ISO 27001, ISO 27701, ISAE 3402, and GDPR.

All the EPAM's regulations are available for employees and published in the EPAM Ethics and Compliance Library. The key ISMS and Data Privacy Regulatory are reviewed on an annual basis.

More details about regulations for managing security, availability, resilience, and confidentiality of Mobitru are described in the section "Control activities" below.

3.3.6 Data

Mobitru is not a master-system regarding app creators' data. Mobitru stores data created and uploaded by customers, e.g. mobile applications and automated tests binaries. User owning the data can remove/change it at any time. Obsolete data is removed by the DevOps Team.

Mobitru gets some registration information about application users from the EPAM Identity Access Management system (EPAM SSO) and Profile Service (PSR). Mobitru does not store personal data of users, only user ID is used for user authentication. For more information please refer to the section 3.3.1 "Mobitru architecture".

Data stored by Mobitru is encrypted and stored according to EPAM policies. Each service and support team are responsible for managing the security, availability and confidentiality of the data.
Mobitru data in use and at rest are stored in EPAM server rooms in Budapest, Boston and Minsk.
Data encryption at rest:

- *Linux Unified Key Setup (LUKS)* disk encryption is used for hardware servers.

Data encryption in transit:

- TLS and encryption key management approach is used, for more details refer to https://tools.ietf.org/html/rfc5246.

3.4. INCIDENT MANAGEMENT

During the period of *01-May-2025 through 31-Oct-2025* no identified system incidents have occurred that:

- Were the result of controls that were not properly designed or implemented or operating effectively to achieve one or more principal service commitments and system requirements.
- Otherwise resulted in a significant failure in the achievement of one or more principal service commitments and system requirements.

3.5. THE APPLICABLE TRUST SERVICES CRITERIA AND RELATED CONTROLS

3.5.1 APPLICABLE TRUST SERVICES CRITERIA

The Trust Services Categories in scope for the purposes of this report are as follows:

- *Security.* Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.
- *Availability.* Information and systems are available for operation and use to meet the entity's objectives. Availability is assured by backing up critical infrastructure (e.g. power, network channels, servers) and information, usage load balancing tools.
- *Confidentiality.* Information designated as confidential is protected to meet the entity's objectives.

3.5.2 CONTROLS RELATED TO THE APPLICABLE CRITERIAS

EPAM has selected and developed control activities to mitigate risks and achieve the set objectives. EPAM's control activities are defined through the policies and established organizational procedures. EPAM has implemented various methods for communicating organizational documents, procedures authorities, and responsibilities to employees to ensue effectiveness and compliance with control activities. They are as follows:

- EPAM Ethics and Compliance Library – an internal resource with all applicable policies, procedures, and other organizational documents;
- The Competence framework;
- Employee Handbook - https://info.epam.com/landing.html;
- Annual mandatory trainings.

3.5.2.1 Security

Security category refers to protection systems or data from a malicious threat actor or an unintentional internal threat including attack, damage, or unauthorized access. EPAM has designed and implemented the following general security documents: Cloud Security, Network security, Physical and Logical access Management, Data Encryption and Digital Signing, Vulnerability management and Penetration testing, Secure Development, Patch Management, etc.

Cloud Security defines the main concepts of security in the EPAM Cloud Service, specifies the main approaches, rules and regulations applied to ensure the security of the EPAM Cloud assets in public regions. The EPAM Cloud follows the industry standard shared responsibility model. All virtual machine images in the public cloud by default comply with the corporate requirements for virtual resources safety and security. Each cloud provider enables a set of services according to its service catalogue. It enables basic security settings for each service, according to the provider's rules and regulations. The instances that belong to a project can be accessed only by the members of this project; the access is authorized by the Microsoft Entra ID.

Network Security encompasses all physical and software measures that the EPAM puts in place to protect networks from unauthorized access, misuse, destruction, and modification by insiders (employees, contractors, vendors) and outsiders (cybercriminals, hacktivists, other intruders). Network security features rules and configurations are designed and implemented by the EPAM to protect integrity, confidentiality, and accessibility of computer networks and data.

3.5.2.1.1 Logical Access Management

Strong authentication and access controls are implemented to restrict administrative access to production systems, internal support tools, and Customer data. Access is restricted using unique user ID and assigned authentication method (PIN, passwords, OTP, Physical Key, etc.). The preferred method for EPAM Users is Passwordless Authentication which enhance the security and user experience when accessing EPAM systems and applications by eliminating the need for traditional passwords and providing alternative means for user authentication. Information access rights are assigned to users on a ‘minimum necessary’ and ‘need-to-know’ basis. The segregation of the incompatible duties principle is applied and verified before authorizing new access privileges.

The EPAM units which administer the EPAM Services Production environments use Privileged accounts. Privileged access management includes the Privileged Account Renting Service, Privileged Access Workstations, and logical privileged account separation based on the categories of users and their roles. Privileged Accounts are used only in a protected environment: protected workstation or hardened Jump server.

Privileged/Administrative accounts for Systems and Applications including Administrator and Operator service accounts (e.g., System Administrator, Database administrators, Network administrators, IT security team) access rights are reviewed at least quarterly. Extended/privileged access rights to Applications are reviewed at least twice a year.

User access rights depend on the user project roles and automatically follow the changes in the Applications.

Access rights to systems and applications are changed/revoked immediately in case of user dismissal, or change in the user role or job function. The Core IT Team settles and manages automated reconciliation procedures of active and dismissed employees in the Entra ID and People Management systems.

Some additional access granting and revocation specifics for Mobitru are documented in the Application Security Plan.

3.5.2.1.2 Physical Access Management

The EPAM has implemented and regularly verifies strong physical security measures for protection of development centers, critical infrastructure, and protected areas such as data centers, server rooms, and other IT premises. To prevent unauthorized access, all the EPAM offices are locked and can only be unlocked using electronic access cards (E-cards) issued to each employee. The offices cannot be entered without an E-card. Access rights to the EPAM premises or protected area are granted to a person based on job roles and functions to prevent unauthorized access. Entrances and emergency exits are equipped with Video Surveillance System, Automated Access Control System, and/or Mechanical access control. All offices are protected with fire alarm systems.

Some additional access granting and revocation specific for Mobitru is documented in the Application Security Plan.

3.5.2.1.3 Data Encryption

Hard drive encryption is enforced for all EPAM managed workstations with Windows, MAC, and Linux OS. Compliance with this requirement is monitored by the IT Security department.

3.5.2.1.4 Hardening Standards and Software Package control

The EPAM has settled and maintains Hardening Standards for Servers, Workstations, and Network devises. Standards include security and compliance agents, antimalware, and latest available system software.

These standards are implemented in the Standard EPAM's images that are managed and updated by the Core IT Team.

The EPAM also maintains standard installation software package and list of approved freeware that can be installed on the EPAM's workstations. Standard Installation Software Package includes only supported up-to-date versions of system software. Expired OS decommission schedule is developed and performed by the Core IT Team. Unauthorized software is monitored and detected during a Software Audit..

3.5.2.1.5 Patch Management

To prevent exploitation of technical vulnerabilities and establish standard procedures for safe and timely installation of patches, the EPAM performs patch management. The procedure is applied to the components of information technology infrastructure (hardware, software, and services) on the following layers: Network, Operating systems, Database, Software, Cloud, Data Center, and Security Software.

Application infrastructure is managed by the Global and Application teams.

OS updates are tested by the Core IT division and installed on servers and workstations monthly. New releases and patches for the database are evaluated by the development team and installed when additional functionality is needed or vulnerability is detected.

Cloud infrastructure is updated when additional functionality is needed or vulnerability is detected.

All patches are downloaded from relevant system vendors or trusted sources. Each patch's source is authenticated, and the integrity of the patch is verified. All patches are submitted to an antivirus scan upon download.

3.5.2.1.6 Secure development

The EPAM has developed and maintains processes, guidelines, and templates for project management, product/application development, testing, securing, and changing. The principle of segregation of duties and segregation of environments is applied and followed in development process. Application version control is implemented.

The EPAM has adopted the following main development phases:

- Definition;
- Design;
- Construction;
- Testing;
- Acceptance & Handover;
- Maintenance.

Each phase contains security related activities that are assessed and confirmed by the Global Application Security Team. These activities are aimed to define risks, design proper application security architecture, implement relevant security mitigations measures, setup regular security code review and, as a result, get secure application.

3.5.2.1.7 Change management

The EPAM has developed and maintains the Change Management Process for ensuring that changes are recorded, assessed, planned, tested, implemented, and evaluated in a controlled manner. Requests for changes to applications including upgrades and fixes are registered, prioritized, and implemented if consistent with development plans. All changes to applications are tested in accordance with test plans that may include appropriate testing types according to the EPAM procedures. Then, the changes shall be approved before moving into production.

Mobitru Change Management is performed in accordance with the Change Management Process documented in the Project Management Plan.

Mobitru uses an agile development methodology to manage tasks within team-based development environments. Separate environments are used for development, testing, and production.

3.5.2.1.8 Vulnerability Management and Penetration Testing

Every asset of EPAM is subject to periodic Vulnerability assessment and penetration testing.

Goals and objectives of vulnerability assessments vary based on the evaluation requirement itself. Internal vulnerability assessment is mandatory for all assets (hardware, virtual servers, web applications, containers, public cloud assets) and optional for Internet-facing devices/systems/applications. External vulnerability assessment is mandatory for all Internet-facing devices/systems/applications and exceptional for some key internal applications/endpoints. Periodic vulnerability assessment both internal & external are conducted on weekly basis by IT Security division.

Internal and external penetration testing - is mandatory for all assets (hardware, virtual servers, web applications, containers, public cloud assets) and for Internet-facing devices/systems/applications. Internal penetration testing is conducted semiannually, external penetration testing - annually. Internal and external penetration testing is planned and managed by IT Security division.

Third party Penetration Testing is conducted annually.

EPAM uses vulnerability scanning tools to scan the internal and external-facing network, as well as configurations in Cloud Services (AWS, GCP, Azure). Results are emailed to the relevant system owner for triaging and, if they determine it to be necessary, creating a ticket for resolution.

Mobitru application is covered by the following vulnerability assessments methods:

- Host-based vulnerability scanning;
- Cloud configuration monitoring;
- Software composition analysis (SCA);
- Vulnerabilities identified internally by security reviews or engineering teams;
- SAST/DAST scans;
- Penetration testing.

3.5.2.1.9 Incident Management

EPAM has developed and applied two incident management processes: for general incidents and for information security (IS) incidents. The purpose of the processes is to minimize the negative impact of incidents by restoring normal service operation as quickly as possible and minimize security risks.

Both incident types are identified, tracked, and processed in the EPAM’s Support Portal.

Incidents can be detected and registered manually or by the EPAM’s automated systems.

The key factor for detecting information security events is the EPAM’s personnel. All employees are responsible for reporting any suspicious events, IS breaches, and weaknesses, possible fraudulent activities, and other anomalies during their daily work to the EPAM’s Support Portal.

Technical information security events can be detected by automatic means alerts made by audit trail analysis facilities, firewalls, intrusion detection systems, and anti-malicious code (including viruses) tools. In each case IS events are stimulated by pre-set parameters. The Security Operations Center (SOC) monitors alerts are produced by the automated systems and take measures for each security breach investigation.

For Technical Incidents identification and registration on Application/ Data base level Zabbix tool is used with pre-set parameters of monitoring and reacting on events.
Incident management flow includes the following steps:

- Incident Detection and Registration;
- Incident Classification and Assignment;
- Incident Investigation and Recovery;
- Incident Review;
- Incident Closure.

3.5.2.1.10 Vendor security

The EPAM has a formal framework and regulation policies for managing the lifecycle of vendor relationships including how to assess, manage, and monitor its suppliers to ensure an appropriate control environment consistent with the EPAM's security, availability, and confidentiality commitments.

As part of the onboarding process, high-risk vendors are subject to a risk assessment and detailed review by the EPAM internal subject matters experts. This involves evaluating the supplier's control environment and overall security posture based on information contained in supplier questionnaires, compliance reporting (e.g., SOC2), and policies. Vendor agreements, including terms and conditions, any security, confidentiality, and availability related commitments, are also reviewed and signed prior to engaging with any vendor.

Mitigating, resolving, or accepting any risks that were identified during the due diligence process is handled and documented by the appropriate subject matters experts and the designated EPAM reviewers and approvers.

The following requirements are also implemented for vendors with access to the EPAM's or Customer's personal data:

- If vendor is a legal entity, the Data Protection Agreement (DPA) shall be signed.
- If vendor is an individual, NDA and working contract shall be signed. The Legal Team responsible for a particular country can provided up-to-date templates.

For vendor providing software, application security requirements are formulated by the Global Application Security Team after the security assessment for the vendors producing software.

3.5.2.2 Availability and Resilience

The availability category refers to the accessibility of the system and stable operation of the Service. The availability and Resilience of Application depend on many aspects of the EPAM's operation, including Business continuity and Disaster recovery management.

The EPAM recognizes the importance of establishing and maintaining a comprehensive Business Continuity Management (BCM) Program to protect the continuity of critical business. The EPAM has established BCM practices, procedures, and policies that provide resilience and recovery for critical locations, staff, systems, vendors, and processes on a global level throughout the organization.

The goals of the BCM Program are to identify the threats and their potential impacts and provide a framework for building enterprise resilience:

- Maintain uninterrupted service whenever possible, and when necessary, effectively coordinate recovery from unavoidable disruptions effectively and efficiently.

1. Safeguard employees, revenue, and customer satisfaction while minimizing increased costs in the event of an unplanned interruption to the business.
2. Respond to emergency situations in a safe, effective, and timely manner and return to normal operations upon recovery.

The EPAM performs business impact assessments (BIA) for Services to support its business continuity program with relevant information. Based on the BIA, the services are assigned with appropriate rank. Depending on the rank, the following parameters have been established for the service: working hours, service request and incident processing timeframes, availability targets and service failure resilience, recovery point objective and disaster recovery planning and testing, backup location.

3.5.2.2.1 Disaster recovery

A disaster recovery procedure is in place and reviewed on an annual basis by an authorized person. Procedures for disaster recovery execution are defined, reviewed, tested, and in place. The procedure describes, at a high level, the purpose, objectives, scope, critical dependencies, RTO/RPO, and roles/responsibilities.

Disaster recovery tests are performed in a simulated environment on an annual basis. After disaster recovery tests are performed, outputs of the tests are captured, analyzed, and discussed to determine the scope of the next steps for continuous improvement of the tests. The improvement efforts are captured within engineering tickets and followed through as appropriate.

3.5.2.2.2 Backup

All production servers, databases, project and personal shared network folders are under backup. Daily Disk Backups (Incremental Backup) are performed at the end of each business day. Weekly Full Tape Backups are performed every Sunday. Monthly and Yearly Full Tape Backups shall be performed at the end of each month and year, respectively. To ensure data consistency and prevent data loss, a quarterly backup test is performed.

Backups for EPAM Applications hosted in Public Cloud are scheduled with respect to Recovery Point Objective (RPO) defined Service ranking and operational guideline and kept at least for 7 calendar days as the default period of backup process.

All Mobitru production databases are under daily full backup. Backups are stored in EPAM dedicated private storage at least for 3 months. To ensure data consistency and prevent data loss, a semiannual backup test is performed by Mobitru DevOps Team.

3.5.2.3 Confidentiality

The EPAM has established data classification schema and rules for information asset handling based on the classification.

There are three general Confidentiality classes established in the EPAM:

- Public - freely shared information.
- Confidential - any data leakage, loss, or damage of which can cause harm to data originator, owner, EPAM, or Customer.
- Strictly confidential - any data leakage, loss, or damage of which can cause significant harm to data originator, owner, EPAM, or Customer.

The EPAM defines the following Data categories by origin:

- Personal data - data relating to living individuals who can be identified from those data, or from those data and other information, which is in the possession of, or is likely to come into the possession of, the data controller.
- Customer data – data belonging to the Customer.
- Project/program/account data-information created during the project/program/account life-cycle.
- EPAM data - information owned by EPAM.

All employees share the responsibility to safeguard information with an appropriate level of protection:

- Information shall be classified in terms of legal requirements, value, and criticality.
- Information shall be labeled to manage appropriate handling.
- Media being disposed of shall be securely deleted.
- Media containing the EPAM information shall be protected against unauthorized access, misuse, or corruption during transport.

The EPAM Data Classification scheme and key classification rules:

The EPAM data category by origin	Confidentiality class		
	Public	**Confidential**	**Strictly confidential**
Personal data	Restricted unless other stated by the data owner	By default, any data type not belonging to Public or Sensitive class is considered confidential	Predefined types: Racial or ethnic origin, Political opinions, Religious or philosophical beliefs, Trade union membership, Biometric data, Genetic data, Health, and types depending on a particular Country's Legislation
Customer data	Restricted unless other stated by the Customer		Predefined types: Strategic information plans; Customer's know-how. Declared as sensitive by the originator or owner
Project / program / account data	Restricted unless other stated by management		Predefined types: Contract data; Financial data about the project; Declared as sensitive by the originator or owner
EPAM data	Restricted unless other stated by management		Predefined types: EPAM financial information; Information about customers; Strategic information, plans, and trade secrets; Declared as sensitive by the originator or owner

The EPAM complies with laws and regulations (including GDPR) related to the privacy and protection of personal data of all individuals who interact with the EPAM's business. The EPAM sets outgroup-wide principles for how we collect, process, and use personal data. The EPAM has developed security controls to protect data based on the leading security and auditing standards: ISO 27001:2022, ISAE and ISO 27701.

Mobitru communicates changes to confidentiality commitments to its users through the Privacy Policy section on official a site when applicable: https://mobitru.com/.

3.5.2.3.1 Data retention and erasure

Data retention is assured according to the Data Retention Policy and Obfuscation rules for the EPAM's data. Data retention period is 12 months after user account deactivation. User data is deleted automatically after the expiration of the retention period.

Data deleting on demand is handled based on the request from the EPAM Data Privacy Office.

When the application is being decommissioned or old data storages are not supported, secure data removal is performed. The following steps shall be applied.

- Decision about application decommissioning or removal of data storage shall be made.
- Secure data deletion without a possibility to restore the data shall be performed.
- Evidence that the data was securely removed shall be documented.

For Mobitru customer defines and applies Data retention and erasure principles.

3.6. COMPLEMENTARY USER ENTITY CONTROLS (CUECS)

The EPAM's controls related to the Mobitru cover overall internal controls for each user entity of the Application. But certain controls are in operation within the user entity organizations. This section describes those controls that should be in operation at user entity organizations. Each user entity must evaluate its own internal control to determine whether the identified CUECs have been implemented and are operating effectively. Management of user entities is responsible for the following:

Criteria	Complementary User Entity Controls
CC2.3	User entities are responsible for understanding and adhering to the contents of their service contracts, including commitments related to system security, availability, processing integrity, and confidentiality.
CC3.2, CC7.2, CC7.3, CC7.4, CC7.5	User entities are responsible for reporting any identified security, availability, processing integrity, and confidentiality issues.
CC6.1, CC6.2, CC6.3	User entities properly authorize users who are granted access to the resources and monitor continued appropriateness of access
CC6.1, CC6.7	User entities enforce desired level of encryption for network sessions User entities ensure stable internet connection with sufficient bandwidth.
CC6.1, CC6.3, CC6.6, CC6.7, CC6.8, CC7.1	User entities secure the software and hardware used to access Mobitru.
CC5.1, CC6.1, CC6.7	User entities are responsible for data privacy controls related to collection, processing and deletion of data stored in Mobitru

3.7. COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS (CSOCS)

Mobitru utilizes subservice organizations - Amazon Web Services (AWS) as a critical vendor and has applied to it all rules and verifications described above. The EPAM management receives and reviews the Amazon Web Services SOC 2 report annually. In addition, through its operational activities the EPAM management monitors the services performed by Amazon Web Services to determine whether operations and controls expected to be implemented at the subservice organization are functioning effectively.

Rather than duplicate the control tests, controls at Amazon Web Services are not included in the scope of this report. CSOCs are expected to be in place at Amazon Web Services related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability.

The subservice organization controls presented below shall not be regarded as a comprehensive list of all the controls that shall be employed by the subservice organization:

Criteria	Complementary Subservice Organizations Controls
CC6.1	AWS is responsible for maintaining controls over logical access management including privileged access. AWS is responsible for encryption data in transit.
CC6.7	AWS is responsible for encryption at rest uploaded or created Customer data. AWS is responsible for key management process and cryptographic techniques management.
CC6.4	AWS is responsible for restricting physical access to data centers to authorized personnel. AWS is responsible for 24/7 monitoring of data centers by closed circuit cameras and security personnel. AWS is responsible for installation electronic intrusion detection systems to be capable detect breaches in data center server locations.
A1.2, CC7.2	AWS is responsible for preventing environmental threads in data centers by installation cooling systems, battery and generator backups, smoke detection, dry pipe sprinklers. AWS is responsible for overseeing the regular maintenance of environmental protections at data centers.

Criteria	Complementary Subservice Organizations Controls
	AWS is responsible for monitoring environmental threats, incidents and events that impact AWS assets.
CC7.2	AWS is responsible for security logs protection and access restriction to authorized personnel. AWS is responsible for implementation mechanisms to detect attempts and prevent connections to the organization's network by unauthorized devices.
CC8.1	AWS is responsible for maintaining controls over changes management to the platform services.

3.8. SPECIFIC CRITERIA NOT RELEVANT TO THE SYSTEM

There were no specific security, availability, or confidentiality Trust Services Criteria as outlined in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria) that were not relevant to Mobitru as presented in this report.

Additional Processing Integrity and Privacy controls are not relevant to Mobitru.

3.9. SIGNIFICANT CHANGES

During the audited period *from 01-May-2025 through 31-Oct-2025*, functionality of Mobitru was extended with support for browser-based testing in addition to mobile devices, and AI-assisted execution services (Model Context Protocol (MCP) servers). They did not result in changes to system boundaries, trust service criteria in scope, deployment models, categories of users or data processed, subservice organizations, or the design and operating effectiveness of relevant controls.

4. Description of procedures performed by the service auditor

This section presents the following information provided by EPAM:

- The controls established and specified by EPAM to achieve the specified Trust Services Criteria.

Also included in this section is the following information provided by the service auditor:

- A description of the tests performed by the service auditor to determine whether the service organization's controls were operating with sufficient effectiveness to achieve specified Trust Services Criteria.
- The results of the service auditor's tests of controls.

We have examined the attached description of the system of EPAM Systems Inc.'s (NYSE: EPAM) (hereafter 'EPAM' or the 'Service Organization') internal control system relating to Mobitru. We have performed our examination based on the criteria for a description of a service organization's system set forth in DC Section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report ("description criteria"), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period May 1, 2025 to October 35, 2025, to provide reasonable assurance that EPAM's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality ("applicable trust services criteria") set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

Our testing of EPAM's controls was restricted to the Trust Services Criteria and controls to achieve those listed in the matrices in this section of the report and was not extended to controls described in system description but not included in the aforementioned matrices, or to controls that may be in effect at user organizations. It is each user auditor's responsibility to evaluate this information in relation to the controls in place at each user organization. If certain complementary controls are not in place at user organizations, EPAM's controls may not compensate for such weaknesses.

We applied the following criteria for assessment of internal control environment:

1. In assessing the suitability of the criteria to evaluate the service organization's description of its system, the service auditor determined if the criteria encompass:
   a. Whether the description presents how the service organization's system was designed and implemented, including, as appropriate:

i. The description presents EPAM's system that was designed and implemented throughout the period May 1, 2025, to October 31, 2025, in accordance with the description criteria.

ii. The controls stated in the description were suitably designed throughout the period May 1, 2025, to October 31, 2025, to provide reasonable assurance that EPAM's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and if user entities applied the complementary controls assumed in the design of EPAM's controls throughout that period.

iii. The controls stated in the description operated effectively throughout the period May 1, 2025, to October 31, 2025, to provide reasonable assurance that EPAM's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization and user entity controls assumed in the design of EPAM's controls operated effectively throughout that period.

iv. Whether the description includes relevant details of changes to the service organization's system during the period covered by the description.

v. Whether the description omits or distorts information relevant to the scope of the service organization's system being described, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities and their auditors and may not, therefore, include every aspect of the service organization's system that each individual user entity and its auditor may consider important in its particular environment.

2. In assessing the suitability of the criteria to evaluate the design of controls, the service auditor determined if the criteria encompass, whether:

   a. The service organization has identified the risks that threaten achievement of the Trust Services Criteria stated in the description of its system; and

   b. The controls identified in that description would, if operated as described, provide reasonable assurance that those risks do not prevent the Trust Services Criteria from being achieved.

Deloitte performed procedures that were considered necessary in the circumstances to evaluate whether individual key control activities were operating with sufficient effectiveness to provide reasonable, but not absolute assurance that the Trust Services Criteria were achieved during the period covered by this report.

The tests were also designed to provide a basis for evaluating the fairness of the control descriptions. In designing the tests, the following factors were considered:

1. The nature of the Trust Services Criteria to be achieved;
2. The nature of the control activity being tested;
3. The type of evidential matter available;
4. The assessed level of control risk (i.e., assessment of probability and impact of control activities malfunctioning); and
5. The expected efficiency and effectiveness of the proposed test.

Deloitte performed operating effectiveness testing by using a sampling methodology. When designing the sample, Deloitte considered the purpose of the procedure and the characteristics of the population from which the sample was drawn. Sampling involved:

1. Determining a sample size sufficient to reduce sampling risk to an acceptably low level;
2. Selecting items for the sample in such a way to reasonably expect the sample to be representative of the relevant population for the entire period and likely to provide a reasonable basis for conclusions about the population for the entire period;
3. Treating a selected item to which the practitioner is unable to apply the designed procedures or suitable alternative procedures as a deviation from the prescribed control;
4. Investigating the nature and cause of deviations or misstatements identified and evaluating their possible effect on the purpose of the procedure and on other areas of the engagement;
5. Evaluating the results of the sample, including sampling risk;
6. Evaluating whether the use of sampling has provided an appropriate basis for evaluating conclusions about the population that has been tested.

The Tests of Effectiveness covered a period from May 1, 2025 to October 31, 2025.

Further information on the Tests of Effectiveness and Test Results can be found in the charts below.

TRUST SERVICES CRITERIA, EPAM CONTROL ACTIVITIES AND TEST RESULTS BY DELOITTE

The following information is provided:

1. The column “**Trust Services Criteria**” shows the applicable trust services criteria specified by the American Institute of Certified Public Accountants.
2. The column “**EPAM Control Activity**” states the measures that were specified by EPAM in order to achieve the Trust Services Criteria;

Trust Criteria	EPAM Control Activity
CC1.1. The entity demonstrates a commitment to integrity and ethical values.	**IR117.** Information systems strategies and long- and short-term plans have been formulated and approved by management to support the overall business strategy and information systems requirements of the entity. Information systems performance is monitored by management. **IR126.** Mandatory trainings are provided to all employees working within EPAM according to Mandatory Training Program Work Instruction (including trainings on ethical values, quality, security and data privacy, health and safety). The required trainings are determined based on company requirements. The training attendance is documented and monitored by People Management team. **IR001.** Formal selection criteria are developed to control the IT vendor selection. Management monitors compliance with Technical Procurement Work Instruction. The approved vendor list (AVL) is the primary source for procurement. AVL template is prepared. Vendor evaluations are performed once a year by Global Procurement Director in cooperation with the local EUS Managers (VEFs). **IR157.** Information security tools and techniques are used to restrict access to information resources (e.g. data files, utilities, transactions, programs). Management reviews compliance with internal security policies and approves the implementation and configuration of information security tools and techniques related to logical security. Appropriate corporate policy is in place for granting access privileges for users by the application/system/database/operation system owners and operators and annually reviewed. **IR501.** EPAM prepares, regularly reviews, and updates as needed the company's Code of Ethical Conduct, which is made available to employees, suppliers, and all others publicly on the company's publicly available webpage. Appropriate levels of disciplinary action are

This report is intended solely for the information and use of the management of EPAM, its clients who have used EPAM’s services, and the independent auditors of its clients, and is not intended to be, AND SHOULD NOT BE, USED BY ANYONE OTHER THAN THESE SPECIFIED PARTIES.

	imposed for violations of the Code of Ethical Conduct. EPAM maintains a whistleblowing reporting system, which includes internal reporting channels and its EthicsLine. The EthicsLine is an online channel that allows for confidential and anonymous submission of matters that may violate EPAM's Code. **IR502.** EPAM has established the Background Check Screening Policy that details the different background verifications that new hires are subject to in line with local regulations. EPAM performs screening of new hires that as a minimum include the check of proof of identity, proof of right to work, and global sanctions. Notwithstanding the examination of past activity during the recruitment process, Background Check Screening Policy lists EPAM locations where additional employment verification, education verification, and/or criminal background checks are performed, considering the restrictions of local limitations on the process. **IR503.** EPAM has established IT Security and Privacy Policies and communicates it to all employees. Security policies define requirements for security, availability, confidentiality and privacy including the definition of employee and management responsibilities. IT Security and Privacy Policies are periodically reviewed.
CC1.2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	**IR504.** EPAM's Audit Committee has a reguar meeting to discuss internal and external audit matters by providing an oversight on the company's internal control operation. **IR505.** The board of directors are elected to act on behalf of the company's shareholders that are independent from EPAM's operative management.
CC1.3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	**IR123a.** The necessary skills and experience required for the positions according to EPAM's business needs are clearly defined before hiring staff. EPAM Talent Acquisition team is responsible for the recruitment process. The skills and required experience are set by the Resource Managers. Acquired skills are stored and linked to the employee profile. **IR123b.** Resource and Project Managers evaluate staff performance. People Management monitors the performance evaluation process. Staff performance and evaluations records are stored and linked to the employee profile. **IR506.** Ownership of critical business environments, processes, applications and established IT controls as part of the company's IT control framework are assigned to employees, acknowledged and documented. Management reviews are in place for key controls in a documented form that is monthly prepared.

	IR507. EPAM has an organizational chart defined and documented that clearly states the reporting lines and areas of authority. The organizational chart is regularly updated.
CC1.4. The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	**IR117.** Information systems strategies and long- and short-term plans have been formulated and approved by management to support the overall business strategy and information systems requirements of the entity. Information systems performance is monitored by management. **IR123a.** The necessary skills and experience required for the positions according to EPAM's business needs are clearly defined before hiring staff. EPAM Talent Acquisition team is responsible for the recruitment process. The skills and required experience are set by the Resource Managers. Acquired skills are stored and linked to the employee profile. **IR123b.** Resource and Project Managers evaluate staff performance. People Management monitors the performance evaluation process. Staff performance and evaluations records are stored and linked to the employee profile. **IR126.** Mandatory trainings are provided to all employees working within EPAM according to Mandatory Training Program Work Instruction (including trainings on ethical values, quality, security and data privacy, health and safety). The required trainings are determined based on company requirements. The training attendance is documented and monitored by People Management team. **IR502.** EPAM has established the Background Check Screening Policy that details the different background verifications that new hires are subject to in line with local regulations. EPAM performs screening of new hires that as a minimum include the check of proof of identity, proof of right to work, and global sanctions. Notwithstanding the examination of past activity during the recruitment process, Background Check Screening Policy lists EPAM locations where additional employment verification, education verification, and/or criminal background checks are performed, considering the restrictions of local limitations on the process. **IR503.** EPAM has established IT Security and Privacy Policies and communicates it to all employees. Security policies define requirements for security, availability, confidentiality and privacy including the definition of employee and management responsibilities. IT Security and Privacy Policies are periodically reviewed.
CC1.5. The entity holds individuals accountable for their internal	**IR117.** Information systems strategies and long- and short-term plans have been formulated and approved by management to support the overall business strategy and information

control responsibilities in the pursuit of objectives.	systems requirements of the entity. Information systems performance is monitored by management. **IR126.** Mandatory trainings are provided to all employees working within EPAM according to Mandatory Training Program Work Instruction (including trainings on ethical values, quality, security and data privacy, health and safety). The required trainings are determined based on company requirements. The training attendance is documented and monitored by People Management team. **IR503.** EPAM has established IT Security and Privacy Policies and communicates it to all employees. Security policies define requirements for security, availability, confidentiality and privacy including the definition of employee and management responsibilities. IT Security and Privacy Policies are periodically reviewed. **IR506.** Ownership of critical business environments, processes, applications and established IT controls as part of the company's IT control framework are assigned to responsible service group acknowledged and documented. Management reviews are in place for key controls in a documented form that is quarterly prepared. **IR507.** EPAM has an organizational chart defined and documented that clearly states the reporting lines and areas of authority. The organizational chart is regularly updated.
CC2.1. The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	**IR145.** The information systems organization includes a Service Desk function that acts on user queries regarding systems. Incidents are recorded in a centralized log. Service Groups personnel monitor the log to ensure timely distribution and resolution of user queries. Service groups check the progress of reported issues which are assigned to responsible personnel via Service Desk tickets. I**R154.** A risk assessment, which involves valuation of business information resources and identification and assessment of the levels of risks present, has been performed to identify appropriate and cost-justifiable information security architecture. The risk assessment is performed annually. The IT and Facility Management have implemented suitable information security architecture to ensure that there is appropriate physical and logical security. During the risk assessment, an asset registry, threats regarding infrastructure property, risk classification and review of results of risk assessment are prepared. **IR506.** Ownership of critical business environments, processes, applications and established IT controls as part of the company's IT control framework are assigned to responsible service group acknowledged and documented. Management reviews are in place for key controls in a documented form that is quarterly prepared. **IR508.** Independent internal audit function is in place that objectively evaluates performed processes, work products and services against a predifined audit criteria. Internal Audit is

	also responisble for identifying and documenting noncompliance issues, proposal for imprevement and providing feedbacks to auditees and managers on the results of internal audit activities. EPAM performs periodic Information Security Management System (ISMS) and Privacy Information Management System (PIMS) internal audits and results are reviewed with appropriate management. EPAM makes available relevant audit reports and certifications to communicate the state of internal control system to customers. **IR554b.** A risk assessment, which involves valuation of business information resources and identification and assessment of the levels of risks present, has been performed to identify appropriate and cost-justifiable information security architecture according to the Secure Development of Internal Applications Guideline. The application development team, in cooperation with the BSS Application Security Team have implemented suitable Solution Architecture of the application to ensure its appropriate cyber security controls. Security risk assessment and Threat modeling are performed prior moving Application to production. Any significant change (major release) go through Security impact analysis, that can lead to Threat modeling and Security risk assessment artifacts update.
CC2.2. The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	**IR126.** Mandatory trainings are provided to all employees working within EPAM according to Mandatory Training Program Work Instruction (including trainings on ethical values, quality, security and data privacy, health and safety). The required trainings are determined based on company requirements. The training attendance is documented and monitored by People Management team. **IR503.** EPAM has established IT Security and Privacy Policies and communicates it to all employees. Security policies define requirements for security, availability, confidentiality and privacy including the definition of employee and management responsibilities. IT Security and Privacy Policies are periodically reviewed. **IR508.** Independent internal audit function is in place that objectively evaluates performed processes, work products and services against a predefined audit criteria. Internal Audit is also responsible for identifying and documenting noncompliance issues, proposal for improvement and providing feedbacks to auditees and managers on the results of internal audit activities. EPAM performs periodic Information Security Management System (ISMS) and Privacy Information Management System (PIMS) internal audits and results are reviewed with appropriate management. EPAM makes available relevant audit reports and certifications to communicate the state of internal control system to customers. **IR509.** EPAM has established a description (Communications Work Instruction and processes in order to maintain and clarify communication methods for internal commnuication as well as communication with EPAM's Partners and Customers.
CC2.3. The entity communicates with external parties regarding	**IR508.** Independent internal audit function is in place that objectively evaluates performed processes, work products and services against a predefined audit criteria. Internal Audit is also responsible for identifying and documenting noncompliance issues, proposal for

matters affecting the functioning of internal control.	improvement and providing feedbacks to auditees and managers on the results of internal audit activities. EPAM performs periodic Information Security Management System (ISMS) and Privacy Information Management System (PIMS) internal audits and results are reviewed with appropriate management. EPAM makes available relevant audit reports and certifications to communicate the state of internal control system to customers. **IR044a.** Management approves all decisions to provide application system development, testing, support, consultancy and maintenance services to EPAM’s clients by signing the contracts (Master Service Agreements) in order to ensure that provided services are consistent with the organization's systems plans and strategies.
	IR509. EPAM has established a description (Communications Work Instruction and processes in order to maintain and clarify communication methods for internal commnuication as well as communication with EPAM's Partners and Customers.
CC3.1. The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	**IR116.** The selection of new vendors is according to Vendor Management Policy. Global procurement team maintains the Approved Vendor List (AVL) for all approved IT vendors and performs review on a yearly basis. All of them are approved by Global Procurement Director. AVLs and VEFs are stored together. **IR154.** A risk assessment, which involves valuation of business information resources and identification and assessment of the levels of risks present, has been performed to identify appropriate and cost-justifiable information security architecture. The risk assessment is performed annually. The IT and Facility Management have implemented suitable information security architecture to ensure that there is appropriate physical and logical security. During the risk assessment, an asset registry, threats regarding infrastructure property, risk classification and review of results of risk assessment are prepared. **IR554b.** A risk assessment, which involves valuation of business information resources and identification and assessment of the levels of risks present, has been performed to identify appropriate and cost-justifiable information security architecture according to the Secure Development of Internal Applications Guideline. The application development team, in cooperation with the BSS Application Security Team have implemented suitable Solution Architecture of the application to ensure its appropriate cyber security controls. Security risk assessment and Threat modeling are performed prior moving Application to production. Any significant change (major release) go through Security impact analysis, that can lead to Threat modeling and Security risk assessment artifacts update.
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.	**IR116.** The selection of new vendors is according to Vendor Management Policy. Global procurement team maintains the Approved Vendor List (AVL) for all approved IT vendors and performs review on a yearly basis. All of them are approved by Global Procurement Director. AVLs and VEFs are stored together.

	IR154. A risk assessment, which involves valuation of business information resources and identification and assessment of the levels of risks present, has been performed to identify appropriate and cost-justifiable information security architecture. The risk assessment is performed annually. The IT and Facility Management have implemented suitable information security architecture to ensure that there is appropriate physical and logical security. During the risk assessment, an asset registry, threats regarding infrastructure property, risk classification and review of results of risk assessment are prepared. **IR506.** Ownership of critical business environments, processes, applications and established IT controls as part of the company's IT control framework are assigned to responsible service group acknowledged and documented. Management reviews are in place for key controls in a documented form that is quarterly prepared. **IR554b.** A risk assessment, which involves valuation of business information resources and identification and assessment of the levels of risks present, has been performed to identify appropriate and cost-justifiable information security architecture according to the Secure Development of Internal Applications Guideline. The application development team, in cooperation with the BSS Application Security Team have implemented suitable Solution Architecture of the application to ensure its appropriate cyber security controls. Security risk assessment and Threat modeling are performed prior moving Application to production. Any significant change (major release) go through Security impact analysis, that can lead to Threat modeling and Security risk assessment artifacts update.
CC3.3. The entity considers the potential for fraud in assessing risks to the achievement of objectives.	**IR510.** EPAM is performing a fraud risk assessment on an annual basis or in case of major change in its business processes that has the main goal to identify various types of fraud and evaluate their criticality to business objectives. The fraud risk assessment considers incentives, pressures, opportunities and rationalizations.
CC3.4. The entity identifies and assesses changes that could significantly impact the system of internal control.	**IR116.** The selection of new vendors is according to Vendor Management Policy. Global procurement team maintains the Approved Vendor List (AVL) for all approved IT vendors and performs review on a yearly basis. All of them are approved by Global Procurement Director. AVLs and VEFs are stored together. **IR154.** A risk assessment, which involves valuation of business information resources and identification and assessment of the levels of risks present, has been performed to identify appropriate and cost-justifiable information security architecture. The risk assessment is performed annually. The IT and Facility Management have implemented suitable information security architecture to ensure that there is appropriate physical and logical security. During the risk assessment, an asset registry, threats regarding infrastructure property, risk classification and review of results of risk assessment are prepared. **IR511.** EPAM performs business impact assessments (BIA) for EPAM BSS services in order to support its business continuity program with relevant information. BIAs are also used to determine which controls shall be developed and implemented in order to meet

	business and information classification objectives. EPAM stores a comprehensive list of critical IT elements on the BSS Service Rank intranet page.
	IR554b. A risk assessment, which involves valuation of business information resources and identification and assessment of the levels of risks present, has been performed to identify appropriate and cost-justifiable information security architecture according to the Secure Development of Internal Applications Guideline. The application development team, in cooperation with the BSS Application Security Team have implemented suitable Solution Architecture of the application to ensure its appropriate cyber security controls. Security risk assessment and Threat modeling are performed prior moving Application to production. Any significant change (major release) go through Security impact analysis, that can lead to Threat modeling and Security risk assessment artifacts update.
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.	**IR145.** The information systems organization includes a Service Desk function that acts on user queries regarding systems. Incidents are recorded in a centralized log. Service Groups personnel monitor the log to ensure timely distribution and resolution of user queries. Service groups check the progress of reported issues which are assigned to responsible personnel via Service Desk tickets.
	IR154. A risk assessment, which involves valuation of business information resources and identification and assessment of the levels of risks present, has been performed to identify appropriate and cost-justifiable information security architecture. The risk assessment is performed annually. The IT and Facility Management have implemented suitable information security architecture to ensure that there is appropriate physical and logical security. During the risk assessment, an asset registry, threats regarding infrastructure property, risk classification and review of results of risk assessment are prepared.
	IR508. Independent internal audit function is in place that objectively evaluates performed processes, work products and services against a predefined audit criteria. Internal Audit is also responsible for identifying and documenting noncompliance issues, proposal for improvement and providing feedbacks to auditees and managers on the results of internal audit activities. EPAM performs periodic Information Security Management System (ISMS) and Privacy Information Management System (PIMS) internal audits and results are reviewed with appropriate management. EPAM makes available relevant audit reports and certifications to communicate the state of internal control system to customers.
	IR510. EPAM is performing a fraud risk assessment on an annual basis or in case of major change in its business processes that has the main goal to identify various types of fraud and evaluate their criticality to business objectives. The fraud risk assessment considers incentives, pressures, opportunities and rationalizations.

	IR512b. EPAM performs continuous vulnerability assessments on the cloud environment in order to ensure the ongoing evaluation of its infrastructure such as the patch levels of virtual server images or network and other security configuration.
	IR511. EPAM performs business impact assessments (BIA) for EPAM BSS services in order to support its business continuity program with relevant information. BIAs are also used to determine which controls shall be developed and implemented in order to meet business and information classification objectives. EPAM stores a comprehensive list of critical IT elements on the BSS Service Rank intranet page.
	IR554b. A risk assessment, which involves valuation of business information resources and identification and assessment of the levels of risks present, has been performed to identify appropriate and cost-justifiable information security architecture according to the Secure Development of Internal Applications Guideline. The application development team, in cooperation with the BSS Application Security Team have implemented suitable Solution Architecture of the application to ensure its appropriate cyber security controls. Security risk assessment and Threat modeling are performed prior moving Application to production. Any significant change (major release) go through Security impact analysis, that can lead to Threat modeling and Security risk assessment artifacts update.
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.	**IR504.** EPAM's Audit Committee has a regular meeting to discuss internal and external audit matters by providing an oversight on the company's internal control operation.
	IR508. Independent internal audit function is in place that objectively evaluates performed processes, work products and services against a predefined audit criteria. Internal Audit is also responsible for identifying and documenting noncompliance issues, proposal for improvement and providing feedbacks to auditees and managers on the results of internal audit activities. EPAM performs periodic Information Security Management System (ISMS) and Privacy Information Management System (PIMS) internal audits and results are reviewed with appropriate management. EPAM makes available relevant audit reports and certifications to communicate the state of internal control system to customers.
CC5.1. The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	**IR154.** A risk assessment, which involves valuation of business information resources and identification and assessment of the levels of risks present, has been performed to identify appropriate and cost-justifiable information security architecture. The risk assessment is performed annually. The IT and Facility Management have implemented suitable information security architecture to ensure that there is appropriate physical and logical security. During the risk assessment, an asset registry, threats regarding infrastructure property, risk classification and review of results of risk assessment are prepared.

	IR511. EPAM performs business impact assessments (BIA) for EPAM BSS services in order to support its business continuity program with relevant information. BIAs are also used to determine which controls shall be developed and implemented in order to meet business and information classification objectives. EPAM stores a comprehensive list of critical IT elements on the BSS Service Rank intranet page. **IR513.** Data classification scheme is in place that classifies information based on their criticality and data classification rules are established regarding data storage, transmission and deletion. Information Asset Management Guideline and Data encryption and digital signing work instruction are in place to guide on users on the application of cryptography in alignment with EPAM's data classification scheme. **IR514b.** EPAM maintains a system privileges and application access list that documents granted permissions to access, change or develop systems considering incompatible roles within the organization. Appropriate mechanisms are implemented in order to ensure the security of cloud infrastructure and related elements such as the management plane, virtual environments, containers and container images, access to public cloud services. **IR554b.** A risk assessment, which involves valuation of business information resources and identification and assessment of the levels of risks present, has been performed to identify appropriate and cost-justifiable information security architecture according to the Secure Development of Internal Applications Guideline. The application development team, in cooperation with the BSS Application Security Team have implemented suitable Solution Architecture of the application to ensure its appropriate cyber security controls. Security risk assessment and Threat modeling are performed prior moving Application to production. Any significant change (major release) go through Security impact analysis, that can lead to Threat modeling and Security risk assessment artifacts update.
CC5.2. The entity also selects and develops general control activities over technology to support the achievement of objectives.	**IR157.** Information security tools and techniques are used to restrict access to information resources (e.g., data files, utilities, transactions, programs). Management reviews compliance with internal security policies and approves the implementation and configuration of information security tools and techniques related to logical security. Appropriate corporate policy is in place for granting access privileges for users by the application/system/database/operation system owners and operators and annually reviewed. **IR229a.** A formal methodology or process is used to guide the acquisition, development or maintenance of hardware, application systems, network and communication software and systems software including approving levels, purchase limits, selecting, evaluating, classifying, etc.

	IR048. All systems software purchases are in line with the Technical Procurement Policy. Only system software provided by approved vendors are acquired.
	IR010#. The entity has formal agreement(s) to obtain technical or application support from outside contractors and/or software vendors to ensure availability of such support. Management monitors compliance with these agreements. All system software installations are performed using image files. There are two ways of system software deployment based on hardware type (endpoint or server) For endpoints: The latest version of Standard Installation Software Package is deployed automatically on each endpoint using Microsoft AutoPilot (Intune MDM) within initial device setup. OS Image may be used for deployment as an exception for special cases. For servers: Standard Installation Server Package is added in OS Image file for further OS deployment. OS Image file version history for servers and endpoints is updated, uploaded, and stored for later reference.
	IR506. Ownership of critical business environments, processes, applications and established IT controls as part of the company's IT control framework are assigned to responsible service group acknowledged and documented. Management reviews are in place for key controls in a documented form that is quarterly prepared.
CC5.3. The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	**IR145.** The information systems organization includes a Service Desk function that acts on user queries regarding systems. Incidents are recorded in a centralized log. Service Groups personnel monitor the log to ensure timely distribution and resolution of user queries. Service groups check the progress of reported issues which are assigned to responsible personnel via Service Desk tickets.
	IR157. Information security tools and techniques are used to restrict access to information resources (e.g., data files, utilities, transactions, programs). Management reviews compliance with internal security policies and approves the implementation and configuration of information security tools and techniques related to logical security. Appropriate corporate policy is in place for granting access privileges for users by the application/system/database/operation system owners and operators and annually reviewed.
	IR506. Ownership of critical business environments, processes, applications and established IT controls as part of the company's IT control framework are assigned to responsible service group acknowledged and documented. Management reviews are in place for key controls in a documented form that is quarterly prepared.
CC6.1. The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security	**IR157.** Information security tools and techniques are used to restrict access to information resources (e.g., data files, utilities, transactions, programs). Management reviews compliance with internal security policies and approves the implementation and configuration of information security tools and techniques related to logical security. Appropriate corporate policy is in place for granting access privileges for users by the

events to meet the entity's objectives.	application/system/database/operation system owners and operators and annually reviewed. **IR073.** Application owners authorize the nature and extent of user access privileges, and such privileges are periodically reviewed by application owners to ensure access privileges remain appropriate. User access is controlled through passwords or other mechanism. User access rights are revoked if the user account is terminated. **IR080#.** All software and data are checked for viruses before being loaded onto the entity's systems, thus Endpoint Detection and Response software is installed on all hosts. **IR010#.** The entity has formal agreement(s) to obtain technical or application support from outside contractors and/or software vendors to ensure availability of such support. Management monitors compliance with these agreements. All system software installations are performed using image files. There are two ways of system software deployment based on hardware type (endpoint or server) For endpoints: The latest version of Standard Installation Software Package is deployed automatically on each endpoint using Microsoft AutoPilot (Intune MDM) within initial device setup. OS Image may be used for deployment as an exception for special cases. For servers: Standard Installation Server Package is added in OS Image file for further OS deployment. OS Image file version history for servers and endpoints is updated, uploaded, and stored for later reference. **IR506.** Ownership of critical business environments, processes, applications and established IT controls as part of the company's IT control framework are assigned to responsible service group acknowledged and documented. Management reviews are in place for key controls in a documented form that is quarterly prepared. **IR512b.** EPAM performs continuous vulnerability assessments on the cloud environment in order to ensure the ongoing evaluation of its infrastructure such as the patch levels of virtual server images or network and other security configuration. **IR513.** Data classification scheme is in place that classifies information based on their criticality and data classification rules are established regarding data storage, transmission and deletion. Information Asset Management Guideline and Data encryption and digital signing work instruction are in place to guide on users on the application of cryptography in alignment with EPAM's data classification scheme. **IR514b.** EPAM maintains a system privileges and application access list that documents granted permissions to access, change or develop systems considering incompatible roles within the organization.

	Appropriate mechanisms are implemented in order to ensure the security of cloud infrastructure and related elements such as the management plane, virtual environments, containers and container images, access to public cloud services.
	IR515b. Virtual cloud network is appropriately segmented into private and public subnets based on the criticality of IT elements and business needs. Network perimeter protection is in place that includes logical devices to prevent and detect unauthorized access. Security controls are utilized to connect to cloud resources.
CC6.2. Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	**IR157.** Information security tools and techniques are used to restrict access to information resources (e.g., data files, utilities, transactions, programs). Management reviews compliance with internal security policies and approves the implementation and configuration of information security tools and techniques related to logical security. Appropriate corporate policy is in place for granting access privileges for users by the application/system/database/operation system owners and operators and annually reviewed.
	IR073. Application owners authorize the nature and extent of user access privileges, and such privileges are periodically reviewed by application owners to ensure access privileges remain appropriate. User access is controlled through passwords or other mechanism. User access rights are revoked if the user account is terminated.
	IR514b. EPAM maintains a system privileges and application access list that documents granted permissions to access, change or develop systems considering incompatible roles within the organization. Appropriate mechanisms are implemented in order to ensure the security of cloud infrastructure and related elements such as the management plane, virtual environments, containers and container images, access to public cloud services.
CC6.3. The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	**IR157.** Information security tools and techniques are used to restrict access to information resources (e.g., data files, utilities, transactions, programs). Management reviews compliance with internal security policies and approves the implementation and configuration of information security tools and techniques related to logical security. Appropriate corporate policy is in place for granting access privileges for users by the application/system/database/operation system owners and operators and annually reviewed.
	IR073. Application owners authorize the nature and extent of user access privileges, and such privileges are periodically reviewed by application owners to ensure access privileges

	remain appropriate. User access is controlled through passwords or other mechanism. User access rights are revoked if the user account is terminated. **IR514b.** EPAM maintains a system privileges and application access list that documents granted permissions to access, change or develop systems considering incompatible roles within the organization. Appropriate mechanisms are implemented in order to ensure the security of cloud infrastructure and related elements such as the management plane, virtual environments, containers and container images, access to public cloud services.
CC6.4. The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	**IR586.** Physical access to the Development/Delivery/Business center is restricted to authorized individuals. Physical access to critical protected areas (Data Center, Server room and Stock with valuable assets exceeding $100K USD) is monitored with CCTV and strictly restricted to individuals who require such access to perform their job responsibilities. Management approval is required before access is granted. Access to critical protected areas are annually reviewed.
CC6.5. The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	**IR105.** The Core IT Services Group plans and schedules retention of data and disc and tape backups of EPAM servers including incremental and full backups; the local EUS team under the management of Core IT Services Group is responsible for the erasure and release of media when retention is no longer required. Core IT Services Group yearly reviews retention and release records and documents the results in yearly management reviews. **IR525.** EPAM has defined Data Privacy policies and procedures in place to determine the requirements for data retention, secure disposal, data subject request, access or refusal to personal information. In case of correction is requested, after appropriate authentication, EPAM updates or corrects personal information.
CC6.6. The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	**IR157.** Information security tools and techniques are used to restrict access to information resources (e.g., data files, utilities, transactions, programs). Management reviews compliance with internal security policies and approves the implementation and configuration of information security tools and techniques related to logical security. Appropriate corporate policy is in place for granting access privileges for users by the application/system/database/operation system owners and operators and annually reviewed. **IR073.** Application owners authorize the nature and extent of user access privileges, and such privileges are periodically reviewed by application owners to ensure access privileges remain appropriate. User access is controlled through passwords or other mechanism. User access rights are revoked if the user account is terminated.

	IR080#. All software and data are checked for viruses before being loaded onto the entity's systems, thus Endpoint Detection and Response software is installed on all hosts.
	IR515b. Virtual cloud network is appropriately segmented into private and public subnets based on the criticality of IT elements and business needs. Network perimeter protection is in place that includes logical devices to prevent and detect unauthorized access. Security controls are utilized to connect to cloud resources.
CC6.7. The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	**IR157.** Information security tools and techniques are used to restrict access to information resources (e.g., data files, utilities, transactions, programs). Management reviews compliance with internal security policies and approves the implementation and configuration of information security tools and techniques related to logical security. Appropriate corporate policy is in place for granting access privileges for users by the application/system/database/operation system owners and operators and annually reviewed.
	IR513. Data classification scheme is in place that classifies information based on their criticality and data classification rules are established regarding data storage, transmission and deletion. Information Asset Management Guideline and Data encryption and digital signing work instruction are in place to guide on users on the application of cryptography in alignment with EPAM's data classification scheme.
	IR516. EPAM Work Instructions are available to minimize the risk of data loss: Mobile Device Handling and Removable Digital Media Handling documents. The usage of removable media is decided based on project requirements
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.	**IR512b.** EPAM performs continuous vulnerability assessments on the cloud environment in order to ensure the ongoing evaluation of its infrastructure such as the patch levels of virtual server images or network and other security configuration.
	IR080#. All software and data are checked for viruses before being loaded onto the entity's systems, thus Endpoint Detection and Response software is installed on all hosts.
	IR082. Software licenses purchased by EPAM are registered in HP Asset Manager. Windows and MAC based computers across EPAM network are scanned centrally by SNOW software inventory system, and compared with license information in HP Asset Manager. Scan period depends on multiple conditions and vary from 1 days to 1 months. On a monthly basis License Management Support team prepares audit reports on any

	exceptions identified and sends automatic email notification to the users concerned and ensures that either licenses are obtained, software is removed, or license information updated. **IR050a.** Application developments and modifications are tested in accordance with test plans that include applicable testing types as defined in the contract. Performed testing is properly documented.Tests are performed in a separate environment before the new code is implemented in the production system. **IR517.** EPAM has established a configuration management process that includes the planning, identification and auditing of configuration changes in line with project and product requirements. Change management process is in place to detect the changes of software or configuration parameters.
CC7.1. To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	**IR157.** Information security tools and techniques are used to restrict access to information resources (e.g., data files, utilities, transactions, programs). Management reviews compliance with internal security policies and approves the implementation and configuration of information security tools and techniques related to logical security. Appropriate corporate policy is in place for granting access privileges for users by the application/system/database/operation system owners and operators and annually reviewed. **IR050a.** Application developments and modifications are tested in accordance with test plans that include applicable testing types as defined in the contract. Performed testing is properly documented.Tests are performed in a separate environment before the new code is implemented in the production system. **IR050b.** New in-house developed or purchased applications and changes to applications are tested in accordance with test plans that may include appropriate testing types according to EPAM procedures; then approved by appropriate data / system owners prior to moving into production. Management monitors implementation of all such changes **IR010#.** The entity has formal agreement(s) to obtain technical or application support from outside contractors and/or software vendors to ensure availability of such support. Management monitors compliance with these agreements. All system software installations are performed using image files. There are two ways of system software deployment based on hardware type (endpoint or server) For endpoints: The latest version of Standard Installation Software Package is deployed automatically on each endpoint using Microsoft AutoPilot (Intune MDM) within initial device setup. OS Image may be used for deployment as an exception for special cases. For servers: Standard Installation Server Package is added in OS Image file for further OS deployment. OS Image file version history for servers and endpoints is updated, uploaded, and stored for later reference.

IR517. EPAM has established a configuration management process that includes the planning, identification and auditing of configuration changes in line with project and product requirements. Change management process is in place to detect the changes of software or configuration parameters.

IR518b. EPAM stores a comprehensive list of critical devices and systems on the BSS Service Rank intranet page.
EPAM performs logging and monitoring on critical applications and infrastructure elements that include virtual network appliances, operating systems, containers, databases and EPAM developed or third party acquired applications, middleware, hypervisors or hardware equipment.

CC7.2. The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.

IR145. The information systems organization includes a Service Desk function that acts on user queries regarding systems. Incidents are recorded in a centralized log. Service Groups personnel monitor the log to ensure timely distribution and resolution of user queries. Service groups check the progress of reported issues which are assigned to responsible personnel via Service Desk tickets.

IR116. The selection of new vendors is according to Vendor Management Policy. Global procurement team maintains the Approved Vendor List (AVL) for all approved IT vendors and performs review on a yearly basis. All of them are approved by Global Procurement Director. AVLs and VEFs are stored together.

IR157. Information security tools and techniques are used to restrict access to information resources (e.g., data files, utilities, transactions, programs). Management reviews compliance with internal security policies and approves the implementation and configuration of information security tools and techniques related to logical security. Appropriate corporate policy is in place for granting access privileges for users by the application/system/database/operation system owners and operators and annually reviewed.

IR586. Physical access to the Development/Delivery/Business center is restricted to authorized individuals. Physical access to critical protected areas (Data Center, Server room and Stock with valuable assets exceeding $100K USD) is monitored with CCTV and strictly restricted to individuals who require such access to perform their job responsibilities. Management approval is required before access is granted. Access to critical protected areas are annually reviewed.

IR503. EPAM has established IT Security and Privacy Policies and communicates it to all employees. Security policies define requirements for security, availability, confidentiality

	and privacy including the definition of employee and management responsibilities. IT Security and Privacy Policies are periodically reviewed. **IR508.** Independent internal audit function is in place that objectively evaluates performed processes, work products and services against a predefined audit criteria. Internal Audit is also responsible for identifying and documenting noncompliance issues, proposal for improvement and providing feedbacks to auditees and managers on the results of internal audit activities. EPAM performs periodic Information Security Management System (ISMS) and Privacy Information Management System (PIMS) internal audits and results are reviewed with appropriate management. EPAM makes available relevant audit reports and certifications to communicate the state of internal control system to customers. **IR512b.** EPAM performs continuous vulnerability assessments on the cloud environment in order to ensure the ongoing evaluation of its infrastructure such as the patch levels of virtual server images or network and other security configuration. **IR515b.** Virtual cloud network is appropriately segmented into private and public subnets based on the criticality of IT elements and business needs. Network perimeter protection is in place that includes logical devices to prevent and detect unauthorized access. Security controls are utilized to connect to cloud resources.
CC7.3. The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	**IR145.** The information systems organization includes a Service Desk function that acts on user queries regarding systems. Incidents are recorded in a centralized log. Service Groups personnel monitor the log to ensure timely distribution and resolution of user queries. Service groups check the progress of reported issues which are assigned to responsible personnel via Service Desk tickets. **IR509.** EPAM has established a description (Communications Work Instructions) and processes in order to maintain and clarify communication methods for internal communication as well as communication with EPAM's Partners and Customers. **IR518b.** EPAM performs logging and monitoring on critical applications and infrastructure elements that include virtual network appliances, operating systems, containers, databases and EPAM developed or third party acquired applications, middleware, hypervisors or hardware equipment. **IR521.** EPAM maintains a complete, accurate and timely record of detected or reported unauthorized disclosures (including breaches) of personal information.
CC7.4. The entity responds to identified security incidents by executing a defined incident	**IR145.** The information systems organization includes a Service Desk function that acts on user queries regarding systems. Incidents are recorded in a centralized log. Service Groups personnel monitor the log to ensure timely distribution and resolution of user queries.

response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Service groups check the progress of reported issues which are assigned to responsible personnel via Service Desk tickets. **IR509.** EPAM has established a description (Communications Work Instructions) and processes in order to maintain and clarify communication methods for internal communication as well as communication with EPAM's Partners and Customers **IR512b.** EPAM performs continuous vulnerability assessments on the cloud environment in order to ensure the ongoing evaluation of its infrastructure such as the patch levels of virtual server images or network and other security configuration. **IR520b.** EPAM has established appropriate security measurements to ensure business continuity and disaster recovery for cloud infrastructure that includes multi zone deployment, load balancing, read replicas of databases etc. EPAM critical services (applications) developed step by step disaster recovery plans. Disaster Recovery Plans are tested annually in order to ensure that disaster recovery procedures can be implemented in real emergency situations. Dedicated teams are reperforming such tests in a timely manner. Lessons learned are analyzed and incidents response plan and recovery procedures are improved. **IR521.** EPAM maintains a complete, accurate and timely record of detected or reported unauthorized disclosures (including breaches) of personal information.
CC7.5. The entity identifies, develops, and implements activities to recover from identified security incidents.	**IR519.** EPAM's business continuity program is regularly reviewed and tested. When testing business continuity program the testing includes as per relevant, the development of testing scenarios, consideration of relevant system components, scenarios that consider the potential for the lack of availability for key personnel and revision of continuity plan and systems based on the test results. **IR520b.** EPAM has established appropriate security measurements to ensure business continuity and disaster recovery for cloud infrastructure that includes multi zone deployment, load balancing, read replicas of databases etc. EPAM critical services (applications) developed step by step disaster recovery plans. Disaster Recovery Plans are tested annually in order to ensure that disaster recovery procedures can be implemented in real emergency situations. Dedicated teams are reperforming such tests in a timely manner. Lessons learned are analyzed and incidents response plan and recovery procedures are improved.
CC8.1. The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements	**IR050a.** Application developments and modifications are tested in accordance with test plans that include applicable testing types as defined in the contract. Performed testing is

changes to infrastructure, data, software, and procedures to meet its objectives.	properly documented.Tests are performed in a separate environment before the new code is implemented in the production system.
	IR050b. New in-house developed or purchased applications and changes to applications are tested in accordance with test plans that may include appropriate testing types according to EPAM procedures; then approved by appropriate data / system owners prior to moving into production. Management monitors implementation of all such changes **IR062.** Change management plans are prepared for all new installations or modification of systems software. New systems software, configurations and updates are tested and approved by Core IT Services Group. They prepare new operating system configurations in accordance with corporate standards. In case of system patches, they are tested first; there is no auto-approval of patches. **IR044a.** Management approves all decisions to provide application system development, testing, support, consultancy and maintenance services to EPAM's clients by signing the contracts (Master Service Agreements) in order to ensure that provided services are consistent with the organization's systems plans and strategies. **IR045.** Management approves acquisition of computer hardware in order to ensure that such purchases and developments are consistent with the organization's system plans and strategies. The purchase orders are registered and approved in Cost Tracking Center (CTC) system. **IR517.** EPAM has established a configuration management process that includes the planning, identification and auditing of configuration changes in line with project and product requirements. Change management process is in place to detect the changes of software or configuration parameters.
CC9.1. The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	**IR154.** A risk assessment, which involves valuation of business information resources and identification and assessment of the levels of risks present, has been performed to identify appropriate and cost-justifiable information security architecture. The risk assessment is performed annually. The IT and Facility Management have implemented suitable information security architecture to ensure that there is appropriate physical and logical security. During the risk assessment, an asset registry, threats regarding infrastructure property, risk classification and review of results of risk assessment are prepared. **IR554b.** A risk assessment, which involves valuation of business information resources and identification and assessment of the levels of risks present, has been performed to identify appropriate and cost-justifiable information security architecture according to the Secure Development of Internal Applications Guideline. The application development team, in cooperation with the BSS Application Security Team have implemented suitable Solution Architecture of the application to ensure its appropriate cyber security controls. Security risk

This report is intended solely for the information and use of the management of EPAM, its clients who have used EPAM's services, and the independent auditors of its clients, and is not intended to be, AND SHOULD NOT BE, USED BY ANYONE OTHER THAN THESE SPECIFIED PARTIES.

	assessment and Threat modeling are performed prior moving Application to production. Any significant change (major release) go through Security impact analysis, that can lead to Threat modeling and Security risk assessment artifacts update.
CC9.2. The entity assesses and manages risks associated with vendors and business partners.	**IR001.** Formal selection criteria are developed to control the IT vendor selection. Management monitors compliance with IT Technical Procurement WI. The approved vendor list (AVL) is the primary source for procurement. AVL template is prepared. Vendor evaluations are performed once a year by Global Procurement Director in cooperation with the local EUS Managers (VEFs). **IR116.** The selection of new vendors is according to Vendor Management Policy. Global procurement team maintains the Approved Vendor List (AVL) for all approved IT vendors and performs review on a yearly basis. All of them are approved by Global Procurement Director. AVLs and VEFs are stored together. **IR109.** Global Procurement organizes review of vendor's SLAs done by IT country heads and Head of Data Center Operations collects their feedbacks for each vendor on a yearly basis according to the Technical Procurement Work Instruction. **IR154.** A risk assessment, which involves valuation of business information resources and identification and assessment of the levels of risks present, has been performed to identify appropriate and cost-justifiable information security architecture. The risk assessment is performed annually. The IT and Facility Management have implemented suitable information security architecture to ensure that there is appropriate physical and logical security. During the risk assessment, an asset registry, threats regarding infrastructure property, risk classification and review of results of risk assessment are prepared. **IR010#.** The entity has formal agreement(s) to obtain technical or application support from outside contractors and/or software vendors to ensure availability of such support. Management monitors compliance with these agreements. All system software installations are performed using image files. There are two ways of system software deployment based on hardware type (endpoint or server) For endpoints: The latest version of Standard Installation Software Package is deployed automatically on each endpoint using Microsoft AutoPilot (Intune MDM) within initial device setup. OS Image may be used for deployment as an exception for special cases. For servers: Standard Installation Server Package is added in OS Image file for further OS deployment. OS Image file version history for servers and endpoints is updated, uploaded, and stored for later reference. **IR554b.** A risk assessment, which involves valuation of business information resources and identification and assessment of the levels of risks present, has been performed to identify appropriate and cost-justifiable information security architecture according to the Secure Development of Internal Applications Guideline. The application development team, in cooperation with the BSS Application Security Team have implemented suitable Solution Architecture of the application to ensure its appropriate cyber security controls. Security risk assessment and Threat modeling are performed prior moving Application to production.

	Any significant change (major release) go through Security impact analysis, that can lead to Threat modeling and Security risk assessment artifacts update.
A1.1. The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	**IR025#.** Management reviews systems performance or utilization reports and monitors that adequate action is taken upon identification of inefficient performance and formulate and implement solutions. **IR522.** Capacity planning activities are undertaken to allow extra capacity (human resources and hardware) to be commissioned before projected bottlenecks/overloads materialize. Resource plan which contains the necessary skills and human resource is available for each project, monitored and kept up to date by the Project/Delivery Manager.
A1.2. The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	**IR099.** Batch and on-line backup are performed according to the schedule and daily monitored globally by Core IT Services Group to ensure successful and timely completion, including a review and resolution of any exceptions. Backups are tested on quarterly basis to ensure consistency and to prevent data loss **IR105.** The Core IT Services Group plans and schedules retention of data and disc and tape backups of EPAM servers including incremental and full backups; the local EUS team under the management of Core IT Services Group is responsible for the erasure and release of media when retention is no longer required. Core IT Services Group yearly reviews retention and release records and documents the results in yearly management reviews. **IR154.** A risk assessment, which involves valuation of business information resources and identification and assessment of the levels of risks present, has been performed to identify appropriate and cost-justifiable information security architecture. The risk assessment is performed annually. The IT and Facility Management have implemented suitable information security architecture to ensure that there is appropriate physical and logical security. During the risk assessment, an asset registry, threats regarding infrastructure property, risk classification and review of results of risk assessment are prepared. **IR519.** EPAM's business continuity program is regularly reviewed and tested. When testing business continuity program the testing includes as per relevant, the development of testing scenarios, consideration of relevant system components, scenarios that consider the

	potential for the lack of availability for key personnel and revision of continuity plan and systems based on the test results. **IR520b.** EPAM has established appropriate security measurements to ensure business continuity and disaster recovery for cloud infrastructure that includes multi zone deployment, load balancing, read replicas of databases etc. EPAM critical services (applications) developed step by step disaster recovery plans. Disaster Recovery Plans are tested annually in order to ensure that disaster recovery procedures can be implemented in real emergency situations. Dedicated teams are reperforming such tests in a timely manner. Lessons learned are analyzed and incidents response plan and recovery procedures are improved. **IR554b.** A risk assessment, which involves valuation of business information resources and identification and assessment of the levels of risks present, has been performed to identify appropriate and cost-justifiable information security architecture according to the Secure Development of Internal Applications Guideline. The application development team, in cooperation with the BSS Application Security Team have implemented suitable Solution Architecture of the application to ensure its appropriate cyber security controls. Security risk assessment and Threat modeling are performed prior moving Application to production. Any significant change (major release) go through Security impact analysis, that can lead to Threat modeling and Security risk assessment artifacts update.
A1.3. The entity tests recovery plan procedures supporting system recovery to meet its objectives.	**IR519.** EPAM's business continuity program is regularly reviewed and tested. When testing business continuity program the testing includes as per relevant, the development of testing scenarios, consideration of relevant system components, scenarios that consider the potential for the lack of availability for key personnel and revision of continuity plan and systems based on the test results. **IR520b.** EPAM has established appropriate security measurements to ensure business continuity and disaster recovery for cloud infrastructure that includes multi zone deployment, load balancing, read replicas of databases etc. EPAM critical services (applications) developed step by step disaster recovery plans. Disaster Recovery Plans are tested annually in order to ensure that disaster recovery procedures can be implemented in real emergency situations. Dedicated teams are reperforming such tests in a timely manner. Lessons learned are analyzed and incidents response plan and recovery procedures are improved.
C1.1. The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	**IR157.** Information security tools and techniques are used to restrict access to information resources (e.g., data files, utilities, transactions, programs). Management reviews compliance with internal security policies and approves the implementation and configuration of information security tools and techniques related to logical security. Appropriate corporate policy is in place for granting access privileges for users by the application/system/database/operation system owners and operators and annually reviewed.

	IR503. EPAM has established IT Security and Privacy Policies and communicates it to all employees. Security policies define requirements for security, availability, confidentiality and privacy including the definition of employee and management responsibilities. IT Security and Privacy Policies are periodically reviewed. **IR513.** Data classification scheme is in place that classifies information based on their criticality and data classification rules are established regarding data storage, transmission and deletion. Information Asset Management Guideline and Data encryption and digital signing work instruction are in place to guide on users on the application of cryptography in alignment with EPAM's data classification scheme. **IR105.** The Core IT Services Group plans and schedules retention of data and disc and tape backups of EPAM servers including incremental and full backups; the local EUS team under the management of Core IT Services Group is responsible for the erasure and release of media when retention is no longer required. Core IT Services Group yearly reviews retention and release records and documents the results in yearly management reviews.
C1.2. The entity disposes of confidential information to meet the entity’s objectives related to confidentiality.	**IR525.** EPAM has defined Data Privacy policies and procedures in place to determine the requirements for data retention, secure disposal, data subject request, access or refusal to personal information. In case of correction is requested, after appropriate authentication, EPAM updates or corrects personal information. **IR105.** The Core IT Services Group plans and schedules retention of data and disc and tape backups of EPAM servers including incremental and full backups; the local EUS team under the management of Core IT Services Group is responsible for the erasure and release of media when retention is no longer required. Core IT Services Group yearly reviews retention and release records and documents the results in yearly management reviews.

EPAM CONTROL ACTIVITIES, TEST PROCEDURES AND TEST RESULTS BY DELOITTE

The following information is provided:

1. The column “**Control ID**” shows the unique identifier of particular controls.
2. The column “**EPAM Control Activity**” states the measures that were specified by EPAM in order to achieve the Trust Services Criteria;
3. The column “**Deloitte Test Procedures**” states the measures and test with which Deloitte tested whether the controls of EPAM have been operating effectively;
4. In the column “**Test Results**”, a conclusion based on the assessment of effectiveness is given.

Control ID	EPAM Control Activity	Deloitte Test Procedures	Test Results
IR117.	Information systems strategies and long- and short-term plans have been formulated and approved by management to support the overall business strategy and information systems requirements of the entity. Information systems performance is monitored by management.	Inquiry with relevant personnel about IT strategy and planning procedures. Observed the long term IT strategy and short term IT budgets are in place. During the testing, inspected the management review report to ascertain whether management reviewed the IT strategy, the budget and monitored the information systems and projects.	No relevant exceptions noted
IR123a.	The necessary skills and experience required for the positions according to EPAM's business needs are clearly defined before hiring staff. EPAM Talent Acquisition team is responsible for the recruitment process. The skills and required experience are set by the Resource Managers. Acquired skills are stored and linked to the employee profile.	Inquiry with relevant personnel on HR procedures related to hiring and staff evaluation. Inspected the relevant policies for each locations relating to this control activity: • Global People Management Process Description • Guide for New Employee • Employee Recruitment • Talent Aqusation Process Description On a sample selection the following was inspected: • The necessary skills definition is available before hiring • Newly gained skills are uploaded in HR system • Updated skills are monitored • Management review is performed to ensure that HR policies are applied and employee records are stored • Resource Manager set up the necessary skills of a new employee • EPAM Talent Acquisition Team is responsible for the recruitment process • Open position with position description exist	No relevant exceptions noted
IR123b.	Resource and Project Managers evaluate staff performance. People Management monitors the performance evaluation process. Staff performance and	Inquiry with relevant personnel about performance assessments and trainings. Inspected the relevant policies for each locations relating to this control activity: • Global People Management Process Description	No relevant exceptions noted

This report is intended solely for the information and use of the management of EPAM, its clients who have used EPAM’s services, and the independent auditors of its clients, and is not intended to be, AND SHOULD NOT BE, USED BY ANYONE OTHER THAN THESE SPECIFIED PARTIES.

Control ID	EPAM Control Activity	Deloitte Test Procedures	Test Results
	evaluations records are stored and linked to the employee profile.	On a sample selection the following was inspected: • Regular performance evaluation is performed • Regular evaluation performed by proper responsible personnel • Management quarterly reviews the training plan and communicates it to employees	
IR126.	Formal or on-the-job training is provided to all full-time employees (exceptions are defined on the Feedback KB portal) within the computer processing environment based on annual performance assessments and it is monitored by People Management. The required trainings are determined based on the project requirements. The training attendance is documented and kept on track, inspected by People Management. Training service centers are available for all employees that also includes trainings on ethical values and data privacy.	Inquiry with relevant personnel about performance assessments and trainings. Inspected the relevant policies relating to this control activity: • Global People Management Process Description • Organizational Training Process Description • Mandatory Training Program On a sample selection the following was inspected: • Formal or on-the-job training is provided to all personnel within the computer processing environments • Regular performance evaluation is performed • Management regularly reviews the training plan and communicates it to employees • Automatic e-mail notifications are sent to employees and management about overdue trainings	No relevant exceptions noted
IR099.	Batch and on-line backup are performed according to the schedule and daily monitored globally by Core IT Services Group to ensure successful and timely completion, including a review and resolution of any exceptions. Backups are tested on quarterly basis to ensure consistency and to prevent data loss.	Inquiry with relevant personnel on daily processing and batch jobs. Inspected the relevant policies relating to this control activity: • Backup Description which defines the backup process and the backup software On a sample selection the following was inspected: • Logs created by automated jobs are informative and allow analytics to be performed upon • On-line and batch processing logs are inspected and in case any failure, timely investigation is made • Management quarterly reviews the processing	No relevant exceptions noted

Control ID	EPAM Control Activity	Deloitte Test Procedures	Test Results
IR105.	The Core IT Services Group plans and schedules retention of data and disc and tape backups of EPAM servers including incremental and full backups; the local EUS team under the management of Core IT Services Group is responsible for the erasure and release of media when retention is no longer required. Core IT Services Group yearly reviews retention and release records and documents the results in yearly management reviews.	Inquiry with relevant personnel on planning and schedule of backups. Inspected the relevant policies relating to this control activity: • Backup Description which defines the backup process and the backup software On a sample selection the following was inspected: • Backup log files are in place • Backup processing logs are inspected and in case any failure, timely investigation is made • Backup log files are reviewed • Management yearly reviews the retention and release records	No relevant exceptions noted
IR145.	The information systems organization includes a Service Desk function that acts on user queries regarding systems. Incidents are recorded in a centralized log. Service Groups personnel monitor the log to ensure timely distribution and resolution of user queries. Service groups check the progress of reported issues which are assigned to responsible personnel via Service Desk tickets.	Inquiry with the relevant personnel about service desk procedure. Inspected the relevant policies relating to this control activity: • Incident Management Process Description that provides instructions to respond to computer security-related incidents. On a sample selection the following was inspected: • Service Desk ticket logs are available and include all necessary relevant information (date, time, location, issue description, status) • Service Desk requests are resolved timely and in case any threshold crossed, timely investigation is made • Service Desk's performance is monitored monthly and status reports are available • Timely processing index and Reopen index for the reported incidents are calculated for the audited period for the in scope locations and concluded that these are met KPI thresholds set by the management	No relevant exceptions noted
IR001.	Formal selection criteria are developed to control the IT vendor selection. Management monitors compliance with IT Technical Procurement WI.	Inquiry with relevant personnel on vendor selection procedures. Inspected the relevant policies relating to this control activity:	No relevant exceptions noted

Control ID	EPAM Control Activity	Deloitte Test Procedures	Test Results
	The approved vendor list (AVL) is the primary source for procurement. AVL template is prepared. Vendor evaluations are performed once a year by Global Procurement Director in cooperation with the local EUS Managers (VEFs).	• Technical Procurement Work Instruction which defines the process of vendor selection and vendor evaluation The following was inspected: • Vendor selection criteria are developed • Vendor evaluation form is defined • Approval levels are defined and mandatory approvers are automatically selected • Evaluation form is completed and approved for new vendors • Vendor evaluation is performed in accordance with the Work Instruction • Vendor service characteristics are part of the vendor evaluation • Management reviews the compliance with the Work Instruction	
IR116.	The selection of new vendors is according to Vendor Management Policy. Global procurement team maintains the Approved Vendor List (AVL) for all approved IT vendors and performs review on a yearly basis. All of them are approved by Global Procurement Director. AVLs and VEFs are stored together.	Inquiry with relevant personnel on vendor selection procedures. Inspected the relevant policies relating to this control activity: • Technical Procurement Work Instruction which defines the process of vendor selection and vendor evaluation. On a sample selection the following was inspected: • Approved vendor lists are available • Global Procurement Team performed the review of AVLs • The vendors on the vendor list are approved	No relevant exceptions noted
IR109.	Global Procurement organizes review of vendor's SLAs done by IT country heads and Head of Data Center Operations collects their feedbacks for each vendor on a yearly basis according to the Technical Procurement Work Instruction.	Inquiry with the relevant personnel about service level monitoring. On a sample selection the following was inspected: • SLAs are stored and inspected for relevant vendors in HP Asset Manager that are approved by IT country heads	No relevant exceptions noted
IR157.	Information security tools and techniques are used to restrict access to information resources (e.g., data files, utilities, transactions, programs). Management	Inquiry with the relevant personnel on information security tools and policies.	No relevant exceptions noted

This report is intended solely for the information and use of the management of EPAM, its clients who have used EPAM's services, and the independent auditors of its clients, and is not intended to be, AND SHOULD NOT BE, USED BY ANYONE OTHER THAN THESE SPECIFIED PARTIES.

Control ID	EPAM Control Activity	Deloitte Test Procedures	Test Results
	reviews compliance with internal security policies and approves the implementation and configuration of information security tools and techniques related to logical security. Appropriate corporate policy is in place for granting access privileges for users by the application/system /database/operation system owners and operators and annually reviewed.	Inspected the relevant policies relating to this control activity. The following was inspected: • Access to systems and applications document exists • Access to workstations and portable devices has been implemented and compliant with logical access policies • Antivirus system tool has been implemented • Network protection including firewall and intrusion detection system has been implemented • VPN (virtual private network) has been implemented • Management review has been performed on this control	
IR073.	Application owners authorize the nature and extent of user access privileges, and such privileges are periodically reviewed by application owners to ensure access privileges remain appropriate. User access is controlled through passwords or other mechanism. User access rights are revoked if the user account is terminated.	Inquiry with the relevant personnel on information security tools used for access restriction. Inspected the relevant policies relating to this control activity: • Access to Systems and Applications Work Instruction which contains guidance about the procedures of granting access privileges for users by the application/system owners • Information Security policy which contains instructions to collect and clarify basic security issues addressed in EPAM Systems offices On a sample selection the following was inspected: • Application owners authorize the nature and extent of user access privileges • Terminated employees have no access to EPAM internal systems • User access is controlled through passwords and passwords are changed and complex in AD • New user creation is initiated • Approving user profiles is enforced in the system by automatic mechanism • Management review has been performed on this control	Exception noted There was no periodically user access review performed for privileged user access group (Support EPM-HELP IAM Processing group) at Access system (access.epam.com). Mitigation procedure: the members of this group do not change frequently. All of user authorization grants were approved, and user revocations were performed appropriately during scope period.

Control ID	EPAM Control Activity	Deloitte Test Procedures	Test Results
IR154.	A risk assessment, which involves valuation of business information resources and identification and assessment of the levels of risks present, has been performed to identify appropriate and cost-justifiable information security architecture. The risk assessment is performed annually. The IT and Facility Management have implemented suitable information security architecture to ensure that there is appropriate physical and logical security. During the risk assessment, an asset registry, threats regarding infrastructure property, risk classification and review of results of risk assessment are prepared.	Inquiry with relevant personnel on IT risk assessments. Inspected the relevant policies and documentation relating to this control activity: • Security Risk Management for IT Services and Locations which defines how the risk and business impact assessment is performed and how the environmental control mechanisms are reviewed • Asset Registry which collects EPAM's assets • Risk Assessment Spreadsheet which contains the calculation for risk determination The following was inspected: • Risk and business impact assessment is performed • Management yearly reviews and updates the risk assessment and the effectiveness of environmental control mechanisms • Risk assessment process is in place • Risk assessment includes determination and impact of assets regarding daily operation • Risk strategy is defined in case of identified risks	No relevant exceptions noted
IR050b.	New in-house developed or purchased applications and changes to applications are tested in accordance with test plans that may include appropriate testing types according to EPAM procedures; then approved by appropriate data / system owners prior to moving into production. Management monitors implementation of all such changes	Inquiry with relevant personnel on internal application development procedures. Inspected the relevant policies and documentation for each location relating to this control activity: • Change Management for Internal Services Process Description • Configuration Management Process Description On a sample selection the following was inspected: • In case of in-house development, development plans are prepared • In case of modifications, test plans and test cases were prepared where relevant • In case of modification, tests were performed in a separate environment	No relevant exceptions noted

This report is intended solely for the information and use of the management of EPAM, its clients who have used EPAM's services, and the independent auditors of its clients, and is not intended to be, AND SHOULD NOT BE, USED BY ANYONE OTHER THAN THESE SPECIFIED PARTIES.

Control ID	EPAM Control Activity	Deloitte Test Procedures	Test Results
		• In case of modification, changes to the production systems were approved by the relevant management	
IR229a#.	A formal methodology or process is used to guide the acquisition, development or maintenance of hardware, application systems, network and communication software and systems software including approving levels, purchase limits, bidding procedure, selecting, evaluating, classifying, and approving vendors.	Inquiry with the relevant personnel on acquisition, development and maintenance methodology. Inspected the Technical Procurement Work Instruction to ascertain that it guides the procedure of acquisition. Through inspection of the Technical Procurement Work Instruction the following was ascertained: • Approving levels are defined • Bidding procedures are defined • Selecting, evaluating, classifying and vendor approving processes are defined	No relevant exceptions noted
IR048.	All systems software purchases are in line with the Technical Procurement Policy. Only system software provided by approved vendors are acquired.	Inquiry with relevant personnel on system software purchases. Inspection of the relevant policies relating to this control activity: • Technical Procurement Work Instruction Inspected that systems software purchases are performed by Business Systems and Services. On a sample selection the following was inspected: • Acquisition of system software is approved • Approved Vendor List is maintained	No relevant exceptions noted
IR010#.	The entity has formal agreement(s) to obtain technical or application support from outside contractors and/or software vendors to ensure availability of such support. Management monitors compliance with these agreements. All system software installations are performed using image files.	Inquiry with relevant personnel on systems software support and maintenance. Inspected the relevant policies relating to this control activity: • Technical Procurement Work Instruction, which defines how to procure and implement new assets • Hardware Quality Control Checking Work Instruction, which defines the quality control checking workflow On a sample selection the following was inspected: • Support agreements exist	No relevant exceptions noted

Control ID	EPAM Control Activity	Deloitte Test Procedures	Test Results
	There are two ways of system software deployment based on hardware type (endpoint or server) For endpoints: The latest version of Standard Installation Software Package is deployed automatically on each endpoint using Microsoft AutoPilot (Intune MDM) within initial device setup. OS Image may be used for deployment as an exception for special cases. For servers: Standard Installation Server Package is added in OS Image file for further OS deployment. OS Image file version history for servers and endpoints is updated, uploaded, and stored for later reference.	• Management reviews the support agreements with vendors • EPAM approved image files are utilized • Version history for image files is maintained • Standard Installation Server Package are utilized	
IR045.	Management approves acquisition of computer hardware in order to ensure that such purchases and developments are consistent with the organization's system plans and strategies. The purchase orders are registered and approved in Cost Tracking Center (CTC) system.	Inquiry with relevant personnel on IT procurement. Observed that the purchase orders are registered and approved in the Cost Tracking Center. Inspected the relevant policies relating to this control activity: • Technical Procurement Work Instruction, which defines how to procure and implement new assets On a sample selection the following was inspected: • Acquisitions are approved by the relevant personnel	No relevant exceptions noted
IR025#.	Management reviews system performance or utilization reports and monitors that adequate action is taken upon identification of inefficient performance and formulate and implement solutions.	Inquiry with relevant personnel on systems performance monitoring. Observed that EPAM uses hardware monitoring system (EPAM Cloud Orchestrator) for hardware monitoring. The functionality is to generate reports listed by location, server, time period, etc. On a sample selection the following was inspected: • Regular management review on system performance is performed	No relevant exceptions noted

This report is intended solely for the information and use of the management of EPAM, its clients who have used EPAM's services, and the independent auditors of its clients, and is not intended to be, AND SHOULD NOT BE, USED BY ANYONE OTHER THAN THESE SPECIFIED PARTIES.

Control ID	EPAM Control Activity	Deloitte Test Procedures	Test Results
		• Cloud Orchestrator data are available	
IR501.	EPAM prepares, regularly reviews, and updates as needed the company's Code of Ethical Conduct, which is made available to employees, suppliers, and all others publicly on the company's publicly available webpage. Appropriate levels of disciplinary action are imposed for violations of the Code of Ethical Conduct. EPAM maintains a whistleblowing reporting system, which includes internal reporting channels and its EthicsLine. The EthicsLine is an online channel that allows for confidential and anonymous submission of matters that may violate EPAM's Code.	Inquiry with relevant personnel on the maintenance of the company's Compliance Program. Inspected the relevant policies and documents relating to this control activity: • Code of Ethical Conduct • Anti-harassment, anti-discrimination and anti-retaliation policy The following was inspected: • Code of Ethical Conduct is available, approved and updated within the required time frame • Latest version of the Code of Ethical Conduct is published on the company's webpage • Ethics Line is accessible for employees through the company's webpage • Availability of Ethics Line is communicated to employees • Reported violations are registered and handled	No relevant exceptions noted
IR502.	EPAM has established the Background Check Screening Policy that details the different background verifications that new hires are subject to in line with local regulations. EPAM performs screening of new hires that as a minimum include the check of proof of identity, proof of right to work, and global sanctions. Notwithstanding the examination of past activity during the recruitment process, Background Check Screening Policy lists EPAM locations where additional employment verification, education verification, and/or criminal background checks are performed, considering the restrictions of local limitations on the process.	Inquiry with relevant personnel on HR procedures related to background checks and screening. Inspected the relevant policy relating to this control activity: • Background Check and Screening On a sample selection the following was inspected: • Defined background checks and screening procedures have been performed	No relevant transaction to test

Control ID	EPAM Control Activity	Deloitte Test Procedures	Test Results
IR503.	EPAM has established IT Security and Privacy Policies and communicates it to all employees. Security policies define requirements for security, availability, confidentiality and privacy including the definition of employee and management responsibilities. IT Security and Privacy Policies are periodically reviewed.	Inquiry with relevant personnel on the maintenance of the company's policies. Inspected the relevant policies and documents relating to this control activity: • Artifact Management Process Description • Statement of Applicability - Global • Relevant Information Security and Privacy policies The following was inspected: • Information Security and Privacy policies required by the company are established and regularly reviewed • Policies are available for employees on the company's intranet site • Updates to policies are communicated to employees • Automatic notifications are implemented for compliance team when a policy review is required	No relevant exceptions noted
IR504.	EPAM's Audit Committee has a regular meeting to discuss internal and external audit matters by providing an oversight on the company's internal control operation.	Inquiry with relevant personnel on the performed activities of Audit Committee. The following was inspected: • Meeting minutes of Audit Committee meetings are available • Responsible persons are represented themselves at the meeting • Relevant topics, including external and internal audit matters are discussed	No relevant exceptions noted
IR505.	The board of directors are appointed to act on behalf of the company's shareholders that are independent from EPAM's operative management.	Inquiry with relevant personnel on the performed activities of Board of directors. The following was inspected: • Lists of members of executive management and board of directors are available • Board of directors are independent from management	No relevant exceptions noted

Control ID	EPAM Control Activity	Deloitte Test Procedures	Test Results
IR506.	Ownership of critical business environments, processes, applications and established IT controls as part of the company's IT control framework are assigned to responsible service group acknowledged and documented. Management reviews are in place for key controls in a documented form that is quarterly prepared.	Inquiry with relevant personnel on the IT asset management. Inspected the relevant policies and documents relating to this control activity: • IT asset management process description The following was inspected: • List of critical business environments, processes, applications and IT controls are identified and assigned to employees • Control owners are aware of their designation • Management Monitoring Reviews reviews are performed and documented for key controls	No relevant exceptions noted
IR507.	EPAM has an organizational chart defined and documented that clearly states the reporting lines and areas of authority. The organizational chart is regularly updated.	Inquiry with relevant personnel on the maintenance of the company's organizational chart. Inspected the relevant policies and documents relating to this control activity: • Quality Management System Guideline The following was inspected: • Up-to-date organizational chart is available • Organizational chart clearly states the reporting lines and areas of authority	No relevant exceptions noted
IR508.	Independent internal audit function is in place that objectively evaluates performed processes, work products and services against a predefined audit criteria. Internal Audit is also responsible for identifying and documenting noncompliance issues, proposal for improvement and providing feedbacks to auditees and managers on the results of internal audit activities. EPAM performs periodic Information Security Management System (ISMS) and Privacy Information Management System (PIMS) internal audits and results are reviewed with appropriate management.	Inquiry with relevant personnel on the company's internal audit processes Inspected the relevant policies and documents relating to this control activity: • Internal Audit Process Description The following was inspected: • Independent Internal Audit Function is in place • Annual Information Security Management System internal audit has been performed and report is available for Global Services	No relevant exceptions noted

Control ID	EPAM Control Activity	Deloitte Test Procedures	Test Results
	EPAM makes available relevant audit reports and certifications to communicate the state of internal control system to customers.	• Annual Information Security Management System internal audit has been performed and report is available • Annual Information Security internal audit has been performed and report is available • Annual Privacy Information Management System audit has been performed and report is available • Identified audit issues are registered and statuses are tracked • Certification registry is available	
IR509.	EPAM has established a description (Communications Work Instructions) and processes in order to maintain and clarify communication methods for internal communication as well as communication with EPAM's Partners and Customers.	Inquiry with relevant personnel on the company's communication methodologies and channels. Inspected the relevant policies and documents relating to this control activity: • Communication Work Instruction • Public Media Statements and Social Media policy • Internal News Preparation and Distribution Work Instruction The following was inspected: • Communications Work Instruction document is available and kept up-to-date • Requirements for internal and external communications are defined in the company's policies	No relevant exceptions noted
IR510.	EPAM is performing a fraud risk assessment on an annual basis or in case of major change in its business processes that has the main goal to identify various types of fraud and evaluate their criticality to business objectives. The fraud risk assessment considers incentives, pressures, opportunities and rationalizations.	Inquiry with relevant personnel on the Fraud risk assessment procedure. The following was inspected: • Yearly Fraud risk assessment has been performed • Relevant fraud risks have been identified and evaluated their criticality to business objectives • The fraud risk assessment considers incentives, pressures, opportunities and rationalizations • Mitigating controls have been identified and risks have been mitigated to an acceptable level and evaluated their criticality to business objectives	No relevant exceptions noted

Control ID	EPAM Control Activity	Deloitte Test Procedures	Test Results
IR512b.	EPAM performs continuous vulnerability assessments on the cloud environment in order to ensure the ongoing evaluation of its infrastructure such as the patch levels of virtual server images or network and other security configuration.	Inquiry with relevant personnel on the vulnerability assessment and penetration testing processes. Inspected the relevant policies and documents relating to this control activity: • Vulnerability assessment and penetration testing work instruction The following was inspected: • Regular internal penetration tests have been performed for internal applications as per defined by EPAM • Regular external penetration tests have been performed for web-facing applications and network • Qualys vulnerability management system is implemented and scans the IT infrastructure on a daily basis	No relevant exceptions noted
IR513.	Data classification scheme is in place that classifies information based on their criticality and data classification rules are established regarding data storage, transmission and deletion. Information Asset Management Guideline and Data encryption and digital signing work instruction are in place to guide on users on the application of cryptography in alignment with EPAM's data classification scheme.	Inquiry with relevant personnel on the data classification and encryption procedures. Inspected the relevant policies and documents relating to this control activity: • Asset management guideline • Data encryption and digital signing work instruction The following was inspected: • Data classification scheme is in place • Data handling rules for different classes of data are established and documented in relevant policies regarding data storage, transmission and deletion	No relevant exceptions noted
IR514b.	EPAM maintains a system privileges and application access list that documents granted permissions to access, change or develop systems considering incompatible roles within the organization. Appropriate mechanisms are implemented in order to ensure the security of cloud infrastructure and related elements such	Inquiry with relevant personnel on the User Management process. Inspected the relevant policies and documents relating to this control activity: • Cloud Security Work Instruction and the Cloud Permissions matrix	No relevant exceptions noted

Control ID	EPAM Control Activity	Deloitte Test Procedures	Test Results
	as the management plane, virtual environments, containers and container images, access to public cloud services.	- KnowledgeBase (Confluence page) where the User Accesses are detailed The following was inspected: - Privileged level access lists are in place - User access granting and revocation process is in place - Roles and their access level detailed in the Cloud permission matrix including incompatible roles	
IR516.	EPAM Work Instructions are available to minimize the risk of data loss: Mobile Device Handling and Removable Digital Media Handling documents. The usage of removable media is decided based on project requirements	Inquiry with relevant personnel on mobile device and removable media handling. Inspected the relevant policy relating to this control activity: - Mobile Device Handling Work Instruction - Removable Digital Media Handling Work Instruction The following was inspected: - Mobile Device Handling Work Instruction document is available and kept up-to-date - Removable Digital Media Handling Work Instruction document is available and kept up-to-date	No relevant exceptions noted
IR517.	EPAM has established a configuration management process that includes the planning, identification and auditing of configuration changes in line with project and product requirements. Change management process is in place to detect the changes of software or configuration parameters.	Inquiry with relevant personnel on configuration management. Inspected the relevant policies and documents relating to this control activity: - Configuration Management Process Description The following was inspected: - Configuration management baseline is available - Configuration changes are registered in the ESP system, and required details defined by the baseline are included - Critical configuration items are registered and updated in CMDB	No relevant exceptions noted

This report is intended solely for the information and use of the management of EPAM, its clients who have used EPAM's services, and the independent auditors of its clients, and is not intended to be, AND SHOULD NOT BE, USED BY ANYONE OTHER THAN THESE SPECIFIED PARTIES.

Control ID	EPAM Control Activity	Deloitte Test Procedures	Test Results
IR518b.	EPAM stores a comprehensive list of critical devices and systems on the BSS Service Rank intranet page. EPAM performs logging and monitoring on critical applications and infrastructure elements that include virtual network appliances, operating systems, containers, databases and EPAM developed or third party acquired applications, middleware, hypervisors or hardware equipment.	Inquiry with relevant personnel on logging and monitoring procedures. Inspected the relevant policies and documents relating to this control activity: • Security Logging and Monitoring Work Instruction The following was inspected: • Security logging is implemented to identify malicious activities • Monitoring tool is implemented for performance monitoring • Performance monitoring tool sends automatic alerts, identified issues are handled in the ESP system	No relevant exceptions noted
IR511.	EPAM performs business impact assessments (BIA) for EPAM services in order to support its business continuity program with relevant information. BIAs are also used to determine which controls shall be developed and implemented in order to meet business and information classification objectives.	Inquiry with relevant personnel on the business impact assessment procedures. Inspected the relevant policies and documents relating to this control activity: • Global Business Continuity Plan The following was inspected: • Impact score calculation scheme is available • Tier category is calculated and assigned for each IT service • Control and maintenance requirements are defined for different tier categories	No relevant exceptions noted
IR554b.	A risk assessment, which involves valuation of business information resources and identification and assessment of the levels of risks present, has been performed to identify appropriate and cost-justifiable information security architecture according to the Secure Development of Internal Applications Guideline. The application development team, in cooperation with the BSS Application Security Team have	Inquiry with relevant personnel on the User Management process Inspected the relevant policies and documents relating to this control activity: • Secure Development of Internal Application policy • Operational Risk Management for Services and Locations process description • Security Risk Assessment and Threat Model document.	No relevant exceptions noted

This report is intended solely for the information and use of the management of EPAM, its clients who have used EPAM's services, and the independent auditors of its clients, and is not intended to be, AND SHOULD NOT BE, USED BY ANYONE OTHER THAN THESE SPECIFIED PARTIES.

Control ID	EPAM Control Activity	Deloitte Test Procedures	Test Results
	implemented suitable Solution Architecture of the application to ensure its appropriate cyber security controls. Security risk assessment and Threat modeling are performed prior moving Application to production. Any significant change (major release) go through Security impact analysis, that can lead to Threat modeling and Security risk assessment artifacts update..	The following was inspected: • Risk Assessment had been performed • Suitable solution architecture had been implemented • All the required documentation had been created	
IR586.	Physical access to the Delivery/Development Centers and other sensitive locations is restricted to authorized individuals.	Inquiry with relevant personnel on physical security. Inspected the relevant policies for each location relating to this control activity: • Information Resources Physical Security Work Instruction and EPAM Physical And Infrastructural Security Policy which contain procedures to monitor and restrict access the processing locations Based on performed walkthroughs, the following was inspected: • Buildings are guarded and entrance doors are monitored, records are kept • Server rooms are monitored and restricted to individuals who require such access to perform their job responsibilities • Local IT management approves access rights to server room, and only authorized employees have access rights	No relevant exceptions noted
IR511.	EPAM performs business impact assessments (BIA) for EPAM BSS services in order to support its business continuity program with relevant information. BIAs are also used to determine which controls shall be developed and implemented in order to meet business and information classification objectives. EPAM stores a comprehensive list of critical IT elements on the BSS Service Rank intranet page.	Inquiry with relevant personnel on the business impact assessment procedures. Inspected the relevant policies and documents relating to this control activity: • Global Business Continuity Plan The following was inspected: • Impact score calculation scheme is available • Tier category is calculated and assigned for each IT service	No relevant exceptions noted

Control ID	EPAM Control Activity	Deloitte Test Procedures	Test Results
		- Control and maintenance requirements are defined for different tier categories	
IR519.	EPAM's business continuity program is regularly reviewed and tested. When testing business continuity program the testing includes as per relevant, the development of testing scenarios, consideration of relevant system components, scenarios that consider the potential for the lack of availability for key personnel and revision of continuity plan and systems based on the test results.	Inquiry with relevant personnel on the business continuity program and BCDR tests. Inspected the relevant policies and documents relating to this control activity: - Global Business Continuity Plan - Global Statement of Business Continuity The following was inspected: - Business continuity and disaster recovery plan are available - Business continuity and disaster recovery tests are available	No relevant exceptions noted
IR520b.	EPAM has established appropriate security measurements to ensure business continuity and disaster recovery for cloud infrastructure that includes multi zone deployment, load balancing, read replicas of databases etc. EPAM critical services (applications) developed step by step disaster recovery plans. Disaster Recovery Plans are tested annually in order to ensure that disaster recovery procedures can be implemented in real emergency situations. Dedicated teams are reperforming such tests in a timely manner. Lessons learned are analyzed and incidents response plan and recovery procedures are improved.	Inquiry with relevant personnel on the business continuity and disaster recovery plans and DRP tests. Inspected the relevant policies and documents relating to this control activity: - Disaster Recovery Plan for the application in-scope - DRP test documentation for the application in-scope The following was inspected: - Disaster recovery plan is available - DRP test are performed on a yearly basis - Appropriate steps are taken in case of and issue is detected during the DRP tests	No relevant exceptions noted
IR522.	Capacity planning activities are undertaken to allow extra capacity (human resources and hardware) to be commissioned before projected bottlenecks/overloads materialize. Resource plan which contains the necessary skills and human resource is	Inquiry with relevant personnel on capacity planning. The following was inspected: - Quarter BSS review and report are performed on global processes including assumptions and expectations so that estimate capacity for future	No relevant exceptions noted

This report is intended solely for the information and use of the management of EPAM, its clients who have used EPAM's services, and the independent auditors of its clients, and is not intended to be, AND SHOULD NOT BE, USED BY ANYONE OTHER THAN THESE SPECIFIED PARTIES.

Control ID	EPAM Control Activity	Deloitte Test Procedures	Test Results
	available for each project, monitored and kept up to date by the Project/Delivery Manager.	• Necessary human resources are registered for the Mobitru project in Staffing Desk	
IR515b.	Virtual cloud network is appropriately segmented into private and public subnets based on the criticality of IT elements and business needs. Network perimeter protection is in place that includes logical devices to prevent and detect unauthorized access. Security controls are utilized to connect to cloud resources.	Inquiry with relevant personnel on the network protection Inspected the relevant policies and documents relating to this control activity: • Cloud Security Work Instruction The following was inspected: • Virtual network is segmented • Perimeter protection (including firewalls) is implemented • VPN is utilized to connect to EPAM's resources	No relevant exceptions noted
IR521.	EPAM maintains a complete, accurate and timely record of detected or reported unauthorized disclosures (including breaches) of personal information.	Inquiry with relevant personnel on data privacy. The following was inspected: • Detected and reported unauthorized disclosures (including breaches) are registered and handled.	No relevant exceptions noted
IR525.	EPAM has defined Data Privacy policies and procedures in place to determine the requirements for data retention, secure disposal, data subject request, access or refusal to personal information. In case of correction is requested, after appropriate authentication, EPAM updates or corrects personal information.	Inquiry with relevant personnel from the project team and the global Data Privacy team. Inspected the relevant policies and documents relating to this control activity: • Data Privacy Framework • Data Privacy Work Instruction • EPAM Global Privacy Policy • DSAR (Data subject access request) Flow document The following was inspected: • Personal information is corrected after user authentication	No relevant exceptions noted

This report is intended solely for the information and use of the management of EPAM, its clients who have used EPAM's services, and the independent auditors of its clients, and is not intended to be, AND SHOULD NOT BE, USED BY ANYONE OTHER THAN THESE SPECIFIED PARTIES.

5. Additional Information provided by EPAM Systems Inc.

5.1 BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING

EPAM Systems recognizes the importance of establishing and maintaining a comprehensive Business Continuity Management (BCM) Program to protect the continuity of the critical business processes that support its customers. EPAM Systems has established BCM practices, procedures and policies that provide resilience and recovery for critical locations, staff, systems, vendors and processes on a global level throughout the organization.

EPAM Systems has developed a Global Business Continuity Plan (BCP) to enable the recovery of its critical business functions and critical site operations during a disruption, while minimizing adverse impacts on EPAM's customer satisfaction and revenue. As part of this effort, a Business Impact Analysis (BIA) is performed on an ongoing basis across key corporate functions. The BIA identifies EPAM's critical processes, technologies and third-party vendors needed to continue or resume operations as soon as possible following a disruption.

The EPAM Systems BCM Program was derived from generally accepted business continuity guidelines in order to create a customized program for EPAM Systems' unique organizational structure and culture. The BCM Program has sponsorship at the executive level, as well as throughout each local operating region, in order to promote the success of business continuity objectives throughout the entire organization.

The EPAM Systems BCM Program includes:

- Global and set of Local Business Continuity and Disaster recovery Plans developed to maintain business continuity in each of EPAM major locations, regularly reviewed and updated to reflect changes in the organization.
- Business impact analysis (BIA) and risk assessment to identify critical processes, understand impacts of downtime and reveal vulnerabilities.
- Fully operational Disaster Recovery Plans (DRP) to provide disaster recovery and business continuity for critical services.
- A set of Account-level Business Continuity and Disaster Recovery Plans created to ensure customers' contractual obligations.
- An integrated suite of tools for mass notification, risk and compliance tracking, and infrastructure monitoring, enabling rapid communication during incidents, continuous visibility into emerging threats, and proactive management of the organization's resilience posture.
- Governance structure detailing roles and responsibilities of key personnel involved in BCM.
- Communication procedures to share information about the incident with employees, shareholders and customers, among others.
- Proactive measures to minimize the exposure to potential business disruptions.

- Procedures for recovery in the event of a business disruption while maintaining integrity of information and security.
- Regular testing and simulation exercises to validate the effectiveness of the BCM plans with documentation of test results and lessons learned for continuous improvement.
- Training programs to ensure employees are aware of their roles and responsibilities during a business disruption.

Ultimately, the ongoing goals for the EPAM Systems BCM Program are to:

- Protect employee safety
- Maintain customers' contractual obligations
- Uphold customer service levels
- Maintain stakeholders' confidence
- Mitigate revenue loss from an event

As a part of the BCM Program, EPAM is committed to maintaining a comprehensive Crisis Management strategy for effective crisis response, including clear escalation paths, communication protocols, decision-making structures, and involving key stakeholders to ensure coordinated action during critical events.

5.2 RECENT ANALYST RECOGNITIONS AND AWARDS

A full breakdown of EPAM's 2025 analyst recognitions and awards are described below;

Analyst Evaluations:

A snapshot of EPAM's 2025 analyst recognitions and awards are listed below;

Awards & Industry Rankings:

EPAM Named to Newsweek's 2025 Top 100 Most Loved Workplaces for the Fifth Consecutive Year (2021 - 2025) - https://www.newsweek.com/rankings/most-loved-workplaces-2024?sf203027558=1

EPAM Named 2025 Best Places to Work - https://www.glassdoor.com/Award/Best-Places-to-Work-LST_KQ0,19.htm

EPAM is a Great Place to Work® 4 Times Over - https://www.greatplacetowork.in/great/company/epam-systems-india-pvt-ltd, https://greatplacetowork.com.sg/gptwcertified/epam-singapore/, https://greatplacetowork.com.vn/vietnam-best-workplaces-2022-medium-large/, https://www.greatplacetowork.pl/certyfikowane-firmy-2/epam-systems-poland

EPAM Named to Fortune 1000 List for the 7th Year in a Row - https://fortune.com/ranking/fortune500/search/

EPAM on Forbes World's Best Employer List - https://www.forbes.com/lists/worlds-best-employers/

EPAM Wins 2025 SEAL Sustainable Service Award - https://sealawards.com/sustainability-award-2025/

EPAM Recognized for Eight Best-In-Class AI Initiatives at Brandon Hall HCM Excellence Awards - https://excellenceawards.brandonhall.com/winners/

Ad Age Agency Report - #19 on worlds largest Agency companies - https://adage.com/article/datacenter/introducing-agency-report-2023/2481036

Google Cloud Oil & Gas Partner of the Year - https://cloud.google.com/awards/partners

Partner Awards

Winner of the 2024 Microsoft Partner of the Year Award in Gaming - https://partner.microsoft.com/en-us/inspire/awards/winners#tab-4

2024 Databricks Global Partner Award - https://www.databricks.com/blog/databricks-announces-2024-global-partner-awards

Commercetools Partner of the Year - https://www.epam.com/services/partners/commercetools?utm_source=linkedin&utm_medium=social&utm_campaign=partner-commercetools&utm_term=partner-of-the-year

EPAM Google Cloud Partner of the Year - https://cloud.google.com/awards/partners

Analyst Evaluations:

A snapshot of EPAM's 2025 analyst recognitions are listed below;

This report is intended solely for the information and use of the management of EPAM, its clients who have used EPAM's services, and the independent auditors of its clients, and is not intended to be, AND SHOULD NOT BE, USED BY ANYONE OTHER THAN THESE SPECIFIED PARTIES.

A leader in the Gartner®: Magic Quadrant™ for Custom Software Development Services, Worldwide 2025https://www.gartner.com/interactive/mq/7222330?ref=solrResearch&refval=514992677

A Leader in the Gartner®: Emerging Magic Quadrant™ for Generative AI Engineering - Innovation Guide for Generative AI Engineering

A Visionary in the **Gartner®: Magic Quadrant™ for** Digital Experience Services - https://www.gartner.com/document-reader/document/7122730?ref=solrResearch&refval=514993575&

A Star Performer in the Everest Life Sciences Digital Services PEAK Matrix® Assessment 2025 - Life Sciences Digital Services PEAK Matrix® Assessment 2025 - Everest Group Research Portal

Named a Top Engineering Services Firm in Everest Engineering Services Top 50™ - https://www.everestgrp.com/everest-group-engineering-services-top-50/

A Leader in IDC MarketScape for Worldwide Experience Design Services - https://my.idc.com/getdoc.jsp?containerId=US52973225&pageType=PRINTFRIENDLY

A Leader in IDC MarketScape for Worldwide Experience Build Services - https://my.idc.com/getdoc.jsp?containerId=US52973125&pageType=PRINTFRIENDLY

A Strong Performer in the IDC MarketScape for Worldwide Enterprise Strategy Consulting Services 2025 - https://my.idc.com/getdoc.jsp?containerId=US52035225&pageType=PRINTFRIENDLY

A Strong Provider in the IDC MarketScape for Worldwide Digital Business Strategy Consulting Services 2025 - https://my.idc.com/getdoc.jsp?containerId=US52036025&pageType=PRINTFRIENDLY

A strong Provider in the Forrester Wave™ for Connected Product Engineering Services - The Forrester Wave™: Connected Product Engineering... | Forrester

A Strong Provider in the Forrester Wave™ for AI Technical Services - The Forrester Wave™: AI Technical Services, Q4 2025 | Forrester

EPAM Recognized as a Top IT Sourcing Vendor in Europe - https://whitelane.com/europe-2024-2025

5.3 EPAM SYSTEMS AUDIT CERTIFICATIONS

Audit Firms & Certification Bodies

Deloitte	SOC 1 - ISAE 3402	SOC 2 - ISAE 3000	SOC 3 - ISAE 3000	
DNV	ISO/IEC 27001	ISO/IEC 27001 & ISO/IEC 27701	ISO 50001	TISAX
AperSky	PCI DSS	IASME	Cyber Essentials Plus	CyberVadis
SGS	ISO 9001	ISO 14001	LRQA	ISO 13485
ISO/IEC 20000-1	DQS	ISO/IEC 27001	CREST	CREST

This report is intended solely for the information and use of the management of EPAM, its clients who have used EPAM's services, and the independent auditors of its clients, and is not intended to be, AND SHOULD NOT BE, USED BY ANYONE OTHER THAN THESE SPECIFIED PARTIES.

Certificates / Audit Reports by Regions:

ISO/IEC 27001	SOC 1 (ISAE 3402) Type 2 SOC 2 / SOC 3 (ISAE 3000) Type 2	TISAX	ISO 9001 (Software Development)
EPAM GLOBAL • EPAM Global, Business Systems and Services AMERICAS • Mexico, Guadalajara • United States, Boston APAC • China (Shenzhen, Suzhou) • India (Hyderabad, Pune, Bengaluru) EMEA • Belarus, Minsk • Belgium, Brussels • Bulgaria, Sofia • Georgia, Tbilisi • Germany, Berlin, Frankfurt • Germany, Test IO • Hungary (Budapest, Debrecen, Szeged) • Kazakhstan (Almaty, Astana, Karaganda) • Latvia, Riga • Lithuania (Vilnius, Kaunas) • Netherlands, Hoofddorp • Poland (Gdansk, Krakow, Katowice, Warsaw, Wrocław) • Romania, Bucharest • Switzerland, Zurich • Ukraine - EPAM Systems, EPAM Digital LLC, (Kyiv, Lviv) • United Kingdom (London, Newcastle)	EPAM GLOBAL • EPAM Global, Business Systems and Services AMERICAS • United States, Boston • Mexico, Guadalajara APAC • China, Shenzhen • India, Hyderabad • Singapore, Singapore EMEA • Belarus, Minsk • Bulgaria, Sofia • Czech Republic, Prague • Hungary, Budapest • Hungary, Debrecen • Hungary, Szeged • Poland, Gdansk • Poland, Katowice • Poland, Krakow • Poland, Warsaw • Poland, Wroclaw • Spain, Malaga • Ukraine - EPAM Systems, EPAM Digital LLC, Kyiv	EMEA • Germany, Frankfurt **PCI-DSS** EMEA • Belarus, Minsk • Hungary, Budapest • Hungary, Szeged • India, Pune • UAE, Dubai **CyberVadis** EPAM SYSTEMS, INC. **Cyber Essentials / Plus** Cyber Essentials and Cyber Essentials Plus EMEA • EPAM Systems Ltd, United Kingdom	AMERICAS • United States (Newtown, Boston) • Argentina (Buenos Aires, Cordoba) • Mexico, All cities APAC • India, All cities • China (Shenzhen, Suzhou) EMEA • Armenia, All cities • Belarus, All cities • Georgia, All cities • Germany, All cities • Hungary, All cities • Kazakhstan (Almaty, Astana, Karaganda) • Lithuania, All cities • Netherlands, All cities • Poland, All cities • Serbia, All cities • Sweden, All cities • Switzerland, All cities • Ukraine, All cities • United Kingdom, All cities
	SOC 2 / SOC 3 (ISAE 3000) Type 2	**CREST**	**ISO 9001 (Physical Product)**
	EPAM GLOBAL • EPAM Global, Business Systems and Services EMEA • Hungary (Budapest, Szeged)	Cyber security services: • The Americas • EMEA	AMERICAS • United States (Newtown, Boston) EMEA • Belarus, Minsk • Lithuania, Vilnius • Poland, Gdansk
ISO/IEC 27701	**Sarbanes-Oxley Act (SOX)**	**ISO 14001**	**ISO 13485**
EPAM GLOBAL • EPAM Global, Business Systems and Services	EPAM SYSTEMS, INC. Audited annually since 2014	AMERICAS • United States, Newtown EMEA • Germany, All cities • Kazakhstan, All cities • Lithuania, All cities • Netherlands, All cities • Poland, All cities • Serbia, All cities • Sweden, All cities • Switzerland, All cities • United Kingdom, All cities	AMERICAS • United States (Boston, Newtown) APAC • India, Hyderabad EMEA • Belarus, Minsk • Croatia, Zagreb • Hungary, Budapest

This report is intended solely for the information and use of the management of EPAM, its clients who have used EPAM's services, and the independent auditors of its clients, and is not intended to be, AND SHOULD NOT BE, USED BY ANYONE OTHER THAN THESE SPECIFIED PARTIES.

ISO/IEC 27001	SOC 1 (ISAE 3402) Type 2 SOC 2 / SOC 3 (ISAE 3000) Type 2	TISAX	ISO 9001 (Software Development)
		ISO 50001	ISO/IEC 20000-1
		EMEA • Hungary (Budapest, Szeged, Debrecen)	AMERICAS • United States (Newtown) EMEA • United Kingdom (London)

Achievements by Locations:

Country / Entity	Location	Certification / Audit Report	Valid Until
EPAM SYSTEMS, INC.	Newtown	Sarbanes-Oxley Act (SOX)	28-Feb-2025
EPAM SYSTEMS, INC., UNITED STATES, BOSTON	Boston	ISO/IEC 27001 SOC 1 (ISAE 3402) TYPE 2 SOC 2 / SOC 3 (ISAE 3000) TYPE 2 ISO 9001 ISO 9001 (physical product) ISO 13485	31-May-2026 15-Dec-2025 15-Dec-2025 24-Apr-2028 01-Aug-2026 24-Jul-2026
EPAM GLOBAL, BUSINESS SYSTEMS AND SERVICES	Newtown	SOC 1 (ISAE 3402) TYPE 2 SOC 2 / SOC 3 (ISAE 3000) TYPE 2 SOC 2 / SOC 3 (ISAE 3000) TYPE 2 (SaaS) ISO/IEC 27001 ISO/IEC 27701 ISO 9001	15-Dec-2025 15-Dec-2025 30-Jan-2026 31-May-2026 31-May-2026 24-Apr-2028
UNITED STATES	Newtown	ISO 13485 ISO 14001 ISO 9001 (physical product) ISO 9001 ISO 20000-1	24-Jul-2026 14-May-2026 01-Aug-2026 24-Apr-2028 12-Oct-2028
ARGENTINA / VATES	Buenos Aires Cordoba	ISO 9001	17-Jul-2026
ARMENIA	All cities	ISO 9001	24-Apr-2028
BELARUS	Minsk	ISO/IEC 27001 SOC 1 (ISAE 3402) TYPE 2 SOC 2 / SOC 3 (ISAE 3000) TYPE 2 ISO 13485 ISO 9001 (physical product) PCI-DSS	26-Oct-2026 15-Dec-2025 15-Dec-2025 24-Jul-2026 01-Aug-2026 23-Sep-2020
	All cities	ISO 9001	24-Apr-2028
BELGIUM	Brussels	ISO/IEC 27001	31-May-2026
BULGARIA	Sofia	ISO/IEC 27001 SOC 1 (ISAE 3402) TYPE 2 SOC 2 / SOC 3 (ISAE 3000) TYPE 2	31-May-2026 15-Dec-2025 15-Dec-2025

Country / Entity	Location	Certification / Audit Report	Valid Until
CROATIA	Zagreb	ISO 13485	24-Jul-2026
CHINA	Shenzhen	ISO/IEC 27001 SOC 1 (ISAE 3402) TYPE 2 SOC 2 / SOC 3 (ISAE 3000) TYPE 2 ISO 9001	31-May-2026 15-Dec-2025 15-Dec-2025 24-Apr-2025
	Suzhou	ISO/IEC 27001 ISO 9001	31-May-2026 24-Apr-2025
CZECH REPUBLIC	Prague	SOC 1 (ISAE 3402) TYPE 2 SOC 2 / SOC 3 (ISAE 3000) TYPE 2	15-Dec-2025 15-Dec-2025
GEORGIA	Tbilisi	ISO/IEC 27001	31-May-2026
	All cities	ISO 9001	24-Apr-2028
GERMANY / Test IO	Berlin	ISO/IEC 27001	31-May-2026
GERMANY	Berlin	ISO/IEC 27001	31-May-2026
	Frankfurt	ISO/IEC 27001	31-May-2026
	All cities	ISO 14001	14-May-2026
		ASPICE	31-Dec-2025
		TISAX (Frankfurt)	31-Jul-2028
	All Cities	ISO 9001	24-Apr-2028
HUNGARY	Budapest	ISO/IEC 27001 SOC 1 (ISAE 3402) TYPE 2 SOC 2 / SOC 3 (ISAE 3000) TYPE 2 ISO 13485 PCI-DSS ISO 50001	31-May-2026 15-Dec-2025 15-Dec-2025 24-Jul-2026 01-Aug-2026 14-Mar-2020 05-Apr-2026
	Debrecen	ISO/IEC 27001 SOC 1 (ISAE 3402) TYPE 2 SOC 2 / SOC 3 (ISAE 3000) TYPE 2 ISO 50001	31-May-2026 15-Dec-2025 15-Dec-2025 05-Apr-2026
	Szeged	ISO/IEC 27001 SOC 1 (ISAE 3402) TYPE 2 SOC 2 / SOC 3 (ISAE 3000) TYPE 2 PCI-DSS ISO 50001	31-May-2026 15-Dec-2025 15-Dec-2025 14-Mar-2020 05-Apr-2026
	All cities	ISO 9001	24-Apr-2028
INDIA	Hyderabad	ISO/IEC 27001 SOC 1 (ISAE 3402) TYPE 2 SOC 2 / SOC 3 (ISAE 3000) TYPE 2	31-May-2026 15-Dec-2025 15-Dec-2025
	Pune	ISO/IEC 27001 PCI-DSS	31- May-2026 26-Sep-2024

Country / Entity	Location	Certification / Audit Report	Valid Until
	Bengaluru	• ISO/IEC 27001	31-May-2026
	All cities	ISO 9001	24-Apr-2028
KAZAKHSTAN	Almaty	ISO/IEC 27001 ISO 9001	31-May-2026 14-Dec-2027
	Astana	ISO/IEC 27001 ISO 9001	31-May-2026 14-Dec-2027
	Karaganda	ISO/IEC 27001 ISO 9001	31-May-2026 14-Dec-2027
	All cities	ISO 14001	07-Mar-2026
LATVIA	Riga	ISO/IEC 27001	31-May-2026
LITHUANIA	Vilnius, Kaunas	ISO/IEC 27001 ISO 9001 (physical product)	31-May-2026 01-Aug-2026
	All cities	ISO 9001	24-Apr-2028
	All cities	ISO 14001	14-May-2026
MEXICO	Guadalajara	ISO/IEC 27001 SOC 1 (ISAE 3402) TYPE 2 SOC 2 / SOC 3 (ISAE 3000) TYPE 2	31-May-2026 15-Dec-2025 15-Dec-2025
	All cities	ISO 9001	24-Apr-2028
NETHERLANDS	Hoofddorp	ISO/IEC 27001	31-May-2026
	All cities	ISO 9001 ISO 14001	24-Apr-2028 14-May-2026
POLAND	Gdansk	ISO/IEC 27001 SOC 1 (ISAE 3402) TYPE 2 SOC 2 / SOC 3 (ISAE 3000) TYPE 2 ISO 9001 (physical product)	31-May-2026 15-Dec-2025 15-Dec-2025 01-Aug-2026
	Krakow	ISO/IEC 27001 SOC 1 (ISAE 3402) TYPE 2 SOC 2 / SOC 3 (ISAE 3000) TYPE 2	31-May-2026 15-Dec-2025 15-Dec-2025
	Katowice	ISO/IEC 27001 SOC 1 (ISAE 3402) TYPE 2 SOC 2 / SOC 3 (ISAE 3000) TYPE 2	31-May-2026 15-Dec-2025 15-Dec-2025
	Warsaw	ISO/IEC 27001 SOC 1 (ISAE 3402) TYPE 2 SOC 2 / SOC 3 (ISAE 3000) TYPE 2	31-May-2026 15-Dec-2025 15-Dec-2025
	Wroclaw	ISO/IEC 27001 SOC 1 (ISAE 3402) TYPE 2 SOC 2 / SOC 3 (ISAE 3000) TYPE 2	31-May-2026 15-Dec-2025 15-Dec-2025
	All cities	ISO 9001 ISO 14001	24-Apr-2028 14-May-2026
ROMANIA	Bucharest	ISO/IEC 27001	31-May-2026
SERBIA	All cities	ISO 9001 ISO 14001	24-Apr-2028 14-May-2026

This report is intended solely for the information and use of the management of EPAM, its clients who have used EPAM's services, and the independent auditors of its clients, and is not intended to be, AND SHOULD NOT BE, USED BY ANYONE OTHER THAN THESE SPECIFIED PARTIES.

Country / Entity	Location	Certification / Audit Report	Valid Until
SPAIN	Malaga	SOC 1 (ISAE 3402) TYPE 2 SOC 2 / SOC 3 (ISAE 3000) TYPE 2	15-Dec-2025 15-Dec-2025
SINGAPORE	Singapore	SOC 1 (ISAE 3402) TYPE 2 SOC 2 / SOC 3 (ISAE 3000) TYPE 2	15-Dec-2025 15-Dec-2025
SWEDEN	All cities	ISO 9001 ISO 14001	24-Apr-2028 14-May-2026
SWITZERLAND	All cities	ISO 9001 ISO 14001 ISO/IEC 27001	24-Apr-2028 14-May-2026 31-May-2026
UKRAINE EPAM Systems LLC, EPAM Digital LLC	Kyiv	ISO/IEC 27001 SOC 1 (ISAE 3402) TYPE 2 SOC 2 / SOC 3 (ISAE 3000) TYPE 2	31-May-2026 15-Dec-2025 15-Dec-2025
	Lviv	ISO/IEC 27001	31-May-2026
	All cities	ISO 9001	24-Apr-2028
UNITED ARAB EMIRATES	Dubai	PCI-DSS	26-Sep-2024
UNITED KINGDOM	London	ISO/IEC 20000-1	12-Oct-2028
	All cities	ISO/IEC 27001 Cyber Essentials Cyber Essentials Plus ISO 14001 ISO 9001 CREST	31-May-2026 29-May-2025 19-Aug-2025 14-May-2026 24-Apr-2028 01-Jan-2026