GUIBERT & CO
CERTIFIED PUBLIC ACCOUNTANTS

445 Park Avenue – 9th Floor
NEW YORK NYC 10022
TEL: (212) 447-1300
FAX: (212) 447-5017

80, RUE BLANCHE
75009 PARIS
TEL: 01-55-31-77-77
FAX: 01-40-16-90-49

cegedim.cloud

International Standard on Assurance Engagements 3402 (Type II)

IT HOSTING SERVICES SYSTEM

From January 1st, 2024 to December 31, 2024

CONTENT

1. INDEPENDENT AUDITOR'S ASSURANCE REPORT ON THE DESCRIPTION OF CONTROLS, THEIR DESIGN AND OPERATING EFFECTIVENESS

To the Board of Directors of **CEGEDIM.CLOUD**:

We have been engaged to report on the description of the **IT Hosting Services System** of **CEGEDIM.CLOUD** throughout the period from January 1st, 2024 to December 31, 2024, and on the design and operation of controls related to the control objectives stated in the description.

Our examination included procedures to obtain reasonable assurance about whether:

(1) the accompanying description presents fairly, in all material respects, the aspects of the Company's controls that may be relevant to a user organization's internal control as it relates to an audit of financial statements;
(2) the controls included in the description are suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily and user organizations and sub-service organizations applied the controls contemplated in the design of the company's controls; and
(3) such controls are in operation throughout the period from January 1st, 2024 to December 31, 2024.

The responsibilities of CEGEDIM.CLOUD

CEGEDIM.CLOUD is responsible for: preparing the description and accompanying assertion on pages 7-8, including the completeness, accuracy and method of presentation of the description and assertion; providing the services covered by the description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

Auditor's responsibilities

Our responsibility is to express an opinion on the description of the **IT Hosting Services System** of **CEGEDIM.CLOUD** and on the design and operation of controls related to the control objectives stated in that description, based on our procedures. We conducted our engagement in accordance with International Standard on Assurance Engagements 3402, "Assurance Reports on Controls at a Service Organization", issued by the International Auditing and Assurance Standards Board. That standard requires that we comply with ethical requirements and plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organization involves performing procedures to obtain evidence about the disclosures in the service organization's description of its system, and the design and operating effectiveness of controls. The procedures selected depend on the auditor's judgment, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein, and the suitability of the criteria specified by the service organization and described at pages 7-8.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Limitations of Controls at a Service Organization

The description of the **IT Hosting Services System** of **CEGEDIM.CLOUD** is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in its own particular environment. Also, because of their nature, controls at a service organization may not prevent or detect all errors or omissions in processing or reporting transactions. Also, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organization may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in the report. The criteria we used in forming our opinion are those described on pages 7-8. In our opinion, in all material respects:

(a) The description fairly presents the **IT Hosting Services System** as designed and implemented throughout the period from January 1st, 2024 to December 31, 2024;

(b) The controls related to the control objectives stated in the description were suitably designed throughout the period from January 1st, 2024 to December 31, 2024; and

(c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from January 1st, 2024 to December 31, 2024.

Description of tests of controls

The specific controls tested and the nature, timing and results of those tests are listed on pages 18 until 27.

Intended users and purpose

This report and the description of tests of controls on pages 18 until 27 are intended only for customers who have used **CEGEDIM.CLOUD Hosting Services System**, and their auditors, who have a sufficient understanding to consider it, along with other information including information about controls operated by customers themselves, when assessing the risks of material misstatements of customer's financial statements.

January 10th, 2025

Guibert & C

ASSERTION BY THE SERVICE ORGANIZATION

The accompanying description has been prepared for customers who have used the IT hosting 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 of material misstatements of customers' financial statements. CEGEDIM.CLOUD confirms that:

(a) The accompanying description fairly presents the IT hosting services for processing customers' transactions throughout the period from January 1st, 2024 to December 31, 2024. The criteria used in making this assertion were that the accompanying description:

(i) Presents how IT hosting services were designed and implemented, including:

- The types of services provided, including, as appropriate, classes of transactions processed,
- The procedures, within both information technology and manual systems, by which those transactions were initiated, recorded, processed, corrected as necessary, and transferred to the reports prepared for customers.
- The related accounting records, supporting information and specific accounts that were used to initiate, record, process and report transactions; this includes the correction of incorrect information and how information was transferred to the reports prepared for customers.
- How IT hosting services dealt with significant events and conditions, other than transactions.
- The process used to prepare reports for customers.
- Relevant control objectives and controls designed to achieve those objectives.
- Controls that we assumed, in the design of IT hosting services, would be implemented by user entities, and which, if necessary to achieve control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by ourselves alone.
- Other aspects of our control environment, risk assessment process, information system and communication, control activities and

monitoring controls that were relevant to processing and reporting customers' transactions.

(ii) Includes relevant details of changes to the service organization's IT hosting services during the period from January 1st, 2024 to December 31, 2024.

(iii) Does not omit or distort information relevant to the scope of the IT hosting services being described, while acknowledging that the description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect that each individual customer may consider important in its own particular environment.

b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from January 1st, 2024 to December 31, 2024. The criteria used in making this assertion were that:

(i) The risks that threatened achievement of the control objectives stated in the description were identified.

(ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved.

(iii) The controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period from January 1st, 2024 to December 31, 2024.

Frédéric LE GUILLOU
CEO

2. MANAGEMENT DESCRIPTION OF THE CONTROLS IMPLEMENTED BY CEGEDIM.CLOUD

I. Management presentation of the activity of CEGEDIM.CLOUD

CEGEDIM.CLOUD is a global technology and service company, capable of hosting any type of new application, and a solution provider. It benefits from data centers grouped in two regional campuses in France, ensuring IT security and compliance best practices are effectively deployed at all times.

CEGEDIM.CLOUD has extensive expertise in datacenter facilities management as well as in the management of application and cloud services, and designs and implements methods and architectures with very high availability, which meet its customers' most stringent security requirements, and in particular standards governing the hosting of sensitive clients' data & records.

CEGEDIM.CLOUD, thanks to its technical expertise, places at clients' service managed infrastructures enabling them to concentrate on their core business, in an optimal manner and while accessing securely to their data at their discretion.

II. Management description of the control environment, of its assessment of risks and of the systems and procedures put in place to monitor the controls

Control environment

The management of **CEGEDIM.CLOUD** champions an in-house risk control culture, notably through distributing & posting internally validated procedures directed to IT teams.
Management encourages open communications in order to enable employees who so wish to communicate their questions to the appropriate in-house parties.
Oversight of the correct operation of day-to-day activities under the enterprise's key processes is carried out by management as part of its general responsibilities.
Also, staff competencies are managed on a regular basis to ensure new competencies are in place to meet clients' evolving needs.

Risk assessment

Risk assessment within **CEGEDIM.CLOUD** is focused on data security and integrity, and on ensuring continuity of operations. Internal procedures are in place to cover these risks. In addition, an Intranet is in place in order to bring together in a single location all information related to data security and integrity.

Monitoring the controls
Within **CEGEDIM.CLOUD** a dedicated Compliance manager is responsible for monitoring the effectiveness of the controls and for updating the internal control system **of CEGEDIM.CLOUD**. Control activities are carried out by the different teams of **CEGEDIM.CLOUD** as part of their day-to-day activities, and adequate supervision is ensured internally at defined frequencies.

III. Management description of information and communication systems

The internal systems and procedures of CEGEDIM.CLOUD

The Compliance manager ensures that internal procedures are updated, pertinent and validated at appropriate management level.

Internal systems guaranteeing the existence of historical records and complete documentation of client changes are in place. Each client request or incident is handled internally by a dedicated team, based on severity as well as response time-objectives.

All requests for assistance are handled at service desk level. These requests or incidents can originate from internal parties (typically CEGEDIM Business Units) or from outside clients directly. To that end, a dedicated ticketing tool is used in a consistent manner internally for most processes. A general usage of this tool is meant to enhance overall standardization as well as data traceability.

Also, a dedicated service portal is in place at clients' service, enabling practical access to their information and ensuring data integrity at all times. Finally, information access management is properly monitored from an independence and segregation-of-duties standpoint.

IV. Management description of control objectives and associated control activities

The control objectives and the description of control activities of **CEGEDIM.CLOUD** are set out in Section 3 "Audit report".

CEGEDIM.CLOUD proposes a description of controls over its **IT Hosting Services System**.

CEGEDIM.CLOUD has formalized a risk and control matrix for each of the 12 processes defined within the **IT Hosting Services System**. These 12 management matrices served as the basis for the review work we performed, which included a design review phase as well as an operational effectiveness (testing) phase.

The 12 matrices totaled 32 control objectives "CO" corresponding to a total of 74 control activities.
Listing of the 12 processes:

1. Event Management: 1 control objective; 2 control activities.

Detect any event that can occur within a defined scope, analyze and qualify event that can be at the source of an incident. An event is typically a detected occurrence on information systems with potential impact on services. All incidents originate from an event; however all events do not necessarily turn into an incident. Event management is handled in accordance with the defined internal procedure document.

2. Incident Management: 2 control objectives; 7 control activities.

React to incident with the objective to properly treat their impact. Reinstate services in accordance with contractual commitments. An incident is an event that alters or can alter availability, data integrity, services rendered to clients, as well as audit trail.
Incident management presents how incident items are treated, coordinated in a controlled manner and in accordance with a defined procedure (in terms of analysis, priority setting, expected evidence to retain, communication throughout the life of the incident, and advancement of statuses until closing via the dedicated centralized ticketing tool).
Incident management is handled in accordance with the defined internal procedure document.

3. Request Management: 2 control objectives; 4 control activities.

Provide a centralized communication channel to enable any concerned party (internal to Cegedim or external) to send a request item electronically. Ensure to treat any received request item in a standardized manner within the tool in place, to respect treatment delays, to record communication and responses for information traceability purposes. Guarantee an effective service quality as well as general client satisfaction. Request items are handled internally in a coordinated manner ensuring qualification, treatment and closing of all treated items.
Request management is handled in accordance with the defined internal procedure document.

4. Problem Management: 2 control objectives; 5 control activities.

Find the cause as well as the related solution of a problem that originates in one or many incidents. Moving forward, minimize the probability of recurrent incidents from occurring again, as well as their impact. Prevent new incidents or problems from appearing. Typically, a problem is a situation where the root cause of one or several incidents (concerning the same impact and preferred solution) is being investigated within the dedicated problem management team. Also, proactively, a problem item can be opened internally with no related specific incident per se, but based on situations that require general improvement. A standardized workflow is followed (with specific IT tool) to treat problem items in a pertinent manner and to ensure information traceability and on-going communication to concerned parties.
Problem management is handled in accordance with the defined internal procedure document.

5. Supplier Agreement Management: 3 control objectives; 8 control activities.

Manage business relationship with suppliers used at Cegedim.Cloud level. Update the list of current suppliers for traceability purposes. Manage contracts with suppliers throughout the life of these contracts, and follow-up on contract signature or renewal requests as necessary. Manage purchase requests internally, validate independently corresponding purchase orders, and ensure E-Mail communication is traced and archived for a proper audit trail. Manage the performance review of key suppliers, ensuring that services rendered are in line with IT security requirements as well as business internal expectations.
Supplier management is handled in accordance with the defined internal procedure document.

6. Service Level Agreement Management: 3 control objectives; 6 control activities.

Define, formalize and document the levels of services provided to clients and the attached commitments; ensuring expectations, measurement and reporting of service levels are formally agreed upon with clients and characterized within the contracts signed by both parties.
Also, service delivery and service levels are regularly reviewed and monitored against the targets set forth in the contractual documents and service levels are reported to clients at a pre-defined frequency and formally communicated (or made available) for its review.
Performance, client satisfaction and feedback are frequently measured and reviewed to ensure service levels are adequate and meet contractual commitments.
Service level management is handled in accordance with the defined internal procedure document.

7. Service Configuration Management: 3 control objectives; 6 control activities.

Manage and optimize inventory of IT resources and their configuration operated or hosted at Cegedim.Cloud level. Ensure each resource is effectively assigned to one owner. Control necessary tools to CMDB. Maintain overtime the integrity of IT resources and their configuration. Ensure traceability on configuration change. Configuration management is handled in accordance with the defined internal procedure document.

8. Access Management: 4 control objectives; 8 control activities.

Grant to Cegedim IT users necessary and sufficient rights within the IT systems in place, and physical accesses to datacenters (as defined in the internal policy) to properly accomplish their mission. Ensure IT treatments for new rights are processed within agreed time objectives. Ensure that actions such as IT right creation, modification and removal are properly traced and recorded for a proper audit trail.
Access management is handled in accordance with the defined internal procedure document.

9. Project Deployment and Production: 2 control objectives; 7 control activities.

Assert that projects for services or clients are appropriately appraised, defined, planned for, and implemented. Project outcome and expectations are formally agreed upon and defined up-front with the end-user. Also, the planification and testing of works are systematically accounted for and documented.
Delivery and implementation are monitored and tested to ensure proper functioning in line with the pre-defined expected outcome. Projects are delivered with the predictable level of service and in compliance with the applicable norms and standards as requested by the end-user.
Project deployment and production is carefully planned for, work advancement is reviewed and assessed.
Project deployment and production is handled in accordance with the defined internal procedure document.

10. Request for Change Management: 4 control objectives; 6 control activities.

Guarantee within the entire IT infrastructure and environments managed by Cegedim.Cloud that change items are recorded, authorized, prioritized, and that integrations and general deployment follow a defined procedure. Also, negative impacts (if any) on services are expected to be minimized to an acceptable level and daily operations improved. Communication to concerned clients is made within expected time-limits.
Change management (as defined internally) expands on how change items (internal to Cegedim.Cloud or client ones) are handled. A change item concerns any addition, deletion or modification to an item on an actual service, with a potential impact on this service for which Cegedim.Cloud is responsible.
Request for change management is handled in accordance with the defined internal procedure document.

11. Information Security Management: 4 control objectives; 9 control activities.

Ensure that best practices are deployed internally in terms of IT governance and security management issues at large. Typically, ensure that different key topics such as crisis management, antivirus, network surveillance tools, patches, external IP scanning tools, backup procedures, restoration requests, and datacenter environmental controls are covered and handled internally via a dedicated specialized team.
Security management is documented formally in many respects, namely through its Group Information Systems Security Policy, Information Security Management System Policy, and Security Assurance Plan.

12. Continuity: 2 control objectives; 6 control activities.

Manage the ability to continue delivering services at acceptable and pre-defined levels following a major unwanted event. The areas of application include the group's data centers, physical offices, employees, as well as general IT infrastructure and hosting services.
Plan, implement, and verify the effectiveness of business continuity and information security continuity measures. In a crisis situation, ensure the effective management of the established action plans and ensure a return to normal operations.

3. WORK PERFORMED BY THE INDEPENDENT AUDITORS

I. Introduction

Each control objective is followed by details of the control activities implemented by **CEGEDIM.CLOUD**. The description of the control activity is accompanied by a description of the tests performed, in order to determine if the controls in place are operational and adequately documented. The results of the tests state if the control objectives are effective for the period from January 1st, 2024 to December 31, 2024.

Please refer to appendix 1 for details regarding the sampling methodology.

- ✓ We firstly reviewed internal controls as they were designed and stated corresponding matrices, and ensured that they were adequately designed to mitigate corresponding risks and meet corresponding control objectives.
- ✓ We then performed effectiveness tests on random and representative samples, in order to ensure that the controls are operationally effective. This testing phase was divided into two sub-phases, one "testing phase I" (in June and July 2024), and one "testing phase II (remediation)" that took place between November and December 2024.

Note: These sample selections (to be considered as representative) were always based on source documents requested by us. We ensured that data integrity, accuracy, and completeness (i.e. encompassing the full populations of requested events / items over our audit period) was effectively in place and satisfactory.

Tests were either performed on-site, or remotely. If performed remotely, audit evidence could be observed via video conferencing first and subsequently communicated via a secured shared platform.

Also, as part of this engagement, an in-person (physical) tour took place in 2024 for the CEGEDIM data center located in Boulogne (France), owned by CEGEDIM;. Concerning the Labège (company owned) and Balma datacenters (outsourced), a physical tour took place in December 2024 and all pertinent maintenance documents could be effectively received as requested and audited.

II. Effectiveness tests performed by the auditors

Obj.	Control objectives		Details of Control Activities	Test scripts	Test results
1. EVENT MANAGEMENT					
CO-1	Detect events that occur within the defined scope Analyze and qualify these events that might result in an incident	EVT-1	The process owner ensures (as described in an updated & formalized procedure document) that events can be properly and timely detected, analyzed, recorded and followed-up until closure in a standardized manner.	Review available operating procedure for pertinence and completeness. Perform a walkthrough of the event management workflow system to verify that it allows for adequate completion of process steps (timely detection, analysis, recording, follow-up and closure).	EFFECTIVE
		EVT-2	A dedicated service desk has access to documentation and tools (such as a monitoring console) for detecting early events and anticipating potential upcoming incidents.	Select a sample of production servers and check that they are properly monitored Select a sample of alerts on the monitoring console and check that there is a corresponding ticket for recording, analysis and follow-up Ensure that the standardized actions per type of alerts are formalized in order to help the service desk to respond in a timely and standardized manner in case of an incident.	EFFECTIVE
2. INCIDENT MANAGEMENT					
CO-2	Manage incidents in a proactive or reactive way in order to minimize their frequency and impact. Timely restore services to contractually agreed service level agreements	INC-1	The incident management process is formalized in order to ensure adequate capture, prioritization and standardized management of incidents until resolution and closure.	Review available procedure for pertinence and completeness. Perform a walkthrough of the incident management workflow system to verify that it allows for adequate completion of process steps (timely detection, recording, prioritization, escalation, analysis, follow-up and closure).	EFFECTIVE
		INC-2	A Single Point of Contact (SPOC) was set up to be the interface between IT and customers. The SPOC ensures that any incident ticket is recorded, analyzed, qualified as defined in the process. Depending on the scope / perimeter of the incident, either the SPOC manages the incident through resolution and closure or the SPOC escalate the incident to the appropriate skilled group.	Select a representative sample of incident tickets and verify that incidents are consistently and effectively detected, recorded, analyzed, treated, communicated and closed throughout the audit period.	EFFECTIVE
		INC-3	A planning of shift per team member is duly formalized in order to ensure that time-shifts are properly staffed.	Verify that a planning shift is in place, and properly staffed for the entire audit period.	EFFECTIVE
		INC-4	A priority matrix is formally defined, and implemented within the ticketing tool in place	Review the incident management procedure and verify that adequate priority levels are defined for incident handling. Select a representative sample of incident tickets and verify that prioritization is consistently and effectively applied.	EFFECTIVE
		INC-5	A process for the management of major incidents is formalized and applied.	Review the incident management procedure and verify that it includes clear instructions for the management of major incidents.	EFFECTIVE

Obj.	Control objectives		Details of Control Activities	Test scripts	Test results
		INC-6	In case of a major incident, the impacted customer is kept informed of the progress on issue resolution and, if necessary, an incident report is sent upon resolution.	Select a representative sample of major incident tickets and verify that incident status is consistently and effectively communicated to impacted customers and collect corresponding incident reports.	EFFECTIVE
CO-3	Monitor incident management activities by analyzing key performance indicators and taking corrective actions when necessary.	INC-7	Incident management key performance indicators are formalized, measured and analyzed.	Check that KPI are measured as defined in the SOP (standard operating procedure) and that they are also formally analyzed.	EFFECTIVE
3. REQUEST MANAGEMENT					
CO-4	Manage requests in an organized manner, through well defined and adequate requesting, authorization, and execution channels. Requests are treated in a timely manner as defined in service level agreements. Control requests with a potential impact on information systems security Ensure quality of services	REQ-1	A formal request process is in place in order to record, qualify, manage and close all requests in a standardized manner.	Review available operating procedure for pertinence and completeness.	EFFECTIVE
		REQ-2	A Single Point of Contact (SPOC) was set up in order to be the interface between the IT department and clients. The SPOC ensures that requests are standardized through an effective automated workflow that allows appropriate request handling, with proper escalation if needed. Users with an AD account (client or IT) can make a request via the request catalog service.	Perform a walkthrough of the request management workflow to verify that it allows for adequate completion of process steps (timely detection, recording, prioritization, escalation, analysis, follow-up and closure). Select a representative sample of request tickets and verify that requests are consistently and effectively recorded, analyzed, treated, communicated and closed throughout the audit period.	EFFECTIVE
		REQ-3	The process owner ensures that notifications are consistently sent to clients throughout the treatment of any given request ticket concerning its status advancement.	Select a representative sample of request tickets and verify that request status is consistently and effectively communicated to customers.	EFFECTIVE
CO-5	Monitor request management activities by analyzing key performance indicators and taking corrective actions when necessary.	REQ-4	Key performance indicators are properly defined, formalized and analyzed.	Check that KPI are measured as defined in the SOP and that they are also formally analyzed.	EFFECTIVE
4. PROBLEM MANAGEMENT					
CO-6	Reduce the probability of occurrence for repeated incidents. Identify the root cause for groups of incidents as well as the corresponding resolution Minimize subsequent impacts.	PBM-1	An operating procedure is defined and followed internally and that it describes how to report, track, qualify, investigate as needed, prioritize and close problems in a standardized manner.	Review available operating procedure related to problem management for pertinence and completeness.	EFFECTIVE
		PBM-2	Problems are effectively recorded, qualified, and treated in a standardized manner.	Select a representative sample of problem tickets and verify that they are consistently and effectively detected, recorded, qualified and treated and closed throughout the audit period.	EFFECTIVE
		PBM-3	Notifications are sent to IT requestors concerning problem resolution progress.	Select a representative sample of problem tickets and verify that there are notifications of IT requestors until resolution of the problem.	EFFECTIVE

Obj.	Control objectives		Details of Control Activities	Test scripts	Test results
CO-7	Monitor problem management activities by analyzing key performance indicators, regularly following up on progress, and taking corrective actions when necessary.	PBM-4	Key performance indicators are properly defined, formalized and analyzed.	Check that KPI are measured as defined in the SOP and that they are also formally analyzed.	EFFECTIVE
		PBM-5	The process owner ensures that problem resolution is monitored on a regular basis.	Check that problems are regularly followed up in a formalized manner. Also, check that the selected sample of problems in PBM-2 demonstrates a proper follow-up.	EFFECTIVE
5. SUPPLIER AGREEMENT MANAGEMENT					
CO-8	Supplier Relationship Management: Formalized contracts are managed throughout contracts' life. Sensitive subcontracting engagements are in line with key IT security requirements.	SAM-1	A formal procedure is validated in respect to the supplier general process, including managing supplier selection and contractual agreements, in a standardized manner.	Request and obtain the formal procedure regarding the supplier's management process, and ensure this document is formally validated for the current year, pertinent, with a sufficient detail level, and properly posted on a dedicated electronic folder.	EFFECTIVE
		SAM-2	The Supplier manager ensures that a comprehensive list of current suppliers is in place, updated, and formally saved on a dedicated e-location.	Ensure that the list of current suppliers is complete, properly updated, validated internally with a proper authority level, and posted on a dedicated and protected electronic location.	EFFECTIVE
		SAM-3	The Supplier manager ensures to formally follow-up the state of contractual agreement for each supplier, in respect to contract signatures and validity dates.	For a selection of suppliers, ensure that a contract is formalized, valid, signed, and archived electronically on a dedicated location.	EFFECTIVE
		SAM-4	The Supplier manager ensures that for a list of IT suppliers considered as key, the corresponding "Service report" following a dedicated meeting (referred to as "Copil" or "technical committee") is received at the agreed frequency, and validated internally by the dedicated manager.	For a selection of key suppliers request the "service report" for a random selection of frequencies (either quarterly, or bi-annually), and ensure that each expected report was timely received, carries the expected format (detail level), and could be formally validated internally if needed, (demonstrating proper acceptance of its content).	EFFECTIVE
		SAM-5	The Supplier manager ensures that Purchase Requests are handled internally in a standardized manner, validated and are in agreement with the actual corresponding Purchase Orders (P.O).	Out of the centralized P.O listing, select a representative sample of 2024 orders. For each selected item, ensure the followings: - the original purchase request was formally communicated internally as expected, - an IT management internal validation took place via a formal E-Mail, - validation occurred before the order was processed.	EFFECTIVE
CO-9	Manage the annual performance of suppliers.	SAM-6	The process in place, defined in an standardized manner, is reviewed internally (for assessment purposes) several times a year in order to ensure the process is deployed as expected, suppliers performance is reviewed, and potential improvement opportunities are identified.	Ensure that the supplier management process could be reviewed internally (within the supplier management team) as expected and at this expected frequency.	EFFECTIVE

Obj.	Control objectives		Details of Control Activities	Test scripts	Test results
		SAM-7	The Supplier manager ensures that on an annual basis a set of suppliers are being assessed in term of satisfaction, based on defined criteria.	Verify for 2024 that for a set of suppliers, an assessment exercise took place, and that corresponding results were properly formalized, and communicated internally as expected.	**EFFECTIVE**
CO-10	Manage the activity by analyzing the indicators and identified discrepancies.	**SAM-8**	Process indicators are properly defined and formalized. The process owner ensures that key indicators are measured, analyzed and communicated on a regular basis.	Ensure defined indicators are present, pertinent in term of design, and calculated on a monthly basis. Also, for a random quarter over the audit period, ensure that a regular overall process quarterly review was conducted and formalized by a dedicated presentation document.	**EFFECTIVE**
6. SERVICE LEVEL AGREEMENT MANAGEMENT					
CO-11	Define and formalize Service Level Agreements between Cegedim.Cloud and clients. Monitor service engagement levels.	**SLM-1**	A formal process governing agreement of service level with client, and service level monitoring is formalized.	Obtain and review the process procedure. Verify that it has been validated and properly defines roles, responsibilities and controls within the SLM team.	**EFFECTIVE**
		SLM-2	A formal SLA is in place between Cegedim.Cloud and its clients (both internal and external) and is signed by both parties. The document follows a dedicated template, and is updated if required.	Select a representative sample of actual SLAs for 2024, both for internal (Cegedim BU) and external clients. For each selected item, ensure that SLAs is properly signed-off by both parties, still valid, and that SLAs' template is properly saved on a dedicated electronic location.	**EFFECTIVE**
		SLM-3	In respect to all clients (both internal and external), services provided are formally monitored, and a report (with metrics) detailing client service Key Performance Indicators and levels is shared at the agreed frequency. Metrics can be communicated during the client's dedicated committees or be transmitted via E-Mail.	For a random selection of 2024 external clients, request and obtain the reports and metrics communicated to clients, then for each selected client ensure that: - Reports were communicated at the expected frequency, - Reports include metrics and comparison with expected service levels, - Traceability of transmission is ensured.	**EFFECTIVE**
		SLM-4	Clients can refer to a real time monitoring of their respective service engagements via a dedicated web-access.	Obtain a presentation of clients metrics web-page. For a sample of clients ensure they can access their metrics and that previous periods data is obtainable by the client.	**EFFECTIVE**
CO-12	Monitor the activity by analyzing the indicators and noted discrepancies.	**SLM-5**	Process related key performance indicators are formally measured, analyzed and discussed at the agreed frequency.	For a sample of occurrences (quarters) during the audit period, obtain the process performance review supporting presentation. Ensure Key Performance Indicators are presented and that, when required, corrective actions are discussed.	**EFFECTIVE**
CO-13	Follow-up client satisfaction.	**SLM-6**	A satisfaction survey is conducted on an annual basis in order to assess client satisfaction in respect to Cegedim.Cloud's service. This survey is subsequently analyzed.	Obtain the customer satisfaction survey supporting documentation. Verify that, following satisfaction survey results analysis, that conclusions are shared with management and action plans are suggested.	**EFFECTIVE**

Obj.	Control objectives		Details of Control Activities	Test scripts	Test results
7. SERVICE CONFIGURATION MANAGEMENT					
CO-14	Manage and optimize IT resource inventory as well as their configuration for IT resources managed or hosted by Cegedim.Cloud Ensure all configuration item has an owner. Control necessary tools for a functional CMDB.	CFG-1	The dedicated Manager verifies that the configuration management process is defined. formalized and regularly updated, in order to ensure identification, recording of CI and their configuration. Also, he / she ensures to verify that naming rules for CI are properly defined in the formalized Naming Conventions.	Obtain the configuration management procedure, ensure it is appropriately documented (i.e. includes necessary details over this process), and kept up to date Ensure Naming convention is up to date and published for Cegedim Cloud.	EFFECTIVE
		CFG-2	Cegedim.Cloud staff benefits from all necessary tools needed to record, and track IT resources as well as configuration. CI administrators are granted necessary rights to record and track these IT resources and configuration in CMDB.	Collect the access rights matrix defined by management and assess whether rights are not overly permissive in the CMDB based on the roles and responsibilities of the concerned individuals / groups. Check that access rights in the CMDB have been reviewed against the access rights matrix and corrections have been performed , as expected.	EFFECTIVE
CO-15	Maintain correctness and integrity of IT resources and their configuration. Have traceability of changes of configuration.	CFG-3	The configuration process is in place in order to formally control and treat anomalies on a consistent basis.	Obtain the CMDB anomaly SOP and Work Instruction (W.I). Check that anomalies are treated according to the defined process.	EFFECTIVE
		CFG-4	The dedicated Manager ensures that a physical audit of CI is performed annually and all identified anomalies are recorded and acted upon.	Collect the annual reports of the physical audits of CI Based on a sample, check that anomalies have been logged and acted upon.	EFFECTIVE
		CFG-5	A CI report is formally analyzed and anomalies identified (CMDB data) are recorded and effectively treated as needed.	Select a sample of CI anomalies and ensure there are tickets associated for investigation and resolution	EFFECTIVE
CO-16	Monitor configuration management activities by analyzing key performance indicators, regularly following up on progress, and taking corrective actions when necessary.	CFG-6	KPI on the Configuration management process are formalized, measured and analyzed	Collect KPI and related analysis performed as part of the process review, and ensure they are formalized at the expected frequency.	EFFECTIVE

Obj.	Control objectives		Details of Control Activities	Test scripts	Test results
8. ACCESS MANAGEMENT					
CO-17	Grant sufficient rights to IT systems Ensure continued data confidentiality by enforcing the least privilege principle in granting access to systems and network. Ensure full traceability in respect to all right creations, modifications as well as access right removal.	**ACC-1**	The process-owner ensures that an access management process is formally defined, pertinent and deployed to manage requests, authorization, and granting of access.	Review available policy and operating procedure documents for pertinence and completeness. Verify it includes all access management process steps (request, authorization, granting, modification and removal).	**EFFECTIVE**
		ACC-2	All logical access requests are made within the ticketing tool (except for AD office accounts). Accounts with privileges are authorized by the IT Security Manager. Firewall rule access changes are formally requested and authorized by IT security as defined in IT security standards.	Perform a walkthrough of the request management workflow system to verify that it enables adequate handling of the access request steps. On a sample basis, verify that access granted for privileged accounts, as well as firewall rule changes, were consistently authorized by IT Security management.	**EFFECTIVE**
CO-18	Monitor and trace the use of information systems access.	**ACC-3**	The process-owner ensures that an access management process is formally defined, pertinent and deployed to manage reviews of accesses.	Review available policy and operating procedure documents for pertinence and completeness. Verify it includes the reviews of accesses.	**EFFECTIVE**
		ACC-4	Access reviews are performed on a monthly or quarterly basis, as defined in operating procedure Where applicable, corrective actions are taken by IT security management, and documented in the ticketing system.	Through interviews and review of operational documentation, verify that access reviews were performed in a timely manner by IT security management. When corrective actions were necessary (access removal or modification), verify that a request ticket was raised and treated timely.	**EFFECTIVE**
		ACC-5	Active Directory accounts are deactivated upon employee termination. In addition, a weekly HR extract is prepared by the service desk in order to manage expiring employment contract situations and remove access when necessary.	Perform a walkthrough of the active directory system to verify that automated deactivation of terminated employees is in place. On a sample basis, verify that weekly checks are performed by the helpdesk to remove access in case of expired employment contracts.	**EFFECTIVE**
CO-19	Monitor and trace all accesses to Cegedim.Cloud physical data centers.	**ACC-6**	Procedures are documented related to security measures in place to protect equipment from unauthorized accesses or environmental risks. A physical access control procedure is documented and specify accesses based on a need-to-know.	Collect and review the procedures related to the physical access to the data centers as well as the security measures to protect equipment against environment controls. Ensure these documents are pertinent and hold a sufficient detail level.	**EFFECTIVE**
		ACC-7	List of authorized individuals allowed to access the different zones of the data centers is reviewed and reapproved by CIO twice a year. Data centers are located in discrete locations, they are not visually identifiable, they have video cameras and are under security protection 24/7. Access to data centers is restricted to authorized persons only. Visitors (auditors, prospect or clients) are accompanied by an authorized person. Their visit is recorded.	Ensure the list of authorized individuals has been reviewed twice a year. Visit the data centers and check that access controls are performed as described (including for visitors).	**EFFECTIVE**

Obj.	Control objectives		Details of Control Activities	Test scripts	Test results
CO-20	Monitor access management activities by analyzing key performance indicators and taking corrective actions when necessary.	ACC-8	Key performance indicators (KPI) are defined, measured and analyzed on regular basis.	Verify that indicators as defined in operating procedure are effectively measured. Check on a sample basis, that quarterly process reviews were performed, included review and analysis of indicators, and action plans where applicable.	EFFECTIVE
9. PROJECT DEPLOYMENT AND PRODUCTION					
CO-21	Plan, build, test and implement services efficiently.	DEP-1	A formal process governing project management and implementation is formalized.	Obtain and review the process procedure. Verify that it has been validated and that it properly defines roles, responsibilities and controls with regards to project management.	EFFECTIVE
		DEP-2	Business & functional requirements are formally defined and agreed upon by clients (both internal and external clients).	For a representative sample of 2024 projects, ensure that business & functional requirements are formally documented / validated, and maintained for proper audit trail.	EFFECTIVE
		DEP-3	Documentation and procedure related to the newly implemented service are formalized and up-to-date. Service delivered is properly documented.	For a random selection of 2024 projects, ensure that architecture document for the new / updated service is present, updated as needed, and maintained for proper audit trail.	EFFECTIVE
		DEP-4	Design of the solution and matching with clients' original demand is acknowledged. Formal acceptance of the client is substantiated by the signature of a formal document. Upon final implementation of works, client formally acknowledges the correct functioning of the works by the signature of a second validation statement. Internally, transmission of project information from the project team to the operation team is formalized by signing a specific document.	For a representative sample of clients' projects for 2024, ensure that : - client has formally accepted delivery of work by signing the "PV de recette / PV de livraison". - client has formally accepted implementation and functioning of work by signing the "PV de validation fonctionnelle". - transmission of project information from the project team to the operation team is formalized by signing the dedicated document "PV de livraison".	EFFECTIVE
CO-22	Projects are monitored to ensure budget and time commitments are respected	DEP-5	Project development implementation is followed-up in a dedicated project management tool, "*Clarizen*". The project management tool specifies key project dates as well as role and responsibilities of the stakeholders involved in the project.	For a representative sample of clients' projects for 2024, ensure that project is implemented in the project management tool and that key dates, roles and responsibilities are properly indicated.	EFFECTIVE
		DEP-6	A project committee is conducted at least 5 times a year (for project monitoring and prioritization purposes at management level). A dedicated support document is formalized with key indicators and an updated summary of on-going projects.	For a sample of occurrences ensure that the project committee could be conducted at the expected frequency, and that the expected level of details for the corresponding formal presentation is proper.	EFFECTIVE

Obj.	Control objectives		Details of Control Activities	Test scripts	Test results
		DEP-7	Process related key performance indicators are formally measured, analyzed and discussed at the agreed frequency.	For a sample of occurrences (quarters) during the audit period, obtain the process performance review supporting presentation. Ensure Key Performance Indicators are presented and that, when required, corrective actions are formally discussed.	**EFFECTIVE**
10. REQUEST FOR CHANGE MANAGEMENT					
CO-23	Ensure that all changes are recorded, analyzed, authorized and prioritized. Ensure that changes are developed, integrated and implemented according to the change management procedure, and that negative impacts on services are minimized while operations are improved.	**RCM-1**	A formal change management procedure is maintained to define proper steps for all changes (including urgent changes) to be recorded, analyzed, authorized, prioritized and implemented.	Review available policy and procedure documents for pertinence and completeness.	**EFFECTIVE**
		RCM-2	A workflow process and tools are in place to manage changes (including urgent changes), allowing for proper recording, analysis, authorization, prioritization and implementation, following the segregation of duties principle (change requester, authorizer and implementer are different individuals). Changes are tested prior to being implemented into the production environment, according to the predefined implementation plan.	Check that a pertinent and centralized tool is in place and used on a consistent basis concerning RFC (request for change items). Also, observe that key fields such as change category, priority, and impact can be properly documented in accordance with the agreed procedure.	**EFFECTIVE**
CO-24	All change requests are formally communicated to and authorized by stakeholders based on operational constraints.	**RCM-3**	All non-minor changes are reviewed and approved during a weekly Change Advisory Board.	On a sample basis, verify that all non-minor changes are reviewed and approved during the weekly change advisory board meeting, as recorded in the history of selected RFC (change) tickets.	**EFFECTIVE**
CO-25	All changes are communicated to impacted stakeholders (clients or Cegedim.Cloud).	**RCM-4**	A timely communication is made before each change advisory board meeting to ensure that all stakeholders are informed of upcoming changes.	On a sample basis, verify that email communication was sent to stakeholders ahead of each change advisory board, containing all pertinent information (CAB Agenda, changes, due dates) so an effective meeting can take place.	**EFFECTIVE**
		RCM-5	A maintenance schedule is prepared and updated, and communicated to all stakeholders on a yearly basis.	Through interviews and review of operational documentation, verify that an annual maintenance schedule is prepared and updated, and communicated to stakeholders.	**EFFECTIVE**
CO-26	All changes are communicated to impacted stakeholders (clients or Cegedim.Cloud).	**RCM-6**	Key performance indicators are defined, measured and analyzed on regular basis.	Ensure defined indicators are present, pertinent in term of design, and calculated on a monthly basis. Also, for a random quarter over the audit period, ensure that a regular overall process quarterly review was conducted and formalized by a dedicated presentation document.	**EFFECTIVE**

Obj.	Control objectives		Details of Control Activities	Test scripts	Test results
11. INFORMATION SECURITY MANAGEMENT					
CO-27	Implement organizational and operational security measures to effectively detect, prevent and treat security incidents	**SEC-1**	Policies and procedures are in place to manage information security.	Review available policy and procedure documents for pertinence and completeness: - Group Information Systems Security Policy. - Information Security Management System Policy. - Security Assurance Plan	**EFFECTIVE**
		SEC-2	A security incident management procedure as well as a crisis management procedure are in place. An annual crisis management test is performed to ensure its effectiveness.	Review Incident Management and Crisis Management procedure for pertinence and completeness. Verify that incident and crisis management was formally documented during the year.	**EFFECTIVE**
		SEC-3	Compatible production servers and workstations are protected against malware by an antimalware. Cegedim.Cloud performs the following controls to ensure antivirus protection: - Compatible production servers and workstations of Cegedim.Cloud: control of virus alerts by a SOC Corrective actions are taken upon alert.	Verify on a sample of machines that antivirus is appropriately installed on compatible servers and workstations, and that updates are received as needed, via a representative sample of workstations and servers.	**EFFECTIVE**
		SEC-4	Service account and administrator passwords are stored in an electronic vault. A daily replication of the password database is performed on a redundant site. Daily replication reports are archived. A monthly password database restoration test is performed.	Perform a walkthrough of the password electronic vault system to verify that it is properly secured and adequately functioning. On a sample basis, verify daily replication and monthly restoration of the password database.	**EFFECTIVE**
		SEC-5	Network anomalies are continuously detected using specialized tools, and analyzed and treated by IT security management.	Perform a walkthrough of network surveillance tools. On a sample basis, review evidence of management's treatment of network anomaly alerts.	**EFFECTIVE**
CO-28	Detect and correct information security vulnerabilities to prevent unauthorized access to information systems.	**SEC-6**	On a quarterly basis, server operating system security patches are evaluated in testing and quality assurance environments before being implemented into the production environment. Some machines (Configuration Items) can be excluded upon decision of the customer.	On a sample basis, review RFC tickets and verify that patches were applied to all production servers, and that any exception were justified. Verify that patches were approved, and tested (testing and QA environment) prior to being implemented into production.	**EFFECTIVE**
		SEC-7	External IP addresses are scanned on a weekly basis using specialized tools, and critical vulnerabilities are analyzed and treated by IT security management.	Perform a walkthrough of external IP scanning tools. On a sample basis, review evidence of management's treatment of critical vulnerabilities.	**EFFECTIVE**

Obj.	Control objectives		Details of Control Activities	Test scripts	Test results
CO-29	Manage appropriately environmental risks.	SEC-8	Datacenter security measures (against environmental hazards) are properly formalized and maintained internally, and deployed when necessary. All security systems of the data centers are regularly maintained and checked (air conditioning, generator, UPS, fire protection).	Review documentation presenting the Datacenter security measures (against environmental hazards) Collect latest maintenance reports of each security equipment (fire protection system, air conditioning, UPS, generator, etc.) and verify it has been performed according to constructor recommendations. Finally, verify that anomalies have been acted upon.	EFFECTIVE
CO-30	Monitor the activity by analyzing the indicators and noted discrepancies and taking corrective actions when necessary.	SEC-9	Process related key performance indicators are formally measured, analyzed and discussed at the agreed frequency.	For a sample of occurrences (quarters) during the audit period, obtain the process performance review supporting presentation. Ensure Key Performance Indicators are presented and that, when required, corrective actions are formally discussed.	EFFECTIVE
12. CONTINUITY					
CO-31	Ensure the effectiveness of the business continuity measures implemented within the information system.	CTN-1	A continuity management process is formalized to define the strategy, implement, test, evaluate effectiveness, and improve.	Ensure a continuity management process is formally defined with pertinent information on this operational process, updated and carries sufficient detail level.	EFFECTIVE
		CTN-2	A backup management policy is formalized.	Review the backup management policy and ensure it is properly formalized and that it includes information on backup for systems in production.	EFFECTIVE
		CTN-3	Backup of all production servers (within MyIT) are planned, and monitored in accordance with the backup policy in place.	Select a representative sample of production servers and ensure their backups are effectively monitored.	EFFECTIVE
		CTN-4	Backups are monitored in Centreon, a ticket is automatically logged in a ticketing system and acted upon by appropriate team.	Verify that backup is monitored in Centreon and that there are tickets for anomalies.	EFFECTIVE
		CTN-5	File restoration or environment restoration are performed when requested by a client or following an incident.	Select a representative sample of restoration requests and ensure they have been processed successfully in a timely manner.	EFFECTIVE
CO-32	Monitor continuity management activities by analyzing key performance indicators and taking corrective actions when necessary.	CTN-6	Key performance indicators (KPI) are defined, measured and analyzed on regular basis.	Verify that indicators as defined in operating procedure are effectively measured. Check on a sample basis, that quarterly process reviews were performed, included review and analysis of indicators, and action plans where applicable.	EFFECTIVE

Appendix

Sampling Methodology based on control frequency

Frequency of the control activity	**Sample size to be tested**
Annual	1 occurrence
Monthly	3 occurrences
Weekly	5 occurrences
As indicated by circumstances	20 % of total population (with a maximum sample size of 25)
Automated control	1 occurrence