ISAE 3402 Type 2 (SOC1)

Report on controls placed in operation and test of operating effectiveness

For the period August 1, 2022 to July 31, 2023

EDICOM CAPITAL, S.L.

Contents

1. Independent Service Auditor's Report on the description of controls, their design and operating effectiveness

To the Board of Directors of **EDICOM CAPITAL, S.L. (hereafter EDICOM):**

Scope

We have been engaged to report on EDICOM description at chapter 3 of its Edicom Cloud Service throughout the period August 1, 2022 to July 31, 2023, and on the design and operation of controls related to the control objectives stated in the description.

The information included in chapter 5 of this report is presented by EDICOM to provide additional information to user organizations and is not a part of EDICOM's description of controls placed in operation. The information in chapter 5 has not been subjected to the procedures applied in the examination of the description and on the design and operation of controls related to the control objectives stated in that description.

EDICOM's Responsibilities

EDICOM is responsible for preparing the description and accompanying assertion at chapters 2 and 3 of this report, 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.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on EDICOM's description 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 service 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 chapters 2 and 3.

This review was performed by a team of AUREN multidisciplinary auditors that have highly experience in IT audit. In particular AUREN Information Security work team is composed of many professional experts with recognized certifications such as CISA, CISSP, CISM, ISO/IEC 27001 Lead Auditor. View **Annex 2** for the experience of the audit team and **Annex 3** for a brief presentation of AUREN services.

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

EDICOM's description is prepared to meet the common needs of a broad range of Clients and their auditors and may not, therefore, include every aspect of the system that each individual Client 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 this report. The criteria we used in forming our opinion are those described at chapter 4 and **Annex 1** (Sampling Methodology). In our opinion, in all material respects:

a) The description fairly presents the Edicom Cloud system as designed and implemented throughout the period from August 1, 2022 to July 31, 2023;

b) The controls related to the control objectives stated in the description were suitably designed throughout the period from August 1, 2022 to July 31, 2023; 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 August 1, 2022 to July 31, 2023.

Description of Test of Controls

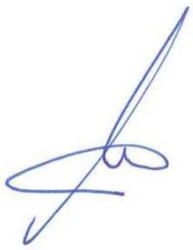
The specific controls tested, and the nature, timing and results of those tests are listed on chapter 4 on this report.

Intended Users and Purpose

This report and the description of tests of controls on chapter 4 are intended only for Clients of Edicom Cloud Service, and their auditors, who have a sufficient understanding to consider it, along with other information including information about controls operated by Clients themselves, when assessing the correct operation of the services provided by EDICOM or, if applicable, the risks of material misstatements of Client's financial statements.

We appreciate the collaboration of EDICOM for the achievement of this audit engagement.

December 11th, 2023



_____

auren

Represented by Francisco Mondragón Peña

Auditor Partner

2. Assertion by EDICOM

The accompanying description of systems and controls performed by EDICOM CAPITAL, S.L. (hereafter EDICOM) on chapter 3 have been prepared for Clients who have used the Edicom Cloud Service, and their auditors who have a sufficient understanding to consider the description, along with other information including information about controls operated by Clients themselves, when assessing the related risks.

EDICOM confirms that:

(a) The accompanying description, on chapter 3, shows faithfully the systems and controls used to process Client's transactions throughout period August 1, 2022 to July 31, 2023. The criteria used in making this assertion were that the accompanying description:

i. Presents how the system was designed and implemented, including:

- The types of services provided, as well as the types of transactions processed.
- The procedures, within both information technology and manual systems, by which transactions were initiated, recorded, processed, corrected as necessary and transferred to the reports prepared for Clients.
- How the system dealt with significant events and conditions, other than transactions.
- Relevant control objectives and controls designed to achieve those objectives.
- Controls that we assumed, in the design of the system, 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 environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that were relevant to processing and reporting Clients' transactions.

ii. Includes relevant details of changes to the service organization's system during the period August 1, 2022 to July 31, 2023.

iii. Does not omit or distort information relevant to the scope of the system being described, while acknowledging that the description is prepared to meet the common needs of a broad range of Clients and their auditors and may not, therefore, include every aspect of the

system that each individual Client 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 August 1, 2022 to July 31, 2023:

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; and

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 August 1, 2022 to July 31, 2023.

During this period, EDICOM held the controls, detailed in this report, adequately designed and effectively working. This assertion is based on tracking activities performed by EDICOM and the revisions or independent audits performed by external third parties which cover at least part of these controls.

However, due to the nature and inherent limitations of controls, there exists the risk which in some cases could be errors which have not been detected.

December 11th, 2023

_____

EDICOM CAPITAL, S.L. (EDICOM)

Represented by José Vilata Tamarit

Joint Chief Executive Officer

3. System description by EDICOM

3.1 Service organization

3.1.1 *Overview of the organization*

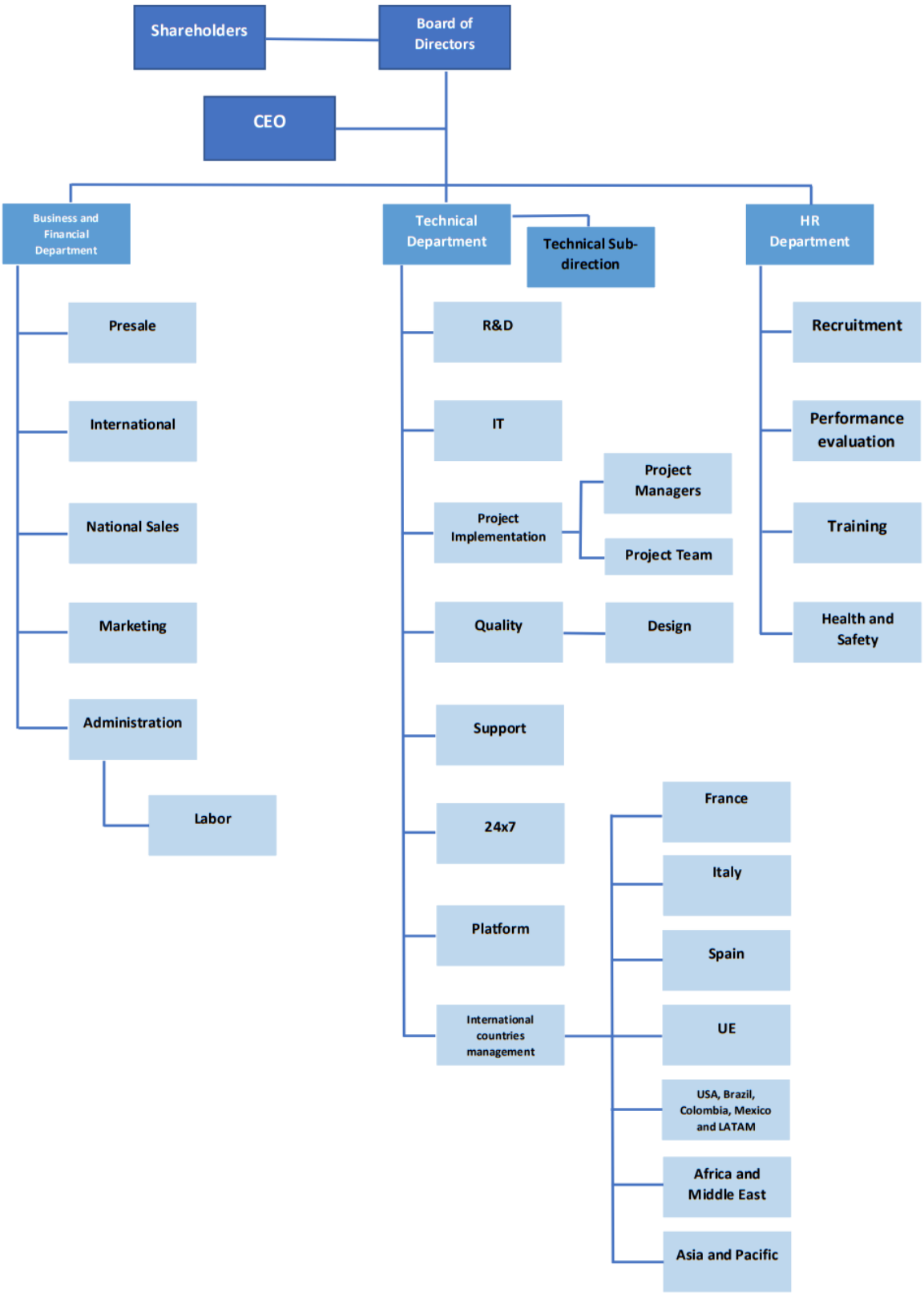
This report is designed to provide information to be used by EDICOM clients and their independent auditors and to meet the requirements of the International Standard on Assurance Engagements 3402, "Assurance Reports on Controls at a Service Organization".

EDICOM is a player in EDI (Electronic Data Interchange) and electronic invoicing sector with widespread recognition for its platforms for the transmission and integration of data between companies.

EDICOM technological solutions, entirely designed in-house, are adapted to the necessities of each client, beyond borders, legislation and technical complexities. This is accomplished through human and technical resources that provide services to clients worldwide on a daily basis to administer and manage their B2B (Business-to-Business) communications platforms.

EDICOM provides its services through its B2B cloud platform to give efficient responses to multiple clients with very different characteristics and needs. EDICOM solutions are designed in line with market requirements, continuously adapting technology and resources to provide coverage to its more than 17.025 clients.

Currently, EDICOM employs 817 professionals throughout its offices in Spain, Mexico, United States, Brazil, Argentina, France, Italy, Morocco and Colombia, positioning this way as a company with a clear international presence. EDICOM's organizational chart is depicted below:


Shareholders
Board of Directors
CEO
Business and Financial Department
Technical Department
Technical Sub-direction
HR Department
Presale
International
National Sales
Marketing
Administration
Labor
R&D
IT
Project Implementation
Project Managers
Project Team
Quality
Design
Support
24x7
Platform
International countries management
France
Italy
Spain
UE
USA, Brazil, Colombia, Mexico and LATAM
Africa and Middle East
Asia and Pacific
Recruitment
Performance evaluation
Training
Health and Safety

3.1.2 *Overview of services*

Services offered by EDICOM can be grouped into the following categories:

- **B2B solutions**: EDICOM's SaaS (Software as a Service) portfolio.
- **Trust services**: Digital certificates related services - issuing, signing, time stamping, long-term archiving, electronic delivering and validation.
- **Advanced services**: Outsourcing B2B cloud platform management related services.
- **Communications Infrastructure**: The technology solutions developed by EDICOM guarantee the generation, translation and integration of all messages exchanged between companies in accordance with the multiple standards in existence (EDIFACT, XML, X12, ODETTE, UBL, VDA, etc.) These messages require a vehicle, a transfer medium for ensuring secure, fast and efficient sending and receiving. For this purpose, EDICOM integrates the best communications infrastructure on its technological platform. A powerful range of specific services for message transmission, meaning messages sent and received, with all transactions to any interlocutor are guaranteed.
- **SignADoc**: A document approval and e-signature solution that applies electronic signatures of different security levels depending on the sensitivity of the information. EDICOMSignADoc generates evidence reports of all interactions that take place during the approval lifecycle of your documents.

A brief description of EDICOM's core services is listed below:

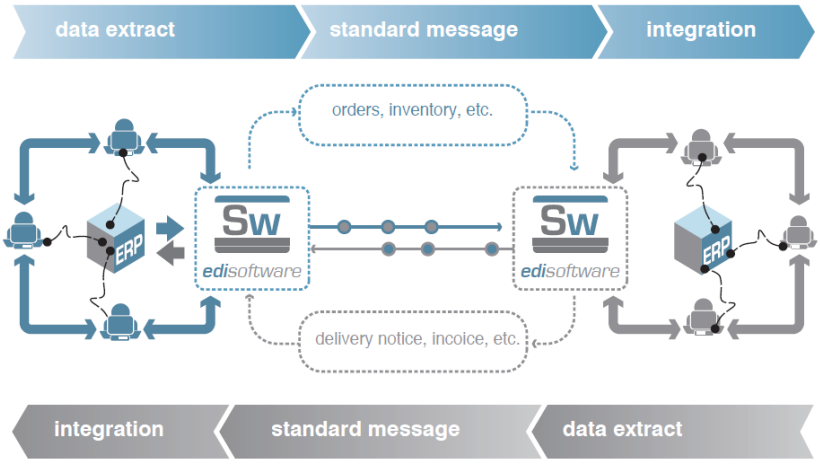
B2B solutions

- **Ediwin XML/EDI Server**

Ediwin XML/EDI Server allows outsourcing the whole technological platform for the transformation, sending, reception and integration of EDI transactions to a service provider.

Integrated solutions are characterized by their capacity to automatically process data messages regardless of the structure of the information contained in the ERP system (Enterprise Resource Planning) where these messages are inbound or outbound.

This technology is commonly known as Enterprise Application Integration (EAI). This way, processing large volumes of transactions between business partners takes place without human intervention, effectively, efficiently and without modifying internal processes.

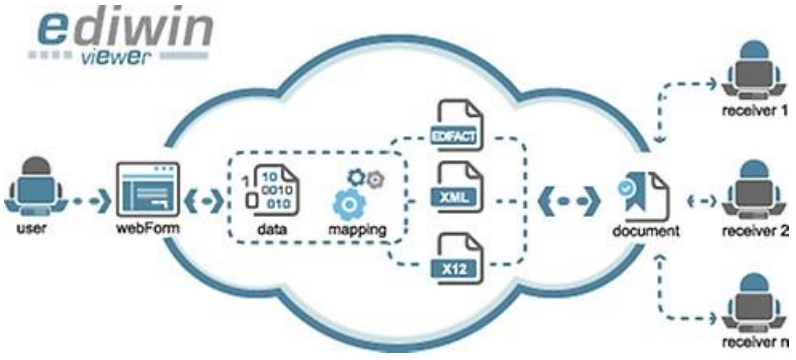


EDI has gained a foothold in the retail sector, as a mean of widespread commercial transactions between distributors and suppliers. Many business sectors have gradually developed their own EDI extension projects and nowadays, it is a reality perfectly established in fields like retailing, healthcare, automobile industry, tourism, public sector, transport, etc.

- **Ediwin Viewer**

For costs and rollout speed, non-integrated solutions constitute the best alternative to start up in XML/EDI communications when the volume of documents to be interchanged is low.

Ediwin Viewer is the web EDI application developed by EDICOM that enables Clients to operate via the Internet with clients and suppliers.



Construction of the different messages is done using web forms that enable the user to compose them quickly and intuitively. Documents such as invoices or shipment notices are introduced directly by the user and EDICOM's B2B cloud platform transforms them to the standard used by the partner.

The application automates part of the document creation process using automatic generation from similar messages. This way, the construction of documents such as invoices is accelerated by automating part of their generation on the basis of the orders received.

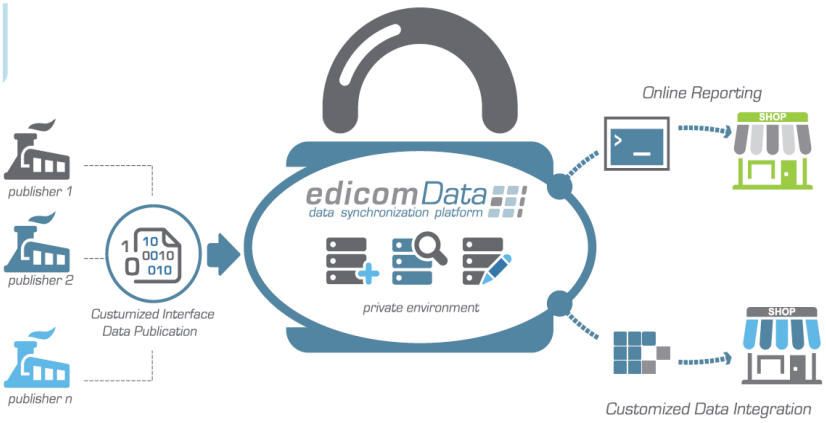
EDICOM's web solutions are an effective and easy option for receiving messages. In this case, documents received are routed by EDICOM's communication network, making them available to the user through the web application.

The solution also supports electronic signatures. Invoices sent and received with digital signatures have complete legal validity and remain stored in EDICOM's document repository for the period set by applicable law. This way, Ediwin Viewer users can avoid document printing and storage.

- **EDICOMData**

EDICOMData is the data pool EDICOM has developed to enable the synchronization of products and services offering between companies that use any data pool connected to the GDSN (Global Data Synchronization Network).

With GDSN, trading partners always have the latest information in their systems and any changes made to one company's database are automatically and immediately provided to other companies which do business with them.



When a supplier and a client are looking for the same up-to-date data, it is more effective and efficient to do business together. The GDSN provides a single point of reference for product information.

The specific integration solution EDICOM has developed also enables data loading and updating processes in internal management systems to be automated to the EDICOMData data pool.

- **Business Mail**

Business Mail is an electronic documents publication platform designed to facilitate sending any type of document (structured, unstructured, images, etc.) to third parties.

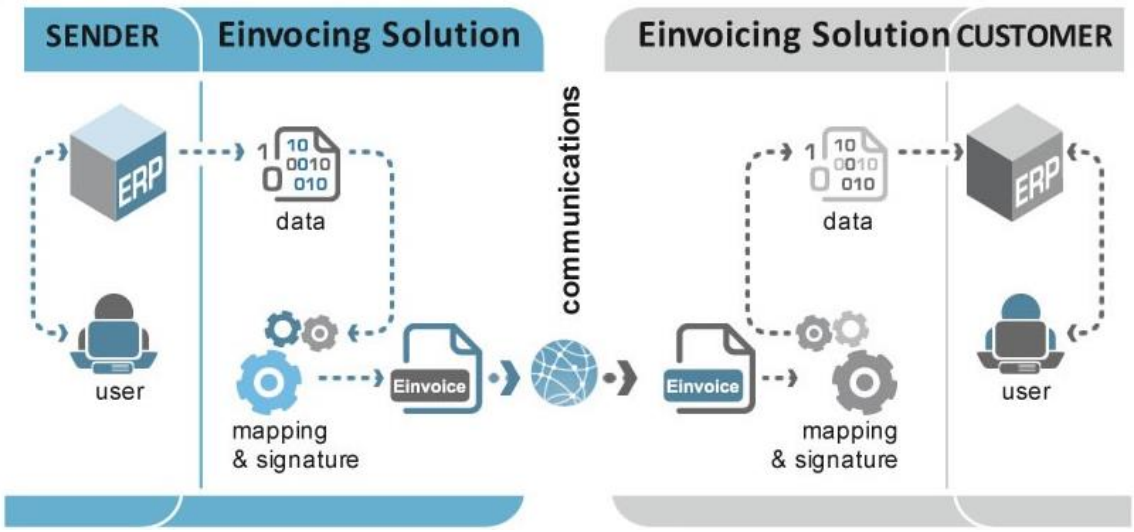
It can be integrated with the sender's EDI or electronic billing solution to send electronic documents in structured format to those partners with no B2B e-commerce solution.

When the sender publishes documents in the platform, the system automatically notifies the receiver of the availability of documents addressed to him. Any action taken on published documents (or failure to perform actions on them) automatically generates notifications directed to the issuer.

- **Electronic Invoice**

An electronic invoice is the functional and legal equivalent of a traditional paper invoice.

However, it is distinguished by being sent via electronic methods, enabling sending and receiving e-invoices almost instantaneously between trading partners.



To construct a fully legal e-invoice, these specific conditions must be met:

- Format: The format of the e-invoice must be fixed and structured. Some of the common formats are: EDIFACT, X12, XML, PDF, etc.

- Transmission: The e-invoice must be exchanged electronically using means of transmission which ensure authenticity and integrity (e.g.: digital signature).

- **VAT Compliance**

The Tax Agencies around the world are heading for the electronic tax compliance, with the goal of improving the control processes of the taxes, simplifying procedures and automating supervision processes. This process also is part of the global trend towards the digitalization of companies. Nevertheless, each country continues laying down their own tax standards. The current architecture of this service is through microservices.

This situation hinders meeting the tax requirements of companies, where technology is a challenge and an opportunity in equal measure, to face the main challenges:

- To have electronic solutions which allow an automated communication with Tax Agencies.

- Global adaptation to different to local taxation systems.

EDICOM has implemented a model of VAT Compliance which brings EDICOM's Clients some benefits:

- **Consolidation**: Companies no longer need to multiply their resources dedicated to tax compliance, otherwise they can centralize all these tasks in one unique solution and country.

- **Integration**: With management systems, performing the required transformations and adaptations on their documents. All these processes are totally clear and transparent to users, and without the need of performing changes in their IT infrastructure.

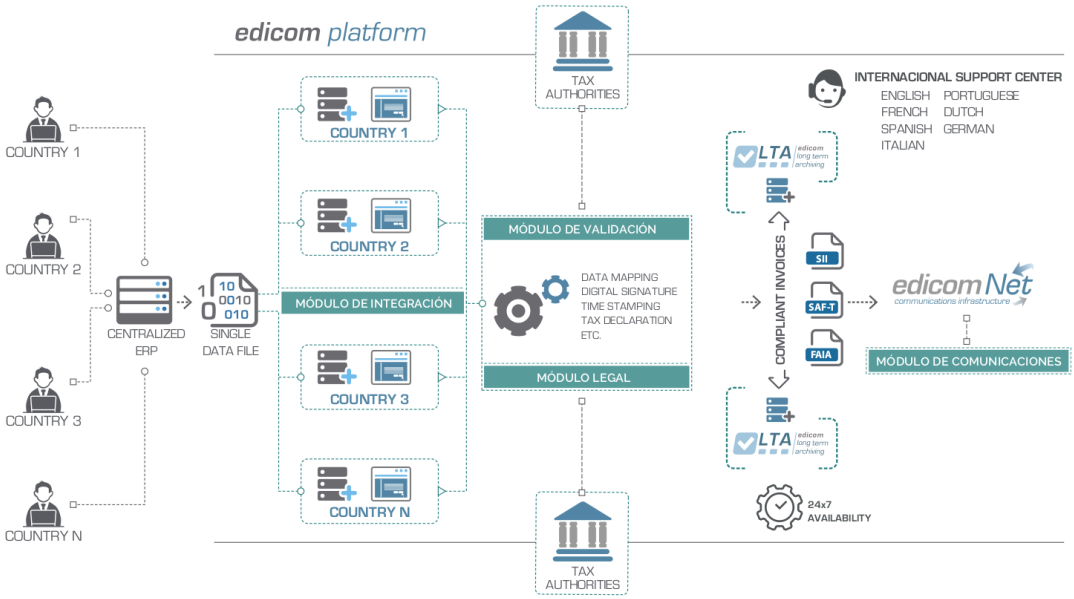
- **Cost savings**: Automatization and centralization increase the companies' efficiency. Because of this, it is possible to squeeze the benefits of digitalization, such as important cost savings.

- **Performance bond**: EDICOM VAT Platform is a platform ready to operate over 60 countries around the world. Its use is a guarantee for companies which avoid possible sanctions due to tax incompliance or incorrect operations.

- **Security and availability**: EDICOM VAT Platform has different certifications, such as ISO/IEC 27001, ISO/IEC 20000-1, High level 2022 ENS or TIER II DESIGN. The commitment acquired by EDICOM with all its Clients with these certifications is to offer the maximum-security guarantees and to keep the SLA defined by EDICOM (99,9% availability).

- **Continuous improvement**: Through its International Observatory of Taxing Compliance (e-Invoicing & VAT), EDICOM performs an active knowledge management to keep permanently updated its solution over regulation changes that could occur periodically in the different countries.

EDICOM has developed an integral solution designed especially for multinationals. It is a B2B2G electronic communications platform with EDI, e-Invoicing compliant and VAT Compliance capabilities.



EDICOM's platform simplifies the communication processes with Tax Agencies in multinational environments. It is the ideal solution for those companies which operate in different markets from centralized management systems and have to be able to manage and send tax documents according to every country legislation and regulation.

Moreover, EDICOM is a Trusted Service Provider according the eIDAS Regulation, what guarantees the security and trustworthiness of signature services and, thanks to the certification of qualified preservation service for qualified electronic seals, EDICOM also provides an electronic and long-term preservation of information to keep the integrity and provide probative value to them.

The platform features are described as follows:

- **Automatization**: EDICOM's solution is integrated with the company ERP to automatize the VAT declaration and any taxing communication.
- **Centralization**: The platform is ready also for electronic invoicing and any commercial or taxing communication.
- **Globalization**: It is a platform suitable in tax compliance in more than 60 countries around the world, so it is possible to centralize all the processes in one unique solution.

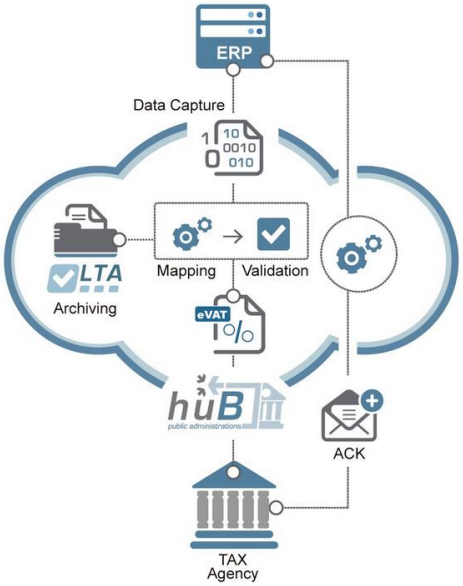
The platform capabilities are described as follows:

- **Data Capture**: EDICOM's solution capture the invoicing data (sent and received) from the Client's ERP or accounting system, in a specific format with the purpose of adapting its internal management system.

- **Mapping**: The Mapping module translate data for each Tax Agency.

- **Validation**: Syntactic validation process is activated to verify and certify that the file has been built according to the defined node structure by the Tax Agency, avoiding future rejections.

- **Connectivity**: Automatically, the system sends the messages to the Treasury's Electronic Office of every country, using a direct and secure connection via Web service protocol.



- **Integration**: In those situations where Tax Agencies send a message with their validation system result, these notifications could be integrated in the own internal system of EDICOM's Client, allowing them an easily and swiftly management of the documents.

- **Electronic Archiving**: EDICOM counts on a genuine added value service which automatizes the electronic archiving, recovery and management process, of any commercial or taxing document which must be archived according with the defined legal retention period. The system also archives the authorities' responses with the corresponding document for futures queries, and recoveries, guarantying the integrity and inalterability of the documents in their archiving process.

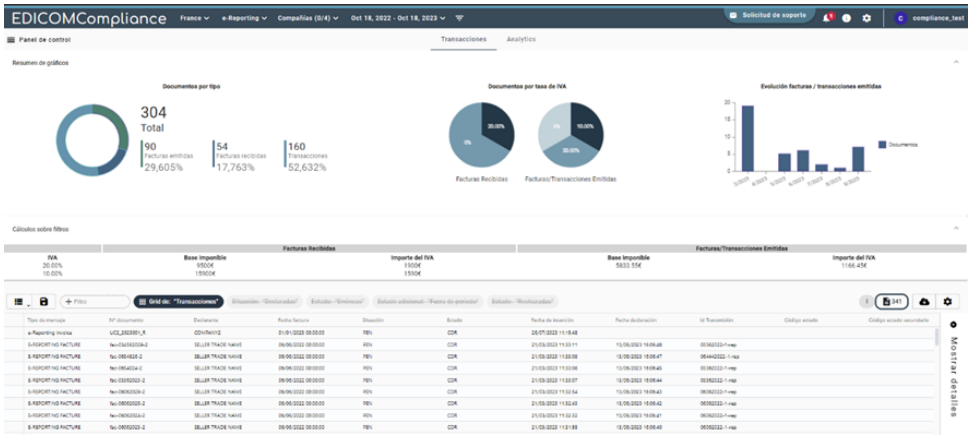
- **EDICOMCompliance**

EDICOM Compliance is an Ediwin Web interface focused on the management and consultation of billing and e-Reporting processes.

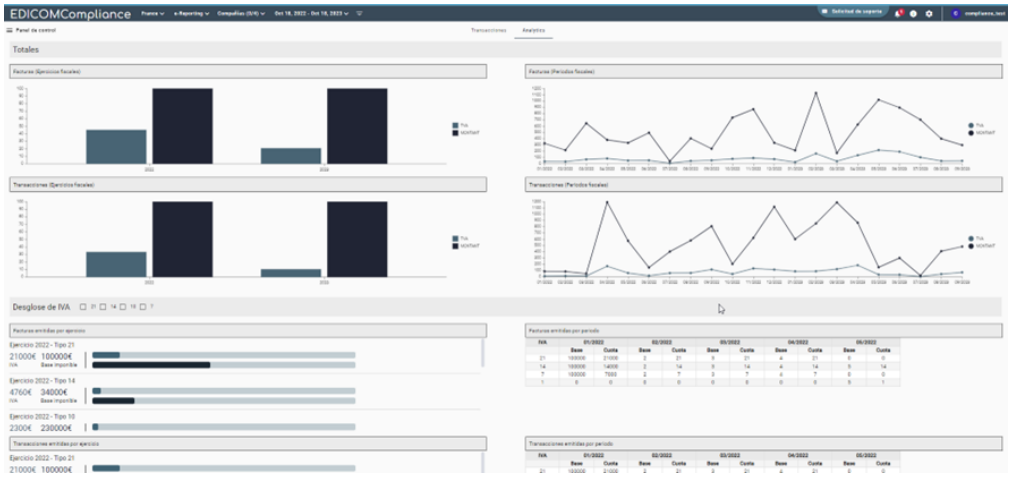
The main aim of the service is to offer EDICOM clients a different vision on the management of Ediwin documents, establishing a new standard and similar interfaces for the different countries where electronic invoices are mandatory.

The key advantage over the traditional Ediwin interface lies in the enhanced functionality of the new interface, allowing for invoice management based on their status, error resolution, and comprehensive monitoring of the entire invoice life cycle.

Establishing a standard interface for different countries allows all users to become familiar with the structure in which information is displayed for the countries in which this solution is implemented.



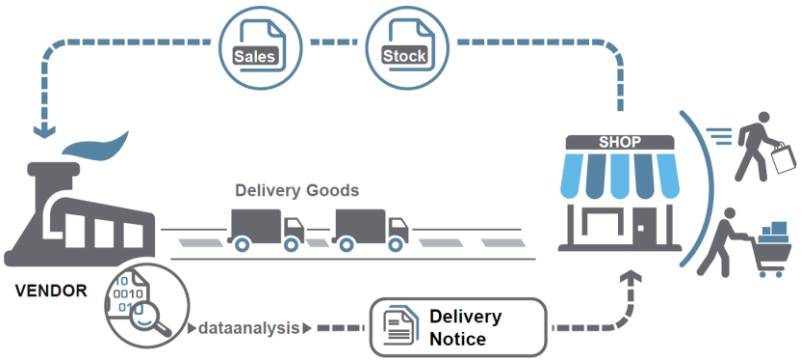
In addition, it is enriched with meaningful graphics for the client that allow monitoring and analysis of billing processes at a higher level.



- **CRP Flow**

CRP Flow is the EDICOM solution which implements CRPA/MI technology (Continuous Replenishment Planning/Vendor Managed Inventory). These systems are part of the ECR (Efficient Consumer Response) initiative to provide the end Client with the greatest value, best service and maximum variety of products.

To this end, synchronization of supply and demand is needed throughout the whole supply chain by means of electronic information exchanged between the parties involved in providing the Client service (supplier, distributor and logistics operator), usually via EDI systems.

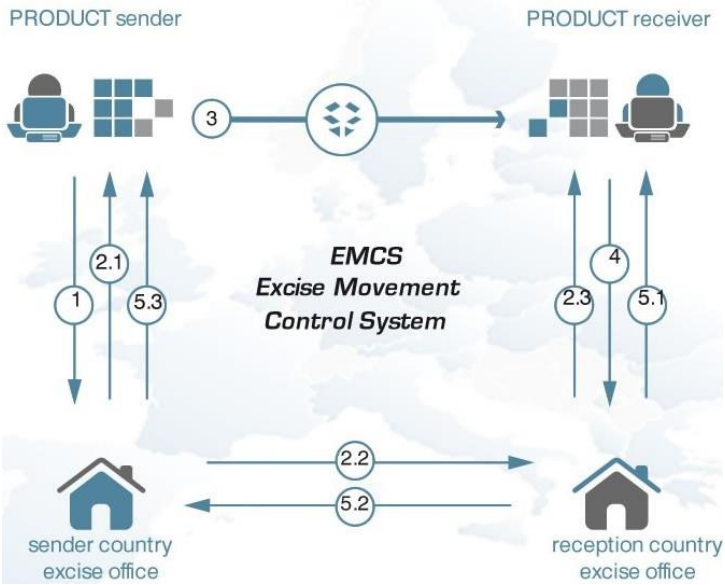


The system generates a result, which proposes specific product orders to the meet forecasted demand. Once these proposals are accepted, the CRP Flow solution integrates these data with the EDI system, generating the final delivery orders which can be printed, exported as a plan or transmitted via EDI.

- **EMCS**

EMCS (Excise Movement Control System) is a system created by the European Union to control movements of products subject to special duties (alcohol, tobacco, hydrocarbons, etc.) between member states.

As of 2011, it is mandatory for all economic operators sending or receiving these types of products throughout the European Union to replace the current administrative support document in paper format by an electronic message, being EDI the standard which provides the highest degree of automation.



This change involves the exchange of information not only between Client and supplier, but also with customs authorities of different countries in line with the technical specifications of each Public Administration on special taxes.

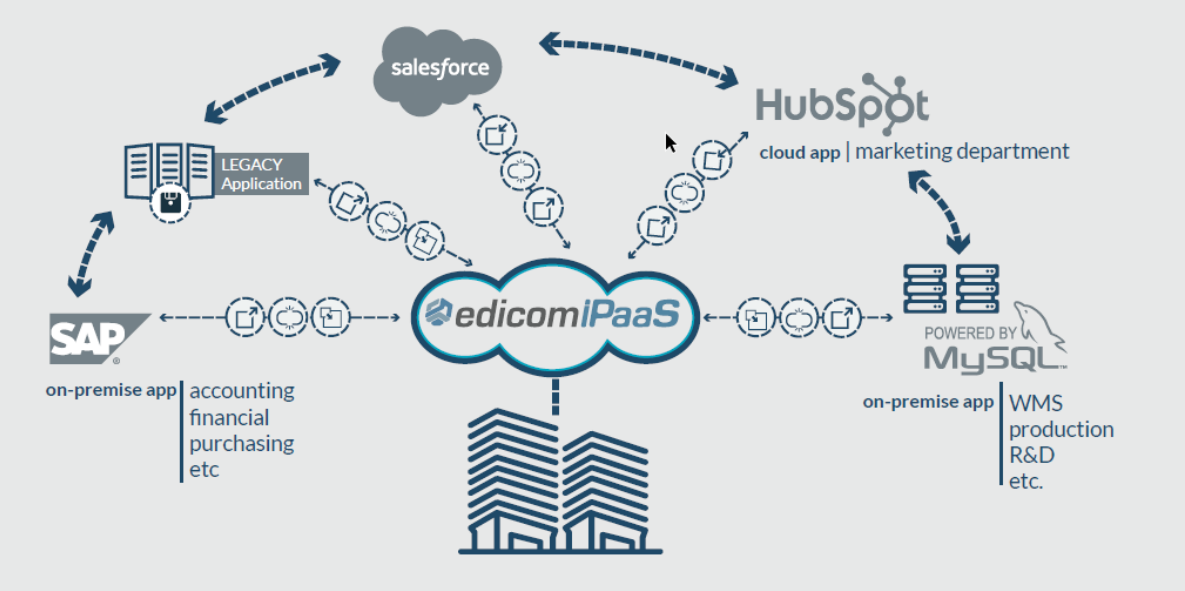
- **EDICOMiPaaS**

The EDICOMiPaaS service, or EDICOM Integration Platform as a Service, is a service to interconnect applications within a company. Companies have a huge volume of data from several sources, the adequate management and processing of which are important in any business. For that reason, EDICOM has developed an integration tool capable to interconnect and synchronize the information from different management application using cloud technology.

The features of iPaaS are:

- **Scalable processes**: an iPaaS offers a programming environment where each user has a group of dedicated resources for its own integration, independently from other running processes.
- **Programmatic control**: iPaaS enables applications in service mode to remotely control the integrations without the development of user interface.
- **Web Interface**: Like other cloud solutions, iPaaS has a web interface to monitor and control the integration processes.
- **Hybrid integration model**: The integration software operates on cloud, but in addition, it allows functionalities to integrate the local running application processes.
- **Default connectors**: the iPaaS platform must include connectors to the main market applications such as CRM, ERP, etc., by default.
- **Data volume**: iPaaS platform must be in constantly evolution, including new connectors which allow to users to simplify the integration processes.

EDICOMiPaaS enables users to interconnect all its management applications through powerful tools available in service-mode exclusively. EDICOMiPaaS combines data transformation solutions and connectivity to integrate all the applications from the Client IT infrastructure (accounting, invoicing, warehouse management, CRM, etc.), independently they are in-house or in cloud.



The features of EDICOMiPaaS are:

- **Cloud based**: the platform technological infrastructure, development, monitoring and maintenance are hosted and managed by EDICOM. This service in outsourcing mode allows to companies to the processes' integration management, meanwhile, the updating and infrastructure maintenance are automated performed and carried out by specialized EDICOM operators.
- **Integrated with the EDICOM solutions**: EDICOMiPaaS platform is integrated with the EDICOM services cloud infrastructure (EDI, electronic invoice, VAT Compliance, electronic signatures, and certificates, etc., due to the native integration with the electronic data interchange B2B2G solutions of EDICOM with any externa management application that might require it.
- **Security and confidentiality**: security audits based on international standards for OWASP (Open Web Application Security Project) vulnerabilities analysis. EDICOM keeps a strict control about security of its data and the suitability of its processes as set out the EDICOM certifications.
- **Total monitoring in real-time**: Integrations are running in real-time, allowing a monitoring in any moment of any integration process executed through simply and easily dashboards on the tools.
- **Scalability and flexibility**: EDICOMiPaaS is sized according to project requirements. The inventory of the applications and their processes could be modified and scaled swiftly suited to the needs.

- **High availability**: It includes by contract, through an SLA (Service Level Agreement), an availability of the 99,9% of the service and access to the platform. This is an important feature to maintain uninterrupted data transfer processes.
- **High performance**: The platform is designed to meet the most discerning projects demands. EDICOMiPaaS is included within the EDICOM cloud infrastructure, which manage more than 500 million transactions per year. Moreover, it has powerful administration and management tools to monitor key stats, the messages flow and the system overall performance.

EDICOMiPaaS capabilities are:

- **Management of publication applications**: Configuration and management of sourcing information applications, which data will be exploited by other applications which will receive the information in a structured manner for an adequate treatment.
- **On-demand connectors**: EDICOMiPaaS implements advanced tools to connectors programming adapted for each application particularity (local database, cloud applications, batch processes, etc.).
- **Mapping tool**: EDICOMiPaaS has specific mapping and data transformation features to adapt the sourcing application interfaces with the requirements of the destiny applications. It allows to manage the transformation schema of data structure, to guarantee the perfect adaptation of any owner file (txt, csv, idoc, etc.), through any protocol or any communication method (synchronous or asynchronous), online or batch.
- **Subscriber application management**: Configuration and management of applications which will receive the data. These applications could subscribe to sourcing applications. Any time there exist a new data schema, all the applications will take the schema, allowing the integration from different IT systems.
- **API repository management**: EDICOMiPaaS manages and updates a growing API inventory to simplify the development of new capabilities which increase the connectivity with the main applications.
- **Automation and orchestration of processes**: EDICOMiPaaS allows to develop tools to rules and scripts programming to automate and orchestrate the integration processes.
- **Alerts management**: EDICOMiPaaS allows custom alert configuration related with traceability and processes status (key processes surveillance, message dump interval, volumes, etc.).

Trust Services

The EDICOM trust services provides companies, communities and physical persons with secure electronic identification mechanisms that enable them to engage in activities where the digital signature replaces the handwritten signature with identical legal guarantees.

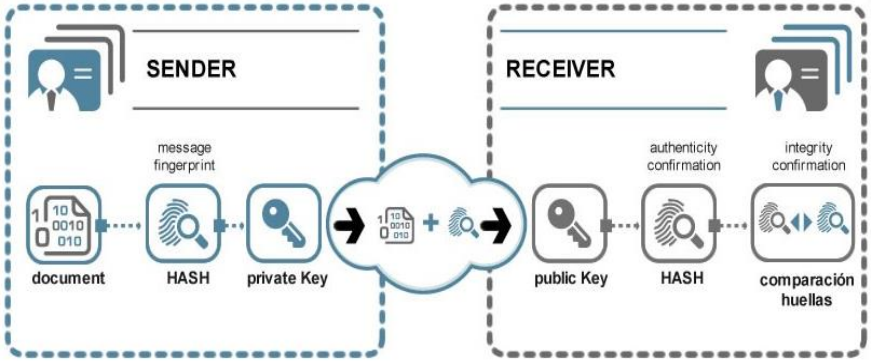
EDICOM now forms part of the Trusted list of qualified providers of electronic trust services (TSL) of the Ministry of Industry, Energy and Tourism, as EDICOM provides qualified trust services in accordance with the relevant provisions laid down in Regulation (EU) Nº 910/2014 of the European Parliament and of the Council of 23 July 2014.

Specifically, the following trust services are provided by EDICOM:

- **Qualified certificates issuance**

EDICOM CA issues qualified certificates for trust services in accordance with the stipulations of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 and Law 59/2003 of 19th December, on electronic signature, and so, has sufficient recognition to operate in all countries of the European Union. The EDICOM CA is responsible for obtaining the corresponding official authorization in those places outside the Union where it operates commercially.

EDICOM issues qualified certificates of use after positive identification of the subject, from qualified electronic signature creation devices or software support, and non-acknowledged certificates whose issue does not require the subject's physical presence at the Registration Authority.



A remote video-identification system is used to verify the identity of the applicant for a certified certificate that guarantees security equivalent in terms of trust to physical presence.

The following types of certificates are issued by the EDICOM CA:

- Qualified signature certificates on qualified electronic signature creation devices (QSCD).

- Qualified signature certificates on software support: Delivered in electronic files that can be downloaded onto hard disks or USB sticks, with no need for external devices to generate signatures.

- Qualified certificates for electronic seals on qualified electronic signature creation devices (QSCD).

- Qualified certificates for electronic seals on software support.

- Organization Validation (OV) TLS Certificates: EDICOM checks to make sure that the applicant actually has the right to the specific domain name, and EDICOM does some investigation of the organization.

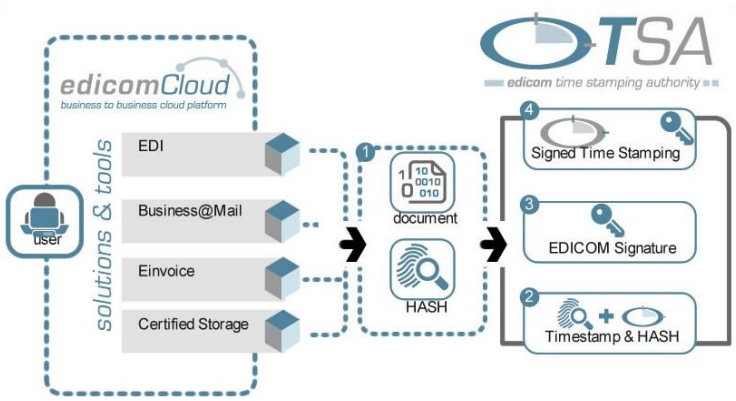
  Client certificates are issued to individuals for authentication in operating systems and email security. Server certificates are issued to domain names for server authentication in SSL (Secure Sockets Layer) services (https) or security purposes in IPSEC tunnels.

- **Preservation of qualified electronic seals**

The seals applied to the document are stored in format XAdES-LT in the application. Therefore, the information necessary for the verification of the information is stored at the time of signing. The information is stored by EDICOM (PCS) controlling the entire process from the creation of seal to storage.

- **Qualified electronic time stamps**

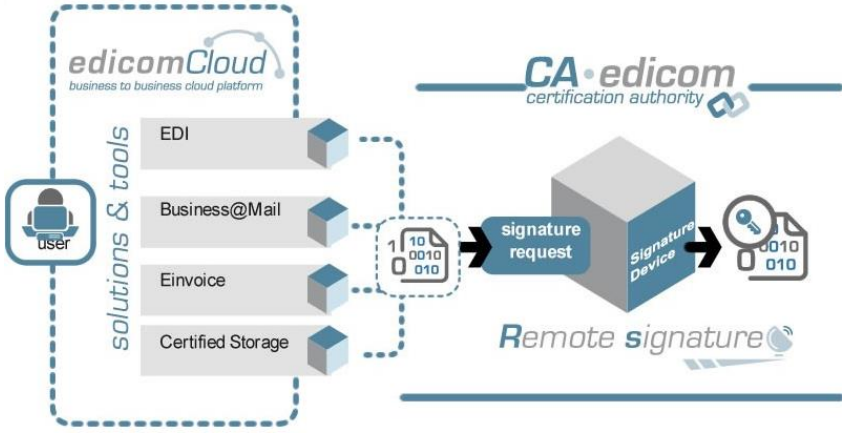
EDICOM's time stamping authority acts as a trusted third party testifying the existence and integrity of electronic data at a specific point in time.



Services described previously use EDICOMNet, the EDICOM VAN (Value Added Network) associated to the Edicom Cloud service, a private network that enables secure delivery, traceability and monitoring of exchanged transactions.

- **Remote signature**

Despite EDICOM's remote signature service is not defined as trust service, EDICOM Crypto Server (ECS), allows using an acknowledged digital signature with certificates stored in secure signature creation devices (SSCD) housed in the EDICOM facilities, through an HTTPS web service interface.



Using the EDICOM Certification Authority remote signature service contributes to avoid potential problems associated with the use of secure devices like smartcards or Hardware Security Modules (HSM), as the service takes charge of management and security of the device used to generate electronic signatures.

- **Delegated signature**

The Certification Authority delegated signature service implies that the client authorizes EDICOM to sign their e-documents, which are equally valid as if they themselves had signed them. It is not defined as trust service.

User-generated documents are signed by the Certification Authority with a certificate issued on behalf of EDICOM, saving the file owner from having to carry out these tasks, as well as maintenance and management of electronic certificates or signature devices.

This electronic signature mode can only be rolled out in those cases where it is expressly authorized under current legislation and for documents where this possibility is specifically acknowledged.

- **Electronic delivery (eDelivery)**

The Electronic Registered Delivery Service (ERDS) provides a secure and trustworthy delivery of electronic messages among parties, generating evidence of the delivery process for a legal responsibility. The evidence could be a declaration of one trustworthy party that a specific event related with the delivery process (message sending, message delivering, message rejection, etc.) happens in a specific moment in time. The evidence can be delivered to the interested party (attached to the message or separated) o could be stored in a repository for future access of the interested party.

EDICOM has structured eDelivery in three (3) systems:

  - EDICOM AS4 Server: The service is implemented over AS4 protocol and allows the connection among EU ERDS nodes, that is to say the system interconnects different ERDS from European Union according to ETSI EN 319 521 and ETSI EN 319 522 family.

    The AS4 protocol has been modelled in a 4-corner model. This model consists in the data interchange among 2 ERDS, one in the sender's systems, and another in the receiver's systems.

  - EDICOM iPaaS eIDAS Server y EDICOM Accounts Server: The service is implemented in an extended model according to ETSI EN 319 522, parts 3 and 4. The iPaaS Server has been modelled such as Black-box model. This model (Black-box) describes the ERDS interactions with the sender and the receivers through an application layer out of the boundaries of the ERDS.

- EDIWIN Server: The service is implemented in an extended model according to ETSI EN 319 522, parts 3 and 4. The EDIWIN Server has been modelled such as Black-box model.

- **Electronic signature and electronic seals validation**

Electronic signatures and electronic seals validation service allows to EDICOM to validate any electronic signature and electronica seal with two (2) kind of access to service:

- WEB interface over HTTP/S protocol. The URL access to WEB interface for electronic signatures and electronic seals validation is:

  https://web.sedeb2b.com/EcsWeb/eidas/validationReport.

- Webservice interface over HTTP/S protocol. The URL access to Webservice interface for electronic signatures and electronic seals validation. The service implementation is performed through an internal HTTP protocol.

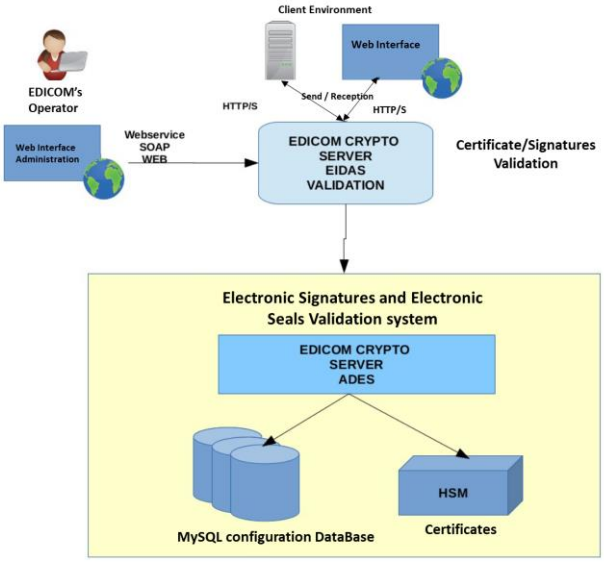
The electronic signature validation assesses the electronic signatures and determines if the signature is Advanced Electronic Signatures (AdES), AdES supported by Qualified Certificate (AdES/QC) or Qualified Electronic Signature (QES).

To obtain this assessment, the validation algorithm is composed by 3 parts:

- Signature validation: there is a validation of the AdES signature according to ETSI EN 319 102-1.

- Certificate checking to confirm that the certificate is valid, and it was qualified for signature o seal in when the certificate was issued.

- Certificate checking to confirm that the certificate is valid, and it was qualified for signature o seal, and it was associated with a Qualified Signature Creation Device (QSCD) at the signature process.



For this checking process the service performs these checks in the certificate/signature issuing:

- Determining the certificate qualification state and its type.

- Checking that in the signature moment, the signing certificate was a qualified certificate and determining if the corresponding private key was protected by a QSCD.

Once the assessment if performed, the validation process results are the following items, codified in XML format:

- Simplified validation report. This report allows to obtain the information in an easily and simplify manner, keeping the most important items. The final user can have a briefing of the validation. The report includes the used policy in the validation moment, document validated, number of signatures and information of each one.

- Detailed validation report. This report includes the following information:

  - Basic Validation Blocks.
  - Validation information for Basic Signatures.
  - Validation information of Time Seals.
  - Validation information of Signatures with Time.
  - Validation information of Signatures with information of Long-Term Validation.
  - Validation information of Signatures which provides Long Term Availability and Validation Integrity.
  - Validation information of Qualification of the Signatures.

All the elements or items of the detailed validation report are fulfilled according to ETSI EN 319 102-1

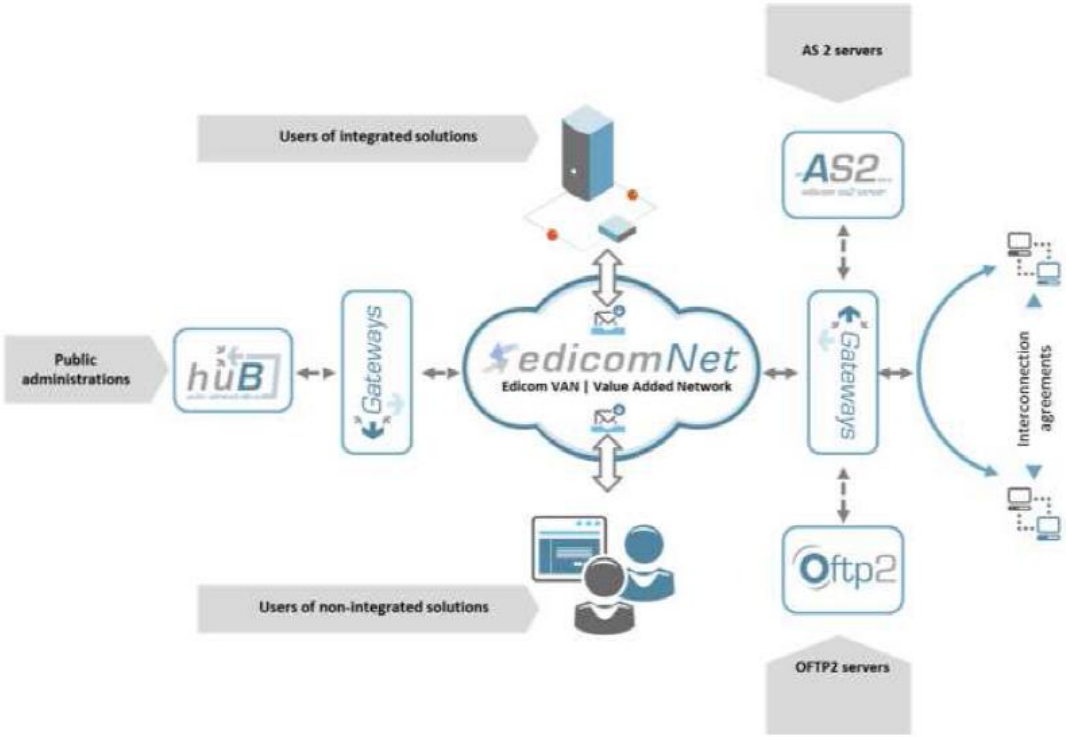
Diagnostic information. This set of data are built from the own signature's information, and also from dynamic recovery information such as revocation data; and extrapolated information such as signature's cryptographic validation. All the information is independent from the applied validation policy.

Communications Infrastructure

- **EDICOMNet**

Processes more than 500 million transactions a year from trading partners present in EDICOM VAN, as well as from other partners present in other proprietary VANs, thanks to multiple interoperability agreements. Multi-protocol and multi-standard, it can connect with any interlocutor and routing all types of messages. Service with high availability and continuous traceability registration.

EDICOMNet operates as a centralized communication management infrastructure, available 24x7 and permanently monitored. EDICOMNet supports, among others, the following protocols:



- **AS2**

Solution for interchanging business documents securely via Internet using data encryption techniques and digital certificates. Communications that implement delivery control generate receipt acknowledgments as a response to messages from the source server.

- **Hub**

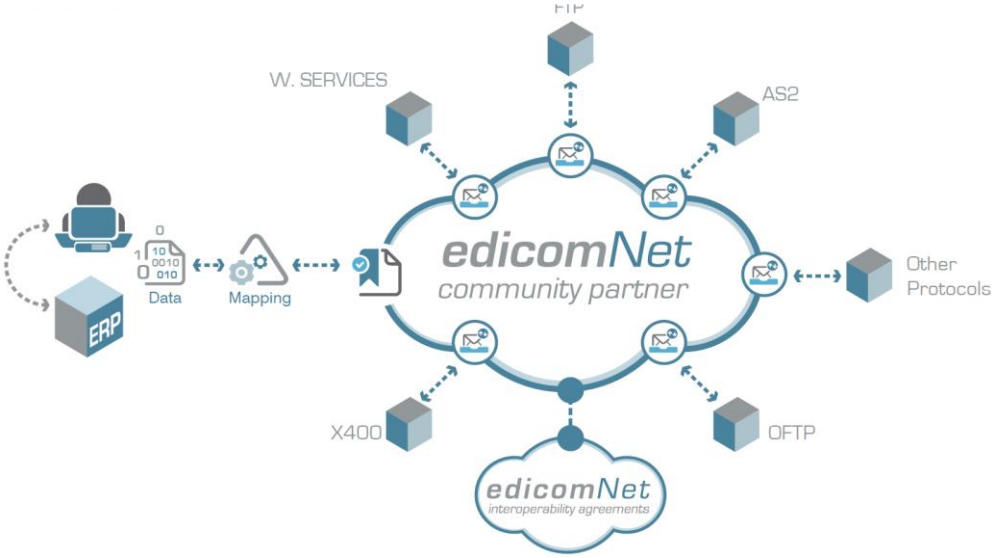
Communication service with direct connectivity to the European Public Administrations. Exempts the user from implementing complex protocols for simplified connection for exchanging information with any administration.

The complexity of point-to-point connections of trading partners with each administration is eliminated. Senders just must indicate the receiving administration and EDICOMNet transmits the message using the syntax, structure and connection protocol specified by each destination.

- **OFTP2**

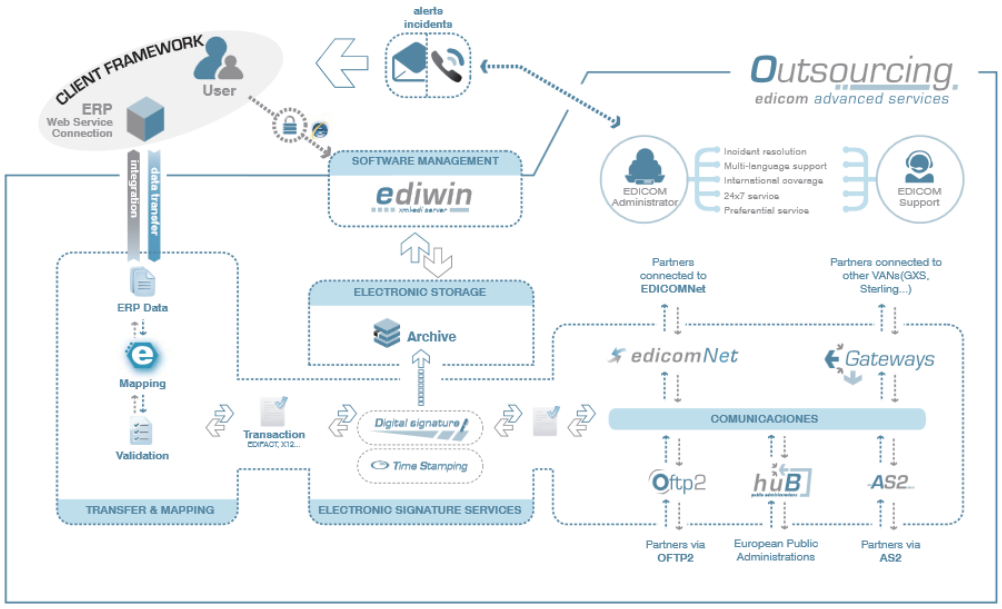
Communication service for the exchange of structured messages in accordance with the Odette File Transfer Protocol standards. It is a protocol which is widely used in the automotive industry and offers numerous advantages:

- Simplifies the exchange of structured EDI transactions and technical CAD/CAM/CAE) documents.
- It has the capacity to re-establish transmission processes in push and pull mode.
- Implements data encryption via asymmetrical cryptography and source verification processes by electronic signature.



Advanced Services

- Outsourcing: EDICOM outsourcing service frees the Client from managing its EDI communications platform as well as its day-to-day operation. EDICOM places a technological infrastructure at client disposal which is monitored 24x7 by dedicated professionals.



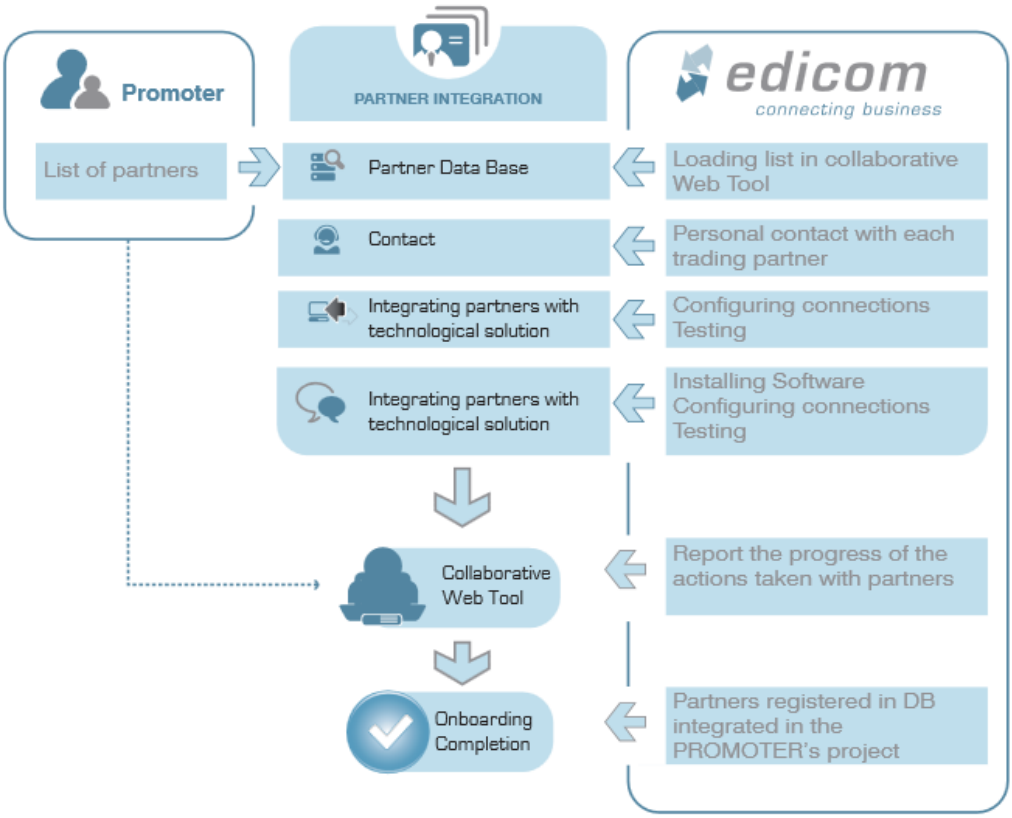
- Preferential Support: Edicom Cloud Service helpdesk is the single point of contact for all incidents and doubts related to the Edicom Cloud Service. Preferential support service, available 9 hours from Monday to Friday (9x5), is a service that attends all types of queries and incidents, and not only emergencies. Additionally, a High Availability Support

Service, available 24 hours from Monday to Sunday (24x7). Attention is exclusively in Spanish and English languages. Clients contact helpdesk using specific phone numbers depending on its country in order to attend the client in its native language. Preferential service level has a specific operator assigned and, in case of necessity, two-level helpdesk is also available.

SERVICE LEVEL	Availability	Maximum response time
STANDARD Maintenance Service	Provided in 9:00 to 18:00 schedule on weekdays	30 MINUTES
PREFERENTIAL Maintenance Service	Provided in 9:00 to 18:00 schedule on weekdays	15 MINUTES
HIGH AVAILABILITY Maintenance Service	Provided 24 hours a day, 7 days a week (every day of the year).	15 MINUTES

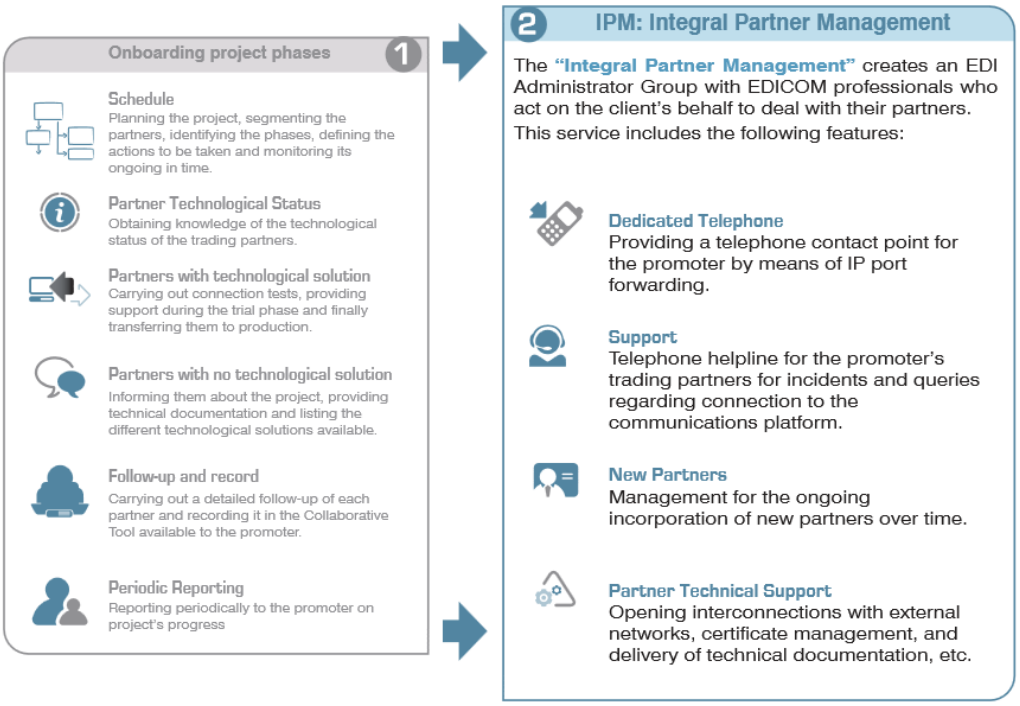
- Onboarding: EDI communications projects often focus their attention on the technological components (platforms, formats, communications, etc.), leaving the management-related aspects for incorporation of trading partners in second place. Nevertheless, this is the part that demands most dedication of time and effort and the one that will determine the success of the project.

  The EDICOM onboarding service deploys an infrastructure of technical and human resources to achieve the integration of trading partners in a brief space of time.



- Integral Partner Management: Once the initial integration of partners through the onboarding service is finalized, the client may ask EDICOM for Integral Partner Management (IPM) service.

  This service involves continuous management for error processing, integration of new messages, configuring new partners, cancellations, etc.



SignADoc

A document approval and e-signature solution that applies electronic signatures of different security levels depending on the sensitivity of the information. EDICOMSignADoc generates evidence reports of all interactions that take place during the approval lifecycle of your documents. The platform features are described as follows:

- Custom Approval Workflows: Workflow design in EDICOMSignADoc consists of setting parameters to define the approvers involved, the level of authentication required and the type of evidence to be collected in each step.

- E-signature platform: Generated by the system, ensures traceability and security of the entire approval process. E-

signature for approval of e-certificates issued in the user's name (qualified certificates, non-qualified certificates, secure signature-creation devices).

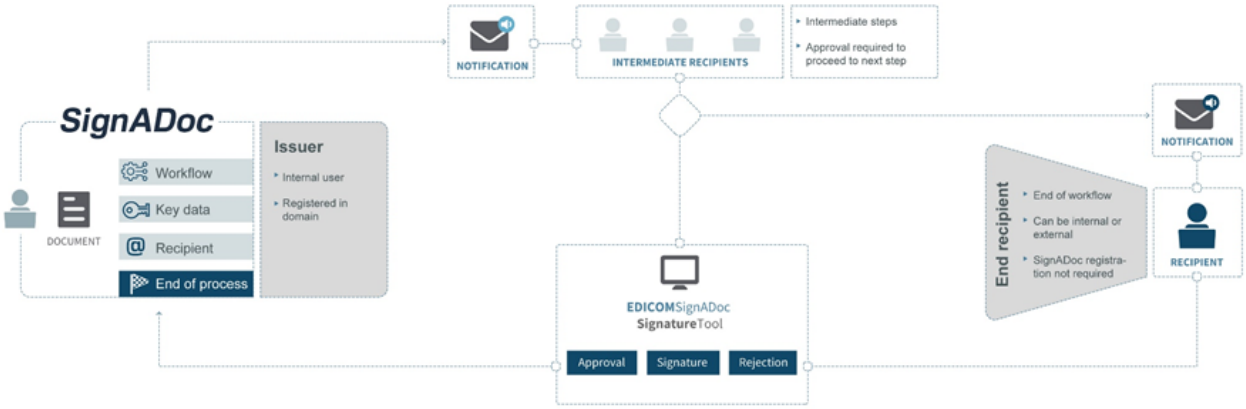
- Evidence Report: The system generates a log of all the different actions taken on the document.

- Trust Service Provider solutions: EDICOMSignADoc integrates with EDICOM Trust Service Provider solutions to issue e-certificates, time stamps and e-signatures and for long-term electronic storage.

- Integrated with the Long-term archiving service for electronic documents (EDICOMLta): This guarantees security and integrity since documents, signatures and evidence of approvals are stored in an eIDAS-certified service.

- Security: EDICOMSignADoc applies security mechanisms audited for compliance with the most important international standards.

- Integration as a Service: Connectivity with any ERP, CRM, or information system, including proprietary or custom applications.



3.1.3 *Key services organization changes occurred in the audit period*

EDICOM provides the new *EDICOM Compliance* service, which consists of a solution that offers clients a new different vision on the management of Ediwin documents, allowing managements based on the invoice's status, the administration of their errors and the monitoring of the invoice life cycle.

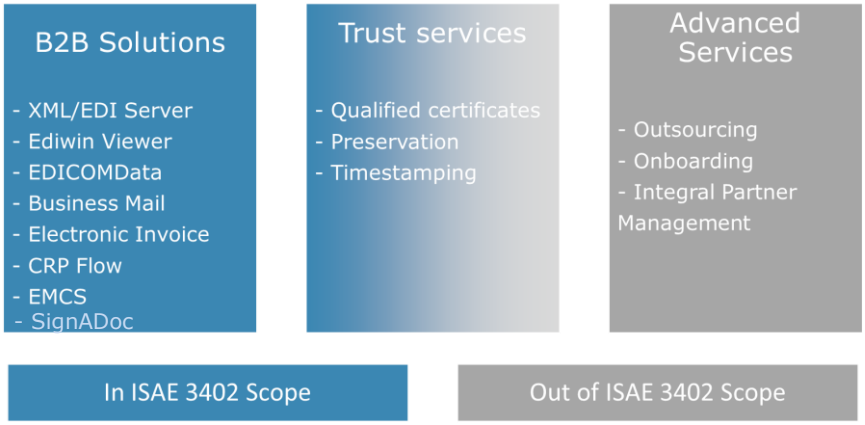
No other significant changes have been identified.

3.2 Services in scope

3.2.1 *General scope description*

This report has been prepared to provide information on the controls applicable to Edicom Cloud Service.

This report features Edicom Cloud Service and focuses on control objectives that are relevant to the internal controls for financial reporting for Edicom Cloud Service clients.



The scope of the report covers the significant business processes that EDICOM has determined are material to its clients from a financial reporting perspective and the supporting general computer controls.

EDICOM management is responsible for the identification of the control objectives and for the manual and automated controls placed into operation to achieve those objectives.

The Edicom Cloud Service includes the following solutions and tools which are served in the B2B cloud platform:

- Ediwin XML/EDI Server.
- Ediwin Viewer.
- EDICOMData.
- Business Mail.
- Electronic Invoice.
- VAT Compliance
- CRP Flow.
- EMCS.
- SignADoc.

In addition, for the following trust services the processes and controls described in chapter 3.4 have been reviewed, and test of operating effectiveness of such controls are included in chapter 4.2:

- Qualified certificates issuance
- Preservation of qualified electronic seals
- Qualified electronic time stamps
- Electronic delivery
- Electronic signature and electronic seals validation

This report is not intended to encompass the control aspects of other EDICOM teams, platforms, services, solutions, tools or procedures not included previously that may interface with Edicom Cloud Service.

3.2.2 *Technical scope description*

The scope of this report consists of the general IT (Information Technologies) controls related to Edicom Cloud Service, which is served in B2B cloud platform. Solutions included in the scope of this report are based on this technological infrastructure and therefore, are subject to established general IT controls.

EDICOM B2B cloud platform is based on a three-tier architecture model. This model of application and infrastructure development contributes to enhancing availability, reliability, integrity and security of the overall system and consists of the following layers:

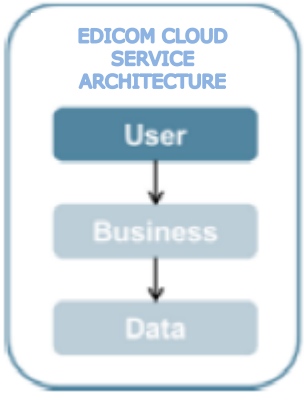
- User services layer.
- Business services layer.
- Data services layer.

EDICOM has three data centres from which it provides its services. One located at EDICOM headquarters (EDICOM Business Centre) and the other, several kilometres away from EDICOM, is contracted with a provider (COLT), this second data centre is a colocation centre in housing mode, where EDICOM has replicated the systems for the provision of services. During the audited period, EDICOM is migrating to an architecture with three simultaneous DPCs. The third DPC (Walhalla), is also a colocation centre in housing mode, where EDICOM is replicating the systems for the provision of services.

These three data centres are interconnected and each of the above services layers (user, business and data) is designed to work according to a high availability schema "Active / Active". This schema allows EDICOM to improve the services availability and fulfil the service level agreements (SLAs) with customers.

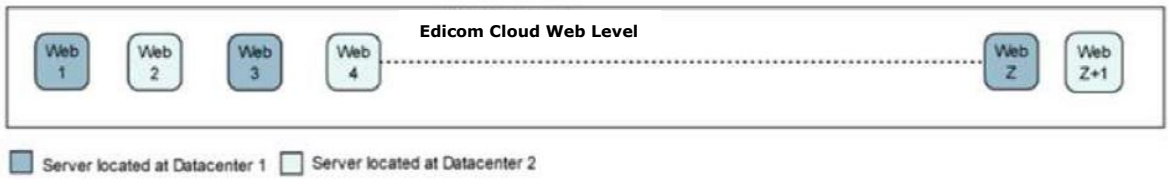
Technical description of each layer is detailed next:

User services layer



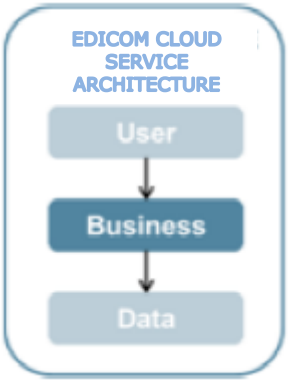
The user services layer consists of a group of webservers which provide access to the web interface of the Edicom Cloud Service. This service layer runs on a Linux platform using Apache HTTPD and Apache Tomcat and has been developed in-house using Java technology.

User services layer is sized for a maximum number of concurrent sessions; therefore, web servers are arranged on this level in order to cover expected workload and to comply with Service Level Agreement (SLA) established with Clients. Load balancers in high availability mode distribute load among web servers.



This layer does not have direct access to data, it just manages Client interaction with the service access portal and delegates data access to the business layer. Nevertheless, actions performed by users through the web-interface could affect the integrity of exchanged messages (e.g.: modifying interlocutor properties, accidentally deleting messages, etc.).

Business services layer



Business services layer consists of a group of application servers which implement logical business rules to allow the reception, transformation and exchange of EDI messages between business partners. This service layer runs in a Linux platform using Apache Tomcat and has been developed in-house using Java technology.

The technological infrastructure of business services layer consists of an integration bus where messages are received from the issuer, transformed and sent to the receiver in a transparent way. Access to the data services layer is also controlled in the business services layer.

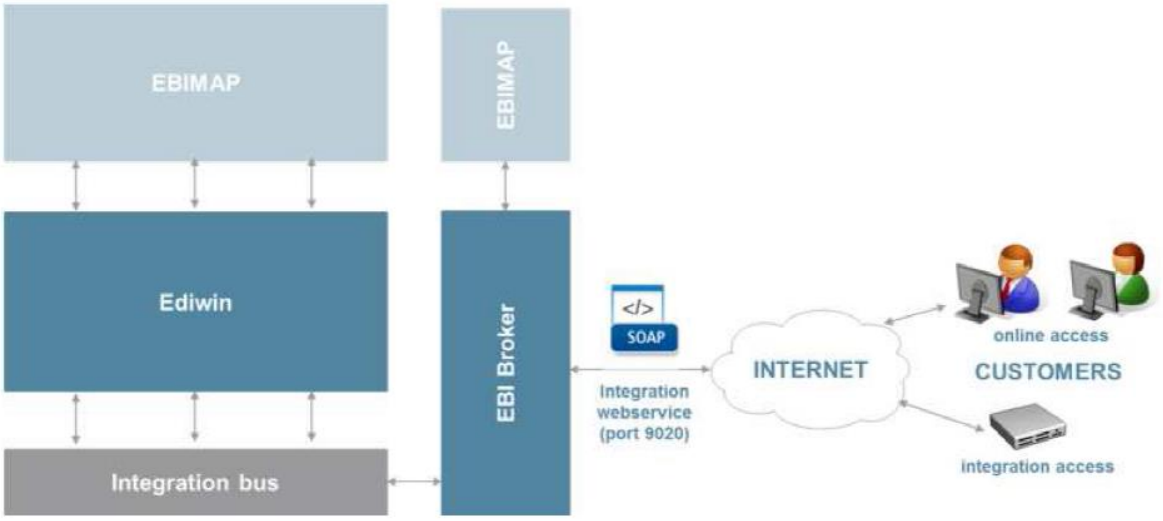
The business services layer is made up of the following pieces of software:

- Ediwin: This application allows the user of Edicom Cloud Service to examine EDI messages exchanged with interlocutors. Other functionalities are described next:
    - Review and print lists of received and sent messages.
    - Generate new documents.
    - Manage read and unread documents.
    - Search documents.
    - Group documents in personal folders to ease management.
- EBI (EDICOM Business Integrator): Software developed to support the whole process of application's integration. Composed of the following modules:
    - EBI Manager: Module used to create rules, link applications, define transformation rules and, in general, configure every single operation performed through EBI.
    - EBI Broker: Controls and manages access to the integration bus.
    - EBI MAP (EDICOM Business Integrator Mapping Tool): Mapping application module which applies transformation rules to source messages in order to adapt them to the destination system.
    - Adaptors: Connect applications and systems installed at Client's data processing centres to the B2B cloud platform hosted by EDICOM. One end of the adaptor is connected to systems at Client's site and the other end is connected to the B2B cloud platform. Depending on Client policies and technological infrastructure, EDICOM allows the use of the following types of adaptors:
        - Standard: Adaptor developed in-house by EDICOM in Java or Delphi technology. This alternative is used by most Clients and communication between Client's DC (Data Centre) and B2B cloud platform is performed through web services over SSL using 256-bit keys.

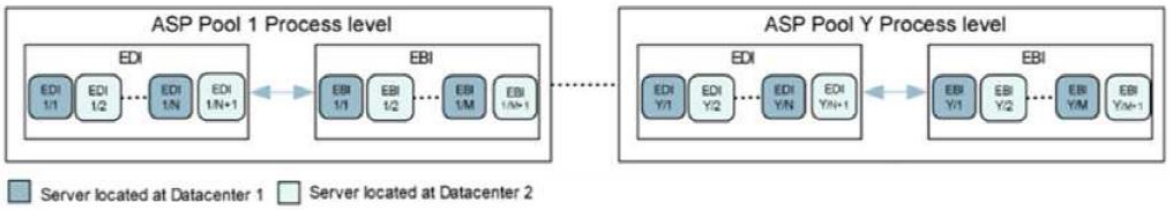
- Client developed adaptor: The Client develops its own adaptor using WSDL (Web Services Description Language) provided by EDICOM.

- File exchange: Adaptor developed in-house by EDICOM which supports the use of file exchange systems through FTP (File Transfer Protocol), SFTP (FTP over SSH) and FTPS (FTP over SSL).

The following diagram depicts the relationship between software modules which support the operation of the business services layer:



Business services layer implements the concept of "pool". An ASP pool is a group of servers which have been arranged to support processing of business layer for a fixed number of Clients depending on the volume of exchanged messages.



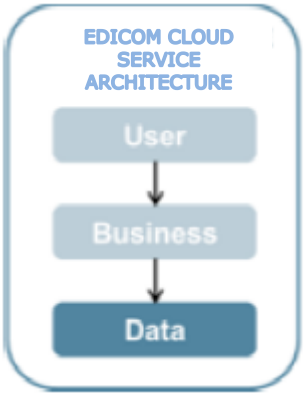
Each pool is initially sized with the necessary servers to provide the service as specified on the standard SLA. If a server is down, the rest of servers in the same pool take over the load while maintenance tasks are conducted without impacting system performance.

Regarding the physical distribution of servers of each pool, Ediwin and its corresponding EBIMAP are installed in a physical server and EBI and EBIMAP are installed in another physical server.

During the period under scope, the business services layer is distributed as follows:

- A group of pools for Ediwin + EBIMAP, half in each DC.
- A group of pools for EBI + EBIMAP, half in each DC.

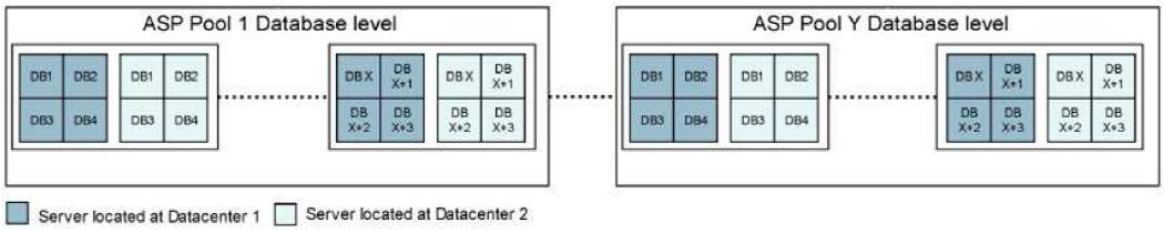
Data services layer:



Data services layer consists of a group of database servers and is accessed through the business services layer. Database management system used by Edicom Cloud Service is MySQL under CentOS, Ubuntu, Elasticsearch, Ceph and Kubernetes.

Services under the scope in this report are supported by three databases. Specifically, they are used by Ediwin, EBIMAP and EBI.

Data services layer also implements the concept of "pool". In this case, an ASP pool is a group of database servers which have been arranged to support processing of data layer for a fixed number of Clients depending on the volume of exchanged messages.



During the period under scope, data services layers is formed by MySQL servers distributed in each DC.

3.2.3 *Edicom Cloud Service supporting organization*

The Edicom Cloud Service is structured in three clearly differentiated processes:

- Edicom Cloud environment installation.
- Edicom Cloud Service provision.

- Edicom Cloud Service cancellation.

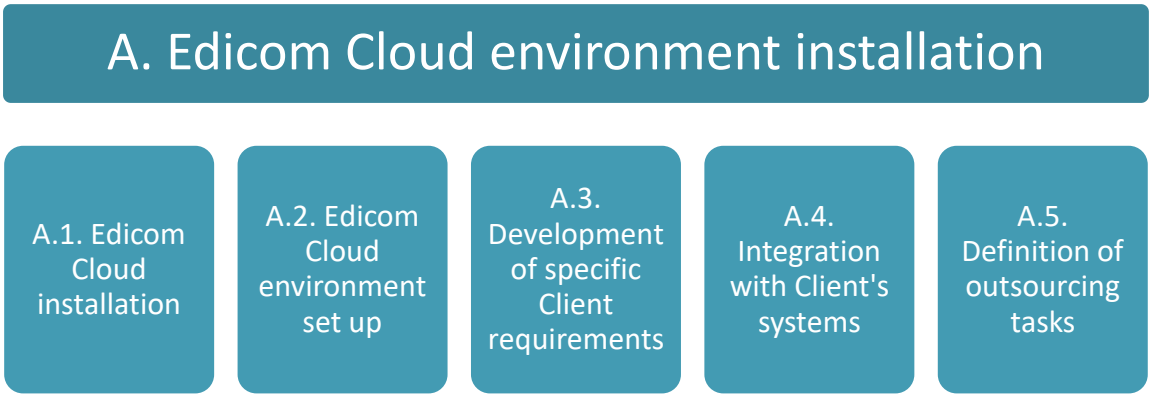
These processes are detailed below from the following perspectives:

- Key activities performed by EDICOM in each process/subprocess.
- Department responsible for executing key activities.

A. Edicom Cloud environment installation

The Edicom Cloud environment installation process defines necessary steps to set up a new Edicom Cloud Service Client in the B2B cloud platform. This process begins once the Sales department has signed a formal contract with a Client.

The sub-processes and key activities of this process are described below:



A.1. Edicom Cloud installation

First step of the Edicom Cloud environment installation process consists of opening a new logical domain in the Edicom Cloud environment. This subprocess is performed by the 24x7 area by request of a project manager from the Consulting department.

A.2. Edicom Cloud environment set up

Setting up a logical domain for a Client in the Edicom Cloud environment requires configuring certain parameters of the installation to adapt the standard environment to Client needs. This subprocess includes, but is not limited to, the configuration of:

- Address books.
- Messages.
- Mailboxes.

- Adaptor used in the exchange of data between Client's systems and B2B cloud platform.
- Predefined alarms.

This subprocess is performed by the Consulting department. Once the Edicom Cloud environment has been set up, the project manager agrees a date with the Client to carry out the integration subprocess.

A.3. Development of specific Client requirements

Clients may request specific developments to personalize its Edicom Cloud installation before service deployment. Custom developments must be analysed by the Consulting department to calculate its cost and once EDICOM and the Client reach an agreement, a formal contract is signed, and the R&D (Research & Development) area starts the development task.

Development of specific Client requirements is not a standard feature of the Edicom Cloud Service and therefore, it is not included within the scope of the present report. In this way, service auditor's procedures do not extend to controls related to development of specific Client requirements.

A.4. Integration with Client's systems

This subprocess comprises the realization of the following tasks to ensure the correct integration of Client's systems and the B2B cloud platform:

- Configuring maps, publishers and subscribers.
- Verifying the integration of messages exchanged through the Edicom Cloud Service and Client's management platform (ERP, custom-developed software, etc.).
- Train the Client on the functionality of the B2B cloud platform.

Previous tasks are responsibility of the Consulting department.

A.5. Definition of outsourcing tasks

The outsourcing service allows Clients to entrust EDICOM with the management of their Edicom Cloud Service. Principal activities of this service are related to EDI interlocutor management and include, but are not limited to:

- Updating address book.
- Incorporating new interlocutors to the Edicom Cloud Service.

- Performing changes to the Value-Added Network (VAN).

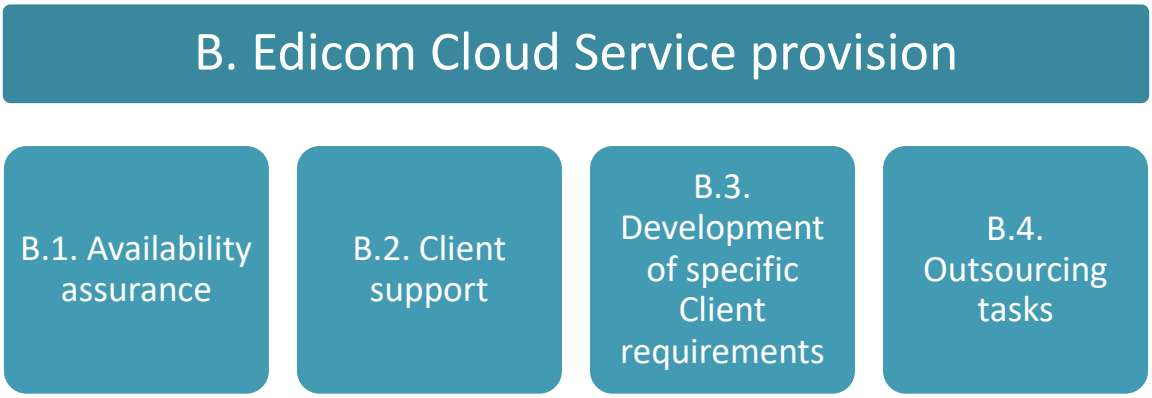
The responsibility of the configuration and operation of the outsourcing service is shared between Consulting and Preferential Helpdesk departments.

Outsourcing service is an additional product to the Edicom Cloud Service and thereby, it is not included within the scope of the present report. In this way, service auditor's procedures do not extend to controls related to outsourcing tasks.

B. Edicom Cloud Service provision

The Edicom Cloud service provision process defines necessary steps to support ongoing service delivery requirements, Client support, new functional requirements and evolution of the Edicom Cloud service.

The subprocesses and key activities of this process are described below:



B.1. Availability assurance

EDICOM monitors continuously its B2B platform to ensure compliance with availability requirements included in Edicom Cloud Service Level Agreement.

Assuring Edicom Cloud availability is responsibility of 24x7, IT and Edicom Cloud Quality manager.

B.2. Client support

Client support subprocess allows Clients to communicate incidents and doubts regarding their Edicom Cloud installation. Response time of the Client support service and resolution time of incidents are included in the Edicom Cloud Service Level Agreement.

Client support is provided by Standard Helpdesk and Preferential Helpdesk areas.

B.3. Development of specific Client requirements

Clients may request specific developments to personalize its Edicom Cloud installation once the service has been deployed. Custom developments have to be analysed by the Consulting department to calculate its cost and once EDICOM and the Client reach an agreement, a formal contract is signed, and the R&D area starts the development task.

Development of specific Client requirements is not a standard feature of Edicom Cloud Service and therefore, it is not included within the scope of the present report. In this way, service auditor's procedures do not extend to controls related to development of specific Client requirements.

B.4. Outsourcing tasks

The outsourcing service allows Clients to entrust EDICOM with the management of their Edicom Cloud Service. Principal activities of this service are related to EDI interlocutor management and include, but are not limited to:

- Updating address book.
- Incorporating new interlocutors to the Edicom Cloud Service.
- Performing changes to the Value-Added Network (VAN).

The responsibility of the configuration and operation of the outsourcing service is shared between Consulting and Preferential Helpdesk departments. Outsourcing service is an additional product to the Edicom Cloud Service and thereby, it is not included within the scope of the present report. In this way, service auditor's procedures do not extend to controls related to outsourcing tasks.

C. Edicom Cloud Service cancellation

The Administration department receives cancellation requests from Edicom Cloud Service Clients. Depending on the service, cancellation can be performed automatically by the Administration department or requires the intervention of 24x7 department.

3.3 Control environment

EDICOM's control environment reflects the position taken by its Board of Directors concerning the importance of internal control. The following is a description of the key elements of EDICOM's control environment related to the delivery of the Edicom Cloud Service:

- Oversight by EDICOM's Board of Directors.
- Risk assessment.
- Monitoring.
- Human Resources policies and practices.
- General computer controls.

EDICOM is organizationally and functionally separate from its Clients. Within EDICOM, specific duties and responsibilities have been established for each functional area.

3.3.1 *Criteria*

The following generic information and control criteria have been used to prepare the overall system and process description, to evaluate whether controls are suitably designed and to evaluate whether controls are operating effectively. These criteria are inspired by international control standards and are based on legal and business requirements linked to the Edicom Cloud Service offered by EDICOM.

- Confidentiality - Concerns the protection of sensitive data from unauthorized disclosure.

- Integrity - Relates to the accuracy and completeness of data as well as to its validity in accordance with business values and expectations.

- Availability - Relates to data and systems being available when required by business processes now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.

- Authenticity - Validates and guarantees the source or origin of data through the proof of identity.

- Traceability - Performances or transfers made can only be assigned to one originator, being able to trace and identify the sources of all inputs.

- Effectiveness - Deals with data being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.

- Efficiency - Concerns the provision of data through the optimal (most productive and economical) use of resources.

3.3.2 *Oversight by EDICOM's Board of Directors*

EDICOM's Board of Directors has the ultimate responsibility of overseeing the business policies of EDICOM. The Board of Directors is composed of internal executives and meets at least four-monthly.

Board of Directors' meeting discussion topics include, but are not limited to:

- Financial statements and other financial information provided by EDICOM to relevant stakeholders.

- Internal controls regarding finance, accounting, legal, regulatory compliance and IT.

- Findings and recommendations identified as a result of internal and external audits.

- Major litigation.

3.3.3 *Risk assessment*

EDICOM's Board of Directors regularly discusses business risks, including financial and technological risks. Risks identified in this process are analysed and given proper consideration in the strategic business plan.

3.3.4 *Monitoring*

EDICOM employs specialists in financial, operational and information systems auditing. These audits are conducted using either internal or external resources and are supervised in the first place by the Chief Financial Officer, Chief Technology Officer and Chief Security Officer, respectively.

As a last resort, the Board of Directors is responsible for the inspection of audit findings and for the implementation of action plans in a correct and timely manner.

Operational monitoring

Management information and reporting systems permit monitoring key controls and performance measurements. Each department establishes and maintains standards to provide the appropriate data to monitor the results of the processes they are responsible for.

Client account monitoring

Each client is assigned an account manager who communicates regularly to discuss issues and client satisfaction. In addition, clients are surveyed to determine client contentment with ongoing service delivery and products. Sales department and Edicom Cloud Quality manager are, respectively, accountable for previous tasks.

Internal and external audit monitoring

EDICOM is subject to reviews by internal and external auditors on a periodic basis. These audits are scheduled yearly by the Board of Directors.

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

- Finance and accounting.
- Project management.
- IT services management.
- Change management.
- Information security.

Supplier monitoring

EDICOM does not subcontract with external providers any of the parts of the service provided to its customers. Sometimes, the provision of services requires suppliers to provide a service (communications, hardware, basic supplies, etc.). Management of suppliers is carried out according to the Supplier Management Procedure whose objective is to carry out an effective management of the suppliers and the services provided, guaranteeing the provision without interruptions and with the corresponding quality of the services themselves according to the needs and commitments acquired with customers.

Based on the requirements of the service provided to EDICOM customers, the needs that the services provided by the suppliers must cover are determined. The selection of suppliers takes into account not only the requirements of the service provided but also considers the costs of the service, the capacity of the supplier, possibilities of expanding the service, the possibility of acquiring several services jointly, security requirements, etc.

EDICOM establishes service level agreements (SLA's) with the suppliers involved in the provision of services, in order to ensure that these service levels comply with the service levels that the organization has signed with its customers. The Supplier Manager monitors the levels of service received to identify and correct any type of deviation that may affect the services offered to customers.

Annually, the Supplier Manager performs an evaluation of the suppliers based on the following criteria:

- Review of service levels
- Adequate billing of the service
- Quality of the service provided
- Repeatability of incidents
- Review of the supplier claims record

3.3.5 *Human Resource Policies and Practices*

Human Resource needs are detected as a result of the capacity management process. Factors which are studied are the following:

- Business development: Based on historical business development data from past twelve months.

- Workload of employees: Comparing current performance indicators against historical key performance indicators which are the optimum to deliver the service to the Client (e.g.: number of incidents solved by Helpdesk operator per day).

- Terminations: Mutual agreement or involuntary.

Vacancies, including job specification and job description, are posted by Human Resources in the corporate webpage and in employment offices of recognized universities.

The recruitment process consists of two parts. First, applications are screened for minimum qualifications and finally, relevant interviews are conducted.

Human Resources policies and procedures are posted on EDICOM's Intranet. These policies include, but are not limited to, the following:

- Corporate code of conduct.
- Confidentiality of information.
- Acceptable use of information systems.

This documentation is provided at the time of signing the contract for new personnel incorporations and requires explicit acceptance.

The core values of EDICOM are posted on EDICOM's corporate code of conduct. These values include integrity, respect, excellence, responsibility and teamwork. EDICOM's code of conduct also serves as a guide to ethical conduct for all employees and covers areas of business conduct and ethics when working with clients, colleagues, suppliers or public in general and addresses conflicts of interest that could arise between the personal conduct of employees and their position in EDICOM. The company will consider as serious misconduct the non-compliance with the rules of conduct contained in EDICOM's corporate code of conduct.

EDICOM has also defined a disciplinary procedure to manage non-compliance with the security policy. In addition, each time an employee logs in through the domain, a banner warning is displayed to reaffirm again the express acceptance of the Security policies, guidelines and corporate code of conduct.

EDICOM has a Corporative Social Responsibility Dossier available on the website (https://careers.edicomgroup.com/edicomgroup-en/corporate-social-responsibility/) where it has been detailed the compromises acquired with the environment, clients, employees and with the society.

An annual assessment plan has been defined by EDICOM in order to check the performance of associates regarding their role. At the Consulting department, upward feedback strategy has been implemented.

EDICOM believes having highly trained professionals are crucial to offer its clients maximum quality services and, consequently, has developed the following continuous training strategy:

- All new EDICOM associates are required to participate in the new starter induction process, which takes about two months, and includes an initial course on information security. This program covers EDICOM's general policies and procedures and assists employees in becoming acclimatized to EDICOM's business philosophy. Training courses are updated regularly to meet changes with technology and internal procedures.

  All new employees are assigned a tutor responsible for coaching and mentoring during their first year at EDICOM. Tutors are responsible for assessing new employees on a monthly basis.

- EDICOM performs, in an annual manner, information security and data protection awareness courses to internal employees. In this way, all EDICOM employees must carry out an annual information security awareness session and at the end of it employees must take a test related to the contents given in the course to confirm whether they have understood them. The 2023 annual course covers basic concepts of information security, such as social engineering and phishing, password management, security on mobile devices and remote work, physical security and social network management, among others.

- Furthermore, throughout the audited period, regular communications have been disseminated to employees with the aim of enhancing their awareness of computer security. These communications have covered various topics, including responsible email usage, information confidentiality, and security responsibilities, among others.

  In order to carry out this task EDICOM has incorporated an integrated platform for security awareness training (KnowBe4) combined with simulated phishing attacks. A customized phishing attack simulation is performed annually. The results are monitored, evaluated and communicated to the personnel.

- Annual training programme specially focused for each employee depending on his position. Courses are divided into the following categories:

  - Internal:

    - Training on EDICOM's products, procedures and methodologies.

    - Health courses in occupational risk prevention.

  - External:

    - Languages: English, Italian, German, French, etc.

    - Competences: Project management, leadership, etc.

    - Technical: Information security, IT service management, software development, etc.

  The content and the trainer of every formative action is evaluated by the assistants in order to check the effectiveness of training provided and as an input to improve the annual training programme.

- Newsletters and memorandums summarize significant events and changes to corporate policy and are issued regularly. Time sensitive information is communicated to employees using email.

- As needed, managers hold staff meetings and one-on-one meetings. These meetings are an opportunity for employees to bring to management's attention any questions or exceptions regarding standard policies.

EDICOM has implemented a Teleworking procedure which describes the requirements that employees must meet in order to telework. Among the security measures implemented, the following stand out:

- It carries out with the Registration of the request and formal approval in JPersonal application.
- ZTNA connection.
- Centralized authentication system through Active Directory.
- Log and audit of remote connections.
- Only equipment provided by EDICOM must be used for teleworking.

3.3.6 *General Computer Controls*

In order to provide reasonable assurance on the effectiveness of the general IT controls supporting EDICOM business processes, an IT control framework has been developed and implemented. It is based on Spanish National Security Scheme High level, ISO/IEC 20000-1 and ISO/IEC 27001 standards, customized for EDICOM specific situation.

This framework is subject to a yearly ISAE 3402 Type 2 audit and a report is delivered to Edicom Cloud Service Clients on request. This framework, together with the yearly audit, assures the consistent application of internal controls and compliance to processes in the IT environment.

For each control objective one or more control activities (including control activities' description, evidence, owners and periodicity) have been identified in order to formalize the EDICOM expectations in terms of control.

3.3.7 *Client Control Considerations*

The controls described in this section cover only a portion of the overall internal controls that should be in place for the processes in the scope of EDICOM ISAE 3402 Type 2. The reader of this document should consider the Client's own internal control activities together with EDICOM's internal controls.

There are various control design features which place responsibility for control procedures upon the clients of EDICOM. The Clients of EDICOM and their auditors should be aware of these issues when establishing their own internal control and audit procedures. As these items represent only a portion of the control procedures at a Client location, Client auditors should exercise judgment in assessing the overall control environment.

These Client control considerations are detailed in the system description (chapter 3.4 of this report) and should not be regarded as a comprehensive list of all controls that should be employed by Clients.

3.4 Processes & controls

Internal control framework defined by EDICOM regarding IT processes which support the Edicom Cloud Service is described in the following section. It is divided in the following control areas:

- Computer operations.
- Security.
- Change and release management.
- Risk assessment, business continuity and data privacy.

Each control area may consist of various control objectives and each control objective may consist of various control activities. Control activities address the technological risks which may affect the client's Edicom Cloud Service.

3.4.1 *Computer operations*

3.4.1.1 Transaction integrity

Transaction integrity is an intrinsic feature of different Edicom Cloud Services modules. Standard integrity related alarms are configured during the Edicom Cloud Service installation subprocess and are aimed at ensuring the integrity of:

- Exchanged messages between the Client and B2B cloud platform and vice versa.
- Exchanged messages between the B2B cloud platform and the receiver and vice versa.
- Transformation rules applied to messages.

Predefined alarms include the automatic detection of the following errors which could affect the integrity of messages:

- Connection: Connection errors between interlocutors and among different software pieces of the B2B cloud platform.
- Mapping: Error when mapping a message to a standard or structure.
- Database: Error when processing messages in database management system.

EDICOM has implanted a tool in order to improve the way the alarms are checked.

Examples of these alarms are detailed below:

- Connection errors:
    - Timeout of any process launched between application system and EBI/IPAAS (or vice versa) or between EBI/IPASS and Ediwin (or vice versa).

      These checks include but are not limited to messages in deposited state during more than two hours, messages in subscribed or pending confirmation state during more than 30 minutes, received messages not processed within two hours, messages blocked (messages not processed after 6 failed attempts).

      Moreover, some Clients could have custom times and alarms which, depending on their Business and their Criticality, are configured and activated.
    - Error when publishing a message in the application system of the issuer.
    - Error when publishing a message in the application system of the receiver.
    - Error when publishing a message from EBI/IPASS into Ediwin.
    - Adaptor between application system and EBI/IPASS has disconnected.
    - Installations which have not registered data traffic a predefined period of time (incoming and outgoing).
- Mapping errors:
    - Errors during mapping process.
    - Messages which have been transformed erroneously.
    - Transformed messages which result in an empty message.

- Database errors:
    - Process locks.
    - Monitor processing of messages in temporary tables.

Moreover, EBI tool has automated configurations to execute processes, which have their own alarm messages, and processes to fix errors such as review messages with erroneous state (due to temporal fails on EDICOM's services or systems) and turn into relaunch process (this allows an easier, faster and automated way to fix error messages). There are rules created on an external system which order EBI to relaunch or fix messages and processes periodically.

When an alarm is raised, it is automatically displayed in EBIMON/CHECKMON, an in-house developed application which is used by 24x7 and IT departments to perform proactive and real-time monitoring of the B2B cloud platform. EBIMON/CHECKMON is a tool which acts as a centralized alarm monitoring system.

R&D has a different tool from EBIMON/CHECKMON to monitor their systems and platforms (ELK –Elasticsearch, Logstash and Kibana). This tool allows R&D to centralize all raised alarms.

Usually, 24x7 staff solve the alarms and it is not necessary to create any incidence. An incident is only created when 24x7 staff cannot solve the alarm and is referred to another department. Moreover, every time an alarm affects a Client or group of Clients, the 24x7 staff register an incident. This incident registers are stored for at least 3 years from their initial registration.

In addition, there is a person who is in charge of reviewing the most repetitive alarms detected by EDICOM's tools. He performs a statistical global review to ascertain the cause of the alarms and its possible solution. EDICOM has developed tools for this task.

Additionally, alarms are stored online in EBIMON/CHECKMON application at least 60 days to allow analysis and traceability of issues and subsequent implementation of corrective actions. These alarms are also included in the backup policy of the B2B cloud platform.

Finally, the Edicom Cloud Service has preventive controls to avoid issues which could affect the integrity of transactions. For example, a set of controls to prevent duplicated messages (incoming or outgoing) can be configured. Activation of previous controls, but not limited to, must be requested by Client

because its configuration depends on its business operations performed through the Edicom Cloud Service.

3.4.1.2 Availability monitoring

The availability SLA of the B2B cloud platform is 99.9%. This availability percentage is calculated considering the considerations specified in the EDICOM Service Level Agreement.

EDICOM employs custom-developed applications and scripts (Service Checking which monitors services to obtain the EDICOM SLA) and system software tools to continuously monitor the availability and performance of the B2B cloud platform. The IT department also uses scripts (computer programs that automate the execution of tasks or commands that could alternatively be executed one-by-one by a human operator) to monitor servers and other aspects such as CPU hard disk performance. EBIMON/CHECKMON receives alarms from both applications and scripts. Monitoring is executed at two different levels:

- Service level: Monitoring the availability of the different services which make up the Edicom Cloud Services from the standpoint of a client. These controls include, but are not limited to, checking the state of the following services:
    - Edicom Cloud Service modules (EBI, EBIMAP, Ediwin, Ediwin Viewer, etc.)
    - Communications services (DNS, gateways with other VANs, etc.)
- Systems level: Monitoring hardware performance and availability. Checks performed vary depending on the type of device:
    - Servers: disk space utilization, memory use, CPU load, free memory in Apache Tomcat, memory used by Java garbage collector, etc.
    - Communication hardware: firewall load, switches performance, availability and throughput of links with ISP providers, VPN (Virtual Private Network) tunnels performance, etc.

Scripts are also used to monitor the following services and devices: Current Load, Current Users, HTTP, PING, Root Partition, SSH, Swap Usage, TOMCAT Processes.

If the script result exceeds any threshold configured, an automated alert is sent to the EBIMON/CHECKMON application and, subsequently, analysed and treated by 24x7 and IT departments.

Alarms are treated by 24x7 and IT operators, depending on the type of alarm and the systems or platforms affected, following the alarm management procedure. Additionally, all alarms are stored online in the EBIMON/CHECKMON application for 60 days to allow analysis and traceability of issues and subsequent implementation of corrective actions. These alarms are also included in the backup policy of the B2B cloud platform. In addition, the system department uses the tool PRTG Network Monitor to supervise all systems, appliance, traffic and applications of IT Infrastructure.

Additionally, EDICOM has a website where all Clients are able to monitor the availability status of their services in real time. The web portal is located at http://status.edicomgroup.com and its use is free of charge.

Client Responsibilities

The Client is responsible for inspecting EDICOM's delivery of service to ensure compliance with contractual obligations and accessing the public website which informs about the status of services being provided by EDICOM.

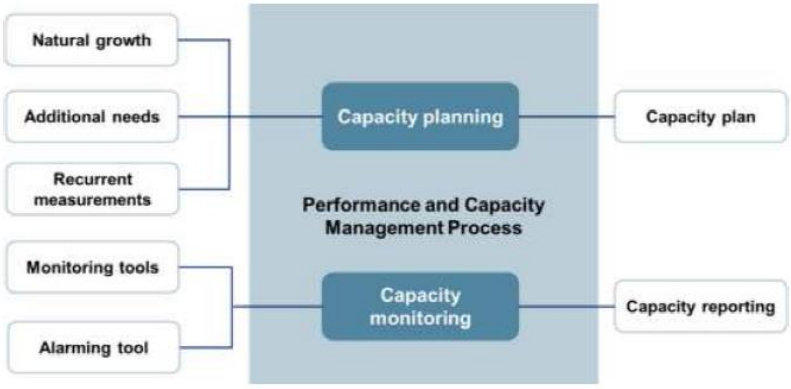
3.4.1.3 Capacity management

The objective of the capacity management process is to ensure that cost-justifiable IT capacity is available in line with the needs of the supported business. Within EDICOM, the IT department is responsible for managing this process. The process consists of two subprocesses:

- The capacity planning subprocess, to determine capacity needs and establish capacity plans.

- The capacity monitoring subprocess, to monitor Edicom Cloud Service performance, capacity usage and provide reporting to management.

The performance and capacity management processes are depicted and described below:



Capacity planning

The capacity planning subprocess encompasses the identification of future capacity requirements. These requirements are based on:

- Natural growth pattern of EDICOM services: The capacity model considers the natural growth pattern of the existing services and required resources for the day-to-day processing. Natural growth predictions are validated jointly by the IT department manager and the technical director.

- Additional requirements for new services to be launched: The capacity requirements of new services are provided by system architects and project managers in charge of designing and developing these new services.

- Actual performance and capacity measurements: Besides the two above-mentioned inputs, the capacity model considers actual measurements taken on different systems. Both business-related data (e.g.: number of exchanged messages) and technical-related data (e.g.: inputs/outputs per second, CPU processing power used, disk capacity used) serve as an input for capacity plans.

Based on natural growth, additional needs and continuous measurements, yearly capacity plans are produced. These plans are forward as well as backward looking, comparing current performance and capacity usage with the previously forecasted data and the estimated future capacity requirements.

Capacity plans are updated at least annually and every time pertinent information that may significantly change or influence the amount of resources forecasted is received.

The output of this subprocess is formally documented in capacity plans which have to be approved by the technical director.

Capacity monitoring

The capacity monitoring subprocess employs the same procedures and tools which are used to continuously monitor the availability and performance of the B2B cloud platform.

Capacity reporting

Reports are generated to provide history of data regarding the evolution of the business volumes and the evolution of the consumed resources. Exception reports are generated on demand or if there are indications of unusual or unknown performance and capacity usage.

The following reports are generated:

- Capacity analysis of the Edicom Cloud Service is performed by the Edicom Cloud Quality manager. These reports are produced approximately every two months, to coincide with the meeting of heads of department with Management.

  This report studies the following topics:

  - Review of actions performed and pending tasks.
  - Review the number of Edicom Cloud and Viewer Clients respect to its limit indicator.
  - Databases traffic measurement.
  - Overview of available capacity (in number of customers and documents moved)
  - Disk space.

  After these analyses, a set of recommendations specific for groups and Clients are produced. Additionally, a follow-up of the recommendations from the previous report is performed.

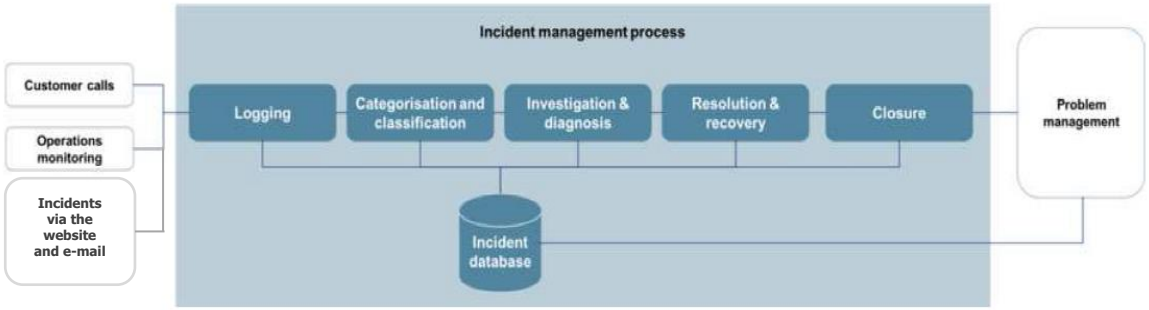
- Internal availability and performance indicators collected by the IT department and shared in the meetings of heads of department with EDICOM's Management when there is any deviation of interest to comment.

- SLA report regarding availability of the Edicom Cloud Service, performed by the manager of the 24x7 department and distributed to Clients with their invoice. This report is generated on a monthly basis.

3.4.1.4 Helpdesk

EDICOM has implemented an incident and problem management process to manage incidents and problems that may affect the operational services delivered to its Clients. Where the incident management process is aimed at the restoration of interrupted or reduced services within predefined timeframes, the problem management process focuses on finding root causes for one or more incidents in order to prevent the recurrence of similar incidents in the future.

The major steps in the incident management process are depicted and further described below:



Incident logging

Incidents are mainly created either based on Client calls, incidents received via website and email, by the Helpdesk service, as well as a result of the monitoring of the operational environment by the 24x7 department.

Most incidents, especially those which are categorized as critical or major incidents, are communicated via phone call to EDICOM, but there is also a dedicated website where Clients can register their incidents (access granted upon request) or through a web form embedded in software applications developed by EDICOM (e.g.: Ediwin Viewer) which has access to the previous URL.

Additionally, Clients can communicate the incidents via email to the Helpdesk staff. EDICOM uses an automatic system that automatically creates from Clients emails a new entry in the incidents tool. In case Helpdesk needs more information about the client or the incident, an automatic response via email is sent to the Client requesting this information. If Clients cannot login through the website, they can always contact EDICOM via phone call.

EDICOM’s clients have available the following website to communicate Helpdesk requests:

https://services.edicomgroup.com/edicomClient

Edicom Cloud Service Helpdesk is the single point of contact for all incidents and doubts related to the Edicom Cloud Service. The Client support centre gives service to EDICOM's Clients in seven different languages, and it is structured in three support levels: standard, preferential and 24x7.

For clients who have 24x7 support, EDICOM will give service only in English and Spanish. There are local 24x7 phones in all EDICOM’s sites (Germany, Italy, France, etc.). Nevertheless, EDICOM does not guarantee service will be provided in the local native language if the technician who attends the call is not a native person.

There is also a support service, available 24 hours from Monday to Friday (24x5). This 24X5 service is a service that addresses all types of queries and incidents, and not only emergencies. Support is exclusively provided in Spanish and English languages. The clients who contract this 24x5 service will be considered as a preferential client. Nevertheless, there may also be preferential clients who do not contract the 24x5 service.

Clients contact Helpdesk using specific phone numbers depending on its country in order to be able to attend the client in its native language, depending on the support level contracted (standard, preferential and 24x7).

As shown in the following graphic, Edicom Cloud SLA defines availability of the Client support centre and response time depending on the service level contracted. A comprehensive set of alarms regarding ongoing incidents to ensure compliance with the agreed support SLAs has been established.

Service Level	Availability	Response Time
STANDARD Maintenance Service	Provided in 9:00 to 18:00 schedule on weekdays.	30 MINUTES MAXIMUM*
PREFERENTIAL Maintenance Service	Provided in 9:00 to 18:00 schedule on weekdays.	15 MINUTES MAXIMUM*
HIGH AVAILABILITY Maintenance Service	Provided 24 hours a day, 7 days a week (every day of the year).	15 MINUTES MAXIMUM*

EDICOM standard support service level has in place a two-level helpdesk, whereas preferential service level has a specific operator assigned and, if necessary, two-level helpdesk is also available. However, if the assigned operator is busy, the Client could be attended by another technician with similar skills or just wait.

An owner is assigned to every incident who is responsible for the management of the incident throughout the incident life cycle, ensuring the timely follow-up, resolution and closure. This process is supported by a ticketing system that supports the incident and problem management process. This tool also provides an automated audit trail, which enables traceability of actions from ticket creation to closure and ensures the incident process flow is properly followed by enforcing formal sign-off.

Incident categorization and classification

Inputs received in the service desk must be categorized in one of the following categories:

- Anomalies which affect or may affect an isolated Client environment (e.g. confidential client data, or security incidents), which are treated according to incident management process (e.g. it is escalated to the corresponding department).
- Recurring anomalies which are not an isolated incident and can produce multiple incidents if root cause is not properly solved. These inputs are managed following the problem management process.
- Request for changes, which are managed following the change management process.

Once the input is categorized as an incident, it is classified based on agreed upon criteria depending on its criticality and nature:

- Category C1: Incidents which have a great impact on a Client or a group of Clients. These types of incidents severely affect the usual operations of a Client due to failures in the service.

- Category C2: Incidents which have a medium impact on a Client or a group of Clients. These types of incidents partially affect the usual operations of a Client or a non-critical flow of its operation due to a parameterization failure in the environment or in the service.

- Category C3: Incidents which have a low impact on a Client or a group of Clients. These types of incidents do not affect the usual operations of a Client and include, but are not limited to, doubts, requests, configuration changes, etc.

Incident investigation and diagnosis

Technical staff has access to the Edicom Cloud installations and to the Configuration Management Database (CMDB) repository where updated and detailed information about configuration items, which support the Edicom Cloud Service, is available.

The ticketing system application enables looking up a complete history of closed incidents and problems, known errors, workarounds and ongoing service requests in order to identify and apply previously acquired knowledge in the minimum possible time.

The Edicom Cloud SLA establishes that 99.5% of incidents closed in a month will be solved in the time depicted in the following table:

Category	Standard maintenance	Preferential maintenance	High availability maintenance
C1	<= 4 hours	<= 2 hours	<= 2 hours
C2	<= 6 hours	<= 4 hours	<= 4 hours
C3	<= 24 hours	<= 24 hours	<= 24 hours

Incident resolution time is defined as the time elapsed between the communication of the incident and its resolution, understanding resolution as EDICOM taking appropriate measures to solve the issue or providing guidelines to the Client to address the issue.

Incident closure

Resolved incidents are formally closed in the ticketing system and actions and procedures applied to solve the incident are documented. In the case of incidents reported by Clients, the Client is contacted to confirm the resolution of the incident for its closure. The incident is closed once EDICOM has notified the Client that the incident is already solved although it could be reopened on Client request.

Clients can re-open the incident ticket, provide additional comments, close again a re-opened ticket or complete the customer satisfaction survey through a public link.

Clients are also informed monthly of the support level indicators included in the Edicom Cloud SLA (maximum response time and resolution time). This report is distributed to Clients with their invoice or through the following link:

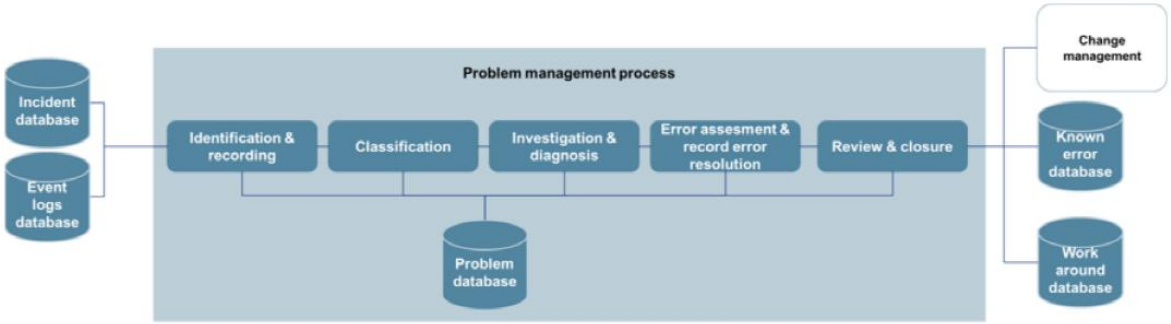
https://services.edicomgroup.com/edicomClient

The Helpdesk department, as part of the capacity management process, collects internal Client support indicators and shares this information with other EDICOM technical departments in technical managers' meetings (bi-monthly).

Additionally, EDICOM has created a separate communication channel to receive complaints. These complaints are logged, tracked and reviewed by EDICOM's Management.

Regarding problem management, the major activities in the problem management process are further described below:

Problem identification and recording



Depending on the source of identification of the problem, problem management can be classified as:

- Proactive: Problems are created as a result of incidents' trends identified when performing periodical reviews of closed incidents. These reviews are performed by the Helpdesk department manager.

- Reactive: Problems are created after analysis of an incident which affects the Edicom Cloud Service.

An owner is assigned to every problem. This individual is responsible for the management of the problem throughout its life cycle, ensuring its timely follow-up, resolution and closure. This process is supported by the same application used for the incident management process.

Problem classification

EDICOM has established the following classification of problems depending on its priority:

- Critical: Problem affects all Clients causing great impact in Edicom Cloud Service provision.

- High: Problem affects a Client exclusively, impacting Edicom Cloud Service provision; or problem affects several Clients, impacting a specific functionality of the Edicom Cloud Service without impacting Edicom Cloud Service provision.

- Medium: Problem affects a Client exclusively, impacting a specific functionality of the Edicom Cloud Service without impacting Edicom Cloud Service provision.

- Low: Problem does not affect Edicom Cloud Service provision.

The Technical Director is informed of critical and high priority problems and she/he is accountable for the allocation of adequate resources and proper coordination.

Problem investigation and diagnosis

Root cause analysis is the first step in problem resolution. Largely, problems are related to hardware and software failures, but they can also arise as a consequence of procedure errors, incorrect documentation or lack of human resources coordination.

Error assessment and resolution

Once root cause analysis has been performed, either the problem is resolved by means of a change or a workaround is implemented, and the problem is accepted and documented in the known error database.

Problem closure

Resolved problems are formally closed in the ticketing system, including a detailed description of the actions performed. The Helpdesk department is informed of solved problems since its resolution may affect ongoing incidents.

Client Responsibilities

The Client is responsible for communicating to EDICOM identified incidents, communicating to EDICOM the closure of incidents, and inspecting EDICOM's delivery of service to ensure compliance with contractual obligations.

3.4.1.5 Backups

Exchanged messages which have been acknowledged by the receiver are kept online in the system for at least 90 days according to the contract, although the Client has the possibility of contracting extra volumes and store messages online during an additional period of time.

This option is not a standard feature of the Edicom Cloud Service and, therefore, it is not included within the scope of the present report since service auditor's procedures do not extend to controls related to the development of specific Client requirements.

When messages are kept offline, they are included in the B2B cloud platform backup policies, which are described below:

- All data from Databases are copied in full daily.
- Daily copies are overwritten every five days (hosted at servers), weekly copies are overwritten monthly (stored on external device) and new monthly copies since April 2019 are stored on Ceph (overwritten annually) and kept during (15 + 2) years. The external devices are stored in a secure location.
- Databases are synchronized in primary and secondary data processing centres and configured in active/active.

Currently the backups are done in Ceph clusters dedicated to archive and history. These clusters are independent from the production environment and accumulate all the copies. Physically, the equipment is located in additional locations (different from the production environment) to provide to the recovery system with geographic independence. For each data there are at least two archive and historical copies, in different locations. Logical security of archive environments is specific to ensure retention and only objects are allowed to be written, not deleted or modified.

Additionally, EDICOM internal systems which support EDICOM's departments' day-to-day operation (e.g.: ticketing system, technical management application, etc.) have a daily full backup policy.

All new backups with data at rest, are encrypted with AES-512 algorithm (data encryption at rest).

The backup process in both environments (B2B and EDICOM internal systems) is partially automated, comprising:

- An automated part: Backups are performed in dedicated servers using system tools and specific backup software (such as Bacula used for internal EDC and scripts plus own DB manager for B2B network).

- A manual part: Backups stored in dedicated backup servers are mirrored (the same copy is replicated on two external devices) in encrypted hard disks and kept in two safes, which have an access control mechanism based on a key. System tools are used to perform mirroring and encryption, but this process is not totally automated and requires IT department operators intervention for the process of switching backup disks.

The correct execution of backups is monitored by the IT department on a daily basis verifying backup logs. Automated alarms in case of backup failures have been configured and integrated in the EBIMON monitoring tool, ensuring appropriate action is taken in case of backup failure.

Restoration tests to ensure recoverability of disk backups are performed after backup completion and, afterwards, twice a year, including also Ceph backups.

Access to the disk backup library stored in a safe is restricted to authorized personnel. As stated in the Edicom Cloud Service Level Agreement, annual backups are stored during at least 15 years. A secure disposal of all copies that are no longer within the retention period is performed annually following the provisions of the media disposal procedure.

Additionally, EDICOM has defined a secure media disposal procedure to destroy in a secure way backups devices which may contain data related to the Edicom Cloud Service and have exceeded the retention life period such as retired storage or retired servers. This procedure indicates information contained in the device must be erased in a safety mode using 2 tools, one for Windows devices and one for Linux devices. Once the information has been erased, the operator must store the report in an EDICOM's documentation path. The report is generated by the erasing tools, and it must contain:

- Erased device serial number.

- Process date.

- Method used to erase information.

- Responsible for the task

Finally, the wiped device must be destroyed or physically disabled, such as by drilling the device, according to the media management procedure following the instructions established for the secure disposal of technology equipment.

3.4.2 *Security*

3.4.2.1 Physical security

The EDICOM's headquarters are called EBC (EDICOM Business Centre). The complex consists of three buildings and two entrances.

The main entrance has a control access mechanism based on a turnstile with an access card, which controls people going in and out. Employees access the headquarters using their personal access card and providers and visitors must request a visitor access card to the reception personnel.

External visits must be explicitly granted by EDICOM employees and visitors must wear the lanyard provided by EDICOM with the visitor access card at all times during the visit. A log of assigned visitor access cards is maintained, and cards must be returned on leaving the building.

The parking entrance has a control access mechanism based on a barrier with an access card. The barrier also incorporates a camera, a bell and an intercom to allow entrance to providers and visitors.

Once the individual has been authorized, the gate of the indoor parking is automatically opened. An outdoor parking is also available inside EDICOM's premises.

Access to the headquarters from the indoor parking requires an access card tin order to be able to use the elevators and, alternatively, to access the headquarters from the outdoor parking is done through the main entrance.

Emergency doors and other doors which allow entrance to the headquarters remain locked while not in use. If doors remain open for a predefined period of time, a sound alarm is activated.

EDICOM has set up a video surveillance security system with internal and external cameras to control main entrance, parking and the outer perimeter of the building. In addition, there are video surveillance installed on the access corridors from the parking, as well as cameras in each access to the different departments' areas along the building have been installed. Furthermore, there is an alarm system which is connected 24x7 to an alarm receiving centre installed at each building. Additionally, a security guard patrols headquarters 365 days a year during nights.

Primary data centre

Access to the primary Data Centre (DC), located in EDICOM Business Centre (EBC), is protected by 4 physical control barriers from the main entrance, which

are controlled by an access control system. This system is based on smartcards and fingerprints accesses. The smartcards are used to access any area, regardless of whether they are restricted areas, and the access privileges are configured through the system. The access to the DC requires a second level of authorization and it is assigned to EDICOM employees on a need-to-have basis. Identification and authentication mechanisms are based on dual control fingerprints and card). All access permissions to the primary DC are periodically reviewed twice a year to validate if they are still valid.

External accesses to the DC (e.g.: maintenance providers, visits, etc.) must be escorted by EDICOM personnel. Access to the Data Centre is logged (authorized accesses and denied accesses), in the same way as the exits from the Data Centre.

Additionally, a video surveillance security system is in place inside data processing facilities.

Environmental control mechanisms to detect smoke, floods and high temperatures are in place. These devices have been configured to automatically trigger an alarm when measurements exceed a predefined threshold. The DC is cooled by redundant air conditioning machines, has a gaseous fire suppression system and has been built using raised floor and dropped ceiling.

For trust services systems there are additional security measures. They are located within the room of the DC inside a security metal cage.

In order to support continuity of operations in case of electric supply failures, EDICOM has set up Uninterruptible Power Supply (UPS) systems and a diesel generator set (up to 48 hours). These systems are periodically reviewed by specialized personnel.

Secondary data centre

EDICOM secondary data centre is located at a COLT facility. The service provided by COLT is a housing or collocation service, where all systems allocated on COLT facilities are managed and owned by EDICOM personnel.

Access to the secondary data centre is controlled by a security guard. In order to access the Data Centre, it is necessary to show an identification document to the security guard who checks if visitors have authorized access to the data centre.

For unauthorized persons, EDICOM must inform COLT prior to the visit. All access permissions to the secondary DC are periodically reviewed twice a year to validate if they are still valid.

External visitors to the data centre (e.g.: providers, auditors, visits, etc.) must be escorted by EDICOM personnel. Accesses through any of the doors of the data centre are logged (including failed accesses).

Additionally, a video surveillance security system is in place inside the data processing facilities.

Environmental control mechanisms to detect smoke, floods and high temperatures are in place. These devices have been configured to automatically trigger an alarm when measurements exceed a predefined threshold. COLT has software tools to automatically manage these alarms. All these systems are periodically reviewed by specialized personnel.

The data centre is cooled by redundant air conditioning machines, has an automatic fire suppression system and has been built using raised floor and dropped ceiling.

In order to support continuity of operations in case of electric supply failures, COLT facilities have set up redundant Uninterruptible Power Supply (UPS) systems and a diesel generator set.

Third data centre

EDICOM is currently in the process of expanding its data centre infrastructure from a two-data-centre setup to a new three-data-centre configuration, with the addition of the Walhalla Data Centre. During the audited period, significant service migration efforts have been undertaken to ensure the availability of provided services.

The Walhalla Data Centre, situated 80 kilometres away from the primary data centre, boasts a TIER IV certification for its infrastructure. Within this facility, EDICOM exclusively manages and owns all systems hosted at Walhalla.

To access this data centre, strict security protocols are enforced. Visitors must present identification to Walhalla personnel responsible for access control. Unauthorized individuals require prior notification to Walhalla by EDICOM.

External visitors, such as providers or auditors, are always accompanied by EDICOM personnel while inside the data centre. All entries into the data centre, including failed attempts, are meticulously logged.

Additionally, an extensive video surveillance system is in operation throughout the data processing facilities.

Environmental controls mechanisms to detect smoke, flood, and high temperature are in place. These devices are configured to trigger alarms

automatically if measurements exceed predefined thresholds. Walhalla has dedicated software tools to manage these alarms efficiently, and all systems undergo regular review by specialized personnel. The data centre is cooled by redundant air conditioning machines, has an automatic fire suppression system and has been built using raised floor and dropped ceiling.

In order to support continuity of operations in case of electric supply failures, Walhalla facilities have set up redundant Uninterruptible Power Supply (UPS) systems and a diesel generator.

3.4.2.2 Logical security - EDICOM

EDICOM has developed an Information Security Policy which states management commitment and sets out EDICOM's approach to managing information security. This policy has been communicated throughout the organization to users in a relevant, accessible and understandable way and is accepted by EDICOM's employees before they join the company.

All employees' sign their contract thereby accepting the EDICOM's Information Security Policy. Additionally, EDICOM hands over the Security Policy to employees on the first training day. In addition, each time an employee logs in through the domain, a banner warning is displayed to reaffirm again the express acceptance of the Security policies and guidelines.

User management

There is a formal user management procedure, integrated within the incident management process, whereby there is a predefined workflow to create, modify and delete user accounts and privileges for employees. EDICOM has also implemented procedures regarding termination to revoke physical and logical security access and to collect any IT assets provided by the company. These procedures are coordinated with the Human Resources department.

The principal aspects of the established identification and authentication policy are described below:

- Identification: User identifiers are unique, and accounts are assigned to individuals to ensure the traceability of the actions performed.

- Authentication: Password policy requires minimum length and complexity construction rules for the definition of passwords. Password duration is defined, and password reuse is prevented for a historical of passwords. Specifically, the following parameters apply:

    - Maximum password age: 180 days.

- Minimum length: 14 characters with complexity rules.
- Account lockout: After 3 incorrect logins.
- Password history: 25 last passwords remembered.

Application accounts used to launch services, which are not linked to a person, do not follow EDICOM's password policy, such as maximum password age, to avoid service's errors or interruptions. This is a standard and commonly accepted practice.

Vendor default passwords are replaced with passwords compliant with default policy and timeout mechanisms have been configured to avoid unauthorized access attempts. In particular, in EDC internal Domain, session is locked after 15 minutes of inactivity and requires a password to unlock. In the B2B Domain, the idle period for lockout session in Viewer is not configured. However, it is the Clients' responsibility to configure this parameter.

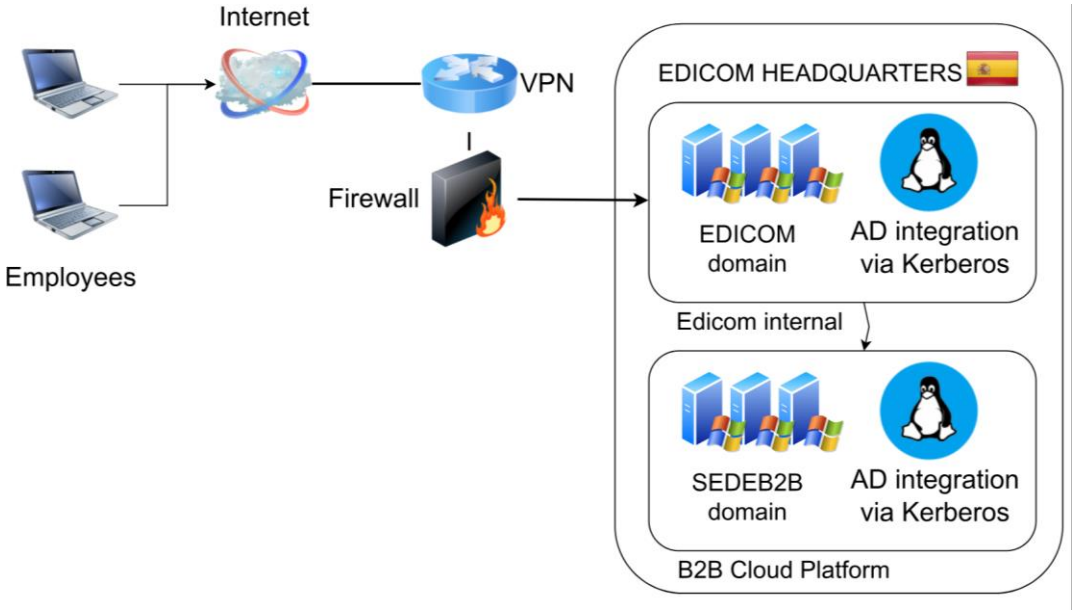
- Authorization: Privileges are assigned following the least-privilege principle, giving users account only those privileges, which are essentially vital to perform its intended functions and ensuring, where possible, segregation of duties.
- Traceability: Activities performed by EDICOM personnel in Edicom Cloud environment are logged.

EDICOM records audit logs to trace user's and Client's actions. These logs are stored online for 185 days. There are two types of audit logs:

- B2B Domain logs: allows EDICOM to identify user logins, access to documents, etc., including date and hour of the action, synchronized with a trustworthy time source Stratum 2 using NTP (Network Time Protocol).
- Ediwin: allows EDICOM to identify configuration changes of the service.

Access to audit logs is restricted to protect the integrity of the audit trail and logs are kept offline, at least, during fifteen years in encrypted backups.

This policy is deployed using Microsoft Active Directory. The structure of the different domain controllers installed at EDICOM headquarters and head offices is described in the following diagram:



Based on the diagram above the logical access architecture is as follows:

- Six domain controllers have been deployed in EDICOM headquarters located in Spain (between primary DPC and secondary DPC). EDICOM domain is used to control access to corporate systems (3 domain controllers) and B2B domain is dedicated to the B2B cloud platform (3 domain controllers).

  Linux systems used by R&D and IT areas are integrated into Active Directory domains through Kerberos.

- In EDICOM head offices from different countries, users connect directly to EDICOM domain located in headquarters (Spain). Access to corporate systems and B2B cloud platform is performed through EDICOM and B2B domains, respectively.

Employees located at EDICOM head offices connect to systems located at headquarters through a VPN connection (ZTNA). VPN password policy is delegated in EDICOM domain. Furthermore, EDICOM has instituted a two-factor authentication system, using the WorkspaceOne access management module, to secure access to corporate resources, applications, and the VPN.

Additionally, quarterly EDICOM performs reviews of a sample of users from both domains in order to detect inactive users or incorrect assignation of privileges. Specifically, each sample includes 25 users and 9 groups of users randomly selected for EDICOM AD and 25 users and 2 groups for SEDEB2B AD. Additionally, data centre accesses, visiting and maintenance cards and generic and service accounts are also included belong to three data centers.

In this way, nominal users are reviewed monthly, and generic and service accounts are reviewed biannually.

For these reviews, EDICOM has performed automated tasks to detect inactive users and to detect users which do not follow the password policy. Inactive users are those who have not log on for at least 90 days. These alarms are generated on EBIMON.

Isolation

Beyond security considerations from a user management perspective, EDICOM has also established mechanisms to isolate particular Client data of an Edicom Cloud installation from the rest of Edicom Cloud installations.

In particular, isolation is implemented via application logic and through a three-tier architecture model which consists of the user services layer, the business services layer and the data services layer. Each one of these layers is detailed below from the standpoint of isolation:

- User services layer: Web servers are shared between all Edicom Cloud Clients because they just provide user graphical interface and redirect requests to the business services layer.

- Business services layer: The Edicom Cloud Service of a Client is exclusively associated with a particular business pool. This way, a Client keeps isolated from the rest of business pools of the B2B cloud platform.

- Data services layer: The Edicom Cloud Service of a Client is associated with one database instance, of a particular pool, which is shared with other Clients. This way, a Client keeps isolated from the rest of database instances of the same data pool and also from the rest of data pools of the B2B cloud platform.

<u>Client Responsibilities</u>

The Client is responsible for:

- Defining an adequate level of privileges for the users created by himself (B2B environment) or requested to EDICOM.

- Administering its own users according to the user management procedure defined in the client organization or, alternatively, communicating EDICOM in a timely way the need of modification of privileges or user's deletion.

- Creating nominative user accounts and supervising user accounts are not shared.

- Defining password requirements in accordance with its information policy or, alternatively, communicating password requirements to EDICOM.

- Granting privileges which allow modification of system security parameters.

- Configuring timeout mechanisms on its own information systems.

3.4.2.3 Logical security – Edicom Cloud Service clients

New Client credentials and identification and authentication policy

Client credentials can be created in the following situations:

- By EDICOM, during the Edicom Cloud installation process: Depending on Client requirements, user accounts linked to a particular domain can vary from a single user with administrator privileges to multiple users with a complex set of roles.

- By EDICOM, per request of the Client after the Edicom Cloud installation process: The Client can request user accounts creation, modification or deletion contacting helpdesk.

- By the Client: Self-created accounts using previously provided users with administration privileges.

Ediwin Viewer supports the definition of the following parameters of the identification and authentication policy:

- Identification: Username identifier and full description.

- Authentication: Password minimum length, password complexity, expiration time, password historical, password change on first login, account lock after failed login attempts, etc.

- Authorization: Types of messages visible by the user (e.g.: orders, invoices, dispatch notes, etc.), actions which can be performed by the users (view/edit/delete messages, print messages, view interlocutors, etc.), user administration privileges, etc.

- Traceability: All user actions are logged and stored inside the service.

This policy is deployed via the application itself. As previously outlined, Ediwin Viewer user security policy is delegated to the Client. Hence, the Client is responsible for defining:

- Nominative user identifiers and communicating users the need of avoiding credentials sharing in order to ensure traceability of actions performed.

- Password authentication policy applied to Client's users in line with client information security policy.

- Authorization level of users, ensuring segregation of duties and least-privilege principle, where possible.

Additionally, EDICOM has implemented for B2B users a multifactor authentication using a One Time Password (OTP) factor. It is developed to be used with market OTP applications, such as Google Authenticator. User can create an entry in the OTP application using a QR code. The OTP factor is compulsory for all eIDAS (electronic IDentification, Authentication and trust Services) services in EDICOM, and Clients could not be able to disable the factor. For the rest of EDICOM services, the Client could (optional) configurate the OTP factor forcing to all Client users to use it, or enable the OTP option, and the Client user will decide, according to the criticality of the information, if it is necessary to use the OTP factor.

In case of the Client miss the OTP factor, the Client is able to recover the factor via email, which is associated to the user.

There is also another authentication mechanism used for Clients (SAML 2.0). SAML 2.0 is a protocol configured individually for each Client. EDICOM has defined several documents that describe the configuration of SAML 2.0 authentication for both the EDICOM and the client’s side. The allowed cryptographic algorithms are RSA 2048 and SHA256.

To activate SAML authentication on Ediwin, two certificates (tokens) are necessary. One of the tokens is generated and delivered by EDICOM to guarantee security in the information exchange channel. This token is signed and encrypted. Once the first token is created, the client performs the reverse operation and generates the second token (encryption is optional). When user tries to login, EDICOM’s system checks the signature and confirms it is a trustworthy user. In addition, it is possible to configure PGP keys for user´s authorization.

EDICOM has deployed two models to configure the protocol, the IDP (Identity Provider) and the SP (Server Provider). In IDP, the Client from its Identity Server will generate the token and call the Ediwin’s endpoint. In SP, Ediwin is

the server provider redirecting the login request to the IDP. These models allow to maintain the access credentials totally guarded and managed by Client.

Verification process of access accounts requests

Access to Edicom Cloud Service through service web portals is controlled by username and password. A formal user management procedure details the required workflow to create, modify and delete user accounts for EDICOM Clients.

The procedure also defines the required actions when Clients request to create a new user account, or a password reset of their accounts in order to verify the identity of the Client and prevent unauthorized access attempts.

There are checks to confirm that the requesting user is registered as a contact for this Client, and he is requested to send an email with his company details. Finally, an email is sent to the Client contact with the account information.

This process was enhanced so that currently there is an authorized contact person ("User Master") for each Client who is responsible for authorising. The requests of other users in her/his company. Moreover, Ediwin Viewer has the capability to force a password change on users in case it is necessary for security reasons.

In case of Client request for support from Helpdesk, the User Call Center (UCC) will use the available resources to guide the Client to solve the incident. Otherwise, Helpdesk will try to solve it or escalate it to the corresponding department. Furthermore, the confidential data (such as passwords) can only be sent through the Client associated email in EDICOM's Database. If a client needs to change the contact email, UCC will only configurate the new email account after performing the corresponding checks and verifications.

Software modules installed at the Client's servers

EBI adaptor is a module of the Edicom Cloud Service which is usually installed at a server located in the Client's data processing centre. This server is administered by the client and, consequently, the Client is fully responsible for implementing the appropriate access control mechanisms in order to ensure the integrity of the information sent to the Edicom Cloud platform.

New Client in Edicom Cloud Service

The Consulting department requests the 24x7 department the creation of the logic domain for the new Client, which adds the new Client to the group of Clients. Afterwards, an Administration account is created, and it is managed by

the Client itself once the Consulting department finishes the Client creation tasks.

This Administration account enables the Client to create more users as required.

Client cancellation

The Administration department receives cancellation requests from Edicom Cloud Service Clients (volunteer cancellation) or due to Client non-payment. Depending on the service, cancellation can be performed automatically by the Administration department or requires the intervention of 24x7 department.

Once a cancellation request is processed, the Client is in a freeze state (temporary state) during a period of time and finally the Edicom Cloud Service of the client is deleted.

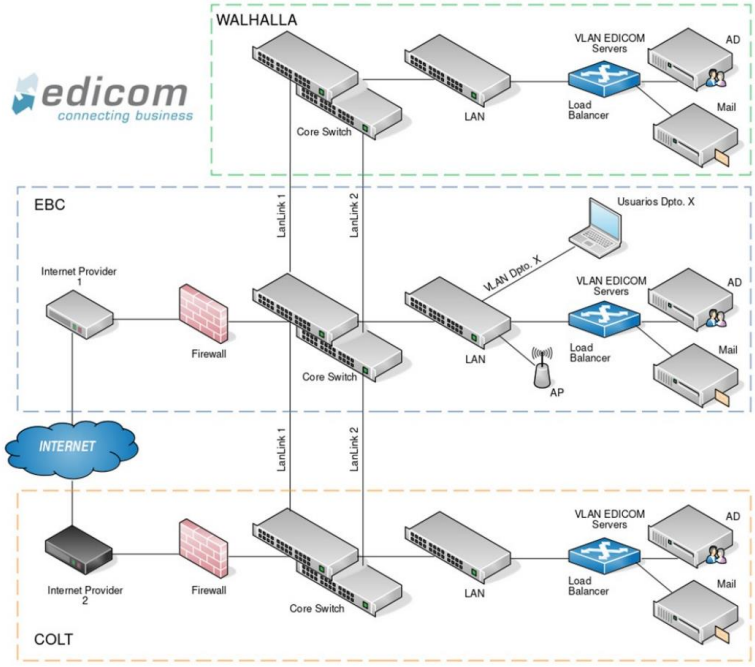
Client Responsibilities

The Client is responsible for providing information to confirm the identity of individuals which perform account management requests.

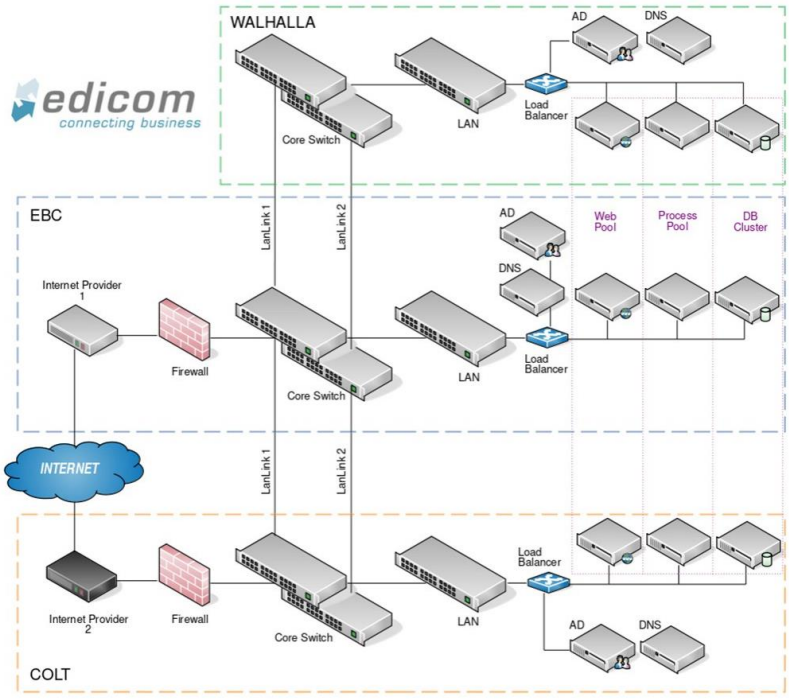
3.4.2.4 Network security

The following logical diagrams illustrate the design of EDICOM's networks:

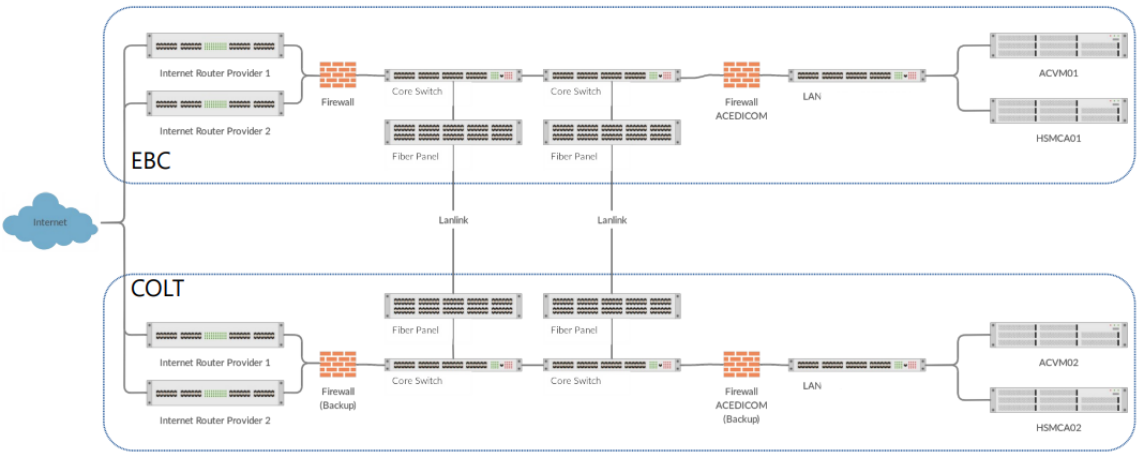
- **Internal corporative EDICOM's network**:

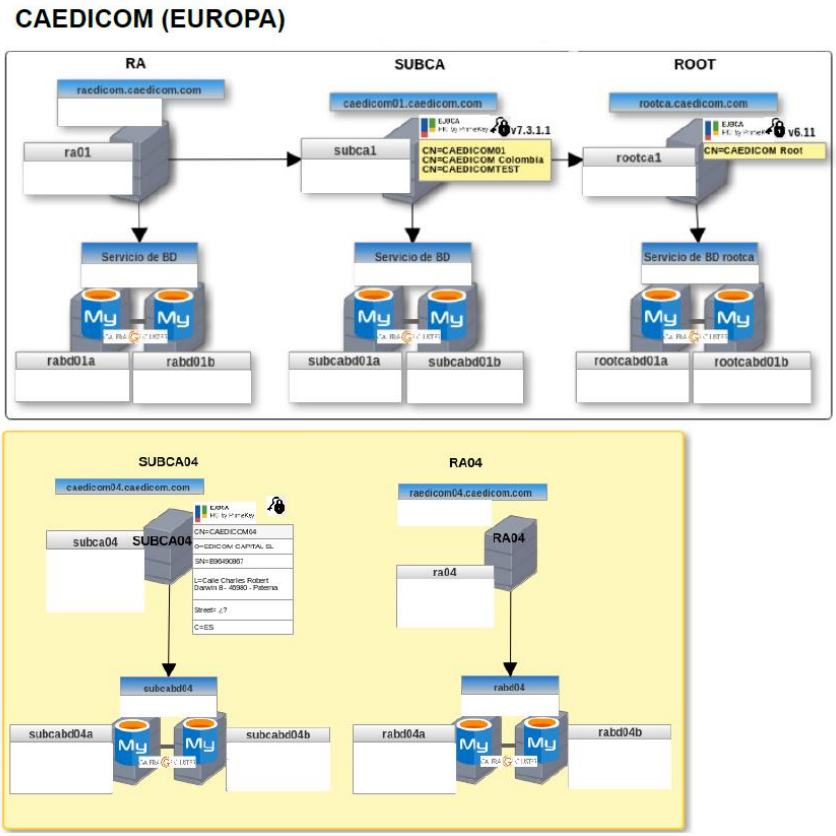


- **Edicom Cloud Service Network**:

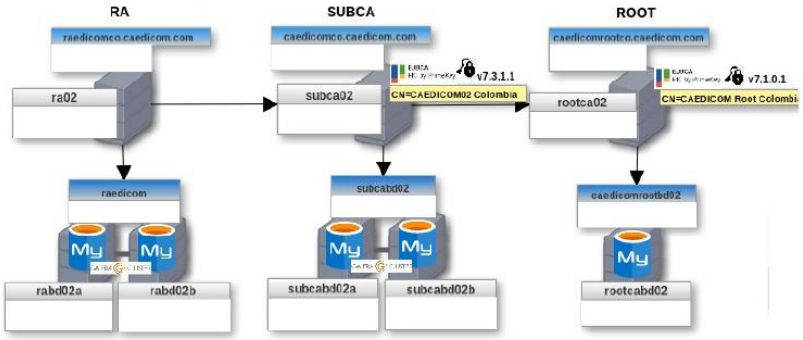


- **Trust Services Network**:

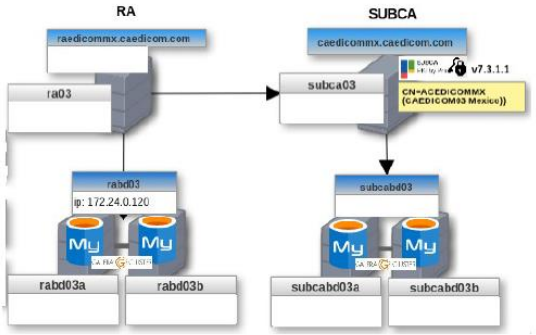




CAEDICOM (COLOMBIA)



CAEDICOM (MÉXICO)



EDICOM follows traffic isolation principles in the design of its network architecture to improve security and performance. Particularly, the following design considerations have been considered:

- Defining subnetworks depending on security requirements and type of services:
    - EDICOM internal: the network where employees' computers and corporative servers (technical management application, file servers, etc.) are connected.
    - B2B cloud platform: the network where Edicom Cloud users, business and data services layer servers are located.
    - EDICOM Certification Authority: the network where servers and HSM (Hardware Security Module) of the EDICOM trust services are connected. The CA network is a sub-LAN within the B2B LAN which has its own Firewall.

- Restricting services exposed to the Internet to the strictly necessary. Specifically, only the following services are authorized:

    - User services layer of the Edicom Cloud Service, web portals which provide online access to Clients to their Edicom Cloud environment. Clients can access thought web portal using their own domain, a user and a password.

    - Integration webservice. EDICOM deploys a software on the Client facilities (it can be remotely installed). This software is completely transparent to the Client.

    - Terminal Server services to access the Edicom Cloud Services which do not have a web portal (e.g., CRP Flow).

- Some Clients require VPN access to the B2B cloud service as required by their own policies. For that reason, EDICOM has two dedicated routers (in high availability mode) for VPN connections and has configured some policies to meet Clients' requirements as long as the device allows the configuration. In case the device does not allow the Client configuration, EDICOM and the Client will have to agree on the connection requirements.

  For the setup of encrypted channels EDICOM uses the IPsec protocol. The traffic goes through a Firewall which allows or rejects the connection.

- All the data in transit is encrypted using the TLS 1.2 (HTTPS) with the cryptographic hash function SHA-256.
- EDICOM has implemented a Zero Trust Network Access (ZTNA) solution to manage access for network resources and services based on EDICOM defined access control policies.

Availability

From the standpoint of availability, the most remarkable aspects are:

- Redundant internet connections with different Internet service providers.

- B2B cloud platform firewalls and load balancers deployed in high-availability mode.

- Three Data Centres (DCs) are interconnected with redundant optical fibre links which follow different physical routes. Moreover, both DCs have a double separated optic fibre channel.

- The DCs are separated by a sufficiently safe distance so that if one DC is affected by a disaster, one of the others can remain unaffected.

- Previous EDICOM's facilities could be used by employees in case of disaster at EBC (EDICOM Business Centre). This backup building has a direct connection with secondary DC and only is activated in case of disaster.

Monitoring

EDICOM's network monitoring activities are executed by the IT area and include, but are not limited to:

- Analysis of network events, using:
    - Network devices' manufacturer applications (e.g.: Cacti, PRTG, etc.).
    - Appliances (e.g.: Stormshield)
    - Databases: (e.g.: C28D)
    - Custom-developed tools (e.g.: EBIMON/CHECKMON).
- Review of a sample of firewall rules, twice a year. Specifically, the sample includes 5 rules of a firewall (firewall and rules randomly selected).
- Vulnerability scan of the perimeter network of the B2B Cloud Platform, annually.
- Security Persistent Monitoring service. Edicom has a service provided by an external SOC (Security Operation Center) for the monitoring of the logs of certain systems. The SOC performs logs reviews using OSSEC (Open Source HIDS SECurity) agents installed in some servers, which capture any relevant events on the server: access logs (both internal network and external network), server capability, and file integrity among others. These logs are then sent to an independent system that is not managed by Edicom system administrators and analysed by a log correlator such as ELK stack, Graylog or Splunk.
- The SOC performs daily reviews and a complete monthly review, immediately alerting Edicom's systems staff in the event that any suspicious activity is detected during the daily review. An analysis of the information collected is performed and a report is generated monthly and delivered to EDICOM including results of: servers monitored, file integrity, relevant events detected.

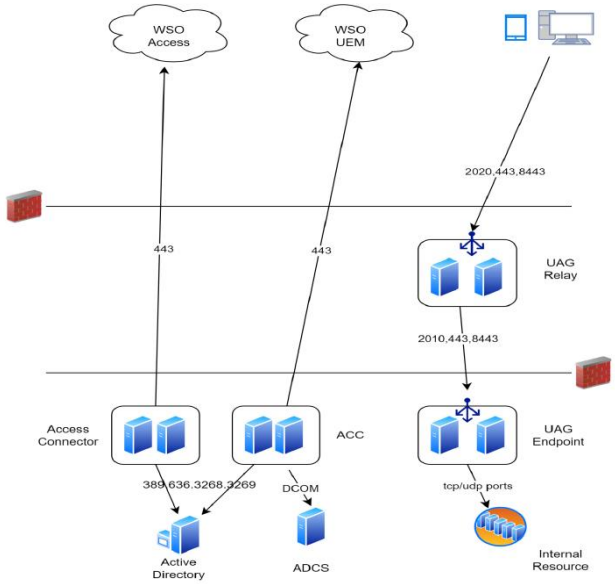
Moreover, EDICOM uses an appliance Stromshield with IDS/IPS, anti-DDoS and WAF (web application firewall).

Software modules installed at Client's servers

As mentioned above, the EBI adaptor is a module of the Edicom Cloud Service which is usually installed at a server located in the Client's Data Centre. This server is administered by the client and, consequently, the Client is responsible for configuring network security infrastructure in order to ensure the integrity of information sent to the B2B cloud platform.

Mobile Device Management

This software allows IT administrators to control, secure and enforce policies on smartphones, tablets and other endpoints from users.



3.4.2.5 Extended Detection and Response

Personal computers and Windows servers which support the technological infrastructure of the Edicom Cloud Service (data services layer) and the internal EDC network have the XDR CORTEX solution installed. Virus definitions are updated daily, for both, personal computers and EDICOM servers.

XDR CORTEX solution include the following features:

- Automatic real-time prevention of malware, ransomware, exploits and fileless attacks.
- Protection of vulnerability profiling techniques used in exploit kits.
- Blocking known network attacks through the deep network inspection engine.
- Prevention of known threats with intelligence obtained in remote sandbox.
- Prevention of unknown threats with local analysis based on artificial intelligence.
- Advanced unknown threat prevention with sandbox-based scanning.
- Prevention of script-based malicious processes.
- Threat protection based on advanced threat behavior.
- Management and comprehensive forensic analysis of security incidents.
- Management of known vulnerabilities in endpoints.
- Information leak alert functionality.
- Analysis of removable devices.

There are automated tasks to check if every personal computer and server has the XDR CORTEX updated. In case it is detected that there are personal computers or servers not updated, an alert is automatically created at the EBIMON tool.

For the R&D and IT departments, personal computers with Linux Operating Systems have SELinux/AppArmor and also XDR CORTEX. Linux Servers (for both Edicom Cloud and EDICOM internal network) have SELinux.

The Antivirus real-time scan is also enabled on EDICOM servers for both Edicom Cloud and EDICOM internal network.

Additionally, the Antivirus scan is enabled on the EDICOM internal network firewall to analyse traffic of HTTP, HTTPS, IMAP and POP3 protocols, FTP, etc. File scan protection is always enabled in real.

Moreover, EDICOM uses an appliance Stormshield with perimeter antivirus, malicious web access log and webpages blacklist and WAF (web application firewall).

Client Responsibilities

The Client is responsible for installing antivirus software on its own information systems.

Secure Mail

Secure Mail is a 24x7 managed email protection service. It has one of the highest levels of prevention, detection and response to threats. It has a web portal that allows management and monitoring in real time.

Objectives of the service are the following:

- Protect against threats and control the load on email servers.
- Reduce the risk of attacks and infections from targeted spam campaigns.
- Reduce the risk of email loss and blacklisting.
- Guarantee business continuity through a redundant and always available architecture.

Main functionalities are the following:

- CVE's tracking.
- Zero Day threat detection.
- Anti-spoofing and anti-phishing.
- Malware and ransomware filtering.
- Domain protection.
- CEO Scam Protection.
- Inspection of URL's and encrypted attachments.
- Tools for forensic analysis.
- Electronic Mail SPF (*Sender Policy Framework*) Protection

3.4.2.6 System Hardering

EDICOM has defined formal procedures and guidelines to normalize the configuration parameters and take cybersecurity into account when configuring systems. The EDICOM cybersecurity department has prepared different types of guidelines depending on the nature of the systems and its operating systems.

These guidelines are based on the CCN-STIC guidelines, published by the CCN-CERT, EDICOM has adapted the CCN-STIC guidelines to the EDICOM system requirements, guidelines are periodically updated and completed with new ones, depending on the new configuration items, threats, and vulnerabilities detected.

EDICOM guidelines are published on the intranet and are used by the system department at the time of deployment of new machines. Additionally, automated tasks are periodically executed to review the configuration of the systems, and check that the configuration applied, matches the configuration parameters defined on EDICOM guidelines.

3.4.2.7 Security patches

EDICOM has defined formal procedures to plan the implementation of security patches released by software providers. The Security patching policy is described below, depending on the type of device:

- Servers:
    - Windows platform –B2B Network Windows Server–: Security patches are installed when performing maintenance tasks or new database server installations. Also, when a server has a hardware incident, IT operators update the Windows platform once they solve the incident. EDICOM has established an update policy for its Windows servers on a monthly basis.
    - Linux platform (user, business and MySQL data services layers): Security patches of software packages (e.g.: Apache Tomcat, Apache httpd, OpenSSL) are planned to be updated as a result of perimeter network assessments (at least, annual Pentests).

      In addition, the IT department also installs security patches when a vulnerability is detected internally. A script is used that checks the updates available for Linux and if there are any updates related to vulnerabilities (CVE) it informs the mailing list of the IT department. In any case, it is checked monthly if there are updates available.

      Security updates are deployed in Linux test and preproduction environments in order to be tested on the B2B Cloud Platform software. There is therefore proactive testing before the installation of security patches on the production environment.
    - Additionally, EDICOM customizes Ubuntu and CentOS Linux distributions tailored to its needs. These distributions include the latest versions of kernel and software packages and are set up when performing maintenance tasks or installations of new servers.

      IT operators only deploy the software packages which are strictly necessary from each distribution.

- Personal computers:

    - Windows platform (Personal Computers and EDC internal Windows Servers): Microsoft platform security patches are reviewed monthly using Windows Server Update Services (WSUS) and once approved by the IT department manager, security patches are usually installed within one week. In most cases, whenever possible, deployment is performed gradually using test user groups.

      Additionally, the IT manager receives monthly alerts for updates of the Microsoft platform. These alerts are programmed to match the Microsoft update release versions.

    - Linux platform: Security updates are installed by Linux users manually. Weekly, the IT department reviews the users' computers to verify that they have an updated version of the operating system.

These software update tasks are logged in the IT department management tool.

Client Responsibilities

The Client is responsible for applying security patches on its own information system.

3.4.2.8 Cryptographic Controls Policy

EDICOM has defined a cryptographic controls policy with the purpose of establishing the minimum requirements when it comes to security in the use of cryptographic controls for the encryption of information. The procedure is reviewed periodically, and the algorithms and cryptographic suites are limited, allowing only those reviewed and that guarantee security according to EDICOM standards.

Hash Functions Algorithms: SHA224 – SHA256 – SHA384 – SHA512

Singing and Asymmetric Encryption Algorithms: RSA and ECDSA

Symmetric Encryption Algorithms: AES (256 bits)

Cryptography used in information exchange:

- Cipher Suites TLS 1.2 y 1.3
- Password exchange, secure account activation procedures (Diffie-Hellman, DHE and ECDHE)

- HMAC algorithm HMAC-SHA2
- Disk encryption personal computer: Bitlocker/LUKS WIN/LINUX AES 256
- Disk encryption servers: LUKS AES 256/512 bits
- Zip Exchange AES-256 ZIP/7Z
- Backup AES 512 bits since 2019, previously AES 256 was used

EDICOM has also defined controls and allowed mechanisms for cryptographic devices used by Edicom for the storing keys and certificates securely, PIN types, level required FIPS certification and authorized uses.

EDICOM has identified different scenarios in where key lifecycle management is necessary, for each scenario the next stages have been defined: key generation, transport to the point of exploitation, custody during exploitation, archived after its withdrawal from active exploitation and destruction stage.

3.4.2.9 Vulnerabilites Management

In order to identify security weaknesses, annual internal and external penetration tests are performed on Edicom's infrastructure, services and web applications. These activities are performed by independent auditors. Customers are also allowed to perform intrusion tests on the services they have contracted.

The goal of the performed security tests is to discover and document the potential vulnerabilities that could adversely affect the analysed assets. The analysis includes the following set of tests:

- Automatic tests
- Advanced manual techniques
- Manual tests

The analysis follows the guidelines of best practices, methodologies and standars (CVSS, OWASP, NIST and OSSTMM)

The vulnerabilities detected in the different tests carried out are collected in a report indicating the impact of the materialisation of the vulnerabilities detected, the details necessary to reproduce them and the recommendations to be followed to mitigate or correct them. For each of the vulnerabilities detected that require treatment, a task is registered in the Edicom internal applications where all the details of the vulnerability detected (risk, systems affected, description, recommendations, etc.) are included.

Once all vulnerabilities have been registered, it is necessary to analyse them in order to prioritise the vulnerabilities according to the level of criticality:

-Critical: The exploitation of the vulnerability may lead to an immediate problem of extreme severity in the service and requires urgent treatment.

- High: The exploitation of the vulnerability may result in a serious problem with the service.

- Medium: The exploitation of the vulnerability may result in a partial impact of the service.

- Low: The exploitation of the vulnerability may result in a minimal impact on the service.

Once the vulnerability tasks have been prioritised, the Scrum Masters will reserve the necessary resources in their planning for their treatment. One of three strategies are adopted:

- Fix: Fix or patch the vulnerability completely so that it cannot be exploited.

- Mitigation: When remediation cannot be achieved or there is not yet a published patch for it, compensating controls or workarounds will be implemented that reduce the probability of the vulnerability being exploited.

- Acceptance / Dismissal: When the vulnerability is considered to have a very low impact on the services and/or the cost of remediation is higher than the service impact of the vulnerability, it is possible to decide not to take measures to correct the vulnerability.

The prioritisation of tasks will be marked by their urgency or importance for the business. The indicative resolution times based on the criticality assigned to each task would be as follows:

- Critical: They will be resolved in a maximum of 48 hours.

- High: To be resolved in the next sprint (between 14 and 28 days).

- Medium: To be resolved in the following sprints (between 1 and 3 months).

- Low: They will be resolved in approximately 6 months.

Moreover, within the scope of the audited period, specific resolution timelines for zero-day vulnerabilities have been established as part of the vulnerability management procedures. Any zero-day vulnerabilities impacting the EDICOM infrastructure are promptly addressed, with resolutions typically achieved within a maximum of 24 hours. For zero-day vulnerabilities associated with software, initial changes or corrections are initiated within the first 24 hours and subsequently implemented within the following 24 hours.

Although these resolution times are indicative, it may be the case that they cannot be met because the vulnerability is considered to have a low impact on

the services and/or the cost of its correction in terms of time and/or resources is higher than the impact of its exploitation.

3.4.2.10 Asset Management

Several types of asset inventories are maintained. All of them are permanently updated and assigned an owner responsible for protecting the confidentiality, integrity, and availability of the information:

1) User or corporate workstation assets:

These assets are managed by the System Department through the Inventory application of the Systems Task Management tool (JSys). The owner of each of them is designated individually.

Biannual inventory reviews are performed as established in the Inventory Review Procedure. In these reviews, a sample of 25 user computers is randomly selected to verify whether the computers:

- Are correctly assigned and labelled

- Have properly installed and updated the antivirus

- Apply the Security patching policy

- Have the disk encryption activated.

Additionally, a review of the software installed on the computer is done to check whether it complies with the Edicom Software Policy.

The rules for acceptable use of Edicom assets are established in the internal Security Regulations and in the Edicom code of conduct and ethics and are formally accepted by each employee.

2) Assets that are needed for the provision of services (Configuration Management Data Base)

These assets are managed by the System Department through the CMDB application of the Systems Task Management tool (JSys). The System Manager has been formally designated as the owner of the CMDB assets in the following categories:

- Services

- Contracts

- Software
- Suppliers
- Support and maintenance contracts
- Infrastructure elements
- Mobile devices
- Physical servers
- Virtual servers
- Communication lines
- Communications equipment

Biannual audits of the assets of the CMDB are performed to detect inconsistency in the information contained following the Configuration Management Procedure.

3.4.2.11 Information Classification

All information existing in the Organization, whether it has been generated internally or externally, it must be classified in accordance with the internal information classification procedures in these three categories:

- **Public Information**, available to the public within its internal means of communication, or that has been published through other official channels.
- **Restricted Information (classified by default)**, information concerning clients through cloud services, parameterization information for each client, and by default any type of information that is not categorized as public or confidential. It cannot be removed from the company without express permission.
- **Confidential Information**, information on the configuration of the systems that provide service to clients and that is expressly qualified by the organization. By default, the following internal information will be confidential, accounting information, payroll information, and personal data of both internal and external personnel.

The Security Manager will establish the measures for the safe treatment of the information, for each of the categories in which it has been classified. EDICOM has specific protection controls for the information treatment depending on its previous classification and the type of channel by which it will be transmitted.

Labelling of paper information

- **Public Information**: Will be labeled as much as possible, explicitly as "Public".
- **Restricted Information**: In general, such information will not be labeled as it will be used internally by the company.
- **Confidential Information**: Include, as far as possible, a Confidential mark and, if applicable, a legend with the restrictions on the use of the information. It will be valid to keep confidential papers in a folder dedicated to this purpose or to keep them in a drawer or cupboard for this purpose (especially in the case of documents generated prior to the implementation of the ISO/IEC 27001 standard).

Labeling of electronic information

- **Public Information**: No Labeling Required.
- **Restricted Information**: No need to tag.
- **Confidential Information**: As far as possible, the level of confidentiality will be indicated in the metadata, in the file itself or its container (mail, compressed file, etc.), provided that it is not explicitly stated in this document. Documentation templates for confidential documents will be used.

Postal Mail Service

- **Public Information**: No special controls.
- **Restricted Information**: Without special controls, you may optionally opt for registered mail.
- **Confidential information:** Sealed container or envelope, sealed with "confidential" labels, inside envelope without indications. Registered mail with acknowledgement of receipt and return in the absence of the final part or courier with equivalent security benefits will be chosen.

Fax service

- **Public Information**: No special controls.
- **Restricted Information**: Avoid the use of fax as much as possible and transmit by e-mail. The receiver of the fax must be next to the Fax Terminal until the sending is complete. The recipient must immediately confirm receipt of the fax.

- **Confidential Information**: The use of fax to send confidential information is prohibited (except for customer configuration information sent to the customer in this case following the instructions for restricted information).

E-mail Service

- **Public Information**: No special controls.
- **Restricted Information**: Use encrypted channels.
- **Confidential Information**: Information must be encrypted. Use Encrypted Channels. You must reasonably ensure that the origin of the message and the destination of the message is from whom and where it is expected to go.

Internet, FTP, or other electronic information transfer service

- **Public Information**: No special controls.
- **Restricted Information**: No special controls.
- **Confidential Information**: Information must be encrypted. Use Encrypted Links. You must reasonably ensure that the origin of the message and the destination of the message is from whom and where it is expected to go.

Storage of information

- **Public Information**: No special controls.
- **Restricted Information**: Without special controls, it is expressly forbidden to remove information from the premises without express permission.
- **Confidential Information**: Information on physical media must be permanently guarded and stored in a secure place. Electronic information must be kept encrypted.

Destruction of information

- **Public Information**: No special controls.
- **Restricted Information**: Paper-based information must be shredded. Information on electronic media must be securely erased (degaussing or low-level formatting) or destroyed on the medium.
- **Confidential information**: Paper-based information must be shredded. Information on electronic media must be securely erased (degaussing or low-level formatting) or destroyed.

Off-site outlet of supports

- **Public Information**: No special controls.

- **Restricted Information**: Password to access the secure device or container. Trusted carriers.
- **Confidential Information**: Encrypting Information. Trusted Carriers. Acknowledgment of receipt upon receipt.

Access logging

- **Public Information**: No special controls.
- **Restricted Information**: No special controls.
- **Confidential Information**: Record of users' access to this information.

3.4.2.12 Security Incidents

EDICOM has implemented a security incident management process to manage security incidents that may affect the operational services delivered to its Clients.

Where the incident management process is aimed at the restoration of interrupted or reduced services within predefined timeframes, the problem management process focuses on finding root causes for one or more incidents in order to prevent the recurrence of similar incidents in the future.

Incident logging

Any Edicom employee is required to report any incident, suspicion, weakness, threat or anomaly that may affect information security. The logging is made through the systems site.

Edicom has monitoring tools for all its systems, which are managed by the Systems area and by the 24x7 support area. The nature of the types of alerts each area receives is different although some of them are common to both departments.

Incident categorization and classification

When a task is classified as a security event, the Security Incident Management Officer and the personnel designated by him receive an automatic alert to coordinate the response to the potential security incident.

In addition, once the security event has been notified, an assessment is carried out by taking into account the impact of the incident on confidentiality, availability or integrity of information.

- Confidentiality Incident: Occurs when unauthorized parties, or do not have a legitimate purpose to access, gain access to the information.

- Integrity Incident: Occurs when the original information is altered and data substitution can be harmful to the individual.
- Availability Incident: Its consequence is that the original data cannot be accessed when needed.
- Traceability Incident: Occurs when it cannot be guaranteed that the actions of an entity can be traced only back to that entity.
- Authenticity Incident: Occurs when the authenticity cannot be guaranteed. legitimacy of the origin of the transmission of information.

Event categories have been created to classify security incidents. For proper management, all security incidents must be classified. The classification of security incidents is done in the Systems Task Management (JSys). Once the input is categorized as a security incident, it is classified based on agreed upon criteria depending on its criticality and nature:

- **Low**: The service is not affected in any way. Some CI of the CMDB have some problems, but by the design of the solution the service remains operational (HA).
- **Medium**: The service is partially affected, there may be a performance issue or partially functionality fail.
- **High**: There is a serious problem with the service or even though it is a partial problem, affects all customers.

Incident investigation and diagnosis

The Security Incident Management Manager or the personnel in charge will set a priority for each of the security incidents or security breaches recorded in the Systems Task Management (JSys) application and will reserve the necessary resources in their planning for their treatment.

The necessary phases for the treatment of security incidents and security breaches are Containment, Solution, Recovery, Collection and Custody of Evidence, Communication, Resolution Report.

Incident closure

In general, the entire incident response process should be properly documented, including the findings of technicians and team leaders.

If necessary, security breaches shall be reported to interested parties, depending on the regulations to which it is subject to. For example, if the security breach has to do with personal data, it will be reported through the Spanish Data Protection Agency (AEPD).

Review of incidents and security breaches

The Security Incident Management Officer and the Data Protection Officer will review at least annually any incidents and security breaches that have occurred with the aim of introducing improvements based on lessons learned from them.

3.4.3 *Change and release management*

The objective of the change and release management process is to ensure that changes are formally managed and properly migrated to production in order to minimize the number of change-related incidents and their impact on the service quality.

This process consists of two main subprocesses:

- The change management subprocess, covering the analysis, development and testing of the changes.
- The release management subprocess, covering the migration of the change from the development and test environments to the production environment.

The major steps in the change and release management process are depicted and further described below:

3.4.3.1 Edicom Cloud service installation

An Edicom Cloud Service new installation is performed by the Consulting and the 24x7 departments, once the Sales department has agreed and signed a professional services proposal with the Client.

Consulting projects require a high degree of interaction between EDICOM and its Clients. Due to this factor, active cooperation of the Client is required during the different stages of the Edicom Cloud environment set up and specially in testing activities.

Analysis

The Edicom Cloud environment set up requires identifying functional requirements with the Client. First of all, high-level requirements are identified by the Sales department. Once the Sales department has identified high-level requirements, the Consulting department, who carries out the installation tasks, contacts the Client to confirm the high-level requirements and project's scope.

From now on, all parties must be in agreement on the high-level requirements. If the Client does not agree with the requirements, the Consulting and Sales departments contact the Client in order to agree the high-level requirements between all parties involved.

The Consulting department uses an EDICOM in-house developed application, JCons, to manage the Edicom Cloud installation task during its life cycle. The following information is registered:

- Client's contact information.
- Project manager and consultant responsible for the task. Every task done is registered in the application including the consultant who did it.
- Consulting services and B2B cloud platform products/services which have been sold.
- Messages which have to be integrated in the B2B cloud platform.
- Functional requirements, which may vary depending on:
    - Systems of the Client (e.g.: standard ERP, custom-developed application, etc.).
    - Type of messages exchanged (e.g.: invoices, orders, delivery notes, etc.).
    - Type of adaptor (e.g.: EDICOM adaptor, developed by the Client, use of exchange systems, etc.)
    - Interlocutor (e.g.: located in EDICOM B2B cloud platform, in other VANs, etc.)
- Every single task has attached several documents and emails related to the Client's and consultants' communications. The consultants register every single process performed or communication with Client (email, phone call…) done.

- EDICOM sends an email which contains an attached file, the project charter, including a clause in the email where Client is in agreement with the project requirements if they do not answer the email within the next 3 working days.

Moreover, EDICOM has developed controls to monitor the tasks performance during the project lifecycle. If a stage or task is not fulfilled, JCons does not allow the project manager to close the task. Another control to monitor the projects checks whether there are still consultants assigned on the pool project preventing the project manager from closing the task if it is the case.

When the project is about to end, EDICOM has included a Client Satisfaction Survey, which is optional. The access to the survey is public and free so that the Client project contact can send the link to the Client's staff who have participated on the service installation to complete the survey.

Development

The Edicom Cloud installation is carried out following EDICOM project management methodology (Efficient Team Methodology; ETM), based on Scrum agile methodology, and Edicom Cloud installation formal procedures. Currently, the Consulting department is organised in several teams based on its competences, in particular, languages and professional experience. Each team is composed of 2 or 3 project managers and around 5 or 6 consultants, including the team manager.

A description of EDICOM's ETM is briefly described below:

- Roles, which imply the following responsibilities:
    - Account manager: Assigning tasks to the area's backlog.
    - Area director: Assigning tasks from the area's backlog to the team's backlog, maintain a balanced backlog among teams and solve planning conflicts among teams.
    - Project manager: Being the interlocutor among all the stakeholders involved, validate scope and specifications of the project/task with the Client, prioritize assigned projects/tasks and estimate its effort, and plan and validate the sprint backlog.
    - Team manager: Being the interlocutor between the project manager and the project team, follow-up the status of different tasks of the sprint, call sprint meetings and being a mentor for the rest of the project team.

- Project team: Validating the requirements and efforts estimation of each task and being able to comply with deadline and with the expected quality.

- Sprint:

  The duration of a sprint is one week. Start and end dates for each sprint are the same for all teams.

- Meetings (per team), whose objectives are:

  - Sprint planning meeting: Solve doubts about the tasks which must be performed by the team in each sprint. The meeting takes place at the beginning of a sprint cycle (on Friday). Attendance of team manager and project team is compulsory, and the attendance of project manager is optional. Estimated duration is half an hour.

  - Plan total meeting: Inform about the scope and planning of a new project which takes longer than a week. The meeting takes place at the beginning of every project with the sprint planning meeting. Attendance of project manager, team manager and project team are compulsory. Estimated duration is a quarter-hour, depending on project.

  - Daily meeting: Analyse the status of the tasks assigned to the project team (not started, ongoing and finished) and detect locks. Attendance of the team manager and project team is compulsory. Maximum duration is 15 minutes.

    Daily meetings are optional under the project manager and team manager decision.

  - Sprint review meeting: Analyse the result of the sprint backlog at the end of the sprint. Assistance of project manager, team manager and project team are compulsory. Estimated duration is half an hour.

  - Retrospective meeting: Optional meetings held when there are point of improvement regarding the previous sprint (e.g.: opportunities to improve the methodology, lessons learned, positive aspects, etc.). Assistance of project manager, team manager and project team are compulsory. Estimated duration is one-two hours.

During the course of the project, the Consulting department make use of a task management application to:

- Describe activities which have been performed, including detailed description, arrangements made with the Client and relevant information generated or received during the task (e.g.: emails, documentation, etc.).

- Monitor pending activities which need to be performed and follow-up automatic alarms every 5 days embedded in the task management application.

- Define milestones and include coordination tasks with the Client.

Test

Tests performed in the Edicom Cloud service new installations can be classified in the following categories:

- Network: Ensure network connectivity among Client, B2B cloud platform and interlocutor.

- Syntactic: Data provided by the Client from its systems is analysed using automated tools to inspect whether it conforms to the arranged format and structure.

- Semantic: Content of data provided by the Client from its systems is analysed using manual and automated tools to inspect whether the content is as expected.

- Transformation: Verify that the rules applied to the messages enable the integration of the messages between the Client and interlocutor systems.

The Quality Assurance department is also involved in this process to test new complements, screens, lists, etc. In the case of complements, the Quality Assurance department has generated several checklists which have to be used by the Consulting department to perform a first stage of testing (syntactic, semantic and transformation).

The aim of this process is to anticipate the detection of errors in previous stages before complements are sent to the Quality Assurance process for review.

The new Edicom Cloud logical domains are created in production environments and, therefore, tests from the standpoint of EDICOM, are performed in production systems.

From the point of view of the Client and the interlocutor, these logical domains are considered test systems until the integration process has finished, so, distinguishing test messages exchanged during this process is a responsibility of both Client and interlocutor.

The results of these tests are stored in every task created in the Consultant Department application (JCons) to manage the whole project. Additionally, EDICOM has a server repository, which is structured as per the location of EDICOM's facilities (Spain, Mexico …) and alphabetical order, where EDICOM stores the test results for all the projects. In the task management application, the consultant registers which tests has been performed and the communications with the Client. If the execution of a test fails, detailed analysis and additional installation tasks are performed until the results of the execution are satisfactory.

Release

Once the tests have been successfully completed, a date is agreed between all involved parties (Client and EDICOM) and the Client integration is then marked as being in production.

After the deployment process has finished, EDICOM requests the Client to confirm Edicom Cloud Service that the new installation is working correctly as well as an authorization to close the project. Once this is done a project closure report is sent by e-mail to the Client.

The project closure report notes that if the client does not indicate otherwise within 5 days the project will be closed with conformity.

For clients with an operating Edicom Cloud, if errors are detected during or after the deployment process, EDICOM has developed a formal rollback procedure with detail of the restoration steps to be performed.

Configuration aspects which could be susceptible to perform a rollback are:

- Address book configuration (Client's customers and suppliers).
- List configuration.
- System schema loading.
- Mapped configuration.
- Scripts configuration.
- Report configuration.

Client Responsibilities

The Client is responsible for:

- Client-side testing
- Reviewing the installation task at the end of a project.

3.4.3.2 Edicom Cloud service provision

Changes regarding Edicom Cloud Service provision are performed by the R&D and IT departments and Quality manager. Edicom Cloud software developments are performed as a result of:

- Incidents and suggestions communicated to the Helpdesk department by Clients or detected by EDICOM, as a result of the incident management process and the problem management process.
- New development requests communicated to the Consulting department by Clients.
- Monitoring and research activities conducted by the R&D & IT department which allow performance, stability, usability or security improvements.
- Strategic issues aligned with the company Management: Market trends and future Client necessities, Competition products.

Analysis

The R&D and IT departments use technical management applications (JDev and JSys) to manage changes regarding the provision of the Edicom Cloud service during its life cycle. The following information is registered:

- Product affected, which can be:
    - Software developed in-house by EDICOM.
    - System software. These changes are typically performed when software vendors release new software versions, major upgrades, service packs, security patches or when the R&D & IT department designs a modification of the technological infrastructure of the Edicom Cloud Service which implies an in-depth change at system software level.

- Source of the change, internal (EDICOM) or external (e.g.: Clients, regulations, etc.).

- Type of change, e.g.: improvement, new functionality, major versions, incident, testing, changes related to ISMS (Information Security Management System), etc.

- Detailed description of the change, including, functional requirements if necessary.

- Criticality, depending on the impact of the change and its implementation cost, can be classified as:

    - High: Affects majority of Clients causing impact in Edicom Cloud Service provision and requires great implementation effort.

    - Medium: Affects several Clients causing impact in Edicom Cloud Service provision and requires moderate implementation effort.

    - Low: Affects several Clients but does not affect Edicom Cloud Service provision or does not affect Clients. Low implementation effort, day-to-day operation.

- Priority, depending on the criticality of the change and the time, this change is added to the backlog (pending tasks to perform). Priority is also set in a change considering Scrum Master's or R&D manager's criteria. There is another field in technical management application to register a deadline, and according with this date, the priority is established.

At the end of each sprint (period of 2 weeks) the Scrum Master and R&D manager prepare the sprint planning for the next sprint based on the priority of every change. Changes with the closest deadline are planned and set in the first place, and the rest of changes are planned according to their priority.

For every single task, the following aspects must be identified in the management application:

- Software developer/ IT operator responsible for executing the change.

- Tester of the change, if applicable. Testing could be an internal testing (R&D department) or external testing (Quality and Testing department). The R&D department performs the integration tests, and the functional tests and web testing are performed by the Quality and Testing department.

R&D department has developed end-to-end tests to automate some testing in specific services (such as eDelivery). These tests replicate browsing activities through the browser.

When it is necessary to perform an external test (Quality and Testing department), a new task is created related to the previous change task and a task flow is started between the R&D department and the Quality and Testing department until testing is completed. It is possible that some external tests (tests performed by the Quality and Testing department may need another external tester from the Consulting department in those cases where they have captured the requirements). For the tests carried out by the R&D department there are also tasks related with. Every result is registered in the management application.

The R&D department has included a field in its technical management application in order to analyse the quality of the provided specifications. Those specifications which are considered incomplete or deficient are rejected and an automatic email is sent to the requestor so that more information can be provided within a timeframe of 48 hours. If the requestor does not provide the information, the same mail will be sent on periodic intervals until the requestor provides the information.

Urgent change management is considered for those tasks that are scheduled to run in less than one sprint time (Kanban task).

Cloud Service standardization and configuration

In order to protect against massive changes in installations and to be more agile in implementation times avoiding manual configuration errors, EDICOM has an area dedicated to coordinate deliveries and updates and ensuring the standardization of processes (Platform).

The main activities performed by the Platform area are:

- Managing the updating processes of all services (both processes and data) by establishing update procedures and annual calendars. Measure the capacity of the SaaSEDI service.
- Ensuring the standardization of processes both in existing services (continuous improvement) and in the new services that are defined.
- Ensuring that the monthly billing processes of our services work properly, are complete and are performed out in a standard and automatic manner.
- Identifying manual processes, analysing them, standardizing them (if they are not) creating (assets) environments where configurations and settings are available in a packaged way promoting standardization and avoiding manual configuration errors.

Development

The change is carried out following EDICOM´s software development and release management methodology. During the course of the project, the R&D and IT departments use the technical management application to track the following:

- Activities which have been performed, including detailed description as well as attaching relevant documents generated or received during the task (e.g.: emails, documentation regarding application design, interfaces, data flow maps, etc.)

- Pending activities which need to be performed, defining milestones and coordinating with other EDICOM departments as appropriate.

EDICOM has developed a set of coding guidelines which have to be followed by programmers. The principal objective of these guides is to define a common programming style so that code can be read and understood by all members of the team.

Moreover, EDICOM uses a quality coding tool named SonarQube. This tool verifies all programmed code (structure, coding, etc.). R&D has also plugins, based on eclipse to normalize the code.

EDICOM has implemented an agile software development framework based on Scrum. Particularly, EDICOM has defined different teams, depending on the type of the developed product:

- Web teams, develops user layers of Edicom Cloud Services.

- Web services, develops services layers of Ediwinws, EBImaweb, RAedicom.

- EDI team, develops Ediwin, EDICOMData and VAT Compliance.

- Multi team, develops EBI, LTA and iPaaS.

- Core team, develops EBIMAP, CRP Flow, SBS

- Internal team develops and maintains the EDICOM’s internal task management applications.

A description of EDICOM's Scrum implementation is briefly described below:

- Roles, which entail the following responsibilities:

- Product owner: Represents the stakeholders, being the voice of the Client and is accountable for ensuring that the team delivers value to the business. This figure is assigned to the R&D manager for every product and service developed by EDICOM.

- Scrum master (one per team): This individual is a facilitator for a development team that uses Scrum and is accountable for removing impediments to the ability of the team to deliver the product goals and deliverables.

- Development team: Delivering new releases of products at the end of each sprint with the expected quality.

- Sprint:

  The duration of a sprint is two weeks. Start and end dates for each sprint are the same for all the teams.

- Meetings (per team), whose objectives are:

  - Sprint planning meeting: Prioritize and prepare the sprint backlog. The meeting takes place at the beginning of a sprint cycle and the estimated duration is 4 hours.

  - Daily scrum meeting: Identifying tasks performed the day before, checking the latest tasks and the current ones to detect locks. Maximum duration is 15 minutes.

  - Sprint review meeting: Used to review the work that was completed and the planned work that was not completed. The meeting takes place at the end of a sprint cycle and estimated duration is 1 or 2 hours.

  - Sprint retrospective meeting: Performed two per year, sprint retrospective meetings are used to reflect on the past sprints and allow continuous process improvements. After each meeting, a minute is made. Meeting estimated duration is 2 or 3 hours.

    EDICOM celebrates sprint planning meeting jointly with sprint review meeting.

Software quality and secure development

EDICOM has developed a project about software quality with an external supplier. A weekly monitoring of development activities is carried out by EDICOM. The source code is hosted in EDICOM systems, specifications are

defined from the beginning and EDICOM's procedures are followed by the external provider. This project is based-on the standard ISO 25000 (Software Product Quality Requirements and Evaluation), to enhance the quality of development activities and deliverables.

The R&D department has adopted specific cryptographic controls in accordance with the general cryptographic policy to ensure secure development. In addition, the R&D department has defined protection controls at the development phase against typical attacks, these controls are implemented at the application level. For instance, there are protection mechanisms against SQLI (Structured Query Language Injection), and specific libraries against SQLI are used at backend. Additionally, Edicom has instituted various protective measures, including the use of control tokens to counter Cross-Site Request Forgery (CSRF) and the implementation of defences against Cross-Site Scripting (XSS).

This standard covers two main processes: software quality requirements specification and evaluation of software quality, supported by the software quality measuring process. Every new project is included in this software development quality review.

The external provider performs software quality monitoring to identify vulnerabilities in the developed source code and delivers monthly reports. In order to perform this quality monitoring, the external provider uses SonarQube, a tool based on OWASP Top 10. Additionally, EDICOM has meetings (twice per year) with the external provider with the purpose of reviewing the indicators of the software quality monitoring.

Test - Software developed by EDICOM

The technical management application (JQuality) is currently used to record the QA department test tasks.

Depending on the relevance of the change, the following tests are performed:

- Standard changes: These changes are considered non-critical and are not tested. They are changes that require a few minutes of work (less than one hour) and are trivial changes (e.g. orthographic correction). They do not usually affect the operation of Edicom Cloud.

- Internal testing: Unit testing is performed by software developers in testing environments. EDICOM has created a group on the B2B Cloud Platform, which is used only by operators, therefore, each one of them has their own environment to test their developments.

The results of internal testing activities are documented in the technical management application, JQuality (bug tracking section), and tested software is stored in the GitLab repository.

- External testing: Once the development activities have finished and unit testing has successfully concluded, the software developer sends an external test request to the Quality Assurance department using the established workflow in the technical management application.

  Next, an external testing request is received by the Quality Assurance department and additional testing is performed in the testing environments. The results of the external testing are documented in the technical management application, and, if testing fails, the development task is sent back to the R&D area changing its state back to coding stage. This flow of transactions is logged in the R&D task management application.

  External testers use procedures and checklists to check if the change has been developed and works correctly. These checklists are predefined from test templates, but also, testers could generate their own checklist to test the developed code. In both cases, the tester indicates the path of the network folder where the used checklists are stored in the technical management application.

  When external tests satisfactorily conclude, tested software is stored in the GitLab repository.

EDICOM has implemented a continuous integration approach to prevent integration problems. This software engineering practice is supported by the following tools:

- JFrog's Artifactory, an open-source tool used to manage software repositories within an organization. Artifactory is the package repository –compiled modules– from where the Jenkins tool takes the packages that are sent to Test and Preproduction environments. Snapshots and releases are stored in Artifactory.

  In Artifactory, software developers have read only permissions to compile their developed code with the Edicom Cloud compiled code. In order to write a new package onto the repository is only available from Jenkins, so writing permissions are execute only for operators with Jenkins access.

- Apache Maven, an open-source build automation tool used primarily for Java projects. In Maven there are the POM (Project Object Model) files stored. Jenkins requests Maven to generate the compiled file.

- Jenkins, an open-source continuous integration tool for software development. Jenkins and GitLab CI is used to compile and deploy software to Test and Preproduction environment.

  Using this approach, the testing environments are updated with the most recent code versions (denominated snapshot versions). In particular, the testing environment is updated automatically twice a day and the preproduction environment is manually updated as required.

- GitLab CI, the testing environment and the preproduction environment is updated automatically every commit on merge request master.

- Workflow tool (deployment to Production environment): Deployments into Production can only be approved by the R&D manager, Edicom Cloud Quality manager (and its two backup) and the IT department. Depending on the deployment, it is approved by one or the other, but usually, approvals are performed by the R&D manager and the Edicom Cloud Quality manager.

  Deployments into Production are coordinated between the Edicom Cloud Quality manager and the R&D department, but they are carried out by the IT department in order to ensure segregation of duties between the preproduction and production environments.

- GitLab, a repository tool. EDICOM has migrated all versions and source code from Subversion to GitLab. Every developer develops the code and uploads it onto a branch of the corresponding repository (project). Then, before the merge task, GitLab compiles and performs a unitary test. Afterwards, if the unitary test is passed, there is a merge to the master branch to the deployment stage. The merge task is only performed by users who have owner privileges. The merge is that the project is packed and GitLab performs a mirror image in the docker. Once all these tasks are completed, the package is ready to be deployed into the production environment.

Test - System changes

In these cases, test plans are designed by the IT area and test and preproduction environments are used to execute the test plans before promoting the new system software version to the production environment. Test plans and tests results are also documented in the technical management application.

Release - Software developed by EDICOM

This step is coordinated between the Edicom Cloud Quality manager and the R&D department and it is performed by the IT department, in order to ensure segregation between preproduction and production environments is in place.

The IT department performs and coordinates the system changes release process with the other EDICOM departments to minimise the impact on the Edicom Cloud Service operation.

EDICOM periodically deploys new software releases which support the Edicom Cloud Service. During the audited period there have been changes in the release procedure and schedule.

All services and applications have been grouped between Communication Platform and SaaSEDI Platform and each of this groups are updated semi-annually avoiding frostbitten and holiday periods.

Prior to the deployment of a new release, the start of a new update cycle is communicated to:

- Technical employees, in order to inform them before the start of the release cycle so that any anomalies during the process can be timely identified. This notification is performed by the Edicom Cloud Quality manager.

- A group of Clients, which include:

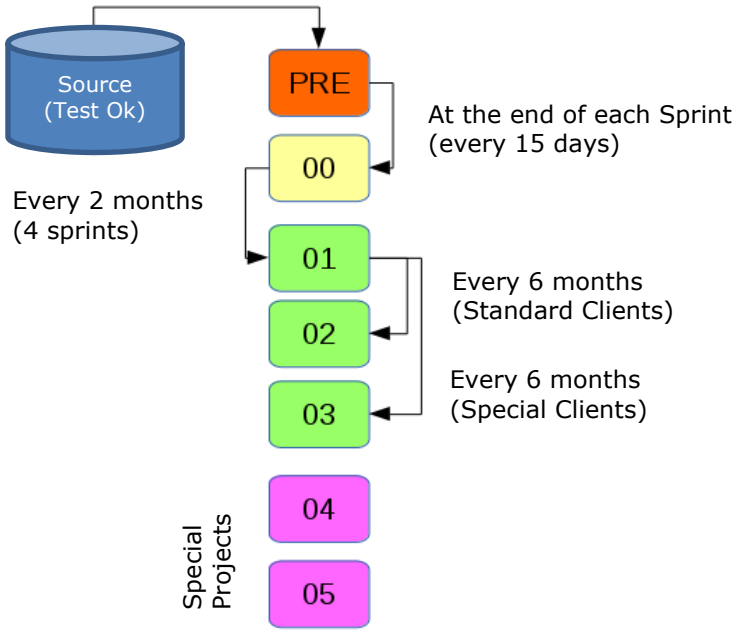
    - Clients who have specifically communicated EDICOM they want to be subscribed to software updates regarding Edicom Cloud Service.

    - Clients which should receive updates notifications for a number of reasons according to EDICOM criteria (e.g.: previous incidents with software releases).

Every software change is registered in a table which is used to create automated notifications to Clients informing them about new release and software changes. Also, these logs are available in EDIWIN, entering to Change Log option on the Help menu.

The Client is responsible for signing up on the Edicom Cloud Service updates communication service and for providing Client contact information to receive the updates communications. The communications are performed by the Helpdesk department manager.

The software which supports the Edicom Cloud Service is deployed in the production environment in various instances, as depicted on the next graphic.



The functionality of the different instances is the following:

- "00" instance: Base instance in the update process. The content of "00" instance is updated at the end of each sprint (every 15 days).
    - A limited number of Clients are deployed in this instance.
- "01" instance: The content of "01" instance is updated every 2 months (4 sprints) or earlier if necessary, based on the number of Clients in "00" instance. A limited number of Clients are deployed in this instance.
    - Clients from "00" instance are moved to "01" instance in order to reduce the number of updates which are applied to their environments.
- "02" instance: The content of "02" instance is updated every 6 months from the "01" instance and coincides with the general release calendar of deployment of EBI, EBIMAP, Ediwin and Ediwin Viewer. New releases are just applied to Clients in "02" instance. "02" instance contains the installation of most Clients.
- "03" instance: The content of "03" instance is also updated every 6 months from the "01" instance, in the same way that the instance "02", but after some weeks of testing on the instance "02".

"03" instance contains the installation of Clients which have been classified as special installations. "02" and "03" instances contains the installations of 99% of EDICOM's Clients.

- "04", "05" and other instances: Host Edicom Cloud Service of a reduced group of Clients (e.g.: different software versions, high degree of personalization, etc.).

Deployment process in "02" and "03" instances is performed using the following schema:

- The R&D manager generates a new software release version with approved changes.

- The preproduction environment (PRE) is updated with the release version. This process is manually performed by the R&D manager development using Jenkins (Jenkins and, since February 2018, GitLab perform some unitary test once they have compiled the software).

- The R&D manager uses the Workflow tool developed by the IT department to request updating a base instance ("00" instance) of production environment (with very few Clients) with the content of preproduction environment.

- The IT department or the Delivery Manager approves the request, and the update process starts automatically. The Workflow tool has automatic controls regarding segregation of duties, specifically:

    - Update requests can be performed just by authorized users, generally, R&D manager, senior software developers and IT department,

    - Update approvals can be performed just by authorized users, generally, IT department, R&D manager and Edicom Cloud Quality manager.

    - The person who requests the update cannot approve it.

- In the first place, Clients from the "02" instance are moved gradually to the base instance. This process is performed progressively in several stages, normally 4. The whole process usually takes between 2 and 3 weeks. This process of redirecting Clients to other instances is done through a configuration file.

- After a few days to ensure that the new software is working properly and correct any problems identified, the same steps are performed for instance "03" (Clients are moved gradually to the base instance).

- When "02" and "03" instances are empty, they are updated with the content of the base instance.

- The Clients from the base instance are moved to the "02" and "03" instances (first the standard Clients).

In case of failures during deployment, the rollback process consists in moving Clients which have been updated, located at the base instance, to the "02" or "03" instances, which contain previous software versions. This mechanism enables the detailed monitoring of the process and reduces the risks associated to the software upgrade.

Once the update plan has finished, the following notifications are sent:

- EDICOM operators receive a report with technical details of changes included in the new release. This notification is sent by the Edicom Cloud Quality manager.

- EDICOM software developers receive a report with incidents originated as a result of the update process, in order to continuously improve the quality of the release management process. This report is generated by the R&D department manager.

- A public changelog is included in updated applications (available in EDIWIN, Change Log option on the Help menu).

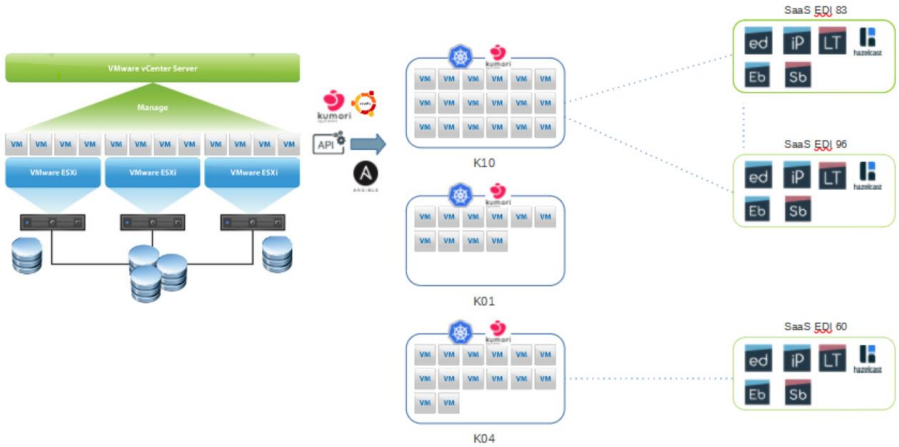
Additionally, records of all the Edicom Cloud Service updates for each Client are maintained as an input to the incident and problem management processes.

To all of the above, it must be added that EDICOM has traditionally worked with real physical servers, but it has already begun to pivot towards a virtual infrastructure, using Kubernetes technology. In this way, the clients are assigned to the different virtual spaces. The objective is oriented towards the virtualization of the different processes.

EDICOM uses Kumori PaaS that runs on clusters of Kubernetes. This technology allows to have fully versioned projects, so it is possible to go back to any version in the infrastructure in production environments. In this way, there are some groups of clients that are served with this technology. For the management of deployments, tools based on Kumori are used, such as kumorictl.

A deployment project consists of three types of objects:

- **Deployment**: It is the part of the project where the specific parameters to instantiate the service are indicated (connection strings, number of instances, CPU resources, memory, etc.)
- **Service**: It is where the topology is defined. Service components, roles and versions of these components, relationships between all components of the service through internal communication channels. And finally, it is defined the channels of access to the service from abroad.
- **Component**: Each of the software projects has a component, which contains a docker and the information on how to pass the parameters and properties from higher layers (services and deployments).



EDICOM also has the Trivy tool that allows it to analyze the vulnerabilities present in an image, identifying the vulnerabilities. Through this tool, analyzes of the images with which the services are deployed are performed and all identified vulnerabilities are patched.

It is noteworthy that the communication between system have been configured with TLS 1.2.

Client Responsibilities

The Client is responsible for requesting subscription to update notifications of Edicom Cloud Service.

3.4.4 *Risk Assessment, Business Continuity and Data Privacy*

3.4.4.1 Risk Assessment

EDICOM has a methodology and documented procedure available to perform risk assessments of its business processes, information security and data privacy. This methodology and risk assessment have been developed to meet the requirements of ISO/IEC 27001, UNE-ISO/IEC 20000-1:2018 and the Spanish National Security Scheme (high level). The appreciation of the risks and the treatment process included in this procedure are based on the generic principles and guidelines defined in the ISO 31000:2018 Standard, Risk management Principles and guidelines.

EDICOM has defined roles within the framework of the analysis methodology of the risk. The three major participants are: the Risk management Committee, the Risk Analysis Manager and Project Managers.

EDICOM has delineated a catalogue comprising nine risk categories to which the organization and its information assets are exposed. Evaluated risks encompass supply chain disruptions, attacks on the logical and physical infrastructure, human errors, information leaks, fraud, and regulatory non-compliance.

This methodology consists of 3 main stages:

- Initial/Preliminary Risk Assessment
- Detailed Risk Assessment and Residual Risk Acceptance
- Risk Treatment Plan

For each stage the following elements are considered:

- Inputs
- Tasks to be performed
- Roles and Responsibilities involved
- Generated Outputs
- Tools used

Preliminary Risk Assessment main tasks are made up of the following:

1. Identify vulnerabilities and threats to which information assets are exposed.
2. Evaluate the changing probability of a threat materializing, compared to the latest risk analysis, and associate it with an estimated frequency.
3. Assess the evolving impact of a threat exploiting a vulnerability on assets, in comparison to the last risk analysis.

4. Establish the risk level as the product of the impact (consequence) associated with a threat (event), multiplied by the probability of occurrence.

Once the initial information risk assessment has been performed, meetings with the defined risk assessment roles are held, to identify different types of measures for those risks which are above the risk acceptance criteria. After that, economic evaluations and security measure evaluations are carried out, to make the decision to treat/mitigate, accept, remove the source, or delegate responsibility for identified risks. Additionally, there is a formal approval of the risk acceptance criteria.

For those risks which are above the risk acceptance criteria, the organization defines and explicitly approves a Risk Treatment Plan (RTP) which includes the necessary actions to minimize the risk below the risk acceptance criteria.

EDICOM's Management agrees to provide the necessary resources to implement the actions within the RTP, based on a cost-benefit analysis, so that the cost of implementing the measure is lower that the potential impact of the risk which EDICOM aims to mitigate.

3.4.4.2 Business Continuity Plan

Information is one of the most important assets for organizations, where information systems and short and long-term availability develop a principal role to business continuity.

An event which has an impact on the availability of the services provided could deteriorate the performance of the organization if it is not possible to restore the services within the required time scales based on Clients' necessities.

The goal of the Business Continuity Plan (BCP) is to guarantee the continuity of EDICOM's critical business processes, minimizing the impact of any contingency, which could take place due to natural disasters, accidents, equipment failure, deliberate human actions or any event which has an impact on the normal service provision, according to EDICOM's service level agreements with its Clients.

As a part of the BCP, EDICOM has performed a Business Impact Analysis (BIA) which has help identify weaknesses and/or threats for each of the business processes and systems.

Additionally, the availability requirements (Recovery Time Objective –RTO– and Recovery Point Objective –RPO–) have been identified for each business process within the scope of the BCP (Edicom Cloud and trust services).

Based on the continuity requirements resulting from the BIA (RTO and RPO), EDICOM has identified a number of contingency scenarios and strategies have been devised to guarantee business continuity in each case.

The different strategies and processes used to recover EDICOM´s systems are documented in the Disaster Recovery Plan (DRP) which covers the following scenarios:

- Lack of key personnel.
- Widespread staff absence
- Unavailability of facilities and/or DCs.
- Critical Hardware failure or downtime.
- Critical Software failure.
- Cyber-attack and/or non-authorized access which affects to public or internal EDICOM systems.
- Main network link failure.
- Prolonged power supply failure.
- Compromise of the services provided by Edicom.

EDICOM carries out tests of its DRP and documents the results on an annual basis. Moreover, the test plan must be approved by Management. These tests allow staff and systems to be prepared in case of contingency. If necessary, both the BCP and DRP are be updated.

In order to deal with possible disaster situations and to coordinate recovery activities in a timely manner, EDICOM has set up a Crisis Committee, of which the EDICOM's Management are members. The Committee is responsible of the evaluation of contingency situation at EDICOM and for the definition of the necessary actions to mitigate the potential impact as well as the coordination of the personnel involved.

The framework of reference to develop EDICOM´s BCP, is the international standard ISO 22301 Business Continuity Management System which provides guidance for the design, elaboration, development and maintenance of a strategy for business continuity management.

EDICOM is aligned with the ISO standard stance as to business continuity management awareness as part of the corporate culture at all levels.

3.4.4.3 Data Privacy and Personal Data Protection

EDICOM has defined data privacy measures, which include technical and organizational measures, to guarantee the security, especially with regards to privacy and confidentiality, of automated (e.g. electronic devices) and non-automated (e.g. data on paper documents, reports) treatment of personal and confidential data, for both EDICOM's internal and Client's data.

These measures are designed to prevent information's unauthorized modification, information loss, information's unauthorized treatment or access.

The following measures amongst others have been implemented:

- Logical Access Control to information systems.
- Physical Access Control to information systems (DC).
- Backup and Data Recovery.
- Media Handling.
- Monitoring and Vulnerability Management.
- Security Incidents Management.
- Data Protection Officer appointment (DPO).
- Records of Processing Activities (RPA).
- Data Protection Impact Assessment (DPIA).
- Procedures to safeguard the rights of the interested parties.

These measures are mandatory for all EDICOM's employees, including external staff (suppliers) with access to EDICOM's information systems.

EDICOM has formally appointed a Security Officer and a Data Protection Officer, which are in charge of making sure the relevant procedures and controls are implemented in alignment with the security standard requirements.

Additionally, an internal data protection audit is performed annually.

3.4.5 *Key process level control changes occurred in the audit period*

Throughout the audited period, EDICOM was actively engaged in a migration process to expand its data centre infrastructure to include a third facility, known as Walhalla. This expansion involved maintaining the primary data centre at EDICOM's own facilities while housing the secondary data centre at COLT facilities.

EDICOM has added the Spanish National Security Scheme at High level certification to the EDICOM IT control framework. The last successfully passed audit (without any finding) took place during the audited period and it was conducted by AENOR.

EDICOM has created a new division within the systems department specifically dedicated to cybersecurity.

4. Independent Service Auditor’s Description of Controls Test and Results

4.1 Introduction

This report is intended to provide Clients of EDICOM with information about the controls at EDICOM that may affect the processing of user organizations' transactions and also to provide users with information about the operating effectiveness of the controls that were tested. This report, when combined with an understanding and assessment of the controls at user organizations, is intended to assist user auditors in (1) planning the audit of user organizations' financial statements and in (2) assessing control risk for assertions in user organizations' financial statements that may be affected by controls at EDICOM.

Our testing of EDICOM's controls was restricted to the system in scope and to the control objectives and related controls 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, EDICOM's controls may not compensate for such weaknesses.

4.2 Test of Operating Effectiveness

Our work has included documentation review (policies, procedures, work instructions and manuals, templates or forms, etc.), interviews with EDICOM’s staff from different departments, and the review of controls deployed on EDICOM’s systems to obtain reasonable assurance and to express an opinion on:

- If the attached control description (see table) reasonably fulfils all aspects which could be relevant to the organization internal control in relation to the services provided.
- If the controls have been adequately designed to achieve the objective described in their description, and if those controls were successfully fulfilled.
- If those controls have been implemented during period August 1, 2022 to July 31, 2023.

The fieldwork consists of the control review performed during the period July 2023 to October 2023, and the sample taken corresponds to period indicated on the scope (August 1, 2022 to July 31, 2023).

Effectiveness tests of the controls have included the tests which have been considered necessary according to the circumstances and to the auditors' professional criteria to assess if controls, and the fulfilment grade, were enough to determine with a reasonable degree of assurance (but not absolutely), that the objectives have been reached during the period indicated in the scope.

In order to achieve it, the operating effectiveness of the controls has been reviewed checking their implementation. For the more relevant controls, a statistical sampling testing has been performed on the population, and for the rest a representative sample selection has been analysed. To determine the sample size, the audit team has considered some characteristics such as total testing population, the control type, the frequency, deviation rate, etc. View **Annex 1** for the Sampling Methodology followed for this report.

Moreover, it should also be mentioned that this operating effectiveness review of the controls was performed under inherent limitations to sampling and, therefore, there could exist impairments or errors which have not been detected.

The following tables show the controls tested, grouped by control objective and indicating their description, test performed, and results obtained. Forty-nine (49) controls have been checked and tested.

Control ID	Control Area	Control Description	Description of Test Performed	Test Result
Control Objective 1: Controls provide reasonable assurance that operations are managed to support the scheduling, execution, monitoring and continuity of IT programs and processes for the complete, accurate and valid processing and recording of transactions.				
A1.1	**Transaction Integrity**	Processing procedures are defined and executed so that transactions are processed to successful completion or are otherwise recovered and reprocessed. *See section 3.4.1.1 for the description of related systems and controls.*	A1.1-1 Interview with Service Level Manager. Inquiry about monitoring and alarms detection handling process. Review of related procedures. A1.1-2 Review alarms configuration (alarms processes and scripts, and time planning to their launch and execution). A1.1-3 Review EBIMON tool, showing different types of integrity alarms. A1.1-4 Inspect a sample of Management meeting minutes where alarm management is analysed. A1.1-5 Review of the procedure to be performed by 24x7 staff for each type of alarm. A1.1-6 A list of all alarms of transaction integrity from EBIMON activated during the audit period was requested and a sample randomly selected. A1.1-7 Inspected a sample of alarms of transaction integrity from EBIMON activated during the audit period to determine whether they were resolved and closed within a reasonable time.	No exceptions noted

Control ID	Control Area	Control Description	Description of Test Performed	Test Result
			A1.1-8 A list of all 24x7 registered incidents related to alarms activated during the audit period was requested and a sample randomly selected. A1.1-9 Inspected a sample of 24x7 registered incidents during the period to determine whether they were resolved and closed within a reasonable time.	
A1.2	**Availability Monitoring**	Performance and availability of the IT environment is measured, reported and reviewed by management to ensure timely execution and complete processing and availability of data. *See section 3.4.1.2 for the description of related systems and controls.*	A1.2-1 Interview with Service Level Manager. Inquiry about SLA management process and its Service Management Tools. Inquiry about EDICOM's SLA with their Clients. Review of related procedures. A1.2-2 Inspect monitoring tools for B2B cloud platform availability and the utilities to monitor hardware availability and performance. A1.2-3 Review the web site to check EDICOM's Services Status. A1.2-4 Review the EBIMON tool, showing different types of availability alarms. A1.2-5 A list of all alarms of availability SLA monitoring from Edicom Cloud and hardware availability during the audit period was requested and a sample randomly selected. A1.2-6 Inspected a sample of alarms of availability SLA monitoring from Edicom Cloud during the period to	No exceptions noted.

Control ID	Control Area	Control Description	Description of Test Performed	Test Result
			determine whether they were resolved and closed within a reasonable time. A1.2-7 Inspect a sample of Management meeting minutes where SLA monitoring is analysed. A1.2-8 Review the SLA monthly report delivered to Clients. A1.2-9 Interview with the IT Manager. Inquiry about systems monitoring process, tools (scripts) and review of related procedures.	
A1.3	**Capacity Management**	Studies are conducted in order to predict future capacity requirements based on natural growth or other aspects which may affect current capacity and performance. Management monitors that action is taken upon identification of inefficient performance. *See section 3.4.1.3 for the description of related systems and controls.*	A1.3-1 Interview with Edicom Cloud Quality Manager. Inquiry about Edicom Cloud Capacity Management process and documented procedure. A1.3-2 Inspect the last annual capacity plan performed by the IT Manager. A1.3-3 A list of all capacity reports performed during the audit period was requested and a sample randomly selected. A1.3-4 Inspect a sample of the capacity reports performed during the audit period to determine whether: capacity reports are performed periodically, are analysed and recommendations are provided. A1.3-5 Inspect a sample of meeting minutes where capacity reports are analysed.	No exceptions noted.

Control ID	Control Area	Control Description	Description of Test Performed	Test Result
			A1.3-6 Interview with IT manager to confirm that capacity reports recommendations are reviewed, and tasks are created to carry them out.	
A1.4	**Helpdesk**	A help desk function that acts on Client queries regarding the service is in place. Incidents are recorded in a centralized tool and monitoring is performed for timely resolution of all user queries. *See section 3.4.1.4 for the description of related systems and controls.*	A1.4-1 Interview with the Incidents and Problems Manager. Inquiry about the Incident Management process and related documented procedures. A1.4-2 Corroborative inquiry about the process to generate the support SLA report distributed to clients on a monthly basis. A1.4-3 Inspected a sample of support SLA reports. A1.4-4 Inspected a sample of minutes of periodic managers meeting related to incidents and problems. A1.4-5 A list of all incidents registered at the incident management tool during the audit period was requested and a sample randomly selected. A1.4-6 Inspect a sample of incidents to ascertain whether incidents have been assigned a starting and resolution date, assigned an owner or incident responsible, categorized and classified (type of incident and priority), investigated during its lifecycle (tasks performed), and solved and closed in a timely manner.	No exceptions noted.

Control ID	Control Area	Control Description	Description of Test Performed	Test Result
A1.5	**Helpdesk**	Management monitors incidents to identify and correct root causes of recurring problems. *See section 3.4.1.4 for the description of related systems and controls.*	A1.5-1 Interview with the Incidents and Problems Manager. Inquiry about the Problem Management process and related documented procedures. A1.5-2 A list of all problems registered at the management tool during audit period was requested and a sample was randomly selected. A1.5-3 Inspect a sample of problems to ascertain whether problems have been assigned starting and resolution date, assigned an owner or problem responsible, categorized and classified (type and priority), investigated to find root cause, and solved and closed in a timely manner.	No exceptions noted.

Control ID	Control Area	Control Description	Description of Test Performed	Test Result
A1.6	**Supplier Monitoring**	Supplier management process takes into account control, evaluation and review. Appropriate service level agreements (SLA's) are established and the service provided by suppliers is monitored, as well as the incidents that have occurred. *See section 3.4.1.4 for the description of related systems and controls.*	A1.6-1 Interview with Supplier Manager. Inquiry about the Supplier Management process and related documented procedures. A1.6-2 New suppliers are evaluated during selection. Validate for new suppliers if a formal evaluation has been carried out. A1.6-3 Service Level Agreements (SLA's) are established with suppliers and are adequately monitored. A1.6-4 There is an annual review of the service provided by suppliers. Deviations and incidents related to suppliers are properly managed	No exceptions noted.

Control ID	Control Area	Control Description	Description of Test Performed	Test Result
Control Objective 2: Controls provide reasonable assurance that data is managed to remain complete, accurate and valid throughout the update and storage process.				
A2.1	**Backups**	Backup processes are monitored for successful execution, and failures are escalated and corrected to ensure data is usable and available for retrieval and restoration if needed. *See section 0 for the description of related systems and controls.*	A2.1-1 Interview with the IT Manager. Inquiry about the backup management process and related documented procedures. A2.1-2 Interview with the IT Manager. Inspected evidences about internal EDC network backup process to ascertain: backup scheduling, backup monitoring results, incident registration in case of backup failure and its timely resolution. A2.1-3 Interview with the IT Manager. Inspected evidences about B2B network backup process to ascertain: backup scheduling, backup monitoring results, incident registration in case of backup failure and its timely resolution. A2.1-4 A list of all tasks created to address backup failures during the audit period was requested and a sample randomly selected. A2.1-5 Inspect a sample of tasks created to address backup failures to ascertain whether they have been adequately solved and closed in a timely manner.	No exceptions noted.

Control ID	Control Area	Control Description	Description of Test Performed	Test Result
A2.2	**Backups**	Periodical restoration of backups is performed as described in the backup policy. *See section 0 for the description of related systems and controls.*	A2.2-1 Interview with the IT Manager. Inquiry about the backup restoration process and related documented procedures. A2.2-2 A sample of backup restoration reports was inspected.	No exceptions noted.
A2.3	**Backups**	Backup media are stored in a secure location and are retained as described in the Edicom Cloud SLA. *See section 0 for the description of related systems and controls.*	A2.3-1 Interview with the IT Operator. Media storage was inspected to ascertain backup media is stored in a safe place. A2.3-2 Inspect whether annual backups are stored and kept for at least 15 years in two different safe-deposit boxes.	No exceptions noted.
A2.4	**Backups**	Backups are archived off-site to minimize risk that data is lost. *See section 0 for the description of related systems and controls.*	A2.4-1 Interview with IT operator. Ascertain whether backups are stored in a safe place in a different building from the one which hosts the Data Processing Centre.	No exceptions noted.

Control ID	Control Area	Control Description	Description of Test Performed	Test Result
A2.5	**Backups**	A secure media disposal procedure is in place. *See section 0 for the description of related systems and controls.*	A2.5-1 Interview with the IT Operator. Inquiry about secure media disposal process and inspection of related procedures, including removal devices procedure. A2.5-2 Inspected a sample of media disposal to ascertain whether secure wipe methods have been employed.	No exceptions noted.
Control Objective 3: Controls provide reasonable assurance that facilities are managed to protect the integrity of information as it is stored by the relevant components of the information technology infrastructure.				
A3.1	**Physical Security**	Physical access to headquarters is restricted to employees or authorized external visitors. *See section 3.4.2.1 for the description of related systems and controls.*	A3.1-1 Interview with the IT Operator. Inquiry about the physical access procedures. A3.1-2 Visual inspection of physical security mechanisms. A3.1-3 Inspect video surveillance system both inside and outside premises. A3.1-4 Inspect a sample of access logs to ascertain whether every single attempt to access EDICOM is tracked and registered. A3.1-5 Inspect a sample of reports of security guards' rounds. A3.1-6 Inspect the contract with the security company and the receptionist staff company.	No exceptions noted.

Control ID	Control Area	Control Description	Description of Test Performed	Test Result
A3.2	**Physical Security**	Physical access to the primary data centre is restricted to personnel who require access to perform their assigned duties. *See section 3.4.2.1 for the description of related systems and controls.*	A3.2-1 Interview with the IT Operator. Corroborative inquiry about EDICOM Data Centre (DC) physical access and visit to the DC. A3.2-2 Ascertain whether individuals allowed to access the DC are authorized. A3.2-3 Inspect whether accesses to the DC are logged. A3.2-4 Confirm that a video surveillance system is in place inside the DC.	No exceptions noted.
A3.3	**Physical Security**	Management has implemented environmental mechanisms to protect information resources located in the primary data centre from susceptibility to environmental threats. *See section 3.4.2.1 for the description of related systems and controls.*	A3.3-1 Interview with the IT Operator. Inspected current DC to ascertain whether the following controls are implemented: redundant air conditioning machines, temperature sensors mechanisms, fire suppression mechanism, raised floor and dropped ceiling, Uninterruptible Power Supply (UPS) and power generation systems. A3.3-2 Inspect automatic alarms associated to environmental control mechanisms. A3.3-3 Ascertain whether maintenance of air conditioning, UPS and power generators have been performed, at least, annually.	No exceptions noted.
A3.4	**Physical Security**	Physical access to the secondary data centre is restricted to personnel who require	A3.4-1 Review of the secondary and Walhalla (third) data centre.	No exceptions noted.

Control ID	Control Area	Control Description	Description of Test Performed	Test Result
		access to perform their assigned duties. *See section 3.4.2.1 for the description of related systems and controls.*	A3.4-2 Interview with the EDICOM IT Operator and with the secondary and Walhalla data centre staff (supplier employees). Corroborative inquiry about the secondary and Walhalla data centre physical access. A3.4-3 Ascertain whether individuals allowed to access the data centre were previously authorized. A3.4-4 Inspect a sample of datacentres access permissions reviews to ascertain they are effectively performed biannually. A3.4-5 Inspect whether accesses to the data centre are logged. A3.4-6 Confirms that a video surveillance system is in place inside the data centre.	

Control ID	Control Area	Control Description	Description of Test Performed	Test Result
A3.5	**Physical Security**	The secondary data centre offers environmental mechanisms to protect information resources located in from susceptibility to environmental threats. *See section 3.4.2.1 for the description of related systems and controls.*	A3.5-1 Interview with the secondary and Walhalla data centre staff (supplier employee). Inspected the data centre to ascertain whether the following controls are implemented: redundant air conditioning machines, temperature sensors mechanisms, automatic fire suppression mechanism, raised floor and dropped ceiling, Uninterruptible Power Supply (UPS) and power generation systems. A3.5-2 Inspect automatic alarms associated to environmental control mechanisms. A3.5-3 Ascertain whether maintenance of air conditioning, fire suppression mechanism, UPS and power generators have been performed periodically.	No exceptions noted.
Control Objective 4: Controls provide reasonable assurance that the configuration of programs and systems security during change management is managed to safeguard against unauthorized modifications to programs and data that result in incomplete, inaccurate of invalid processing or recording of information.				
A4.1	**Logical Security – EDICOM**	Security policies addressing information security risks have been approved by management and are accepted by employees. *See section 3.4.2.2 for the description of*	A4.1-1 Interview with the IT Manager. Inquiry about the Information Security Policy and code of conduct for employees. A4.1-2 A list of all new joiners during audit period was requested and a randomly sample was selected. A4.1-3 A sample of new joiners was analysed to ascertain whether: have accepted EDICOM's Information Security	No exceptions noted.

Control ID	Control Area	Control Description	Description of Test Performed	Test Result
		related systems and controls.	Policy, signed a confidentiality agreement and received an introductory course on information security. A4.1-4 A sample of employees was analysed to ascertain whether: have received annual training on information security awareness and data protection.	
A4.2	**Logical Security – EDICOM**	Management approves the nature and extent of user access. User accounts are reviewed to confirm access privileges remain adequate. *See section 3.4.2.2 for the description of related systems and controls.*	A4.2-1 Interview with the IT Manager. Inquiry about Logical Access Management processes and related documented procedures. A4.2-2 A sample of new joiners was analysed to ascertain new joiner request was performed by the adequate authorized department and new joiner privileges were correctly assigned. A4.2-3 Levels of privileges and authorizations that can be granted in the Viewer application (Edicom Cloud). A4.2-4 Inspect a sample of user reviews to ascertain they are effectively performed biannually (for generic and service accounts) and monthly (for nominal users).	No exceptions noted.

Control ID	Control Area	Control Description	Description of Test Performed	Test Result
A4.3	**Logical Security – EDICOM**	Access for terminated and/or transferred users is removed or modified in a timely manner. *See section 3.4.2.2 for the description of related systems and controls.*	A4.3-1 Interview with the IT Manager. Inquiry about Logical Access Management processes and related documented procedures. A list of all leavers during the audit period was requested and a random sample was selected. A4.3-2 A sample of leavers was analysed to ascertain: • Leaving request was performed by the adequate authorized department. • Leaving request includes leaving date. • Task was performed within the correct timescales. • User has been disabled or deleted from system. A4.3-3 A script execution was run to ascertain inactive users by looking at their last logon date to EDC Domain and B2B Domain (users with more than three months without access to the domain). *Note: nominal users are reviewed by EDICOM monthly, and generic and service accounts on biannually.*	No exceptions noted.

Control ID	Control Area	Control Description	Description of Test Performed	Test Result
A4.4	**Logical Security – EDICOM**	Access is authenticated through unique user IDs. *See section 3.4.2.2 for the description of related systems and controls.*	A4.4-1 Several script executions were run to confirm that there are not shared accounts in EDC Domain and B2B Domain. A4.4-2 Several script executions were run to confirm that there are not shared accounts in a sample of MySQL DB. A4.4-3 Several script executions were run to confirm that there are not shared accounts in a sample of CentOS, Elasticsearch, Kubernetes, Linux and CEPH Operative Systems.	No exceptions noted.
A4.5	**Logical Security – EDICOM**	Access is authenticated through passwords or other mechanisms, in compliance with entity security policies. *See section 3.4.2.2 for the description of related systems and controls.*	A4.5-1 Interview with the IT Manager. Inquiry about the password policies. A4.5-2 Several script executions were run to ascertain whether users in EDC Domain and B2B Domain follow password policies and best practices. A4.5-3 Several script executions were run to ascertain whether users in a sample of MySQL DB follow password policies and best practices. A4.5-4 Several script executions were run to ascertain whether users in a sample of CentOS, Elasticsearch, Kubernetes, Linux and CEPH Operative Systems follow password policies and best practices.	No exceptions noted.

Control ID	Control Area	Control Description	Description of Test Performed	Test Result
			A4.5-5 Interview with the IT Manager. Inquiry about password policy which can be defined in Edicom Cloud service web applications.	
A4.6	**Logical Security – EDICOM**	The ability to make modifications to overall system security parameters, security roles or security configuration over information systems is limited to authorized personnel. *See section 3.4.2.2 for the description of related systems and controls.*	A4.6-1 Several script executions were run to ascertain whether Administrators accounts in EDC Domain and B2B Domain have the correct privileges. A4.6-2 Several script executions were run to ascertain whether Administrators accounts in a sample of MySQL DB have the correct privileges. A4.6-3 Several script executions were run to ascertain whether Administrators accounts in a sample of CentOS, Elasticsearch, Kubernetes, Linux and CEPH Operative Systems have the correct privileges.	No exceptions noted.
A4.7	**Logical Security – EDICOM**	Privileged-level access is authorized, logged and reviewed by management. *See section 3.4.2.2 for the description of related systems and controls.*	A4.7-1 Interview with the IT Manager about access to the Client environment and the traceability mechanisms in place to register actions performed by EDICOM employees when accessing the client's environment.	No exceptions noted.

Control ID	Control Area	Control Description	Description of Test Performed	Test Result
A4.8	**Logical Security – EDICOM**	Systems are protected by time-out mechanisms. *See section 3.4.2.2 for the description of related systems and controls.*	A4.8-1 Interview with the IT Manager. Inspected timeout mechanisms in EDC Domain and Edicom Cloud service web application (Viewer).	No exceptions noted.
A4.9	**Logical Security – Edicom Cloud Service Clients**	The identity of individuals requiring management actions related to Edicom Cloud service accounts is verified. *See section ☐ for the description of related systems and controls.*	A4.9-1 Interview with the Incidents and Problems Manager. Inquiry about the processes and documented procedures related to client access to the Edicom Cloud. A4.9-2 Interview the with Service Level Manager. Inquiry about the processes and documented procedures related to client access to the Edicom Cloud. A4.9-3 Review Ediwin Viewer parameters of the identification and authentication policy. A4.9-4 A list of all Edicom Cloud client access incidents registered at EDICOM's management tool during the audit period was requested and a sample randomly selected. A4.9-5 Inspect a sample of Edicom Cloud client access incidents (security and access to data) to ascertain whether the identity of the requester has been confirmed.	No exceptions noted.

Control ID	Control Area	Control Description	Description of Test Performed	Test Result
A4.10	**Logical Security – Edicom Cloud Service Clients**	Access for cancelled Clients is removed in a timely manner. *See section 3.4.2.3 for the description of related systems and controls.*	A4.10-1 Interview with the Service Level Manager. Inquiry about the Client cancellation processes and related documented procedures. A4.10-2 A list of all access cancellation requests to Edicom Cloud performed by Clients during the audit period was requested and a sample randomly selected. A4.10-3 Inspect a sample of Client cancellation requests to confirm whether they have been acted upon and completed.	No exceptions noted.
A4.11	**Network Security**	Security of perimeter network is assessed periodically. *See section 3.4.2.4 for the description of related systems and controls.*	A4.11-1 Interview with the IT Operator. Inquiry about EDICOM's Perimeter Security Management procedures. A4.11-2 Interview with the IT Operator. Inspect EDICOM's Perimeter Network Schema. A4.11-3 Interview with the IT Operator. Inquiry about the Perimeter Network Reviews procedure. A4.11-4 A list of all Firewall rules reviews performed during the audit period was requested. These reviews are performed biannual. A4.11-5 Inspect two Firewall rules reviews performed during audit period to check that five randomly selected rules have been correctly configured as it is indicated in the procedure.	No exceptions noted.

Control ID	Control Area	Control Description	Description of Test Performed	Test Result
			A4.11-6 Interview with the IT Operator. Inquiry about biannual Vulnerability tests to check vulnerabilities analysis are planned to be performed. A4.11-7 A list of all Vulnerability tests performed during the audit period was requested. These tests are performed biannually. A4.11-8 Inspect the two Vulnerability tests performed during audit period to check tests are performed as it is indicated in the procedure. A4.11-9 Interview with the IT Operator. Inspect monitoring activities from EDICOM Network. A4.11-10 Interview with the IT Operator. Inquiry about monitoring activities procedure.	
A4.12	**Anti-malware**	Antivirus software is installed on computers connected to the entity's network. Virus signature lists are frequently updated and data files on the network are automatically scanned. *See section 3.4.2.5 for the description of*	A4.12-1 Interview with the IT Manager. Review the anti-malware policy and the anti-malware installation procedure for computers and servers. A4.12-2 Interview with the IT Manager. Inquiry about anti-malware solutions installed in the systems (personal computers and servers for both, Edicom Cloud and EDICOM internal network). Inspection of a selection of illustrative evidences about: endpoint anti-malware solutions, server anti-malware solutions, network anti-malware solutions, configuration of anti-malware solutions, real-time scanning,	No exceptions noted.

Control ID	Control Area	Control Description	Description of Test Performed	Test Result
		related systems and controls.	and frequency of signature updates. Secure mail service (tool´s evidence).	
A4.13	**Security Patches**	Software versions are current and supported by vendors. *See section 3.4.2.6 for the description of related systems and controls.*	A4.13-1 Interview with the IT Manager. Inquiry about software updating and patching processes and documented procedures. A4.13-2 Interview with the IT Manager. Inspection of a sample of software update tasks performed, registered in the IT department management tool, and review of WSUS (Windows Server Update Services).	No exceptions noted.
A4.14	**Security Incidents**	Management monitors security incidents to identify and correct root causes of recurring problems. *See section 3.4.1.4.7 for the description of related systems and controls.*	A4.14-1 Interview with the Security Incidents Manager. Inquiry about the Security Incident Management process and related documented procedures. A4.14-2 A list of all Security Incidents registered at the management tool during audit period was requested and a sample was randomly selected. A1.14-3 Inspect a sample Security Incidents to ascertain whether problems have been assigned starting and resolution date, assigned an owner or problem responsible, categorized and classified (type and priority), investigated to find root cause, and solved and closed in a timely manner.	No exceptions noted.

Control ID	Control Area	Control Description	Description of Test Performed	Test Result
Control Objective 5: Controls provide reasonable assurance that new Edicom Cloud installations support business requirements and are tested, validated and authorized prior to being moved to production.				
A5.1	**Edicom Cloud Service Installation**	Edicom Cloud service new installations are performed according to a defined development life cycle methodology. *See section 3.4.3.1 for the description of related systems and controls.*	A5.1-1 Interview with the Change Management responsible of the Consulting department. Inquiry about Edicom Cloud installation processes and documented procedures. A5.1-2 Interview with the Change Management responsible of the Consulting department. Inquiry about how Edicom Cloud installation process is registered in EDICOM's management tool. The installation tasks performed contain: requirements identification and formally documented, client's requirements acceptance, documentation of tasks performed during the project and their tests, client acceptance of the solution, delivering date, project closure report has been sent to Client. A5.1-3 Interview with the Change Management responsible of the Consulting department. Inquiry about rollback procedures.	No exceptions noted.
A5.2	**Edicom Cloud Service Installation**	Requirements are formally documented and approved by the external Client. *See section 3.4.3.1 for the description of related systems and controls.*	A5.2-1 Interview with the Change Management responsible of the Consulting department. A list of all Edicom Cloud installations performed to Clients for the audit period was requested and a sample randomly selected. A5.2-2 Inspect a sample of Edicom Cloud installations to Clients to ascertain whether:	No exceptions noted.

Control ID	Control Area	Control Description	Description of Test Performed	Test Result
			• Requirements have been identified at the beginning of installation, and they are formally documented and communicated to the clients for their approval.	
A5.3	**Edicom Cloud Service Installation**	Changes are tested before being released in the production environment. The results of software tests are documented. *See section 3.4.3.1 for the description of related systems and controls.*	A5.3-1 Inspect a sample of Edicom Cloud installations to Clients to ascertain: • Tests have been performed before deployment in production environment and results have been documented on the management tool. A5.3-2 A list of all the Quality department test Checklists was requested and a sample was randomly selected to confirm that the Consulting department uses this Checklist to perform a preliminary test before transferring the Edicom Cloud installation task to the Quality department so they can perform the quality tests.	No exceptions noted.
A5.4	**Edicom Cloud Service Installation**	Software release dates are agreed with the Client. Installation task is closed jointly with Clients' acceptance. *See section 3.4.3.1 for the description of related systems and controls.*	A5.4-1 Inspect a sample of Edicom Cloud installations to Clients to ascertain whether: • EDICOM and Client have agreed a delivery date. • Installation task has been closed once the Client approves the installation results or after some time without client response, and a project closure report has been sent to the Client.	No exceptions noted.

Control ID	Control Area	Control Description	Description of Test Performed	Test Result
Control Objective 6: Controls provide reasonable assurance that new Edicom Cloud developments support business requirements and are tested, validated and authorized prior to being moved to production.				
A6.1	**Edicom Cloud Service Provision**	Edicom Cloud service new developments are performed according to a software development life cycle methodology. *See section 3.4.3.2 for the description of related systems and controls.*	A6.1-1 Interview with the R&D manager. Inquiry about Edicom Cloud software development process and documented procedures. A6.1-2 Interview with the R&D manager. Review of the technical management application employed to manage changes regarding Edicom Cloud. A6.1-3 Inspected a sample of Sprint retrospective meeting reports. A6.1-4 Inspected a sample of software quality monitoring reports.	No exceptions noted.
A6.2	**Edicom Cloud Service Provision**	Requirements are formally documented and approved by internal/external Client. *See section 3.4.3.2 for the description of related systems and controls.*	A6.2-1 A list of all new Edicom Cloud developments performed during audit period was requested and a sample was randomly selected. A6.2-2 Inspect a sample of new Edicom Cloud developments to determine whether: • Requirements have been correctly identified and they are documented. • Tasks have been classified and prioritized in management tool. • Type of change has been registered in management tool.	No exceptions noted.

Control ID	Control Area	Control Description	Description of Test Performed	Test Result
A6.3	**Edicom Cloud Service Provision**	Changes are tested before being released in the production environment. The results of software tests are documented. *See section 3.4.3.2 for the description of related systems and controls.*	A6.3-1 Interview with the Quality and Testing manager. Inquiry about Edicom Cloud testing process and documented procedures. A6.3-2 Inspect a sample of new Edicom Cloud developments to determine whether: • Test have been performed in a testing environment and their results have been registered.	No exceptions noted.
A6.4	**Edicom Cloud Service Provision**	Software developers are not able to modify software in the repository where tested software is stored. *See section 3.4.3.2 for the description of related systems and controls.*	A6.4-1 Interview with the R&D manager. Corroborative inquiry about the update process of the repository of the tested Edicom Cloud software (Artifactory application), including inspection of privileges of Artifactory application. A6.4-2 Interview with the R&D manager. Corroborative inquiry about the update process of the repository of merged Edicom Cloud software (GitLab application), including inspection of privileges of GitLab application.	No exceptions noted.
A6.5	**Edicom Cloud Service Provision**	Only authorized staff is able to promote software to Preproduction environment.	A6.5-1 Interview with R&D manager. Corroborative inquiry about the process of updating Edicom Cloud Preproduction environments with Edicom Cloud software, including inspection of privileges of Jenkins application. A6.5-2 Interview with R&D manager. Corroborative inquiry about the update process of updating Edicom Cloud	No exceptions noted.

Control ID	Control Area	Control Description	Description of Test Performed	Test Result
		See section 3.4.3.2 for the description of related systems and controls.	Preproduction environments with Edicom Cloud software (GitLab application), including inspection of privileges of GitLab application	
A6.6	**Edicom Cloud Service Provision**	Staff which promotes software to production environment is not involved in the development or testing process. *See section 3.4.3.2 for the description of related systems and controls.*	A6.6-1 Interview with the R&D Manager, Edicom Cloud Quality Manager and IT Manager. Corroborative inquiry about the process of updating Edicom Cloud Production environments with Edicom Cloud software, including inspection of accesses and privileges in the Workflow tool used to promote Edicom Cloud software to Production environment.	No exceptions noted.
A6.7	**Edicom Cloud Service Provision**	Changes are approved by management before being released into the production environment. A release management plan to provide for minimum impact on production is prepared for each deployment. *See section 3.4.3.2 for the description of related systems and controls.*	A6.7-1 Interview with the Edicom Cloud Quality Manager and Release Manager. Inquiry about Delivery Management procedure and Edicom Cloud updating procedure. A6.7-2 A list of all changes (new releases) performed during the audit period was requested and a sample randomly selected. A6.7-3 Inspect a sample of changes (new releases) performed during audit period to check: release dates, emails informing clients and EDICOM operators about delivering a new release, a release task is created to manage the process, software deployment is performed in stages, email with incidents occurred during new release process, a	No exceptions noted.

Control ID	Control Area	Control Description	Description of Test Performed	Test Result
			historical of Edicom Cloud software changes is maintained per client.	
A6.8	**Edicom Cloud Service Provision**	Management has prepared a fall-back process to enable the recovery of the original environment in case of incidents during deployment. The access to tools used in the redirection process is restricted. *See section 3.4.3.2 for the description of related systems and controls.*	A6.8-1 Interview with the Edicom Cloud Quality Manager and Release Manager. Corroborative inquiry about the fall-back process. A6.8-2 Interview with the IT Manager. Inspect privileges of the configuration file used to redirect instances in production environment.	No exceptions noted.
Control Objective 7: Controls provide a reasonable assurance to detect risks which could affect to information systems and these risks are treated.				
A7.1	**Risk Assessment**	EDICOM has a methodology and documented procedure available to perform risk assessments. Risk assessments are performed annually to identify relevant risks to information system	A7.1-1 Interview with the IT Manager. Inquiry about the risk assessment process and documented procedure. A7.1-2 Interview with the IT Manager. Corroborative inspection of the latest risk assessment. A7.1-3 Review the report of the last external audit of the Information Security Management System (ISMS), performed by AENOR.	No exceptions noted.

Control ID	Control Area	Control Description	Description of Test Performed	Test Result
		security (including ASP EDIEDICOM Cloud services (EdicomNet) and Certification Authority). *See section 3.4.4.1 for the description of related systems and controls.*		
A7.2	**Risk Assessment**	A Risk Treatment Plan (RTP) must be defined, formally documented and approved by Management. RTP is developed to treat and minimize risks which affect to information systems. *See section 3.4.4.1 for the description of related systems and controls.*	A7.2-1 Interview with the IT Manager. Corroborative inspection of the latest Risk Treatment Plan (RTP) performed and approved.	No exceptions noted.
Control Objective 8: Controls provide a reasonable assurance that EDICOM owns enough mechanisms to guarantee its business continuity.				
A8.1	**Business Continuity Plan**	There is a documented Business Continuity Plan (BCP) which	A8.1-1 Interview with IT Manager. Inquiry about Business Continuity Plan (BCP). Corroborative inspection of the latest version of the BCP.	No exceptions noted.

Control ID	Control Area	Control Description	Description of Test Performed	Test Result
		mainly includes disaster or adverse situations scenarios which could affect EDICOM, including those with an impact on Edicom Cloud and CA. *See section 3.4.4.2 for the description of related systems and controls.*		
CA8.2	**Business Continuity Plan**	The BCP includes a documented Disaster Recovery Plan (DRP) which contains the detailed actions to perform, in case of a disaster, in order to minimize the impact and to restore the normal operations of business processes within adequate timescale. *See section 3.4.4.2 for the description of*	A8.2-1 Interview with the IT Manager. Corroborative inspection of all existing Disaster Recovery Plans (DRP).	No exceptions noted.

Control ID	Control Area	Control Description	Description of Test Performed	Test Result
		related systems and controls.		
A8.3	**Business Continuity Plan**	The BCP and DRP are tested periodically and test procedures and results are formally documented. Both the BCP and DRP are updated as necessary. *See section 3.4.4.2 for the description of related systems and controls.*	A8.3-1 Interview with the IT Manager. Corroborative inspection of the latest DRP's Test Plan and documented tests and results of DRP's.	No exceptions noted.
Control Objective 9: Controls provide a reasonable assurance that EDICOM and its employees treat information, both internal and Client's information, according adequate privacy and confidentiality standards.				
A9.1	**Data Privacy**	EDICOM has defined a security standard, which is mandatory for all the employees in order to guarantee information privacy and confidentiality, of both internal and Client's information. These standards are documented and	A9.1-1 Interview with the DPO. Corroborative inspection of privacy and confidentiality arrangements. A9.1-2 Interview with the DPO. Inquiry about EDICOM's communication procedure to its employees about data privacy security measures.	No exceptions noted.

Control ID	Control Area	Control Description	Description of Test Performed	Test Result
		distributed to EDICOM's personnel. *See section 3.4.4.3 for the description of related systems and controls.*		

Control ID	Control Area	Control Description	Description of Test Performed	Test Result
A9.2	**Data Privacy**	EDICOM performs a data privacy assessment to ensure adequate data privacy measures are implemented so that data privacy and confidentiality, of both internal and Client's information, is guaranteed. Due to the Regulation (EU) 2016/679 General Data Protection Regulation (GDPR) several measures have been put in place by EDICOM to ensure compliance. *See section 3.4.4.3 for the description of related systems and controls.*	A9.2-1 Interview with the DPO. Inspect Records of Processing Activities, Data Protection Impact Assessment, contractual clauses with suppliers and information clauses, Procedures for attention to the rights of the interested party. A9.2-2 Inspect evidences of the assessments performed by the DPO during the period of appliance.	No exceptions noted.

5. Other Relevant Information Provided by EDICOM

The information in this chapter has not been subject to the review mentioned in this report, is only additional information provided by EDICOM.

5.1 Information Security Management System (ISO 27001)

EDICOM has developed an Information Security Management System (ISMS) based on ISO/IEC 27001 standard (ISO/IEC 27001:2017).

The Edicom Cloud and trust services are in the scope of the ISMS and this control framework complies with annual formal audits to obtain certification according to ISO/IEC 27001 standard.

A high-level overview of the ISMS is detailed next:

- An information security risk analysis to identify information security risks has been performed. This analysis is used to prioritize information security initiatives on a risk-based approach.
- An information security policy has been formally approved by Management and is distributed to all employees.
- An information security architecture addressing identified information security risks has been implemented and is currently operated by EDICOM IT staff.
- A set of information security standards and procedures which develop the information security policy have been created and are continuously updated.
- An information security audit calendar has been formally planned and agreed with management. Audits are internal and external and focus on ISMS compliance and specific information security issues like business continuity, privacy and vulnerability assessment.
- A complete application of ISO 27001 Annex A Controls.

5.2 Information Technology Service Management (ISO 20000)

EDICOM has developed an Information Technology Service Management System (ITSMS) based on ISO/IEC 20000-1 standard.

The Edicom Cloud and trust services are in the scope of the ITSMS, and this control framework complies with annual formal audits to obtain certification according to UNE-ISO/IEC 20000-1:2018 standard.

A high-level overview of the ITSMS is detailed next:

- There is a service management policy.

- Management of service level (service level agreement -SLA-) is performed.
- Capacity reports of the systems that support the services to clients are performed.
- The relevant suppliers are monitored for the provision of services to clients.
- Management of customer complaints and continuous evaluation of customer satisfaction is performed.
- Proper management of changes were made in applications and systems.
- An adequate management of the delivery and deployment of new versions of software (Edicom Cloud) is performed.

5.3 Integrated Management System

EDICOM has developed an Integrated Management System (IMS) to address common policies, standards, procedures and controls required by ISO/IEC 27001:2017 and UNE-ISO/IEC 20000-1:2018 standards.

The last successfully passed audit (without any finding) took place on May 9th and May 17th, 2023, and it was conducted by AENOR (www.aenor.com).

5.4 Health Data Host Certification

EDICOM has developed an Integrated Management System (IMS) to address common policies, standards, procedures and controls required by Health Data Host Certification (Hébergeur de Données de Santé - HDS) standards. The scope of this certification covers the information systems that support the installation and operation processes of the Cloud EDICOM LTA HDS trust service.

The last successfully passed audit (without any finding) took place in July 24th, 2023, and it was conducted by AFNOR (www.afnor.org).

5.5 National Security Scheme High Level Certification

EDICOM has been certified in The National Security Scheme, with the requirements of the RD 311/2022 (royal decree) dated May 3rd, which regulates the National Security Scheme in the field of Electronic Administration. It establishes the security policy in the use of electronic media. It applies to the entire public sector and to its private sector technology providers.

EDICOM has set the system category to a high level for the services provided, the categorization has been reviewed during the audit by external auditors.

The last successfully passed audit (without any finding) took place on May 11st 12nd, 15th and 16th, 2023 and it was conducted by AENOR (www.aenor.com) a degree of compliance greater than L4 (90%) was achieved, the report is dated May 18th, 2023.

6. ANNEX 1 Sampling Methodology followed for this Report

The overall sampling approach followed for the work of the ISAE 3402 Type 2 Report (SOC1) is in accordance with the NIA-ES 530 standard, adapted for its application in Spain through the corresponding Resolution of the ICAC.

The sample size for controls in the ISAE 3402 Type 2 Report (SOC1) depends on the characteristics and size of the population for each control, as well as the frequency of its application, and the expected rate of deviation (control deficiency).

In corresponding cases, complete populations within the scope have been requested from EDICOM for those controls for which a sample is requested for testing and validation.

At EDICOM, due to the maturity of the controls, which have been in place for a long time in the entity, and because the entity is subject to a large number of audits that cover to a greater or lesser extent the controls included in this report, it is assumed that there is a moderate risk of deficiencies in the controls.

For controls of higher frequency and/or impact, a statistical sampling has been conducted, selecting a sample of 10% of the population with a maximum of 25 items. For the rest of the controls, sample sizes have been chosen based on the control frequency, as indicated in the following table:

Control frequency	Sampling size to be tested
Daily / couple times per day	10% of the population, with a maximum of 25 items.
Weekly	5
Monthly	2
Quarterly	2
Annual, Biannual	1
Continuous (always working)	1

Finally, the samples obtained for the different SOC1 tested controls have been taken from period August 1, 2022, to July 31, 2023.

It should be noted that, in some specific cases, at the auditor's discretion, samples from other audits conducted in the entity during the same period could be used.

7. ANNEX 2 AUREN Auditors that prepared this report

Below is detailed AUREN team which have participated in this report:

Francisco Mondragón – Financial Auditing Partner

- Bachelor's degree in Business Administration and Management. Universidad de Valencia.
- Business Studies. University of Nottingham, UK (interchange program "Erasmus")
- Chartered Accountant of ROAC (Official Accounts Auditors Charter).
- **He has 22 years of experience in the field of financial and accounting audits, during these years he has closely collaborated with IT audit teams to review the systems that support the financial data and reports.**
- Financial Auditing Partner at AUREN.
- Highly experienced in internal control reviews (SOX).
- He has worked as a finance auditing manager for leading companies in the field of banking, logistics, automotive and construction.
- Organization and supervision of computer audits assisting Financial Audits: Business Processes review as well as Technological Environment and Information Systems.
- Planning and managing audit teams.

José Miguel Cardona – Project Director, IT Consulting Partner

- Telecommunications Engineer from Universidad Politécnica de Valencia.
- Computer Security Master from UOC (Universitat Oberta de Catalunya).
- Computer Systems Expert Witness.
- CISA, CISSP, CRISC, CISM, ITIL Foundation v3, IRCA Lead Auditor 27001, IRCA Lead Auditor 20000, AMBCI (BS 25999) by Business Continuity Institute, Project Management – PMBOK, Lead Implementer ISO 22301 PECB.
- **He has 21 years of experience in the field of Information and Communication Systems, which more than 17 years specifically in Computer Systems Audits and consulting in Information Security.**
- **He has experience since 01/2005 on Webtrust for Certification Authorities, Baseline Requirements y Extended Validation and since 07/2014 on advisory for eIDAS compliance.**
- IT Security Partner and Director at AUREN.
- He has managed and executed projects about Business Continuity, Security Master Plans, Spanish legislation for Information Security in Public

Administrations (RD 3/2010 –ENS- and RD 4/2010 –ENI-), ISO/IEC 27001:2013, ISO 20000, Auditing and Consulting about Personal Data Protection, etc. assisting to multiple sectors such as financial, assurance, pharma, automotive and distribution industry, etc.

- High experience performing security audits on several systems (AS/400, UNIX, OS/390, Microsoft environments, etc.) and ERPs (SAP R/3, Navision Financials, BAAN, Oracle Applications, etc.), in different sectors such as banking, transport, assurance, industry, services, etc.

José Manuel Barrios – QA and Methodological Advisor - Director

- Computer Engineer from Universidad Politécnica de Valencia.
- DPD Certificate by AEPD (Agencia Española de Protección de Datos) schema.
- CISA, ISO 27001 e ISO 20000 Lead Auditor.
- **He has 21 years of experience in the field of Information and Communication Systems, specifically in Computer Systems Audits and consulting in Information Security.**
- IT Security Manager at AUREN
- ICT Systems Consultor/Auditor (ISO 27001, ISO 20000, ISO 22301, ISO 38500), and ISO 9001 applied to ICT.
- Participation on several projects about Business Continuity Plans and DRPs, as well as the testing performance (BS25999, ISO 22301).
- High experience on SAS70 / ISAE 3402 (SOC1), SOC2 projects.
- Expert on computer audits assisting Financial Audits: Business Processes review as well as Technological Environment and Information Systems.
- Performance of IT controls testing projects.
- Performance of adjustments projects and Personal Data Protection audits to several public administrations and private companies as well as Multinational Corporation.

Felipe García – Senior Auditor - Manager

- Information Technology from Universidad de Sevilla.
- CISM, CISA, SAP GRC, ITIL, CSX-F.
- **He has 10 years of experience in the field of Information Security, specifically in Computer Systems Audits and Consulting.**

- ICT Systems Consultor/Auditor (ISO 27001, ISO 20000, ISO 22301, ISO 38500), and ISO 9001 applied to ICT.
- High experience on SAS70 / ISAE 3402 (SOC1), SOC2 projects.
- Performance of IT controls testing projects.
- Participation on several projects about Business Continuity Plans and DRPs.
- Expert on computer audits assisting Financial Audits: SAP environments.

Information Security Auditors

A team of Information Security Auditors from **auren** with specific relevant training and experience in this type of work has participated in the execution of the audit.

8. ANNEX 3 AUREN presentation and services

auren
TOGETHER FOR YOUR SUCCESS

We help you grow

AUDIT & ASSURANCE
CONSULTING
CORPORATE FINANCE
LEGAL

auren.com

Wide coverage

Professional support in over 70 countries

Companies compete in a global market and need professional support in any country where professional opportunities might appear.

In Auren, this approach is clear for us. With the experience due to our presence with our membership in Antea, Alliance of Independent Firms, with coverage in over 70 countries. We understand and serve all international needs of our customers in a full coordinated way.

Our membership in the Forum of Firms, driven by the Transnational Audit Committee IFAC International Federation of Accountants, ensures compliance with the highest standards of quality.

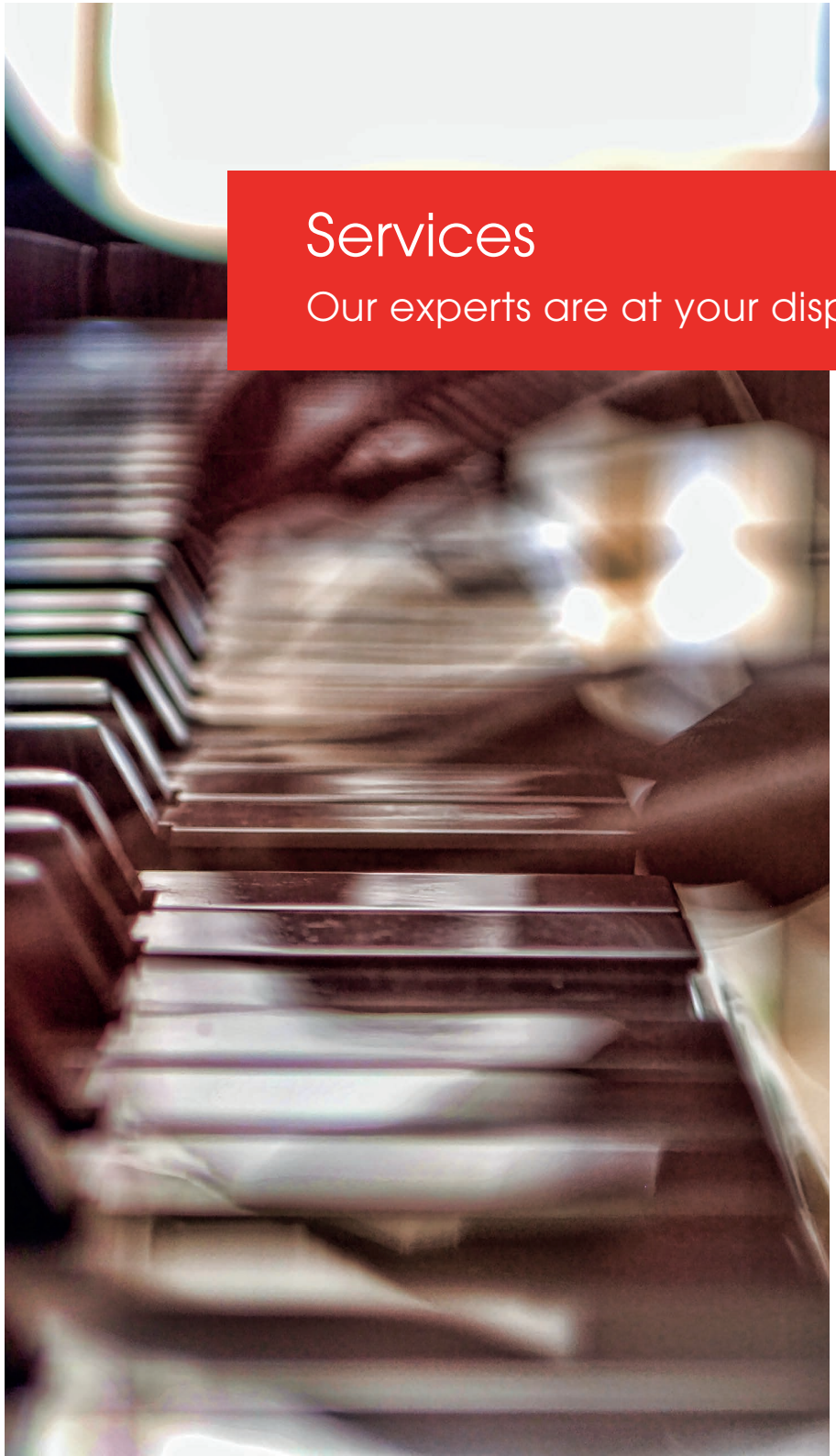
Our clients

Flexibility is one of our attributtes

We are the keystone of the work we perform. Through ongoing collaboration, we create efficient beneficial relationships. All the clients with which we work, regardless of their size, sector or activity, are unique and equally important.

We work to understand their needs, generate trust, provide solutions and help them create the value they need in order to succeed.

Being recommended by a client is our greatest achievement. As a result, each day we try to satisfy and meet the objective of the more than 20,000 clients we have worldwide.



Services

Our experts are at your disposal

Our multidisciplinary nature and experience in sharing projects among different specialists render our actions highly operational, offering services from a global perspective of high quality.

Audit & Assurance
We offer the highest quality through a process of ongoing innovation.

Consulting
We provide solutions with an experienced team focused on obtaining effective results.

Corporate Finance
We provide personalised financial advice on mergers and acquisitions and financial transactions.

Legal
We guarantee peace of mind for companies in the complex environment of legal and tax regulations.

Audit & Assurance

We offer the highest quality through a process of ongoing innovation

The world of financial auditing is changing quickly. At Auren we are in a constant state of innovation in order to offer our clients the best quality at the best price.

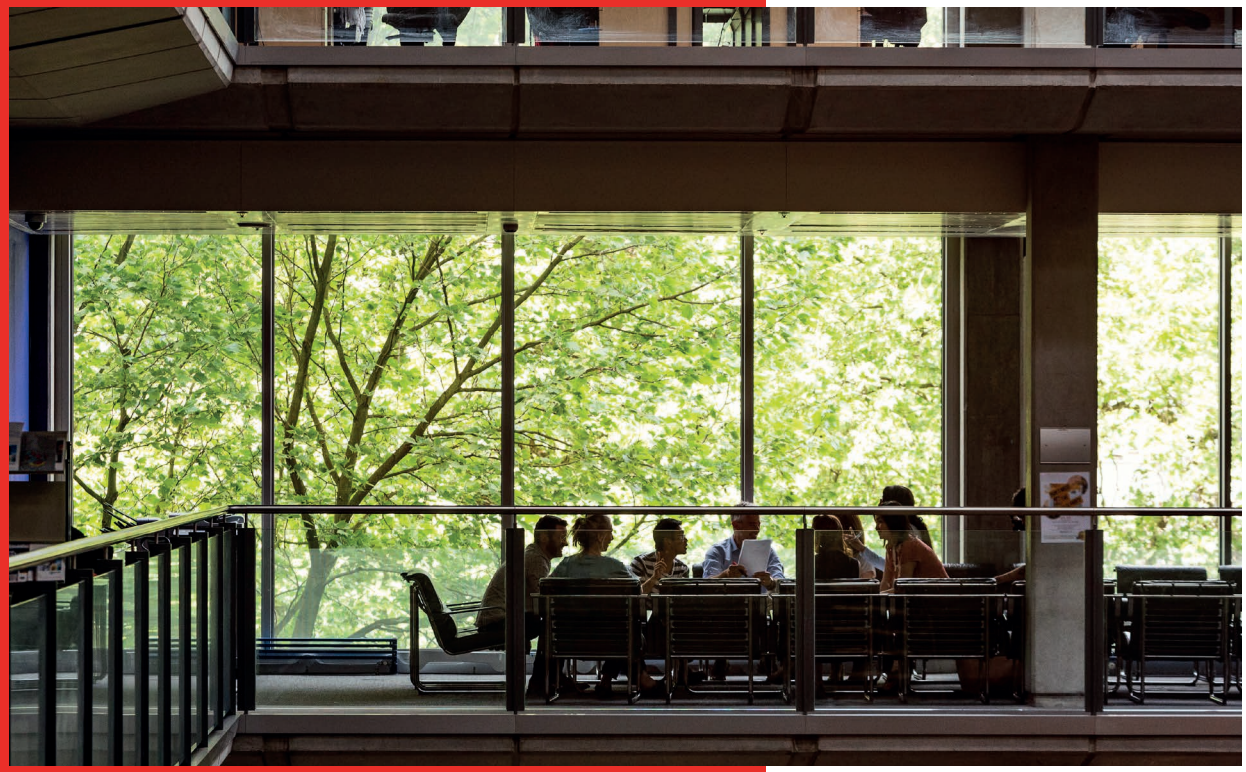
Our quality control system meets the International Standards on Auditing, and Auren is one of the few firms worldwide to have been admitted to the prestigious Forum Of Firms (Transnational Auditors Committee – IFAC). This guarantees compliance with the strictest quality control levels, and in fact Auren has been recognised for years as a standard setter in the field of auditing.

Our audit reports ensure the corresponding interested parties (shareholders, credit institutions, customers, suppliers, employees, regulators, etc.) trust your company's accounts.

Our professionals have specific knowledge of the business and extensive experience in the field of auditing and assurance. We believe that investing in continuing professional development is essential in this sector.

Consulting

We provide solutions with an experienced team focused on obtaining effective results



We provide solutions by working closely with your company using the teams necessary to achieve excellent results.

Our experienced consultants are accustomed to working in complex environments, building on their experience in comparable companies to make the process easier, while controlling the costs of each situation.

We are innovative, experienced and focused on obtaining effective results. Whether you need advice on personnel, IT, organisational or structural matters, to name but a few, our consultancy services will measure up to your expectations.

Our economists, engineers, psychologists, IT experts and other professionals are ready to provide you with the most suitable solution, using a multidisciplinary approach to ensure its effectiveness.

Corporate Finance

We provide personalised financial advice on mergers and acquisitions and financial transactions

We are a leading firm in the field of financial advice and corporate operations. We provide comprehensive support in transactions related to the sale and purchase of companies and businesses. We have a multidisciplinary team of professionals highly specialised in mergers and acquisitions, debt restructuring, financing operations (debt and capital), business valuations, etc.

Our collaboration starts by identifying client needs, creating a strategic plan, rigorously analysing the situation of the business, studying the sector, locating opportunities for investment/ divestment and negotiating and advising on the transaction and its closure.

Aware of the strategic importance of any corporate decision, we assist businesses by giving the utmost professional commitment. We ensure total confidentiality and discretion in all matters we handle. Our professionals have the expertise and experience required to provide this service.

Legal

Our experts provide peace of mind through knowledge and experience

In the complex area of legal and tax regulations, being able to find the best solutions guarantees the peace of mind your company needs.

Our intention is to comply with the law while incurring the lowest costs possible. The difference between simple or excellent advice can mean a great deal to a company, and this is achieved through the knowledge and experience of strong multidisciplinary teams with in-depth knowledge of all regulatory matters.

We interact with our clients to provide them with the most suitable solution, however simple or complex.

Industries

Change offers opportunities and potential. Take advantage of our specific solutions

Each sector of activity has its own features, and we are aware of this at Auren. This is why we coordinate professionals with experience and in-depth knowledge of each sector, guaranteeing the most suitable solution for your company.

We assist our clients by providing a multidisciplinary professional focus, always considering any factors that might affect any decisions to be taken.

We are recognised leaders in several key sectors in the territories where we are present.

360 Solutions

We have a multidisciplinary team of specialists

At present, issues that companies have are complex, interconnected and global. Therefore, they need coordinated services which, with a 360 degree vision, offer solutions with tangible added value.

Auren has always been committed to a multidisciplinary approach, and is therefore one of the few firms on the market capable of offering a 360 solutions.

The partners that Auren chooses for coordinating these services have the holistic vision needed in order to keep a line of permanent direct dialogue open with each client, and to propose case-by-case solutions through the most suitable teams of professionals.

Our values

Honesty and transparency are part of our culture

We defend values which characterise us as a firm, including both those related to our professional activity and those related to ethics, independence, objectivity and professional competence, not forgetting any others showing a personal way of doing things: proximity, proactivity, innovation and being solution-oriented, providing our clients with value.

Proximity
We work closely with clients. We are characterised by our flexibility and permanent availability. We are proactively committed to them.

Innovation
Auren is an innovating firm in the provision of our services, by improving processes and implementing the latest technology. We know the world is in a continual state of change, and we adapt to this.

Multidisciplinary nature and specialisation
We are aware of the growing complexity of the business world, and its global nature. Therefore, Auren has specialised teams in various financial sectors and types of organisations, and we deal with problems from a multidisciplinary perspective: legal, tax, financial, organisational, human resources, etc.

Quality
We guarantee the pursuit of excellence through the qualifications and experience of our professional teams, implementing rigorous and efficient work methods.

Professional ethics
All our actions are performed subject to objectivity, independence of opinion and confidentiality. Our code of conduct represents a commitment and guarantee of the honesty that form part of the culture of Auren.

We contribute value
Our clients seek solutions and appreciate the added value we are able to provide them.

Corporate Social Responsibility

A lot of small things become something big

Professional firms contribute to the general interest of society through their actions. At Auren, we assume the undertaking to collaborate with the economic development of society on ethical bases fostering people's welfare, based on a more prosperous, more just and more sustainable society respectful of human dignity.

In our daily work, we consider the interests of partners and employees, clients, suppliers and other interest groups. We wish to have a positive interest on society and reinforce the common good, seeking the balanced development of people and their environment.

Auren is committed to the Sustainable Development Goals to achieve a better and more sustainable future for all. The 17 Goals were adopted by all UN Member States as part of the 2030 Agenda for Sustainable Development which set out a 15-year plan to achieve the Goals.

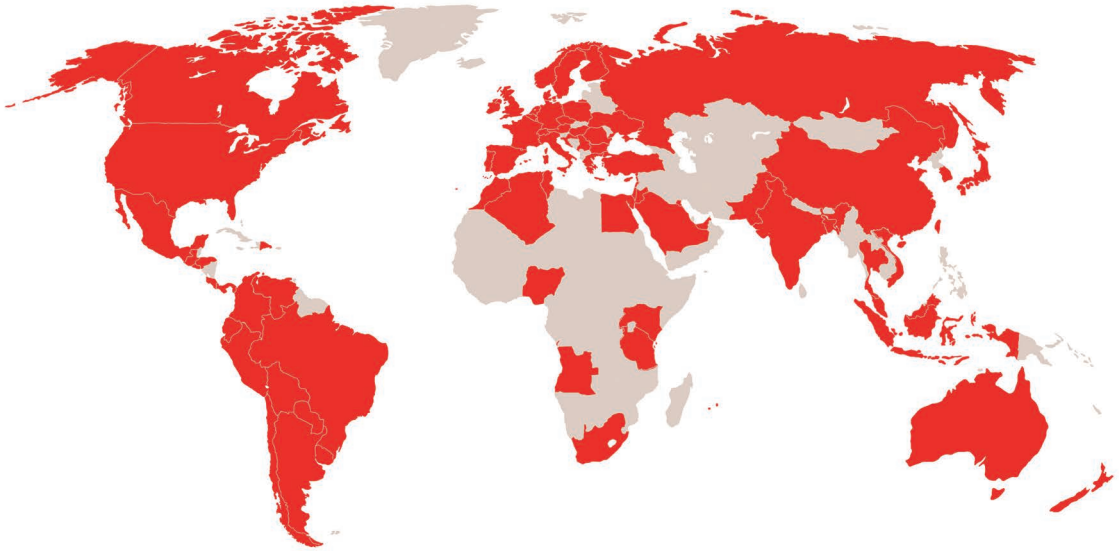
EUROPE
Andorra
Austria
Belgium
Bulgaria
Croatia
Cyprus
Czech Republic
Denmark
Finland
France
Germany
Greece
Hungary
Ireland
Italy
Luxembourg
Malta
Montenegro
Norway
Poland
Portugal
Romania
Russia
Serbia
Spain
Sweden
Switzerland
The Netherlands
Ukraine
United Kingdom

AMERICA
Argentina
Bolivia
Brazil
Canada
Chile
Colombia
Costa Rica
Dominican Republic
Ecuador
El Salvador
Guatemala
Honduras
Mexico
Panama
Paraguay
Peru
Uruguay
USA
Venezuela

MIDDLE EAST AND AFRICA
Algeria
Angola
Egypt
Israel
Jordan
Kenya
Kuwait
Lebanon
Mauricio
Morocco
Nigeria
Saudi Arabia
South Africa
Tanzania
Tunisia
Turkey
UAE
Uganda

ASIA-PACIFIC
Australia
Bangladesh
China
India
Indonesia
Japan
Malaysia
New Zealand
Pakistan
Singapore
South Korea
Thailand
Vietnam

auren ■ Antea Alliance of independent firms ■ ASSOCIATES ■



AUREN AROUND THE WORLD

auren

auren.com

A CORUÑA
lcg@auren.es
+34 981 908 229

ALICANTE
alc@auren.es
+34 965 208 000

BARCELONA
bcn@auren.es
+34 932 155 989

BILBAO
bio@auren.es
+34 946 071 515

CARTAGENA
sjv@auren.es
+34 968 120 382

LAS PALMAS DE GRAN CANARIA
lpa@auren.es
Asesores
+34 928 260 777
Auditores
+34 928 373 506

MADRID
mad@auren.es
+34 912 037 400

MÁLAGA
agp@auren.es
+34 952 127 000

MURCIA
sjv@auren.es
+34 968 231 125

PALMA
pmi@auren.es
Asesores
+34 971 710 047
Auditores
+34 971 725 772

SEVILLA
svq@auren.es
+34 954 286 096

VALENCIA
vlc@auren.es
+34 963 664 050

VALLADOLID
vll@auren.es
+34 983 379 048

VIGO
vgo@auren.es
+34 986 436 922

ZARAGOZA
zaz@auren.es
+34 976 468 010

MEMBER OF THE FORUM OF FIRMS

Member of Antea Alliance of independent firms