



**Report on Controls Placed in Operation at EDICOM**

**As of July 31, 2009**

**Table of Contents**

SECTION ONE .....	3
INDEPENDENT SERVICE AUDITOR’S REPORT .....	3
SECTION II.....	6
DESCRIPTION OF CONTROLS PROVIDED BY EDICOM.....	6
Description of Controls Provided by Edicom.....	7
Purpose of the Service Auditor’s Report.....	7
Edicom Overview.....	7
The Control Objectives.....	8
Relevant Aspects of the Internal Control Environment .....	8
SECTION III .....	12
INFORMATION PROVIDED BY THE SERVICE AUDITOR .....	12
Manage Service Levels.....	13
Manage Change.....	13
Manage Security.....	18
Computer Operations .....	23
SECTION IV .....	28
OTHER INFORMATION PROVIDED BY EDICOM .....	28
Business Continuity Planning for the Enterprise .....	29
ISO/IEC 27001 Certification .....	30



**SECTION ONE**  
**INDEPENDENT SERVICE AUDITOR'S REPORT**

## **Independent Service Auditor's Report**

To the Board of Directors of Intercambio Electrónico de Datos y Comunicaciones, S.L. (Edicom):

We have examined the accompanying description of controls of Edicom and the related ASP EDI service. Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of Edicom's controls that may be relevant to a user organization's internal control as it relates to an audit of financial statements, (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily, and (3) such controls had been placed in operation as of July 31, 2009. The control objectives were specified by the management of Edicom. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

We did not perform procedures to determine the operating effectiveness of controls for any period. Accordingly, we express no opinion on the operating effectiveness of any aspects of Edicom's controls, individually or in the aggregate.

In our opinion, the accompanying description of the aforementioned application presents fairly, in all material respects, the relevant aspects of Edicom's controls that had been placed in operation as of July 31, 2009. Also, in our opinion, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily.

The description of controls at Edicom is as of July 31, 2009 and any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specific controls at the Service Organization is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that changes may alter the validity of such conclusions.



Ernst&Young LLP  
Torre Picasso  
Plaza Pablo Ruiz Picasso  
28020 Madrid

Tel: 91 572 72 00

[www.ey.com/es](http://www.ey.com/es)

This report is intended solely for use by the management of Edicom, its customers, and the independent auditors of its customers.

*Ernst + Young LLP*

July 31, 2009



**SECTION II**  
**DESCRIPTION OF CONTROLS PROVIDED BY**  
**EDICOM**

## **Description of Controls Provided by Edicom**

### **Purpose of the Service Auditor's Report**

The following description is intended to provide user organizations and the independent auditors of user organizations with information about the control objectives of Edicom and the information technology (IT) general control activities performed by Edicom. Specifically, it is to provide sufficient information for the independent auditors of user organizations to obtain an understanding of Edicom's system of internal control to plan their audits. This report was prepared in accordance with the guidance contained in the American Institute of Certified Public Accountants' Statement on Auditing Standards (SAS) No. 70, "Service Organizations", its amendments and interpretations.

Edicom's description of controls has also been prepared to enable relevant user organizations to gain an understanding of Edicom's control activities for purposes of assisting management in their assessment of internal controls over financial reporting in accordance with Section 404 of the Sarbanes-Oxley Act and the Public Company Accounting Oversight Board's (PCAOB) Auditing Standard No. 5 (AS 5).

While the description is intended to focus on the control activities that may be relevant to the internal control structure of Edicom's user organizations, it does not encompass all aspects of the services provided by Edicom.

### **Edicom Overview**

Edicom is a company dedicated to the development and implantation of high performance business-to-business (B2B) transaction systems.

Specialists in consulting and EDI software development (applications and processes) and data integration (XML, EDIFACT, X12, XBRL, etc.), with their own Value Added Network SEDEB2B for secure information transfer, as well as solutions in the field of Continuous Replenishment (CRP) and Traceability.

Edicom dedicates an important part of its resources to research and development of new communications solutions and how to implement the latest technological breakthroughs. The Edicom catalogue covers a wide range of possibilities to deal with any project, independently of the type of partner, volume or size of the client.

With a clear client-centred focus, Edicom has reached a position as provider of communications services to businesses of acknowledged prestige in several sectors where electronic transactions and information technologies are key factors in their commercial and financial activities. Ever since its creation, Edicom has undergone a

very significant sustained growth in terms of client figures, human resources and business volume. This growth has favored expansion to other countries, with the result that Edicom is now present in Spain, France, Italy, United States, Mexico and Argentina. Edicom home page is [www.edicomgroup.com](http://www.edicomgroup.com).

## **The Control Objectives**

Using the COBIT Framework, the Information Technology Governance Institute (“ITGI”) has established control objectives it feels are relevant to organizations as they contemplate Sarbanes-Oxley. Edicom has opted to follow many of the control objectives and figures as outlined by the ITGI, since its membership includes many of the public accounting firms that will read and perhaps rely upon the information contained in this report. Edicom has provided a cross reference (the number behind the objective refers to the figure supplied by the ITGI) to the objectives back to the ITGI guidance that was issued in 2006. Because of redundancy, Edicom has combined some of the control objectives to make it easier for the user to read the report.

## **Client Control Considerations**

The client must evaluate its system of internal controls and management of risks. Since the controls highlighted in this report occur at the Edicom facilities supporting the client outsourcing arrangement and the report only covers a portion of a comprehensive internal control structure, the client must address aspects of the internal control structure that are controlled at their location. This section of the description highlights those portions of the internal control structure where the client may have responsibility to develop and maintain. Reference each individual section of control objectives for important considerations unique for each area. The Client control considerations presented should not be regarded as a comprehensive list of all controls that should be employed by the Client.

## **Relevant Aspects of the Internal Control Environment**

The most widely used framework for internal control for organizations was developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). The key elements of the COSO model are control environment, risk assessment, monitoring, information and communication, and control activities. Edicom has processes in place for each of these key elements to help ensure that operations and entity level controls are effective.

### **Control Environment**

Edicom’s internal control environment reflects the overall attitude, awareness, and actions of management concerning the importance of control and the emphasis given

to controls in the company's policies, procedures, methods, and organizational structure. The following is a description of the key components of Edicom's internal control environment:

#### *Board of Directors*

The Board of Directors is responsible for providing governance and oversight over the strategy, operations and management of Edicom. The Board of Directors is also responsible for approving the corporate security policies and procedures.

#### *Security Committee*

The Security Committee is integrated by Management, the Security Responsible and the Managers of the main areas of the organization. The Security Committee will have annual meetings and is responsible for giving advice to Management regarding security issues. The Security Committee is also responsible for coordinating the periodical reviews and audits and making sure corrective actions are implemented.

#### *Organizational Structure*

The organizational structure of Edicom, which provides the overall framework for planning, directing, and controlling operations, has segregated personnel and business functions into departments according to job responsibilities. This approach allows the organization to clearly define responsibilities, lines of reporting, and communication and allows employees to focus on the specific business issues impacting Edicom's clients.

#### *Managing Controls*

Edicom's management is responsible for directing and controlling operations and for establishing, communicating, and monitoring control policies and procedures. Importance is placed on maintaining sound internal controls and the integrity and ethical values of Edicom personnel. Organization values and behavioral standards are communicated to personnel through policy statements and formal codes of conduct.

#### *Policies and Procedures*

Edicom has developed formal policies and procedures concerning various aspects, including network configuration, application and system software change control, application development, logical access, computer operations, hiring, training/development, performance, appraisals and terminations.

### **Risk Assessment and Monitoring**

#### *Risk Assessment*

Edicom has placed into operation a risk assessment and audit planning process to identify and manage risks that could affect their operation and their ability to provide service to clients. The risk assessment is to be updated on an annual basis and appropriate measures are implemented to address risks detected. This may include revising control procedures, implementing additional control procedures or conducting additional internal audit projects.

### *Monitoring*

Edicom management and technical personnel monitor the quality of the service as a routine part of their activities. To assist them in this monitoring Edicom has defined a series of key performance indicators which are measured on a daily basis by the affected departments. There are monthly meetings held among the Technical Managers where service level performance is reviewed and discussed. Appropriate levels of management review metrics reports on a monthly basis and if necessary corrective actions are put in place.

Monitoring for potential failures in the service provision is also performed by the 24x7 Department and the IS Department. Edicom uses a variety of tools and reports to assist in monitoring the infrastructure environment. Several software tools are utilized in the daily monitoring of server performance and availability.

### **Information and Communication**

Edicom has implemented various methods of communication to help ensure that all employees understand their individual roles and responsibilities over transaction processing and controls and to help ensure that significant events are communicated in a timely manner. These methods include orientation and training programs for newly hired employees, the use of electronic mail messages to communicate time-sensitive messages and information and the use of online policies and procedures. Management encourages frequent staff meetings and open communication at all levels.

Edicom has also implemented methods of communication to help ensure that clients understand their roles and responsibilities, and that significant changes are communicated to clients in a timely manner. During on going tasks each client is assigned a contact person at the company to facilitate communication with Edicom internal resources. For those Clients with extended service contract a contact person in Edicom is available on a permanent basis. Clients are encouraged to communicate questions and problems to Edicom, and such matters are logged and tracked until resolved, with the resolution also reported to the client.

### **Control Activities**

Control activities are the policies, procedures and practices that are put into place to help ensure that business objectives are achieved and risk mitigation strategies are

carried out. Control activities are developed to specifically address each control objective to mitigate the risks identified. The following section, Controls Overview, includes the control activities identified and implemented by Edicom on behalf or in conjunction with its customers.



**SECTION III**  
**INFORMATION PROVIDED BY THE SERVICE**  
**AUDITOR**

## **Overview of Control Objectives and Related Controls**

Controls listed below are specified by Edicom. Detailed descriptions of controls can be found as referenced below. Client control considerations are listed within each control objective section.

### **Manage Service Levels**

**Control Objective 1:** Controls provide reasonable assurance that:

1. Service levels are defined and managed in a manner that satisfies operating requirements and provides a common understanding of performance levels by which the quality of services will be measured. (Figure 20).

#### **Policies and procedures**

As part of the contracting phase, Clients and Edicom develop formal service level agreements for the services provided by Edicom. There is a standard Service Level Agreement where service levels are defined for generic Clients. In case Clients may need specific service level requirements they can be negotiated and included in the SLA. During the contracting phase Clients and Edicom also define the outsourcing requirements of the client to be included in the contract in case this type of service is contracted. Both parties will approve the service levels and on a periodic basis, Edicom will report as to their performance of the services.

There are also key performance indicators defined which are managed and monitored on a daily basis by the different departments involved in the provision of the service. Periodic meetings are held internally where service levels are discussed and corrective actions put in place in case of any deviations detected. These performance indicators are managed and monitored for each client.

#### **Client Control Considerations**

- The Client is responsible for evaluating and monitoring Edicom's delivery of service to ensure conformity with contractual obligations.

### **Manage Change**

**Control Objectives 2, 3, 4 & 5:** Controls provide reasonable assurance that:

2. Technology infrastructure is acquired so that it provides the appropriate platforms to support the operating applications (Figure 15),
3. Policies and procedures that define required acquisition and maintenance processes have been developed and are maintained, and that they define the

documentation needed to support the proper use of the applications and the technological solutions put in place (Figure 17),

4. The systems changes are authorized, appropriately tested and validated prior to being placed into production processes and that associated controls operate as intended and support the operating requirements (Figure 18 and 19).

5. Controls provide reasonable assurance that necessary modifications to the existing production environment are implemented within the timeframes required by documented policies and procedures.

There are two possible scenarios in the manage change process:

1. Installation of a new client in the EDI ASP.
2. Changes to infrastructure and software supporting EDI ASP.

#### *1. Installation of a new client in the ASP*

Commercial agents register installation requests in a special tool to record and track the requests. The request log is reviewed on a daily basis by the Consultancy Department Team Leads who assign each request to a Senior Consultant. The Senior Consultant contacts the client to identify client key contacts and obtain additional information required for the installation process. An evaluation is performed of the volume of the client in order to determine in which ASP group the client should be installed. This is especially important for clients with extended or outsourcing service since their service requirements are greater.

As well as this during the first contact with the client the Senior Consultant asks for a preferred deadline in order to adjust to the client demands. Client demands are registered in the tool and there is a compromise that will be met taking into account that the client timely provides all the information required by the Senior Consultant in order to perform the installation.

A formalized methodology exists for the ASP installations. Once the Senior Consultant obtains all the requirements for the new installation a request is made to the 24x7 Department for the set up of the client environment in the corresponding ASP group. Usually client environment setup is performed at the weekends in order to minimize the impact on the ASP service. When the client environment is created the Senior Consultant begins the integration process.

There is a formalized testing strategy for the integration process. The integration process is performed by the Senior Consultant in collaboration with the client. In order for the Senior Consultant to be able to perform the integration process the client must have performed a number of tasks which have been previously informed to the client. The integration process involves a number of validations, tests and communications between the Senior Consultant and the client that go on until the process runs smoothly and without errors.

When integration is finished the Senior Consultant assigns the parameterization and final installation tasks to a Technician. The Senior Consultant provides the Technician with all necessary information so that he can perform the tasks assigned correctly. The Technician contacts the client to confirm installation dates previously agreed and finishes the installation accordingly.

There is a formalized testing strategy for the final installation process. The Technician performs a complete set of communication and integration tests. The integration testing procedures at this stage include the whole communication path thus ensuring that data exchange is performed correctly and data remains accurate, valid and complete during transmission. As a result all installations are tested prior to installation to production.

In a final step the Technician prepares all required documentation about the installation. This documentation is reviewed by the Senior Consultant and if it is complete and accurate and everything has been performed according to the approved policies and procedures the Senior Consultant marks the task as ready to be closed. Before closing the task the Client is required to provide acceptance for the service installation.

During the whole process the client is made aware of the progress of the installation and if any issues arise that may modify the planned schedule for the installation Edicom will work with the client to revise estimates and schedule to help ensure the installation is made according to the client expectations.

All installations follow the installation process that has been defined for submitting requests, approving, testing and implementing to production. During the process the requests are registered in a special tool with all the relevant information about the installation: name of the requestor, relevant dates, tasks progress, etc.

## *2. Changes to infrastructure and software supporting ASP.*

### **Changes to software supporting ASP**

Clients can request changes to the software supporting the ASP service. Change requests are received by the i+D Department Responsible who approves the change and registers it in a tool to record and track the request. The request ticket includes all relevant information about the change. The request is coordinated with other requests by that particular client and, if necessary, re-priorization occurs.

A formalized methodology occurs for making changes. The developer or development team assigned to the change request work on the change in an environment separate from production. Changes are not made directly to the production environment and typically a developer will not have access to the production environment.

The nature of the change and specifications will determine the extent of the testing performed; however all changes are tested prior to implementation to production.

There is a special testing team in Edicom that is responsible for testing all changes. There is a testing strategy for each software module and when a change is implemented the testing team verifies integrity, validity and completion of the data processed within the module. For more specific changes sometimes personnel of the i+D Department may take part in the testing procedures. Once testing is complete and the change is ready to be made permanently, the approval process begins for the change to move to production.

Before the change can be implemented to production it must be approved by the Service Quality Assurance Manager (SQA Manager). Software modules to be released are first received by this person who reviews the changes, checks for the integrity and validity of the software releases and decides whether they should be transported into production. Releases include changes from different clients since ASP software is standard and there are not specific versions of the software for each client.

Once approved, the SQA Manager plans the software release along with the 24x7 Department. There is a formalized release strategy for changes. The release strategy is planned so that new releases are transported to production in specific timeframes and ASP groups are updated progressively in order to minimize impact on the ASP service. All Edicom professionals are properly informed of the releases schedule so that the corresponding ASP groups can be monitored after the release to detect any anomalies. ASP groups containing extended service clients are intensively monitored due to the greater service requirements of this type of clients. There are back out procedures in case it is necessary to restore the previous configuration.

The final implementation to production of changes is performed by the 24x7 Department. Personnel who develop the change will not implement the change into the production environment thus ensuring segregation of duties. Once tested software releases are copied by the testing team to a specific folder that can only be accessed by the SQA Manager. When approved the SQA Manager copies the software release to a different folder that can only be accessed by the 24x7 Department. As a result transport to production can only be performed by the authorized personnel.

### **Infrastructure changes**

Edicom has formalized a process for managing changes to its infrastructure. Changes are documented, reviewed for risk and operating and security requirements evaluated before their acquisition and implementation to production. When feasible changes are tested in a test environment prior to their implementation to production.

### **Client Control Considerations**

- The Client should ensure that a representative participates in or has input to the service installation process, including participation in testing activities, if applicable.
- The Client should provide Edicom all required information on a timely basis during the service installation process as requested by Edicom.
- The Client should perform all required activities on a timely basis during the installation process as requested by Edicom.
- The Client should provide approvals to Edicom detailing that the installation of the service or change requested has been tested and is appropriate for their current operating environment.
- The Client should contact Edicom if they are experiencing problems with the systems supported by Edicom.
- The Client should report any problems experienced after the service has been installed or a change has been implemented by Edicom that affects their processing environment.

## **Manage Security**

**Control Objectives 5 & 6:** Controls provide reasonable assurance that:

6. Controls provide reasonable assurance that operating systems and subsystems are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data (Figure 22).
7. Controls provide reasonable assurance that IT components, as they relate to security and processing, are well protected, would prevent any unauthorized changes, and assist in the verification and recording of the current configuration (Figure 23).

### **Policies and procedures**

Edicom has developed a formal information security policy that has been approved by an appropriate level of executive management. A framework of security standards has also been developed that supports the objectives of the security policy. These policies and procedures are updated on an as needed basis. All Edicom personnel are made aware of the policies and procedures.

### **Logical Security – User Identification and Authentication**

There are two different domains in the company which grant access to different resources:

1. Edicom domain, which grants access to corporate computing environment.
2. ASP domain, which grants access to ASP service resources.

Access to both domains requires users to be identified with a user ID and authenticated with a personal password. Upon starting Edicom employees are assigned an e-mail address and an enterprise user ID and password to gain access to Edicom's network as well as a user ID and password for the ASP network in case it is needed based on the user responsibilities. To accomplish this, there is a web form which is completed by the employee Responsible or the Administration Department. The request is received by the Information Systems Department that before granting access to systems asks for approval to the Administration Department. Once Administration approval is received the IS Department creates the user ID and password for the Edicom domain. In case the employee needs access to ASP resources a user ID and password is also created for this environment. In the web request form all relevant information about the user profile is included so that the IS Department can grant access to the user with the appropriate profile.

Desktop policies like password settings, antivirus scans/updates, prevention of installing unnecessary software, screen saver password protection and other desktop specific controls are enforced using group security policy. Desktop security policies are similar in both domains (Edicom and ASP). Domain passwords are created and

stored on the systems in one-way encrypted form, have an enforced minimum length, are forced to change on a regular basis and are not reusable once they have been changed. After incorrectly entering the password five times, the user ID is locked out for 3 minutes. After a period of inactivity the workstation is locked and requires a password to unlock.

In most situations user IDs are associated with an individual person. There are some circumstances, however, that warrants the use of user IDs that are associated with a function or application. Examples of these are IDs utilized for training purposes and system jobs. Edicom has identified all these generic users which are properly authorized and controlled.

In addition, the following security procedures are in place:

- When granted access the employee has to sign a special clause stating that he has read and accepts the corporate security policy as well as the corporate security procedures.
- The password is forced to be changed as part of the first login.
- If the employee's responsibilities change, the access is modified to make it commensurate with their responsibility.
- In the event of termination access is removed promptly and the procedure is exactly the same as the new user procedure.
- There is a formalized procedure for user access review every six months.

### **Desktop protection**

Edicom manages virus protection at the desktop level using a third party product. The product will detect and clean a desktop file that contains a virus. The product is implemented to perform real-time protection as files are accessed and an automatic scan of each desktop at least once per week. A user has also the ability to perform random scanning. Updates to the antivirus signatures are done on a daily basis and managed through an automatic software distribution. As well as this a personal firewall is installed and operating on Edicom desktops and autoruns executables are disabled for external devices.

### **E-mail Servers**

A software product manages virus protection for Edicom's email messaging servers. Currently mail to and from international Edicom offices and all inbound and outbound mail from the Internet are scanned for viruses and cleaned automatically. A daily log keeps track of all viruses that are found. Updates to the antivirus signature file are done periodically.

### **Servers**

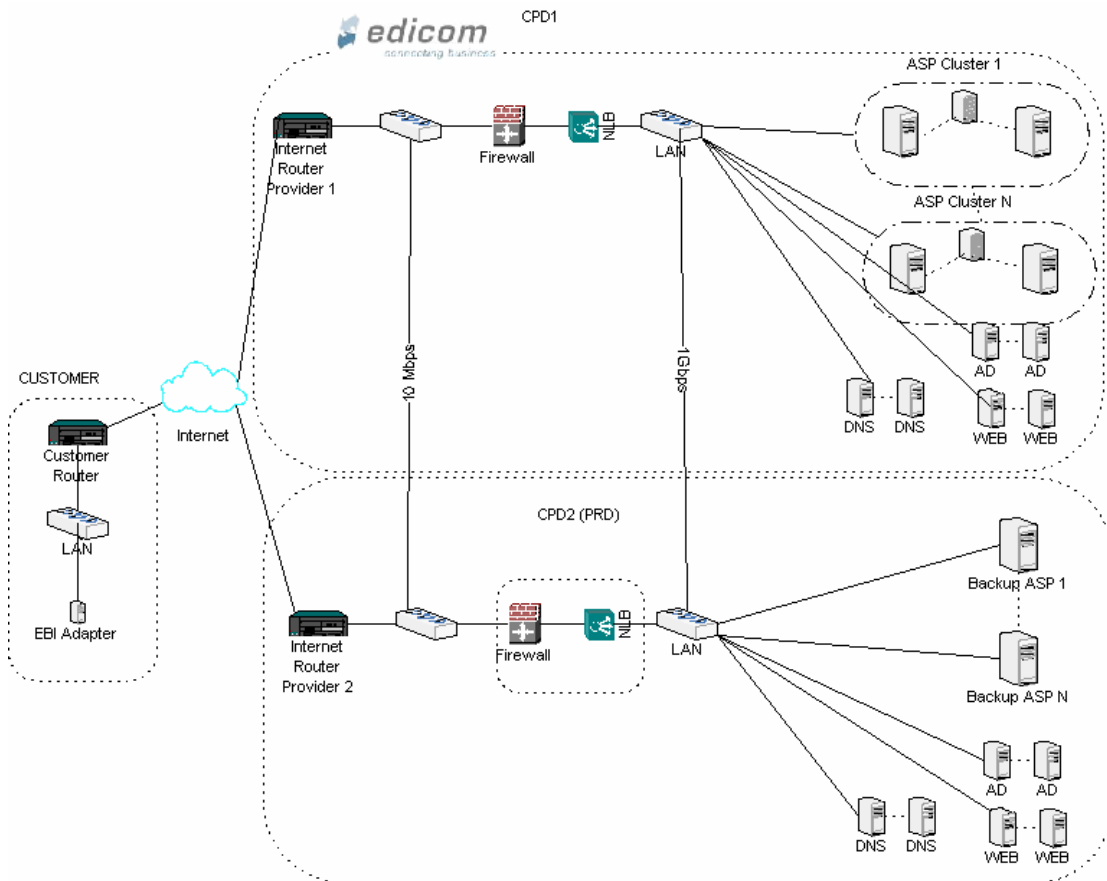
An antivirus software product protects the file and application servers within the Edicom environment. Scans of all servers are done on-line and updates to the antivirus signature files are done on a daily basis.

### Software protection

There are also formalized procedures in the company to prevent the installation of unauthorized software on desktops and servers in Edicom and ASP environments. There is a corporate list of authorized software that is approved by management. There is also a centralized inventory system and on a periodical basis reviews are performed by the IS Department by selecting a sample of desktops and checking if corporate software policies are followed. Any discrepancies are analyzed, investigated and resolved.

### Network security

Communications between clients and Edicom are encrypted using SSL. As well as this Edicom has appropriate network security elements such as firewalls, intrusion detection and vulnerability assessments to prevent unauthorized access via public networks. Firewalls are redundant providing for backup in case of failure of one of the elements. Firewalls logs are periodically monitored by the IS Department to detect potential anomalies and problems.



## **Physical Security**

### *Edicom Data Center*

There are formalized policies and procedures with respect to the physical security of Edicom facilities. These policies and procedures are approved by Senior Management of Edicom. As part of an individual being hired by Edicom, they will undergo a formal background check. This will include an educational verification and reference checks. If the background check comes back with issues or there are performance issues, the person is not offered permanent employment.

The security of the main building where all information systems are located falls under the responsibility of the facilities team. Guards are staffed at nights, 7 days a week and 365 days per year and are positioned at the main entrance of the building which is the unique access point in the building. The security guards are third-party contractors from an outside provider. The facility team is responsible for the maintenance of security monitoring devices such as the closed circuit TV. Surveillance equipment is used to monitor the entry points and various areas within the facility such as the Data Center. Discs produced by this equipment are saved for approximately a week to 30 days, depending on the location. Discs are reviewed on an “as-needed” basis.

The entrance to the main building is protected by a locked door. Visitors must identify themselves and provide a contact person in order to be granted access. Visitors must be accompanied at all times by an authorized person from the company during their visit to the facilities. Entry points into secured areas are controlled with biometric devices and a register of access logs is kept in the access application. Access to secured areas is defined based upon associate job function or, in the case of visitors and vendors, based upon need. Access to restricted areas is granted based upon job responsibilities during the new hires procedure with due authorization by the IT Systems Responsible and access is removed when it is no longer needed.

## **Environmental Safeguards**

The facilities are equipped with smoke and heat detectors for fire detection and a sprinkler system for fire suppression. Hand-held fire extinguishers are available inside and outside the data center. There are not water tanks nearby, overhead pipes or toilet facilities next to the Data Center. As well as this the Data Center is in the second floor of the building so flooding risk is very low.

In the Data Centers where critical computing and communication equipment are located there is an also adequate air conditioning, access to the wiring closets are secure and cabling and equipment is organized and labeled. As well as this critical computing and communication equipment is connected to a UPS battery backup system and a diesel generator. In the event of a power failure, the UPS system will keep the computing and communication equipment running until the system is

switched to the secondary supply (the diesel generator). The UPS and the diesel generators are tested on a periodic basis.

If temperature alarm is triggered the IS Department is informed automatically by means of a monitoring tool and maintenance responsible is sent to investigate and resolve the problem in coordination with the IS Department, including nights and weekends. The rest of the alarms trigger visual and sound alarm signals.

### **COLT Offsite Data Center**

The COLT Offsite Data Center is located in a special building in Valencia, approximately 10 km away from the main data center location. There is no visible indication of what that building is used for. COLT is a data center service provider and as a result the Data Center has all required security measures and certifications to ensure data and information systems integrity and confidentiality. Access to the building is restricted to authorized personnel. Visitors must identify themselves to the security guard at the entrance and access to restricted areas require of proximity badges. There are monitoring and alarm systems which are connected to a security office which monitors the site 24 hours a day and 7 days a week. Motion, fire and water detectors protect the room as part of the alarm system. Maintenance schedules and contracts are in place with third parties for the maintenance of all hardware used in the offsite storage area.

### **Client Control Considerations**

- The Client is responsible for maintaining their own security administrative authority and should have sound security controls, including well-defined user access controls and password policies.
- The Client is responsible for the physical access supporting their internal processing locations.
- The Client is responsible for the maintenance and administration of network or other equipment owned by the Client.

## Computer Operations

**Control Objectives 8, 9 & 10:** Controls provide reasonable assurance that:

8. Any problems and/or incidents are properly responded to, recorded, resolved or investigated for proper resolution (Figure 24).
9. Data recorded, processed and reported remain complete, accurate and valid throughout the update and storage process (Figure 25).
10. Authorized programs are executed as planned and deviations from scheduled processing are identified and investigated, including controls over job scheduling, processing and error monitoring (Figure 26).

### Policies and Procedures

Edicom has developed formal policies and procedures relating to the manage computer operations process. These policies and procedures are approved by Senior Management and updated on an as needed basis. All Edicom personnel are made aware of the policies and procedures.

### Problem and incident management

There are two different incident and problem management systems in the company:

1. Incidents and problems detected by clients and managed by the Client Support Department.
2. Incidents and problems detected and managed by the company.

#### *1. Incidents detected by clients*

The Client Support Department (CAU – Centro de Atención a Usuarios) provides technical support to clients. Clients communicate problems and incidents by telephone or web. There are three different types of service support:

- Standard
- Extended Basic
- Extended

#### *Standard support service:*

The standard support service has a 1<sup>st</sup> level (L1) support team that consists of nine technicians and a 2<sup>nd</sup> level (L2) support team that consists of three technicians. In case none of these support levels can answer the call because they are all busy there is an automatic switchboard that keeps the call on hold. If there are five calls on hold an automatic e-mail is sent to all CAU personnel and a technician belonging to L1 support is assigned to answer calls registered in the switchboard. This technician answers and assigns calls on hold to a L1 or a L2 technician (depending on their

criticality) for their resolution. In case ten calls are on hold in the switchboard two L1 technicians are assigned to answer these calls.

By using this methodology usually every call is answered within a reasonable timeframe even when there are high peak loads. Technicians evaluate the criticality of every call in order to give priority when assigning calls for their resolution.

#### *Extended and Extended Basic support services:*

The Extended Basic support service team consists of three technicians. This service support is targeted at those clients that pay a special fee for this special service but whose incidents and problems are no of special criticality or difficulty.

The Extended support service team consists of eight technicians and as a general rule always one technician must be available. This service support is targeted at those clients that pay a special fee for this special service and whose incidents and problems are critical and with a high level of difficulty.

When an Extended Basic incident cannot be attended it is escalated to the Extended and Standard support teams following this precedence order. Similarly when an Extended incident cannot be attended it is escalated to the Standard support team.

#### *Incident Tool*

A special incident tool is used by CAU for the register and follow-up of incidents and problems till their resolution. The incident tool registers all relevant information about the incident including register and resolution dates which are needed in order to analyze if SLA resolution times agreed are met. There are also different states in the tool for the incidents registered. For instance before closing an incident there is a period of time during which the incident is in “Pending client confirmation” state. Until the CAU does not receive confirmation from the client that the incident has been correctly resolved the incident is not definitively closed in the tool.

The incident tool also provides a number of tools and information that are aimed at the good performance of the CAU and facilitating the monitoring of SLA levels relating to incident and problem resolution. Some of the most important features of the tool are mentioned below:

- The tool provides information about the incidents assigned by technician and their state. This information is reviewed in order to redistribute work load among technicians.
- There are automatic e-mails generated when a L1 technician spends more than 20 minutes attending an incident. L1 incidents should be resolved in a timely manner or otherwise escalated to L2.
- When an incident is assigned from one technician to another the incident enters in “To be contacted” state. The second technician is to contact the client as soon as possible in order to continue the follow-up and resolution of the incident. If the second technician does not contact the client within 30 minutes time the tool generates an automatic e-mail notifying of this circumstance. The

tool will keep generating automatic notification e-mails in shorter intervals until the second technician finally contacts the client.

- When an incident is deleted from the tool an automatic e-mail is generated so that the CAU Responsible becomes aware of this circumstance.

By means of these special features the CAU Responsible controls the department performance.

The tool also provides other information that contributes to the monitoring of the service levels for the incident and problem management:

- There is a list of incidences that have been abandoned (not closed yet for a long time). This list is reviewed to make sure all incidences are followed up to their resolution and are finally closed in the tool.
- There is a list of incidences in “To be contacted” state. This list is reviewed to make sure all incidences which need an action from CAU are properly attended.
- There is a report that shows the percentage of incidences registered and closed in the same day. Since in the SLA it is stated that incidents will be resolved within 1 day it is important that this percentage is close to 100%. Those incidences which are not closed in the same day of register should be pending of client action and under no circumstance the delay should be Edicom responsibility. This report is reviewed on a daily basis to ensure service level agreements are met.
- Historic data of incidents by technician to control technician performance over the month.
- Information about calls registered in the switchboard every hour to control work load and detect CAU personnel necessities.
- Monthly evolution of the number of incidences/day and incidences/hour to analyze work load and detect CAU personnel necessities.

## *2. Incidents detected by Edicom*

The IS Department is responsible for the register, follow up and resolution of incidents related to information systems and infrastructure supporting the ASP service. Incidents can be detected either as a consequence of the monitoring activities carried out directly by the IS Department or reported directly by Edicom employees. Incidents can also be reported by CAU and 24x7 departments when they have not been able to resolve an incident by themselves acting in this case the IS Department as a 2<sup>nd</sup> Level support service.

Incidents are always evaluated and given priority by the IS Manager depending on their impact on the ASP service. Incidents with high impact are prioritized and resolved in the first place. The IS Department also informs the other departments in the company about open issues so that everybody is aware of current incidents and problems pending to be solved. This way the departments involved in the monitoring and maintenance of the ASP service can pay close attention to these issues.

Finally a special tool is used internally in the department for the register, follow up and resolution of incidents. The tool registers all relevant information about the incident.

### **Monitoring**

The monitoring activities in the company for the ASP service are performed by two departments:

- IS Department
- 24x7 Department

The 24x7 Department is responsible for the continuous monitoring of the ASP service. They are also responsible for the resolution of incidents detected. In case they are not capable to resolve an incident by themselves the incident is reported to the IS Department for its resolution. A special monitoring tool is used where the different events to be monitored are configured. There are two main types of alarms configured in the tool: standard and extended. Extended service alarms are given priority to ensure clients with extended service have a higher quality service. Finally the 24x7 Department also performs the monitoring of the service levels agreements related to service availability. The department has an internal service level objective for service availability that is more demanding than the service level agreed with clients to ensure service levels agreements are always met. Service availability statistics are monitored on a continual basis and anomalies are analyzed and investigated. If necessary problems are reported to the IS Department for their resolution.

The IS Department also performs monitoring activities which are more infrastructure and computer operations oriented. The IS Department uses a number of tools to assist in the monitoring. Incidents and problems detected are analyzed, investigated and resolved. Activity logs in the different systems are kept for a period of time of at least one year.

### **Capacity planning and management**

Capacity planning and management activities are performed in the company. The IS and 24x7 departments perform different capacity monitoring activities to detect future capacity necessities and to make sure processing and storage capacity is enough to ensure service levels.

### **Backup and restoration procedures**

There are formalized backup and restoration procedures in the company. There are different backup strategies for the data and programs supporting the ASP service. There are online backups of data stored in the data bases from the Edicom Data Center to the Remote Data Center. As a consequence at any time data and programs are replicated in two different locations. As well as this every six hours there are static backups to the local disks of the servers in the Remote Data Center. Finally there are weekly and monthly backups of data and programs to external tapes which are

encrypted and stored in a fireproof safe in the company facilities. The company also performs periodic restoration tests to ensure the integrity and validity of data and tapes.

#### **Client Control Considerations**

- The Client is responsible for ensuring they report problems identified during processing to Edicom and track those problems.
- The Client is responsible for monitoring network connections they maintain between Edicom and the client site to help ensure connections are secure and operating as expected.

**SECTION IV**  
**OTHER INFORMATION PROVIDED BY EDICOM**

## **Other Information Provided by Edicom**

### **Business Continuity Planning for the Enterprise**

Edicom takes an Industry-Standard Four-Phase Approach to Business Continuity Planning, which relies on an iterative process of identifying the requirements, building recovery strategies, and documenting and testing the recovery plan.

The four phases are:

- Business Impact Analysis
- Recovery Strategies
- Disaster Recovery Plan
- Testing Exercise

### **Recovery Solutions**

- Cyclical backups of data and programs.
- Remote data center (COLT) with on-line replicated data and programs which allows for immediate fall over in case of a disaster in the main data center.
- Systems redundancy (cluster, virtualization, etc.) that provide for high availability of information systems.

### **Disaster Recovery Testing.**

Edicom carries out testing of the Disaster Recovery Plan (DRP) on a periodical basis. The DRP Testing simulates the complete system breakdown in one location and activates the recovery procedures in order to restore service in the remote data center. There are also backup recovery testing procedures where information from backup tapes is restored on a periodical basis. These testing procedures are documented.

### **Business Continuity Plan Review**

The BCP is reviewed every six months or when a relevant change in the information systems has taken place so that the BPC remains operative and up-to-date.

## **ISO/IEC 27001 Certification**

Edicom has adopted ISO/IEC 27001 and has been formally audited and certified compliant with the standard. ISO/IEC 27001 formally specifies a management system that is intended to bring information security under explicit management control. The ASP EDI service has been scoped as the process covered by the ISMS. As a result of the certification process Edicom has undergone the following processes and procedures:

- An organizational top level policy has been developed and published. The policy is supported by subordinate policies.
- A risk assessment has been undertaken, to determine the organization's risk exposure/profile, and identify the best route to mitigate risks. Risk assessment is to be updated on a annual basis.
- Appropriate controls have been selected with respect to those outlined in the standard (and ISO27002), with the justification for each decision recorded in a Statement of Applicability (SOA).
- Controls selected have been implemented in the organization for the process in scope.

Edicom reviews and monitors the information security management system on an on-going basis using the PDCA (Plan-Do-Check-Act) also known as the Deming Cycle. The PDCA is an iterative four-step problem-solving process used in business process improvement.