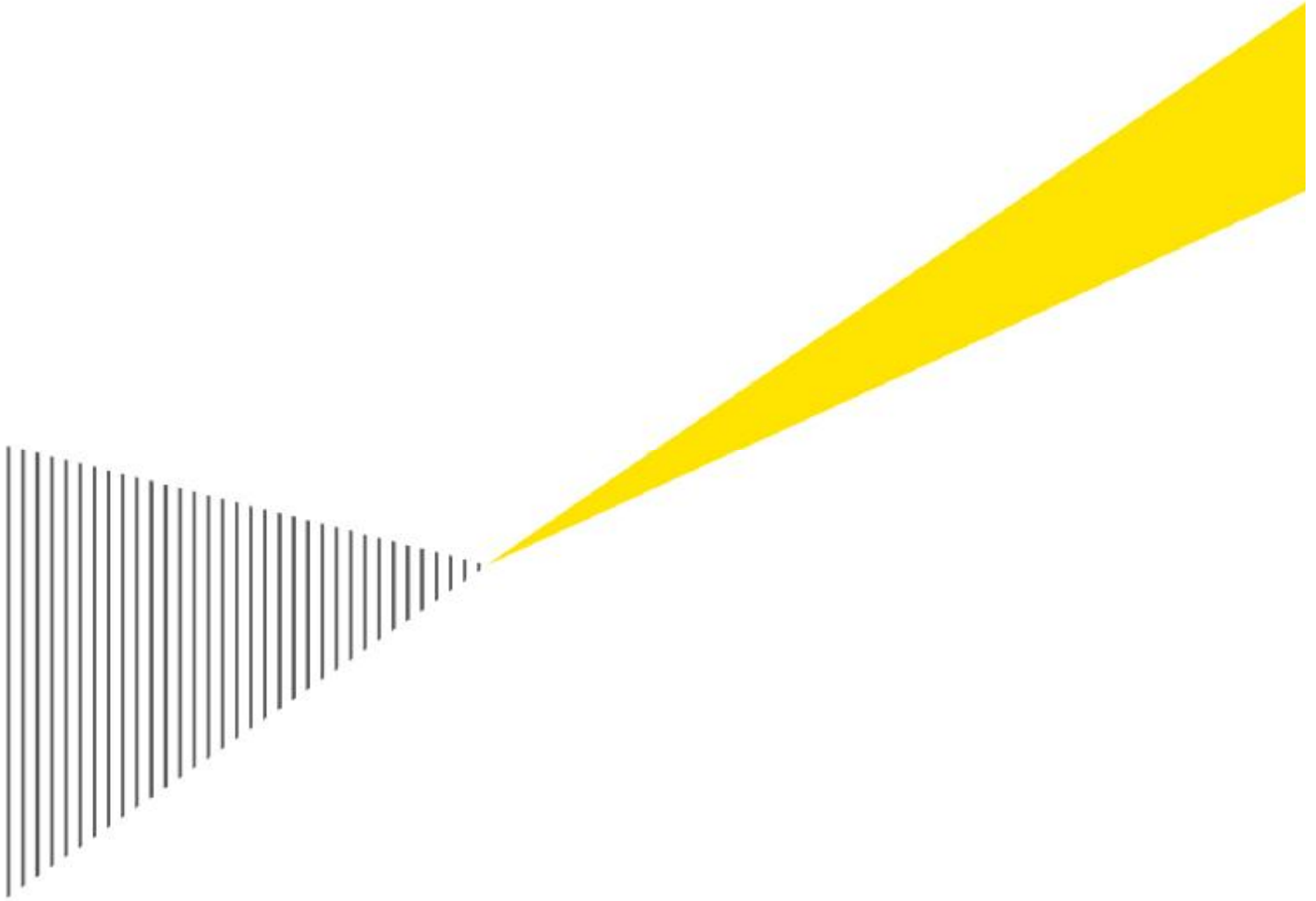


# SysTrust™ Examination Report e-Business and Resilience Centre (“eBRC”)

HITEC Data Centre

1 April 2009 - 31 May 2009



# Table of contents

Auditor's SysTrust™ Report	1
Appendix 1 – eBRC Management's Assertion	3
Appendix 2 – eBRC Management's Detailed Assertion	4
Appendix 3 – HITEC Data Centre System Description	12

# Auditor's SysTrust™ Report

To the Management of  
e-Business and Resilience Centre

We have examined e-Business and Resilience Centre ("eBRC" or the "Company") management's assertion (as described in appendix 1) that, during the period April 1, 2009 through May 31, 2009, eBRC maintained effective controls over its HITEC Data Centre System (hereafter "the System") to provide reasonable assurance that the System:

- ▶ Was protected against unauthorized access (both physical and logical); and
- ▶ Was available for operation and use, as committed or agreed

based on the AICPA/CICA Trust Services **Security** and **Availability** Criteria.

This assertion is the responsibility of eBRC's management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of eBRC's relevant security and availability controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

In our opinion, eBRC management's assertion, referred above is fairly stated, in all material respects, based on the AICPA/CICA Trust Services Security and Availability Criteria.

Because of inherent limitations in controls, error 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 the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to system or controls, or deterioration in the degree of effectiveness of the controls.

eBRC's use of the SysTrust Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

A handwritten signature in black ink, appearing to be 'D. J. P.', with a long horizontal stroke extending to the right.

Ernst & Young S.A.  
Certified Public Accountants  
Luxembourg

27 July, 2009

# Appendix 1 – eBRC Management’s Assertion

## **eBRC’s Assertion Regarding the Effectiveness of Its Controls Over the HITEC Data Centre Based on the SysTrust™ Principles and Criteria**

To the Customers of  
e-Business and Resilience Centre (“eBRC”)

As the directors of eBRC, we are responsible for the design, implementation and maintenance of security and availability measures at the HITEC Data Centre.

eBRC maintained the controls over the security and availability of the HITEC Data Centre to provide reasonable assurance that:

- ▶ The system was protected against unauthorized physical and logical access,
- ▶ The system was available for operation and use at times set forth in service-level statements or agreements,

during the period April 1, 2009 through May 31, 2009, based on the Trust Services Principles and Criteria established by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA).

Our summarized description of the aspects of the System is presented in the accompanying System Description of eBRC’s System in appendix 3.

The Management of  
e-Business and Resilience Centre (“eBRC”)

27 July, 2009

## Appendix 2 – eBRC Management’s Detailed Assertion

**eBRC’s Detailed Assertion Regarding the Effectiveness  
of Its Controls Over the HITEC Data Centre Based on the  
SysTrust™ Principles and Criteria**

# SECURITY

## **SECURITY POLICIES ARE ESTABLISHED, REVIEWED AND APPROVED BY A DESIGNATED INDIVIDUAL OR GROUP.**

eBRC has formalized its Security Policy in a document approved by eBRC's Management and Security Committee. This document is reviewed and adapted as deemed necessary. The Security Policy is completed by one appendix, describing eBRC's physical security requirements.

eBRC's legal department and security department review contractual, legal, and other service level agreements and applicable laws and regulations to evaluate their impact on current system security objectives, policies and standards. Those regulations include the CSSF circulars applicable to the banking and finance sector.

Management meetings are regularly held to ensure that there is clear direction and visible management support for security initiatives. Such meetings seek to promote security through appropriate commitment and adequate resourcing.

eBRC management authorization process for the acceptance of new client facilities is established.

Appropriate contacts with authorities, regulatory bodies, service providers and other telecommunications operators are maintained.

The risks associated with access to eBRC processing facilities by clients and other third parties are assessed and appropriate security controls are implemented.

Arrangements involving client and third party access to the HITEC Data Centre facilities are based on a formal contract containing and detailing all necessary security requirements.

eBRC's security requirements for outsourcing are addressed in a contract agreed between the parties.

## **RESPONSIBILITY AND ACCOUNTABILITY FOR eBRC'S SYSTEM SECURITY POLICIES, AND CHANGES AND UPDATES TO THOSE POLICIES, ARE ASSIGNED.**

The responsibility for the overall security lies with the eBRC's management.

A Security Committee is set up, including Management as well as staff in charge of physical and logical security. Regular meetings are held in order to discuss the security level, the occurrence of incidents and the improvement of security at eBRC. The various responsibilities are documented in related job descriptions. Overall and yearly objectives are fixed and assessed continuously.

Cross-functional and cross-client meetings are taking place for management representatives from relevant parts of the eBRC and clients to coordinate the implementation of security controls.

Security roles and responsibilities, as laid down in eBRC's information security policy, are documented in job descriptions.

An inventory of physical assets associated with each Client is drawn up and maintained. According to the contractual agreements with its clients, eBRC has neither custody nor protective obligations over its client's information systems.

**EBRC HAS PREPARED AN OBJECTIVE DESCRIPTION OF THE SYSTEM AND ITS BOUNDARIES AND COMMUNICATED SUCH DESCRIPTION TO AUTHORIZED USERS.**

Objectives, policies, and standards that support the implementation, operation, and maintenance of security measures are communicated to authorized users for ensuring system security through such means as new hire training, departmental meetings, departmental document sharing.

eBRC also maintains internal security procedures that provide information to staff about security policies and configuration guidelines.

eBRC management and departments ensure that all internal security procedures within their area of responsibility are carried out correctly and are subject to regular review to ensure compliance with defined security policies and standards.

**THE SECURITY OBLIGATIONS OF USERS AND EBRC'S SECURITY COMMITMENTS TO USERS ARE COMMUNICATED TO AUTHORIZED USERS.**

The security setup of the system as well as the use of the security installations are formalized in the client Contract, SLA and User Guide.

These documents are periodically reviewed and adapted if security setup changes occur or customer requirements evolve. They result in amendments to the contract, SLA or Users Guide, signed by both parties.

All eBRC employees and where relevant, external service providers, receive appropriate training and regular updates in security policies and procedures. The violation of eBRC's security policies and procedures by employees or clients is dealt with through a formal disciplinary process.

Arrangements involving users and third party access to eBRC facilities are based on a formal contract containing all necessary security requirements. The IT room Access Control policy is documented to define appropriate level of access.

eBRC has a lease contract and an SLA with the HITEC Data Centre owner, setting forth the rights and obligations of each party as well as setting the service level to be delivered to eBRC and its customers.

HITEC Data Centre owner subcontracts the setup, operating and maintenance work schedules to a renowned, local professional, Paul Wagner & Fils. These work schedules are analyzed and discussed in regular meetings with all parties.

Incident Management is done together with the owner and his subcontractor on an ad-hoc basis. Planned maintenance work is determined in advance at the end of the year for the year after and communicated to eBRC's clients for information and approval.

Maintenance reports are delivered to eBRC and discussed if issues have been detected. Curative maintenance work is then planned together with the impacted clients.

**eBRC COMMUNICATES ITS DEFINED SYSTEM SECURITY POLICIES TO AUTHORIZED USERS.**

Objectives, policies, and standards that support the implementation, operation, and maintenance of security measures are communicated to personnel responsible for ensuring system security through such means as new hire training, service meetings, departmental document sharing.

The entire staff of eBRC is regularly informed of their responsibilities and the security obligations of eBRC during staff meetings and internal trainings.

Responsibilities of the staff in charge of implementing and maintaining system security are communicated through job descriptions and annual evaluation sessions.

**RESPONSIBILITY AND ACCOUNTABILITY FOR eBRC'S SYSTEM SECURITY POLICIES AND CHANGES AND UPDATES TO THOSE POLICIES ARE COMMUNICATED TO ENTITY PERSONNEL RESPONSIBLE FOR IMPLEMENTING THEM.**

The incident management procedures include proper escalation procedures up to the top management of the client, eBRC and its subcontractors.

Clients are systematically informed about incidents affecting the proper use of the system as defined in the contractual agreements.

An incident follow-up is ensured with all parties and an action plan is defined if necessary, until closure of the incident. The whole process is formalized and documented.

Security incidents are reported through appropriate management channels as quickly as possible.

eBRC personnel, service providers and clients of the HITEC Data Centre are required to note and report observed or suspected security weaknesses in, or threats to, systems or services.

The security setup of the system as well as the use of the security installations are formalized in the client Contract, SLA and Users Guide.

These documents are periodically reviewed and adapted if security setup changes occur or customer requirements evolve. They result in amendments to the contract, SLA or Users Guide, signed by both parties.

All eBRC employees and, where relevant external service providers, receive appropriate training and regular updates in security policies and procedures.

The violation of eBRC security policies and procedures by employees or clients is dealt with through a formal disciplinary process.

The IT room Access Control policy is documented to define appropriate level of access.

Arrangements involving users and third party access to eBRC facilities are based on a formal contract containing all necessary security requirements.

The security guards and the eBRC security and technical staff have the necessary systems, procedures and monitoring tools at their disposal to rapidly detect all incidents pertaining to security and technical installations.

Appropriate trainings are provided to keep all involved personnel up to date.

The incident management procedures include proper escalation procedures up to the top management of the clients, eBRC and its subcontractors.

**EBRC USES DOCUMENTED PROCEDURES TO ACHIEVE ITS DOCUMENTED SYSTEM SECURITY OBJECTIVES IN ACCORDANCE WITH ITS DEFINED POLICIES.**

Various IT systems are in place and used to run and monitor the security and technical installations of the HITEC Data Centre:

- ▶ Building Management System,
- ▶ Central Security monitoring and reporting,
- ▶ Access Control,
- ▶ Video Surveillance,
- ▶ Digital recording,
- ▶ Fire detection, and
- ▶ Intrusion detection.

Access to these systems is regulated and controlled by management.

**DOCUMENTED PROCEDURES EXIST TO RESTRICT PHYSICAL ACCESS TO THE DEFINED SYSTEM INCLUDING, BUT NOT LIMITED TO, FACILITIES, BACKUP MEDIA, AND OTHER SYSTEM COMPONENTS SUCH AS FIREWALLS, ROUTERS, AND SERVERS.**

Physical access controls, including 24 hour surveillance cameras, electronic key card system and intrusion detection systems and locked doors limit access to authorized eBRC personnel and other authorized user personnel of the HITEC Data Centre.

External personnel, currently specifically trained security guards from Group4Securicor (“G4S”) are used to control and monitor access to the different areas of the Data Centre, including client IT rooms, telecom rooms or technical production and service areas.

Access security alarms are also redirected for resilience reasons to the headquarters of G4S.

User access privileges are granted in accordance with the documented Client Access Policy which is formalized in the general and particular conditions of the Client Users Guide.

Suggested delivery and loading areas are controlled, and where possible, isolated from information processing facilities to avoid unauthorized access.

**ENCRYPTION OR OTHER EQUIVALENT SECURITY TECHNIQUES ARE USED TO PROTECT USER AUTHENTICATION INFORMATION AND THE CORRESPONDING SESSION TRANSMITTED OVER THE INTERNET OR OTHER PUBLIC NETWORKS.**

No information concerning the technical and security management of the HITEC Data Centre is processed over the internet or shared public networks. Because activities within the system can only be carried out locally (on-site) there is no need to apply encryption to ensure the confidentiality of sensitive or critical information over communication channels.

eBRC has procedures in place to ensure that its system resources are configured consistently. In order to achieve this, eBRC has implemented for the management of its datacenters a Service Management framework based on ITILv3 with a certain number of best practices, including authorization by a Change Advisory Board (“CAB”) body for all changes including pre-approved standard changes.

**DOCUMENTED PROCEDURES EXIST TO PROVIDE THAT PERSONNEL RESPONSIBLE FOR THE DESIGN, DEVELOPMENT, IMPLEMENTATION, AND OPERATION OF SYSTEMS AFFECTING SECURITY ARE QUALIFIED TO FULFILL THEIR RESPONSIBILITIES.**

eBRC is regularly covering the Human Resources Management Process. This includes developing and maintaining job descriptions, as well as elaborating documents pertaining to headcount planning (such as necessary skill sets, the coverage of the needed skills with the current staff and the development path for each individual staff member).

Employee appraisals evaluations are conducted on an annual basis and are performed through interview(s) assessing the employee's competence and achievements. The result of the employee evaluation is cross-checked by eBRC's management.

**DOCUMENTED PROCEDURES EXIST TO PROTECT AGAINST INFECTION BY COMPUTER VIRUSES, MALICIOUS CODES, AND UNAUTHORIZED SOFTWARE.**

eBRC has procedures in place to protect against virus infection. Monitoring is performed by eBRC and security taskforce in order to identify potential security impairment on a timely basis.

**THERE IS A PROCESS TO IDENTIFY AND ADDRESS POTENTIAL IMPAIRMENTS TO eBRC'S ONGOING ABILITY TO ACHIEVE ITS OBJECTIVES IN ACCORDANCE WITH ITS DEFINED SYSTEM SECURITY POLICIES.**

The incident management procedures include proper escalation procedures up to the top management of the client, eBRC and its subcontractors.

Clients are systematically informed about incidents affecting the proper use of the system as defined in the contractual agreements.

An incident follow-up is done with all parties and an action plan is defined if necessary, until closure of the incident. The whole process is formalized and documented.

# AVAILABILITY

## **EBRC DEFINES AND DOCUMENTS ITS POLICIES FOR THE AVAILABILITY OF ITS SYSTEM.**

eBRC has formalized its Security Policy in a document approved by the company's Management and Security Committee. This document is reviewed and adapted as deemed necessary. The Security Policy is completed by one appendix, describing the physical security requirements. The availability criteria of the system as well as the use of the security and technical installations are formalized in the client Contract, SLA and Users Guide. Such documents are periodically reviewed and adapted if security setup changes occur or customer requirements evolve. They result in amendments to the contract, SLA or Users Guide, validated and signed by both parties.

## **RESPONSIBILITY AND ACCOUNTABILITY FOR EBRC'S SYSTEM AVAILABILITY AND RELATED SECURITY POLICIES, AND CHANGES AND UPDATES TO THOSE POLICIES, ARE ASSIGNED.**

The responsibility for the availability management lies with the eBRC's management. A Security Committee is set up, including Management as well as staff in charge of physical and logical security. Regular meetings are held in order to discuss the security level, the occurrence of incidents and the improvement of security. The various responsibilities are documented in the job descriptions of those people. Overall and yearly objectives are fixed and evaluated continuously.

It is to note that eBRC has neither the possibility, ability nor the responsibility for establishing and maintaining its clients' significant information resources. This is the sole responsibility of individual clients.

## **EBRC COMMUNICATES THE DEFINED SYSTEM AVAILABILITY POLICIES TO AUTHORIZED USERS.**

Objectives, policies, and standards that support the implementation, operation, and maintenance of security and technical installations are communicated to personnel responsible for ensuring system security and availability through such means as new hire training, departmental meetings, and departmental document sharing. The Company maintains internal security and availability procedures that provide information to staff about availability requirements, vulnerabilities and configuration guidelines.

## **THE AVAILABILITY AND RELATED SECURITY OBLIGATIONS OF USERS AND EBRC'S AVAILABILITY AND RELATED SECURITY COMMITMENTS TO USERS ARE COMMUNICATED TO AUTHORIZED USERS.**

The availability levels of the system as well as the means to ensure the set level are formalized in the client Contract, SLA and Users Guide. These documents are periodically reviewed and adapted if security setup changes occur or customer requirements evolve. They result in amendments to the contract, SLA or Users Guide, signed by both parties.

eBRC has a lease contract and a SLA with the HITEC Data Centre owner, determining the rights and obligations of each party as well as setting the service level to be delivered to eBRC and its customers. The owner subcontracts the setup, operating and maintenance work schedules to a renowned, local professional, Paul Wagner & Fils. Those work schedules are analyzed and discussed in regular meetings with all parties. Incident Management is assured together with the owner and his subcontractor on an ad-hoc basis. Planned maintenance work is determined in advance at the end of the year for the year after and communicated to eBRC's clients for information and approval. Maintenance reports are delivered to eBRC and discussed if issues have been detected. Curative maintenance work is then planned together with the impacted clients.

Security guards, as well as the security and technical eBRC staff have the necessary systems, procedures and monitoring tools at their disposal to detect rapidly all incidents pertaining to security and technical installations. Trainings are provided to keep everybody up to date.

The incident management procedures include proper escalation procedures up to the top management of the client, eBRC and its subcontractors.

**eBRC USES DOCUMENTED PROCEDURES TO ACHIEVE ITS DOCUMENTED SYSTEM AVAILABILITY OBJECTIVES IN ACCORDANCE WITH ITS DEFINED POLICIES.**

A Risk Assessment of the HITEC Data Centre has been prepared by specialized eBRC staff and validated by the Security Committee. Appropriate countermeasures are in place to mitigate risks.

This risk assessment is adapted if internal or external changes occur that might have an impact on the security and availability levels of the system.

Where appropriate, redundant production and distribution systems are in place to protect the customers ICT systems. This applies to electricity and cold water production and distribution as well as to telecom access routes into the building.

Appropriate measures to protect the clients IT rooms against fire and flood are implemented as well. A state-of-the-art fire detection system, coupled with an automatic "Argonite" fire extinction system protects all IT rooms. Redundant air conditioning terminal units have been installed in technical corridors behind the IT rooms to exclude every water risk from inside. Liquid detection cables are in place within the technical corridors and the IT rooms to rapidly detect the presence of water. Redundant water pumps, monitored with the BMS system are installed to evacuate water coming from external sources like firemen.

eBRC recently opened a second site at a secure distance from "The Cloche d'Or site", the Resilience Centre in Windhof, close to the Belgian border. In case of unavailability of the HITEC Data Centre and under specific contractual agreements, clients may be relocated in this new Data Centre with a total capacity of 5000m<sup>2</sup> of net IT surface, compared to the 1000m<sup>2</sup> of the HITEC Data Centre.

The access control system are backed up to redundant disk arrays

The programs and security parameters of the intrusion detection and fire detection systems are backed up and kept in a safe at the Resilience Centre

The video surveillance system configuration is regularly backed up.

The Company has procedures in place to ensure that its system resources are configured consistently. In order to achieve this, eBRC has implemented for the management of its datacenters a Service Management framework based on ITILv3 with a certain number of best practices including authorization by a Change Advisory Board (CAB) body for all changes, including pre-approved standard changes.

The recruitment process is documented and new hires are subject to reference checks.

The interview process requires separate interviews to assess the candidate's technical competence and industry experience. Employee performance evaluations are conducted on an annual basis.

# Appendix 3 – HITEC Data Centre System Description

## HITEC Data Centre System Description

Based on our discussion with Management, the description of the “System” subject to our evaluation can be summarized as follows.

eBRC is a local-based company specialized in Business Resilience and offering a large portfolio of integrated services in the domain of continuity – including telecommunications, security, and infrastructure and managed services.

The range of services delivered by eBRC can be summarized as follows:

- ▶ Consulting and project management,
- ▶ E-Continuity services including Business Continuity & Infrastructure Services,
- ▶ E-Agility services.

As part of its primary objective to serve its customer needs relative to continuity, security and hosting managed services, the Company benefits from an advanced Business Continuity Centre spread over two distant sites in the Grand Duchy of Luxembourg: HITEC/GOLDBELL located in Gasperich and the Resilience Centre Windhof located in Windhof.

This infrastructure is a global Data Centre fully equipped and secured with private and shared IT rooms, for which specific services dedicated to the management of such facilities are provided, namely:

- ▶ Technical analysis and recommendations,
- ▶ Logical environment design,
- ▶ Technical implementation,
- ▶ Remote central monitoring of all technical and security systems 24x7x365,
- ▶ Permanent system reporting,
- ▶ Preventive and curative technical maintenance.

In addition to the value-added services described above, the Data Centre also meets the needs of customers looking to outsource the facilities required for housing technology and communications equipment used in their own business, providing seamless and secure turnkey infrastructure solutions for value-oriented customers.

The objective of eBRC's Client Services is to provide customers with quality expertise and consultation with technologies provided or supported by eBRC.

The Client Service team consists of over nearly 60 experts, who can provide varying levels of assistance based on customer needs. The team is typically engaged to provide customer specific assistance with a particular solution (business continuity, disaster recovery, data centre infrastructure services, information security and hosting services).

The System service perimeter is strictly limited to the provision of Facilities Management services at the HITEC Data Centre from the point information is received from the Telecommunication operators connections through transmission to customer controlled systems housed in private IT rooms located in the HITEC Data Centre.

The use, control, maintenance and administration activities related to customer-specific hardware and software components residing within the private IT rooms are clearly out of the scope of the System definition.

In providing those Services, the HITEC Data Centre relies on operational support, including performance monitoring, corporate security operations, personnel and facilities located in both HITEC & GOLDBELL sites, which perform similar general services for eBRC as a whole.

The following sections define the boundaries of the system components that make up the HITEC Data Centre "System".

#### Infrastructure and supporting Software

The HITEC Data Centre is located at 11, rue Eugène Ruppert in Gasperich, Luxembourg.

The Data Centre provides private and secure IT rooms reserved for the single use of its customers in which dedicated processing systems (including firewalls, Web servers, load balancers, application servers, database servers etc.) are hosted.

The System description encompasses all physical, hardware and software components required for (a) securing the environmental and physical environment of the HITEC Data Centre building as a whole, as well as for (b) ensuring the proper and safe functioning of the IT rooms within the HITEC Data Centre. As such, physical, hardware and software components (including specific customer facilities, mainframes, servers, networks, programs and other related components) that specifically pertain to the functioning of the dedicated customer processing systems residing within the IT rooms are excluded from the system description and, as a result, are not subject to our current evaluation.

Although, it is to note that hardware and software used for the purpose of dedicated customer needs and installed in separate rooms are subject to formal approval procedures to help ensure they are suitable for use in the Data Centre.

#### People

This encompasses internal and external personnel involved in the operation, use and monitoring of the System, including the individuals responsible for the execution and support of the System's procedures for installation, day-to-day activities and incidents management (see below), the System's users as well as eBRC management.

More specifically, internal and external physical security and eBRC operations personnel who support daily operating activities are located at the GOLDBELL Data Centre. In addition, other external operations support personnel responsible for technical and security operation services are located at the HITEC Data Centre.

eBRC's Management is housed in eBRC's Luxembourg offices.

## Data

This component of the System definition is limited to the information used and supported by the System for the purpose of the Services described above. More specifically it encompasses all input and output data files, databases and other information streams solely required for the provision of those services. As such, it clearly excludes customer information, once those have been transmitted to customer controlled systems housed in private IT rooms.

## Procedures

The HITEC Data Centre is operational 7 days a week, 24 hours a day to provide constant connectivity and service.

Manual and automated procedures have been developed and documented to support the following key processes applicable to the Data Centre as a whole, and/or for each individual IT room:

- ▶ Physical access security,
- ▶ Logical access security,
- ▶ Data Centre operations,
- ▶ System maintenance,
- ▶ Performance monitoring.

