DATE OF THE CAR IMPLEMENTATION VERIFICATION: 20.07.2019

1. AUDITED ORGANISATION IDENTIFICATION

LEGAL NAME OF THE ORGANISATION	ACIN iCloud Solutions S.A.
TRUST SERVICE	DT W 2017.002 Website authentication

2. AUDIT

CAR IMPLEMENTATION VERIFICATION AUDIT TYPE	CAR Documentary verification made on the operative site

This report complements and concludes the assessment of the previous report:

IDENTIFICATION OF THE PREVIOUS AUDIT REPORT	DT W 2017.002 Website Authentication - 2019 Renewal	**PREVIOUS AUDIT DATE**	08.04.2019 to 12.04.2019

3. AUDIT TEAM

NAME	POSITION	REGULATION
Paulo Jorge Martins Borges	Lead Auditor	eIDAS Regulation 910/2014

4. CAR VERIFICATION

During audit activities conducted on the operative site, evidences were collected allowing to verify the effective implementation of each corrective action regarding the non-conformity identified in the following table:

NC ID	CLASSIFICATION	CAUSE ANALYSIS	CORRECTIVE ACTION	DEADLINE	PERSON RESPONSIBLE	ANÁLISE	STATUS	COMMENTS/ASSESSMENT DESCRIPTION
NC.1	NCBI	Lack of an appropriate tool to follow up corresponding incidents and SLAs. No tracing between lessons learned in the context of incidents and risk analysis. The latest version of FO35 has detailed fields that make the time record of incidents clearer.	The JIRA Service Desk tool to manage the life cycle of incidents and SLA monitoring on real-time was implemented. **Related documents:** • MA47_GTS_V1 – Functional Manual of Configuration and Incident Management • PC14_GTS – Incident Management Process • PR27_GTS_V5 – Service Continuity Implementation Plan	30 06 2019	SecAdm – Rodrigo Freitas LeadAud – Sandra Fernández	Concluded	Concluded	The implemented tool includes all the functionalities that allow to meet all referred non-conformity requirements. As it is in an early stage of use, it must be noted that the next audit should assess its operation and all incidents since the date of this report.
NC.2	NCBI	Lack of an alternate site for the restitution of services for certain disruptive incidents	An assessment was conducted about options to other locations in Madeira, being the selection made by PT Telecom´s Datacenter. A secondary site implementation plan has been defined and is being implemented with a deadline of 6 months.	30 06 2019	SecAdm – Rodrigo Freitas LeadAud – Sandra Fernández	Concluded	Concluded	Derived from the complexity of the presented and analysed implementation plan, the corrective action is accepted as capable of addressing the required conformity. The auditor emphasizes that monthly reports on the implementation of the plan should be provided and that, in the next audit, this location should be included in the audit scope and activities for the conformity assessment of the implementation.

			Related documents: • PR27_GTS_V5 - Service Continuity Implementation Plan • MA48_GTS_V1 – Secondary Site Implementation Plan • Physical and Logical Infrastructure Proposal - PTEMPRESAS 4001533/1 • Technological Infrastructure Proposal - ACIN_Projeto_DR_v2019					It must be taken into consideration that the NC includes not only the alternate site, but also the operationalisation of the Business Continuity Plan of GTS.
NC.3	NCBI	No tracing of risk scenarios nor of the lessons learned in the context of tests conducted with the risk analysis. It is not possible to conduct all tests of the BCP due to inability to simulate operating conditions.	The Risk Management methodology was modified in order to define the origin of the sources of risk sources, as well as the RS and Threats ID were added to allow risk mapping, incident management and Service Continuity Plan. A risk analysis was conducted, identifying risks related to Cybersecurity, physical facilities (covering primary and secondary sites) and trust services. It was contemplated in the Secondary Site Implementation Plan that HW components of the PKI infrastructure should be tested in the SCP in the HW implemented in the secondary site, as long as the primary site is fully operational. These tests must be controlled and conducted on regular basis. **Documentos envolvidos:** • PR01_GTS_ V2-Metodologia da Gestão do Risco	30 06 2019	SecAdm – Rodrigo Freitas LeadAud – Sandra Fernández	Concluded	Concluded	The requested integration work of risk scenarios was successfully conducted. Considering the NC.2 corrective action, BCP tests can only be conducted after the implementation of the alternate site. Accordingly, the auditor accepts the resolution of the corrective action, but points out that this topic will be included in scope of the next audit.

			• PR27_GTS_V5 - Service Continuity Implementation Plan • MA47_GTS_V1 – Functional Manual of Configuration and Incident Management • PC14_GTS – Incident Management Process (This CP was not modified; however, it was the base for the JIRA configuration) • MA17_GTS_V2 - Risk Analysis and Treatment Report _2019_july • MA20_GTS_V2-Treatment Acceptance Statement _2019_july • RG03_V3 - Risk Analysis Matrix _GTS_2019 • RG04_V4 - Risk Treatment Matrix _GTS_2019 • RG15_V3 – Risk Sources _GTS_2019 • MA48_GTS_V1 – Secondary Site Implementation Plan • RG27_V3 – Service Continuity and Availability Tests Plan_ACIN_and_GTS					

5. AUDIT TEAM OPINION / DRAFT DECISION

RECOMMENDATION / DRAFT DECISION

As a corollary of the analysis of the implementation of corrective actions and the respective regulatory compliance analysis, it is verified that the “non-conformity” situations were carried out in a sustainable manner and duly complying the requirements of the ETSI standards applicable to trust services.

Therefore, the auditor proposes a **favorable decision to renew the certification.**

RATIONALE:

Throughout the PAC audit, ACIN presented a broad set of evidence demonstrating its commitment to the effective implementation of corrective actions, and demonstrated relevant knowledge and maturity on the aspects involved in each corrective action for the current stage of trust service provision by its team.

ACIN is notified, through the notes contained in the auditor's assessment description, that these issues will be part of the scope of the next audit and it should be demonstrated that they are fully and effectively executed.

6. DISCREPANCIES

In case of disagreement between ACIN and the audit team, for which no consensus was reached, they will be registered in this report and submitted to APCER for clarification, assessment and decision.

Nevertheless, at the time of drafting this report, no disagreements between the organisation and the audit team were identified.

For further information see applicable APCER regulations.

7. ACKNOWLEDGEMENTS

The audit team would like to thank ACIN for its pleasant atmosphere and collaborative effort, ensuring the necessary conditions for the success of this audit.

8. CONFIDENCIALITY

APCER assures, at all levels of its structure, including commissions, external organisations or staff acting in its behalf, the confidentiality of all accessed information during the certification process. APCER reserves the right to provide confidential information to representatives of accreditation agencies and competent verification regulatory authorities. Where APCER is required by law to disclose information to a third party, the client organization or person will be notified in advance of the information to be provided, unless otherwise provided by law.

PERSON RESPONSIBLE	NAME	DATE	SIGNATURE
Lead Auditor:	*Paulo Borges*	10-08-2019	

9. REVIEW AND DECISION

Favourable decision

Certification Scope: **Website authentication**

Comments: After reviewing the documentation produced by the Audit Team in the conduction of the CAR verification audit and based on the findings therein, it is verified that the conditions for maintaining the certification, in the context of Regulation 910/2014 and respective ETSI's, are met.

Certification validity date: **2021-9-16**

PERSON RESPONSIBLE	NAME	DATE	SIGNATURE
Reviewed and decided by:	Fernando Fevereiro Mendes	26-08-2019	Digitally signed by FERNANDO HENRIQUE CONDE DA SILVA FEVEREIRO MENDES Data: 2019.08.26 '12:15:05 +01'00 CARTÃO DE CIDADÃO