Explanatory note to ISAE 3000 and ISAE 3402 statements for 2025

Updated: February 27, 2026
Version: 1.0

Responsible: Peter Kristensen

Introduction

EY has prepared ISAE 3000 and 3402 statements regarding 2025 for cBrain.

With this explanatory note, cBrain wishes to elaborate on and explain some of EY's observations in the statements.

Questions regarding this note are welcome and can be addressed to:

Peter Kristensen: pkr@cbrain.com
Special Advisor - Technical Partner and Compliance

ISAE 3000 observations

No.	cBrain's control activity	Result of EY's test	cBrain's elaboration
B.7	For the systems and databases used in the processing of personal data, system monitoring has been established with an alarm feature.	For 4 customers, F2 was open to TLS 1.0 and TLS 1.1 traffic from November 19 to December 31, 2025. For 1 customer, F2 was open to TLS 1.0 and TLS 1.1 traffic from December 3 to December 31, 2025. In all cases, TLS 1.0 and TLS 1.1 were disabled during the service window on February 8, 2026. No further deviations noted.	Resolved: TLS 1.0 and TLS 1.1 have all been disabled by the service window on February 8, 2026. The protocols have been open at the server level for a limited period of time, but TLS 1.0 and 1.1 require active initiation from the client to be used. The F2 client does not allow traffic on TLS 1.0 and 1.1. Therefore, no traffic has been observed on these protocols and the issue has not had any practical impact on any customers. M4 systems have not been affected by the issue.
B.11	The technical measures established are tested on a regular basis through vulnerability scans. Vulnerability scans are performed quarterly, commencing in the third quarter of 2025 (2025 Q3).	For 4 customers, F2 was open to TLS 1.0 and TLS 1.1 traffic from November 19 to December 31, 2025. For 1 customer, F2 was open to TLS 1.0 and TLS 1.1 traffic from December 3 to December 31, 2025. In all cases, TLS 1.0 and TLS 1.1 were disabled during the service window on February 8, 2026. No further deviations noted.	Resolved: TLS 1.0 and TLS 1.1 have all been disabled by the service window on February 8, 2026. The protocols have been open at the server level for a limited period of time, but TLS 1.0 and 1.1 require active initiation from the client to be used. The F2 client does not allow traffic on TLS 1.0 and 1.1. Therefore, no traffic has been observed on these protocols and the issue has not had any practical impact on any customers. M4 systems have not been affected by the issue.

ISAE 3402 observations

No.	cBrain's control activity	Result of EY's test	cBrain's elaboration
6.2.1	***Mobile device policy*** A formal policy has been established, and appropriate security measures have been implemented to safeguard against the risks which the application of mobile equipment and communication equipment implies. As part of the ongoing control activities, a manual sample-based review is performed every three years to verify that the implemented security measures remain effective and are complied with.	We have not received documentation showing that sample-based reviews of mobile devices in relation to BitLocker and antivirus have been conducted over a three-year period. No further deviations noted.	Encrypting with Bitlocker and installing antivirus is part of cBrain's standard PC setup. cBrain will conduct random checks of mobile devices for Bitlocker and Antivirus before 1/4-26. cBrain has also changed the control to be carried out every year going forward. cBrain's monitoring system will normally raise an alarm if antivirus is not working properly on a PC, so the aforementioned control is an additional manual check.
12.6.1	***Management of technical vulnerabilities*** Data on technical vulnerabilities in information systems is obtained regularly, the company's exposure to such vulnerabilities is reviewed and adequate measures are implemented to handle the inherent risk.	For 4 customers, F2 was open to TLS 1.0 and TLS 1.1 traffic from November 19 to December 31, 2025. For 1 customer, F2 was open to TLS 1.0 and TLS 1.1 traffic from December 3 to December 31, 2025. In all cases, TLS 1.0 and TLS 1.1 were disabled during the service window on February 8, 2026. No further deviations noted.	Resolved: TLS 1.0 and TLS 1.1 have all been disabled by the service window on February 8, 2026. The protocols have been open at the server level for a limited period of time, but TLS 1.0 and 1.1 require active initiation from the client to be used. The F2 client does not allow traffic on TLS 1.0 and 1.1. Therefore, no traffic has been observed on these protocols and the issue has not had any practical impact on any customers. M4 systems have not been affected by the issue.