Action 0206 – update March 2024

CDSP (JRi / AC) to provide an insight into Xoserve's Contract Management of Correla including using the example of the concerns raised in regards to the Major Incident Reporting figures in the February Contract Management Report

1) Provide an update on what is meant by ‘Controllable’:

- *“’**Controllable**’ is defined in the report as ‘Correla Identified the incident and the incident could have been avoided had Correla taken earlier action’. This definition of Controllable pre-dates the DSC+ and is used to describe an incident that may have been avoided if Xoserve/Correla had made a different decision in the past (for example in relation to procurement of a 3rd party supplier) and doesn’t mean that the incident could have been avoided if Correla had been more vigilant/had more resources or tooling available. For example, Controllable may mean if Xoserve had decided to use supplier A instead of supplier B this incident may have been avoided however what is unclear and what we don’t measure are the number of incidents that could have occurred if we had used supplier A.”*

- *The current definition is misleading and we would like to propose an amendment to this to clarify.*

2) Demonstrate the controls that Xoserve has in place to manage the Incident Management Process provided by Correla under the DSC+.

- *There were **5 audits** carried out over the last 12 months that each included Incident, Problem and Change management in the scope of the audits.*

- *These audits were either instructed by Xoserve (ITDR) or they are carried out as a requirement under DSC+.*

- *A brief summary of each audit is on the next slide.*

- ***No recommendations have been made on the incident management process as a result of any of these audits.***

ISAE3402 Audit conducted by KPMG yearly (October 2023/2024 cycle interim and April 2022/2023 cycle year-end)

- *The purpose of the audit is to provide independent assurance on controls over processes related to the billing and invoice activities for DSC+, that have been outsourced to a third party. This includes the UK-Link and Gemini systems.*
- *Audit outcome was an **Unqualified Opinion** with no opportunities for improvements raised for Incident, Problem and Change management.*

ISO9001 Recertification visit September 2023 conducted by Lloyds Register

- *This is a Quality standard to demonstrate the ability to consistently provide products and services that meet customer and regulatory requirements.*
- *No Opportunity for improvements were raised.*

ISO27001 Recertification visit January 2024 conducted by BSI

- *ISO27001 is a standard for the best-practice approach for Information Security Management systems which helps organisations manage their information security by addressing people, processes and technology.*
- *No opportunities for improvements were raised.*

ITDR (Information Technology Disaster Recovery) audit initiated by Xoserve January 2023 conducted by KPMG under co-source arrangement (*due to KPMG skillset and benchmarking capability)*

- *This audit focused on review of relevant ITDR arrangements identified by Xoserve and provided by the third-party Correla. This included a review of management's approach to defining, agreeing, and monitoring ITDR arrangements that are provisioned by the third party.*
- *No improvements raised for Incident, Problem and Change management.*