Report to:	**Audit Committee**
Date:	**13 September 2019**
By:	**Chief Finance Officer**
Title of report:	**Oversight of SAP "Super User" Access Controls – Update**
Purpose of report:	**To update the Committee on the review of SAP "Super User" access raised by Grant Thornton in their 2018/19 Audit Report**

RECOMMENDATIONS – The Audit Committee is recommended to:

(i) Note the update report and actions taken to review SAP "Super User" access.

1. Background

1.1 The Council's external auditors (Grant Thornton UK LLP (GT)) as part of their 2018/19 Audit Findings Report, presented to the Audit Committee on 12 July 2019 and the Governance Committee on 16 July 2019, raised within the report's Action Plan a concern regarding SAP access:

Access to client maintenance functionalities (SCC4) (SAP access providing virtually full system rights). 13 users with firefighter ID's have access to using SCC4. Improper execution of client administration transactions could result in a loss of entire client (SAP system), including information, data and configured functionalities.

Recommendations: The profile should be reserved for use within an emergency and the number of firefighter type ID should be monitored with access being regularly reviewed.

This report provides an update in the actions taken and management response.

1.2 In addition, Internal Audit had undertaken an audit of SAP Application Controls in 2018. The audit opinion was Reasonable Assurance. The audit contained six actions agreed by management, including three rated as medium priority. In the context of the issue raised by GT, it was agreed to undertake a follow-up review to ensure management actions had been undertaken.

2. Supporting Information

2.1 IT&D have undertaken a review of the access to client maintenance functionalities, specifically SCC4, as set out in GT's report. Although there are 13 users which have access to the transaction SCC4, this access alone does not allow them to unlock the production environment. To be able to this, access to the object S_TABU_DIS vales SS and activity 02 is also required.

2.2 SAP access roles are 'packages' of related authorisations in the system usually for a specific business role or a process. In SAP, access to transactions cannot be given directly to the user but have to be delivered in these 'packages'. There are 2 SAP access roles in ESCC with access to SCC4 which are assigned permanently to the 3 Basis Team resources in the internal support team. However, during critical project activities such as during the annual

systems update, access to the SAP basis access roles is granted to extra resources (as authorised by the SAP Technical Manager) to be able to perform critical project activities.

2.3 Going forward the two existing SAP basis access roles will be modified to remove the ability to open the production system for changes with the transaction code SCC4. The access to open the client with direct table access in SAP will also be removed. There will be a new access role built specifically for the opening of the SAP client and the access will only be granted to the internal SAP Basis Team.

2.4 Additional SAP access can only be assigned to the user account without separate authorisation if the request comes from the process owner or if the requested access comes from the list of authorisation roles that do not require the process owner's approval. The Security Team runs monthly and ad hoc reports on user access in order to monitor users with critical transactions or inappropriate data access. The line managers are periodically requested to review their team's SAP access.

2.5 The Internal Audit Report: SAP Application Controls 2019/20 is attached at Appendix A. and presents an audit opinion of Substantial Assurance. Section 6 of the report provides as summary of the originally agreed six management actions and confirms that all but one have been implemented.

2.6 The management action for the development of additional templates to enable changes to be documented by IT&D has not been fully completed. An improved template and process has been developed to help facilitate the change request process in IT&D, but this has yet to be implemented.

3. Conclusion and reasons for recommendations

3.1 The Committee is recommended to note the report and actions taken to review SAP "Super User" access and previously agreed Management Actions from the Internal Audit Report: SAP Application Controls 2018/19.

IAN GUTSELL
Chief Finance Officer

Contact Officer: Ian Gutsell, Chief Finance Officer
Tel. No. 01273 481399
Email: Ian.Gutsell@eastsussex.gov.uk

Local Member(s): All

Background Documents: None