



### Digital controls review of Infor system administration

**Committee**            Audit and Standards

**Date of meeting**    29 November 2019

**Date of report**     19 November 2019

**Report by Assistant Chief Executive**

#### 1. Object of report

To advise the committee on the findings of a digital controls review of the Infor system administration. This engagement is included in the annual Internal Audit plan for 2019/20.

#### 2. Background

The Infor Enterprise Asset Management (EAM) platform is a multi-faceted system which allows SPT to manage assets and inventory including: trains, stations, and track infrastructure as well as building maintenance. EAM systems provide a holistic approach to asset management, allowing tracking of an entire asset lifecycle through to audit trails, safety and compliance and business intelligence.

A systems administrator/data custodian is responsible for the safe custody, transport, storage of data, implementation of business rules and contract management arrangements with the software service provider.

The objective of this engagement was to review the administration and application of the Infor EAM system.

This engagement tested elements of the internal controls and mitigation against SPT 7: loss of digital infrastructure.

#### 3. Outline of findings

Engagement testing (September 2019) found that Infor (EAM) software has been in use since 2009. The system was initially used in Subway stores for inventory management with further roll out to Engineering Maintenance and Facilities Management for work order management.

An implementation plan to roll out Infor (EAM) was agreed in 2016/17. Engagement testing found that the implementation plan requires refresh to reflect current service provision.

The systems administrator for the Infor (EAM) system is the information systems engineer based within the Subway engineering function.

The engagement identified a requirement to review and enhance system administration including user roles and privileges, procedural guidance and training arrangements.

There are areas for improvement, and these areas have been addressed by nine recommendations. Subway engineering management have agreed to implement these recommendations, which are currently being actioned.

Management requested an accelerated follow-up to be undertaken on the recommendations from this engagement. Follow-up testing as at early November found that two of the nine recommendations have been implemented with work continuing to progress the balance.

A follow-up performance review will be undertaken in early 2020 with the findings presented to the next Audit and Standards committee in February 2020.

#### 4. Conclusions

The Audit and Assurance team has undertaken a digital controls review of the Infor system administration. Nine recommendations have been agreed from this engagement.

A follow-up review found that two of the nine recommendations have been implemented, with revised timescales recorded, where appropriate.

Engagement testing found key controls exist but are not applied consistently and effectively.

Reasonable assurance with exceptions can be taken from the internal controls in place.

#### 5. Committee action

The committee is asked to note the contents of this report and agree that the Audit and Assurance Manager submits a further follow-up report on the implementation of the recommendations to the next meeting.

#### 6. Consequences

Policy consequences	<i>None.</i>
Legal consequences	<i>None.</i>
Financial consequences	<i>None.</i>
Personnel consequences	<i>None.</i>
Equalities consequences	<i>None.</i>
Risk consequences	<i>As detailed in the report.</i>

**Name** Valerie Davidson

**Name** Gordon MacLennan

**Title** Assistant Chief Executive

**Title** Chief Executive

For further information, please contact Iain McNicol, Audit and Assurance Manager on 0141 333 3195.

**Reasonable  
assurance  
with exceptions**

**Agreed action plan: Digital controls review of Infor system administration**

No.	Recommendation	Priority	Action Proposed	Lead Officer	Due date
1	<p><u>Documented procedures: system administration and use</u></p> <p>Procedural guidance should be reviewed and refreshed to include:</p> <ul style="list-style-type: none"> <li>• system administration processes and procedures (including process for new users, leavers and changes); and</li> <li>• all workflows and functionality in use.</li> </ul> <p>This refresh should serve as:</p> <ul style="list-style-type: none"> <li>- guidance to system users and an aide-mémoire in relation to training provision;</li> <li>- mitigate any departure from agreed procedures; and</li> <li>- strengthen system resilience arrangements.</li> </ul>	Medium	<p>The system administrator will consult with the Head of Engineering and Digital to identify roles and responsibilities. These roles will then be documented.</p> <p>Procedural guidance will be reviewed and refreshed.</p> <p>Where required, procedures will be incorporated into master file work instructions.</p>	Head of Engineering/ Information Systems Engineer	December 2019
2	<p><u>Infor implementation plan</u></p> <p>The Infor (EAM) implementation plan should be refreshed and maintained. The plan should clearly record the current status of key milestones.</p> <p>Governance arrangements should provide reporting including recording of any slippages and corrective actions required.</p>	Medium	The plan will be updated and progress against milestones regularly monitored and reported to senior management.	Head of Engineering/ Information Systems Engineer	December 2019

No.	Recommendation	Priority	Action Proposed	Lead Officer	Due date
3	<p><u>Monitoring of system service provision</u></p> <p>The system administrator should ensure the security arrangements for system use are in place and regularly monitored. Contract management arrangements include:</p> <ul style="list-style-type: none"> <li>• cloud data back-up arrangements;</li> <li>• risk management including security configurations and security test scans to reduce risk of hacking;</li> <li>• connectivity including access devices (locking down to SPT IP (Internet Protocol) addresses); and</li> <li>• cloud incident response arrangements.</li> </ul> <p>Advice should be sought from Digital to enhance resilience for the role of the Infor systems administrator and guarding against a single point of failure.</p>	High	<p>The system administrator will review the contractual terms and conditions and service level agreement. Where required, clarification will be obtained from the service provider.</p> <p>The systems administrator will liaise with Digital to review resilience arrangements.</p>	Information Systems Engineer	December 2019
4	<p><u>User Acceptance Testing (UAT)</u></p> <p>The systems administrator should maintain a log to evidence all UAT, results and formal sign off. This is an important part of a systems development process.</p>	Medium	Agreed, in future all user acceptance testing will be signed off as complete and satisfactory on handover to live environment.	Information Systems Engineer	Implemented

No.	Recommendation	Priority	Action Proposed	Lead Officer	Due date
5	<p><u>User roles</u></p> <p>The Infor system administrator should contact the software provider to clarify system user roles and privileges and obtain enhanced system usage reports.</p> <p>Thereafter, user roles should be reviewed for adequacy.</p> <p>The requirement for super-user access by any external consultant should be critically reviewed to 'as and when required' access facility.</p> <p>On a regular a basis (i.e. every period) the systems administrator should check external consultant/software supplier/Digital user activity to ensure no unauthorised activity or changes have been made. Exception reports should be developed for this purpose.</p>	High	<p>Agreed. The systems administrator will seek to standardise system user role and privileges reporting.</p> <p>The existing user roles will be reviewed for adequacy.</p> <p>Access will be reviewed to enable 'as and when required' access.</p> <p>System access will be monitored through audit trail functionality.</p>	Head of Engineering/ Information Systems Engineer	December 2019
6	<p><u>Quality, compliance and regulation</u></p> <p>The Infor system administrator should activate and manage audit trail functionality to ensure it meets the requirements of the business.</p> <p>Roles and responsibilities together with system privileges should be reviewed to ensure adequate separation of duties.</p> <p>The audit trail should also facilitate pro-active monitoring of external consultant activity and provide incident alerts.</p>	Medium	<p>Audit trail functionality will be reviewed for adequacy.</p> <p>Agreed. This may be a resource intensive exercise.</p> <p>Agreed. This will continue to be monitored proactively.</p>	Head of Engineering/ Information Systems Engineer	December 2019

No.	Recommendation	Priority	Action Proposed	Lead Officer	Due date
7	<p><u>Password controls</u></p> <p>Password changes should be enforced at regular intervals. Controls should not allow passwords to be flip-flopped. The time lapse permitted prior to system timing out should be reviewed and reduced.</p> <p>Passwords to access Infor should be in accordance with Digital Assets Acceptable Use procedures on password and security.</p>	High	Agreed. The systems administrator in conjunction with Digital will review current password controls, particularly in relation to mobile users with a view to enabling regular password changes.	Information Systems Engineer	December 2019
8	<p><u>Active Directory</u></p> <p>SPT active directory should be mapped to corresponding Infor accounts in the cloud.</p> <p>This will help ensure a corporate approach and control.</p>	High	The systems administrator will liaise with Digital to progress the use of active directory.	Information Systems Engineer	December 2019
9	<p><u>Training</u></p> <p>The systems administrator in conjunction with stakeholders should carry out a training needs assessment for Infor and provide training as required.</p> <p>Training records should be maintained up to date</p>	Medium	<p>The systems administrator will ensure authorised users have been training prior to allowing access to the system.</p> <p>Records will be updated accordingly.</p>	Head of Engineering/ Information Systems Engineer	Implemented

**High:** A fundamental control that should be addressed as soon as possible;

**Medium:** An important control that should be addressed within three months;

**Low:** An issue which is not fundamental but should be addressed within six months to improve the overall control environment.