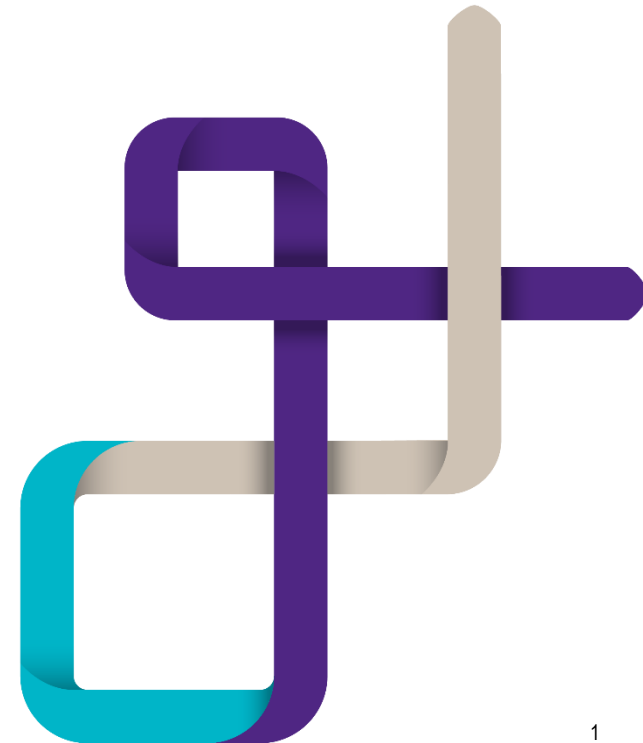


# IT Controls Report

*Year ending 31 March 2018*



University Hospitals of Leicester NHS Trust  
May 2018



# Contents



## Your key Grant Thornton team members are:

Mark Stocks

Engagement Lead

T: 0121 232 5437

E: mark.c.stocks@uk.gt.com

Emily Mayne

Senior Manager

T: 0121 232 5309

E: emily.j.mayne@uk.gt.com

Tess Barker-Phillips

Assistant Manager

T: 0121 232 5428

E: tess.s.barker-Phillips@uk.gt.com

## Section

## Page

### 1. IT Audit Findings

3

The contents of this report relate only to those matters which came to our attention during the conduct of our normal audit procedures which are designed for the purpose of expressing our opinion on the financial statements. Our audit is not designed to test all internal controls or identify all areas of control weakness. However, where, as part of our testing, we identify control weaknesses, we will report these to you. In consequence, our work cannot be relied upon to disclose all defalcations or other irregularities, or to include all possible improvements in internal control that a more extensive special examination might identify. This report has been prepared solely for your benefit and should not be quoted in whole or in part without our prior written consent. We do not accept any responsibility for any loss occasioned to any third party acting, or refraining from acting on the basis of the content of this report, as this report was not prepared for, nor intended for, any other purpose.

Grant Thornton UK LLP is a limited liability partnership registered in England and Wales: No.OC307742. Registered office: 30 Finsbury Square, London, EC2A 1AG. A list of members is available from our registered office. Grant Thornton UK LLP is authorised and regulated by the Financial Conduct Authority. Grant Thornton UK LLP is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. Services are delivered by the member firms. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.

## Key findings

We set out below our key findings against the significant risks we identified through our initial risk assessment and further risks identified through our ongoing review of documents.

1

### Assessment

### Issue and Risk

### Recommendation

  
(AMBER)

#### Proactive reviews of logical access within eFinancials and Active Directory

User accounts and associated permissions within eFinancials and Active Directory are not formally, proactively reviewed for appropriateness. We do however note that there is a process to review the appropriateness of access granted to users able to raise orders within eFinancials however this is limited to one role and does not consider the appropriateness of access granted to the wider user group.

This condition poses the following risks to the organisation:

- a) Gaps in user administration processes and controls may not be identified and dealt with in a timely manner.
- b) Access to information resources and system functionality may not be restricted on the basis of legitimate business need.
- c) Enabled, no-longer-needed user accounts may be misused by valid system users to circumvent internal controls.
- d) No-longer-needed permissions granted to end-users may lead to segregation of duties conflicts.
- e) Access privileges may become disproportionate with respect to end users' job duties.

It is our experience that access privileges tend to accumulate over time. As such, there is a need for management to perform periodic, formal reviews of the user accounts and permissions within Agresso and Active Directory. These reviews should take place at a pre-defined, risk-based frequency (annually at a minimum) and should create an audit trail such that a third-party could determine when the reviews were performed, who was involved, and what access changed as a result. These reviews should evaluate both the necessity of existing user ID's as well as the appropriateness of user-to-group assignments (with due consideration being given to adequate segregation of duties).




#### Management Response:

##### Active Directory

Active Directory user permissions are revised when users change roles on request of their line manager. It is the manager's responsibility to ensure their staff have appropriate (and not excessive) access to network resources and IT systems. IT act on change requests and provide a web based portal from where managers can check the access their staff have been granted within AD.


Staff leaving the organisation have their IT permissions revoked and AD account disabled.

#### Assessment

-  Significant deficiency - risk of significant misstatement
-  Deficiency - risk of inconsequential misstatement
-  No Deficiency

## Key findings

We set out below our key findings against the significant risks we identified through our initial risk assessment and further risks identified through our ongoing review of documents.

Assessment	Issue and Risk	Recommendation
1	 (AMBER)	<b>Andy Carruthers (Chief Technology Officer)</b>  <u>eFinancials</u>  Within eFinancials, the users fall into 3 main categories. Core users, requestors and approvers and I accept that the primary focus for the current reviews is around the requestors. A review / log of core users can be introduced fairly easily however if users have the wrong access they will not be able to carry out the role that they are employed to do, so the risk that the privileges may be disproportionate with their job duties is very low.  The review of approvers is not so straight forward as their access rights can be quite ‘fluid’ due to the nature of the business, but I will look into ways that this can be done – potentially incorporating an alignment with the budget reports that the approvers receive which has not been done before as the two areas of work are managed by two separate areas within Finance  <b>Mick Cook (Senior Finance Manager – Systems Development)</b>

### Assessment

- Significant deficiency - risk of significant misstatement
- Deficiency - risk of inconsequential misstatement
- No Deficiency

## Key findings

We set out below our key findings against the significant risks we identified through our initial risk assessment and further risks identified through our ongoing review of documents.

2

### Assessment

### Issue and Risk

### Recommendation

  
(AMBER)

#### Use of generic system administrator account in eFinancials

It was noted that there the following system administrator accounts are active and passwords are known by all members of the system admin team:

- Efin
- Efintestuser

While we acknowledge that the system automatically generates an audit log tracking user activity, this process does not identify the person in the team who used the account to perform the process

This condition poses the following risk to the organisation:

Generic accounts violate the principle of accountability, where all actions performed in a system can be linked to a named individual. This increases the risk that in the event of an error occurring, either by accident or design it cannot be traced to an individual to enable corrective actions to be taken.

The access rights of those users who perform the system admin functions should be reviewed to enable them to perform these tasks under their own named accounts. Generic accounts should be suspended or where this is not possible, the password should not be made available to more than one person.

#### Management Response:

The eFin and eFintestuser usernames and passwords are embedded within the system to run a range of automated processes including interface uploads. So the passwords can't be changed.

The Finance Systems Team have to know what the passwords are so that we can effectively deal with faults when working with the software provider. If only one person within the team knows the eFin password, what happens if there is a problem with the system while that person is off?

The eFin login is not used by the Finance Systems Team for day to day work as we have our own logins with full eFinancials administrator rights. This situation is likely to be the same for all eFinancials clients.

**Mick Cook (Senior Finance Manager – Systems Development)**

#### Assessment

- Significant deficiency - risk of significant misstatement
- Deficiency - risk of inconsequential misstatement
- No Deficiency

## Key findings

We set out below our key findings against the significant risks we identified through our initial risk assessment and further risks identified through our ongoing review of documents.

3

### Assessment

### Issue and Risk

### Recommendation

#### Weak logical access controls

  
(AMBER)

We noted the following logical access control weaknesses:

- a) Password complexity (i.e. the requirement that passwords must contain more than one character set, such as numbers and letters) was not enforced within eFinancials at time of review
- b) User accounts within eFinancials and Active Directory were not automatically locked (i.e., prevented from future logins) after a predefined, risk-based amount of unsuccessful login attempts

This condition poses the following risk to the organisation:

Compromise of user accounts through password guessing or cracking.

Where screensavers are not enabled after a period of inactivity, the following risks are posed:

- a) Misuse of unattended login sessions by other valid users of the system, leading to loss of accountability of actions performed.
- b) Misuse of unattended login sessions by unauthorised personnel, leading to unauthorised data disclosure or data tampering

Password complexity should be consistently enforced within eFinancials and Active Directory. Screensavers should be enabled after a period of inactivity (e.g. 10 – 15 minutes). Where / if possible, management should enable account lockout controls within Active Directory to address the risk of password cracking. Where / if an account lockout restriction cannot be enforced due to system limitation or other reasons, management should explore other controls designed to address the risk of password cracking within Active Directory and eFinancials. Alternative controls could include increased monitoring of login activity or more stringent enforcement of password length and complexity requirements.

#### Management Response:

##### Active Directory




Active Directory account lockout threshold is not currently enforced, this has been the case to historic operational disruption that was caused when enforced.

##### **Andy Carruthers (Chief Technology Officer)**

##### eFinancials


The key point to note about password complexity within eFinancials, is that this is totally outside of UHL's control as this is embedded within the core product.

#### Assessment

-  Significant deficiency - risk of significant misstatement
-  Deficiency - risk of inconsequential misstatement
-  No Deficiency

## Key findings

We set out below our key findings against the significant risks we identified through our initial risk assessment and further risks identified through our ongoing review of documents.


Assessment	Issue and Risk	Recommendation
3	 (AMBER)	<p>The current eFin v4.1 Security password ‘rules’ do not comply with the complexity requirements. This is improved in the eFin v5.0 Security which does comply with the requirements detailed above, but when we do upgrade to eFin v5.0 later this year, we will be using eFin Single Sign On (SSO), which uses its own security rules, and whilst the password rules within SSO are an improvement on the current v4.1 rules. They do not go as far as the rules within eFin v5.0.</p> <p>I will be discussing this with Advanced to look at ways this can be improved, but getting this changed is not within our control.</p> <p><b>Mick Cook (Senior Finance Manager – Systems Development)</b></p>

### Assessment




- Significant deficiency - risk of significant misstatement
- Deficiency - risk of inconsequential misstatement
- No Deficiency

## Key findings

We set out below our key findings against the significant risks we identified through our initial risk assessment and further risks identified through our ongoing review of documents.

Assessment	Issue and Risk	Recommendation
4  (AMBER)	<p><b>Automated notifications of leaver activity</b></p> <p>Security administrators eFinancials were not being provided automated, proactive notifications of anticipated HR leaver activity, nor were they being provided automated per-occurrence notifications of unanticipated HR leaver activity.</p> <p><u>This condition poses the following risk to the organisation:</u></p> <ul style="list-style-type: none"><li>a) Access to information resources and system functionality may not be restricted on the basis of legitimate business need</li><li>b) Enabled, no-longer-needed user accounts may be misused by valid system users to circumvent internal controls</li><li>c) Terminated employees may continue to access information assets through enabled, no-longer-needed user accounts</li><li>d) Revocation of access rights may not be performed accurately, comprehensively, or on a timely basis</li></ul>	<p>Security administrators of eFinancials should be provided with (a) timely, proactive notifications from HR of leaver activity for anticipated terminations and (b) timely, per-occurrence notifications for unanticipated terminations. These security administrators should then use these notifications to either (a) end-date user accounts associated with anticipated leavers or (b) immediately disable user accounts associated with unanticipated leavers.</p> <p><b>Management Response:</b></p> <p>Although this refers to eFinancials, obtaining this information is down to how HR collate the leaver data. We currently receive a monthly report from HR and this is cross referenced against our eFin user records.</p> <p><b>Mick Cook (Senior Finance Manager – Systems Development)</b></p>

### Assessment

-  Significant deficiency - risk of significant misstatement
-  Deficiency - risk of inconsequential misstatement
-  No Deficiency