

Institute of Technology Blanchardstown

Internal Audit Review of IT Systems Security and Controls

Date: 18 November 2016

Ref: 2016/IT01

Report Distribution

Audit Committee

Top Management Group

Denis Murphy (Secretary/
Financial Controller)

Dave Curran (IT Manager)

Executive Summary

The Review of IT systems security and controls was identified and agreed as an area for review as part of the 2016 Internal Audit plan. The objective was to perform detailed testing of the design and operating effectiveness of key controls and processes in place over IT within Institute of Technology Blanchardstown (ITB' or 'the Institute'). The in-scope systems for testing purposes were the Agresso and Banner systems.

We identified a number of good working practices in ITB, particularly the approach to securing the network and in defining and communicating the roles and responsibilities of staff members within the IT department. Overall we identified 5 findings rated as follows:

Rating	Significance	No. of findings
Grade 1	Critical	1
Grade 2	Substantial	2
Grade 3	Moderate	2

The Grade 1 and 2 findings are summarised below:

- **Access to server and communication rooms is not appropriately restricted.** All levels of senior management have access to two server rooms and seven communications rooms. Access to the rooms is granted by the Estates office without sign off from the IT department. Access to the rooms is not tracked.
- **Weaknesses exist in the joiners, movers, leavers and user access review processes:** Weaknesses were identified within each of these processes which may lead to inappropriate access to systems and data.
- **Password policy does not meet good practice requirements and weak password controls were identified.** This may lead to unauthorised access to systems.

Use of this Report

This report is intended for the information and use of ITB and is not intended to be relied upon by anyone other than ITB. We accept no duty of care and deny all liability to any third party that places reliance on our report.

We have provided no opinion, attestation or other forms of assurance with respect to our services or the information upon which our services are based. We did not audit or otherwise verify the information supplied to us in connection with this engagement, from whatever source, except as specified in our Terms of Reference (Appendix A).

Our work was performed in accordance with the PwC's Internal Audit Methodology which is consistent with the Chartered Institute of Internal Auditors International Standards for the Professional Practice of Internal Auditing. As agreed, the review did not constitute an examination in accordance with full scope generally accepted auditing standards.

Acknowledgement

We would like to thank all personnel who assisted and facilitated us in carrying out this review.

PricewaterhouseCoopers

PricewaterhouseCoopers

November 2016

Audit Overview

Objectives

The objective of the internal audit was to review and test the design and operating effectiveness of the IT general controls, IT policies and procedures that are in place for ITB and in particular for the Agresso and Banner systems.

Scope and Approach

The scope of our work on this internal audit engagement included the following:

- Review of the governance processes over the IT function;
- Review of the general IT control environment including management and support for the corporate email network and the internet;
- Review of the IT policies and procedures against good practice;
- Review of the application of IT policies and the operation of IT general controls over the Banner and Agresso systems. Areas of focus included:
 - Password security and logical access controls;
 - User access administration;
 - Change management;
 - Backup and recovery;
 - Disaster Recovery; and,
 - Business Continuity.

The Core system was deemed out of scope for this review as it was being upgraded during the audit.

Our approach to this review comprised of the following tasks:

- Gained an understanding of the IT policies, procedures and IT general controls in place;
- Performed a desktop review of key relevant IT policies and procedures;
- Conducted meetings with relevant stakeholders;
- Conducted walkthroughs to evaluate the design and implementation of relevant controls and review relevant documentation;
- Performed testing on a sampling basis of the identified key controls to evaluate their operating effectiveness; and,
- Reported any gaps/weaknesses identified.

Summary of Findings

Finding	Rating
1. Access to server and communication rooms is not appropriately restricted	Grade 1
2. Weaknesses exist in the joiners, movers, leavers and user access review processes	Grade 2
3. Password policy does not meet good practice and weak password controls identified	Grade 2
4. Inadequate visibility over IT operations activity	Grade 3
5. IT governance weaknesses	Grade 3

Detailed Findings & Recommendations

1. Access to server and communication rooms is not appropriately restricted

Finding	Rating & Implication	Recommendation	Management Action Plan
<p>All senior management personnel within ITB have access to two server rooms and seven communication rooms via their access cards. This is not in line with best practice as all of the personnel do not require this access as part of their day to day role.</p> <p>The granting of access to employees and 3rd parties to server and communication rooms is the remit of the Estates office rather than the IT Department. Therefore, a request for access to a server or communication room does not require sign off from the IT Department.</p> <p>In addition, PwC observed that a log of access to the server or communication rooms is not maintained.</p>	<p>Grade 1</p> <p>The IT department may not be aware of who is accessing the server rooms which may lead to inappropriate access to the server and /or communications rooms.</p> <p>This represents a significant risk to the security and integrity of the hardware and data being stored in the server rooms.</p> <p>This also leaves ITB open to potential malicious or cyber threats resulting from inappropriate persons having direct physical access to the servers.</p>	<p>In order to ensure that access to the server and communications rooms is restricted to appropriate personnel only, the following measures are recommended:</p> <ul style="list-style-type: none"> Establish a process whereby an access request form requires IT manager sign-off on any request for access to these rooms. Create and maintain an access log for these rooms and enforce its use for all staff and site visitors, including third party contractors. This log should include at a minimum fields for the individual's name, reason for access, and time/date of entering and leaving the room. This access log should be reviewed by an individual of sufficient authority on a regular basis to ensure that only appropriate personnel with a valid reason are accessing the server and communications rooms. 	<p>Management accept the finding that relatively open access to the rooms requires modification and will plan a revised access, permission and review process. Access to the rooms is currently restricted to those with the appropriate permissions and an audit log of users can be run from the door security system, giving details of card used to enter and time and duration of presence. The updated access plan will incorporate the recommendations listed. However, in the context of the Health and Safety aspects of the Institute's operations and, in particular, lone worker issues the following will be addressed in the plan:</p> <ul style="list-style-type: none"> Each door will provide clear visibility from the corridor of the interior working area. Only work that requires an individual's presence in the room is carried out there (many IT functions can be carried out remotely). Estates will notify IT manager/ designated deputy of requirement for access for essential maintenance, cleaning. President and Registrar as line management, HR manager and SFC as holders of the Institute's duty of care to employees and the Estates/Campus Services Manager as H&S duty holders will retain access rights An access log for each room will be

Finding	Rating & Implication	Recommendation	Management Action Plan
			<p>produced for review by the IT manager, registrar or auditor as required.</p> <ul style="list-style-type: none"> - Issues arising from an access review will be considered by a group representing the functions noted in point above <p>Target Date 31st January 2017</p> <p>Responsible Party IT Manager</p>

2. Weaknesses exist in the joiners, movers, leavers and user access review process

Finding	Rating & Implication	Recommendation	Management Action Plan
<p>PwC noted the following weaknesses with respect to the joiners and leavers process:</p> <p><u>Joiners / Movers:</u></p> <ul style="list-style-type: none"> System access is granted by IT to new joiners to the Institute on receipt of a request from the HR department. However, system access is granted by IT to existing Institute staff (i.e. who move internally) on receipt of a request from an appropriate source within the user's Department. Segregation of duty requirements have not been formally defined by the business. Potential segregation of duty conflicts are not formally assessed by the business when requesting user access set up or amendment. <p><u>Leavers:</u></p> <ul style="list-style-type: none"> The "User Exit" policy maintained by ITB states that one of the responsibilities of a leaver is to direct the IT department to delete their network user account and access privileges associated with their role. This is not in line with best practice which would advocate that a responsible individual within the business / organisation should be central to this process (i.e. the line manager) to provide oversight and ensure 	<p>Grade 2</p> <p><u>Joiners/ Movers:</u></p> <p>There is an increased risk that inappropriate or unauthorised access or amendments may be made to systems and data if user access is not defined and implemented based on appropriate segregation of duties, especially when users move in between Departments.</p> <p><u>Leavers:</u></p> <p>Account users departing the Institute may not be removed from the network or applications and may therefore retain inappropriate access to systems and data.</p> <p>Where leaver's system or network accounts are not disabled in a timely manner there is a risk unauthorised or inappropriate access to systems may be gained using the these accounts.</p>	<p><u>Joiners/ Movers:</u></p> <ul style="list-style-type: none"> ITB should create and document a security design document which outlines segregation of duties requirements based on the functional and business requirements of the role / user. This exercise should be led by the business owners of the systems and data and be supported by IT management. Once defined, a formal process should be implemented to review possible segregation of duties conflicts on a regular basis. The review should ensure that any conflicting access (of both IT and business users) is removed or mitigating business process controls identified. <p><u>Leavers:</u></p> <ul style="list-style-type: none"> Terminated employees should have their access to systems and the network removed on or within a short period of time after their leave date. In order to ensure all users are captured by the leaver's process one of the following measures are recommended: <ul style="list-style-type: none"> Utilise functionality within the Core HR system which can ensure that an automated email is sent from the Core HR system to the IT 	<p><u>Joiners /Movers</u></p> <p>Current segregation of duties will be documented and reviewed. As an outcome of the initial review the regularity and process for future reviews will be agreed.</p> <p><u>Movers</u></p> <p>It is agreed that there is a need to identify staff who move between departments and to notify the amended access requirements to the IT Dept. This will form part of the HR process around movers.</p> <p>Target Date</p> <p>31st March 2017</p> <p>Responsible Party</p> <p>Business Owners & IT</p> <p><u>Leavers</u></p> <p>The responsibility to inform the IT Department and direct them to delete user accounts and remove access from those who resign or retire lies with the HR Department – this is documented as part of the 'HR Exit Checklist'. The IT Department are informed of the departure /cessation date via e-mail and requested to remove access and delete accounts.</p> <p>The HR Department agrees to review and update the current manual checklist and to include the Finance Manager/Dept. on the e-mail information and instruction and will also investigate the potential for the</p>

Finding	Rating & Implication	Recommendation	Management Action Plan
<p>that the procedure is carried out adequately.</p> <ul style="list-style-type: none"> When an individual leaves ITB, no formal communication is made to the IT administrators of either of the in-scope applications. Therefore, leavers may retain their access rights inappropriately on the application after their termination date. On review of the user access log, PwC identified two users that had inappropriate access for their role. Retired users ITB e-mail accounts are maintained following termination. <p><u>User access reviews:</u></p> <ul style="list-style-type: none"> Banner is not subject to formal regular user access reviews. Agresso is reviewed on an informal, ad-hoc basis at the discretion of the IT administrator for the system. A formal user access review is scheduled for the network twice per annum, however, in recent times it has only been completed once per annum. 		<p>Administrators of each system signalling that individual's employment is about to end.</p> <ul style="list-style-type: none"> Alternatively, require the user's direct manager to submit a request to remove system and network access on departure. Access to retired users ITB email accounts should be subject to regular recertification. Where access is no longer required, the account should be removed. <p><u>User access reviews:</u></p> <ul style="list-style-type: none"> Review and recertify user access for each key application on a quarterly basis. This review should be formally documented and the reviewer should evidence that they have performed the following procedures: <ul style="list-style-type: none"> Ensure that access privileges remain appropriate. Check that redundant authorisations have been deleted (e.g. for employees who have changed roles or left the organisation) Identify and request removal of inactive accounts in a timely manner (i.e. within one month of quarter end). 	<p>automated email within the Core upgrade.</p> <p><u>Retirees</u></p> <p>Access to a retiree's email account by ITB will be deactivated formally 6 months after the retirement date.</p> <p>Target Date</p> <p>January 2017</p> <p>Responsible Party</p> <p>HR Manager</p> <p><u>User access reviews</u></p> <p>A full user access review will be carried out on all systems by the end of the first quarter 2017. As an outcome of the initial review the regularity and process for future reviews will be agreed. It will also be informed by the access systems of the new or upgraded packages being sourced through Educampus.</p> <p>Target Date</p> <p>31st March 2017</p> <p>Responsible Party</p> <p>Business Owners</p>

3. Password policy does not meet good practice and weak password controls identified

Finding	Rating & Implication	Recommendation	Management Action Plan
<p>During testing of passwords PwC identified the following exceptions to good practice.</p> <ul style="list-style-type: none"> Password History: The password policy does not require the network or either in-scope system to remember previous passwords to prevent reuse. Good practice recommends that systems record the previous 10 passwords used and prevent reuse. Unsuccessful login attempts before account lockout: Neither the network nor the in-scope systems are required to lock after a number of unsuccessful login attempts per the password policy. Good practice recommends a maximum of 5 unsuccessful login attempts before the account is locked. <p>PwC also identified the following weaknesses:</p> <ul style="list-style-type: none"> Due to system limitations, passwords on Banner do not adhere to any of ITB's policy for password parameters. Both Agresso and the network's password specifications do not adhere to ITB's policy regarding maximum password age. "Password History" and "Unsuccessful login attempts before account logout" parameters were not set for Agresso. "Unsuccessful login attempts before account logout" parameters were not set for the network. 	<p>Grade 2</p> <p>Weak password policies within systems or the network increase the risk that logical access controls will be compromised, leading to unauthorised access to systems and data or a malicious user successfully targeting these systems.</p>	<ul style="list-style-type: none"> Amend the ITB password policy to ensure that it aligns to the good practice requirements outlined with the finding. Where system constraints do not allow adherence to ITB password policy, alternative mitigating controls should be identified, implemented and formally monitored. Acceptance of any residual risk should be formally signed off by ITB Senior Management. 	<p>Subsequent to a previous audit, ITB network password complexity and policy were changed to reflect a position similar to the PwC recommendations. The policy proved unsatisfactory to staff and students who reacted by adopting poor practice. Incidents were reported of passwords written on post-its and appended to PC screens and keyboards. Students were continually missing laboratory sessions as they had 'locked' their account and were unable to fully participate in class.</p> <p>An increase in the number of callers to the helpdesk to have their password reset, was also noted. IT management has formed the view that current policy enforcement represents a balanced position in this regard. The current Policy will be reviewed to ensure it reflects best practice and all current practices will be reviewed to ensure compliance with the Policy. Where system limitations allow password specifications will adhere to the Institute policy. Banner will be a continuing problem until the upgrade/new system is installed over the next two years.</p> <p>Target Date 31st January 2017</p> <p>Responsible Party Business Owners and IT Manager</p>

4. Inadequate visibility over IT operations activity

Finding	Rating & Implication	Recommendation	Management Action Plan
<p>ITB outsources elements of its IT operations to HP including; operation of the central IT help desk and incident tracking ticketing system, hosting the Agresso and Banner applications, and backup of these systems. The following issues were noted in relation to this arrangement:</p> <ul style="list-style-type: none"> The HP ticketing system is occasionally circumvented by ITB staff and where an incident arises tickets may be logged directly with HP, via call, rather than going through the help desk function, therefore IT are not aware of all IT issues. IT do not formally monitor open tickets to track timely closure. Back up restore testing is not performed periodically by HP. Through discussion with IT Management it was noted that HP currently provide a Service Review Report to the Institute on an annual basis to compare its responsibilities per the SLA with its performance. However, the current format of these reviews is not useful to the Institute as it generalises HP's performance across all Institutes instead of on an individual basis. 	<p style="text-align: center;">Grade 3</p> <p>There is a risk that data may not be accurately and completely processed.</p> <p>Without formal documentation of the escalation and resolution procedures performed management cannot be sure that operational errors are identified, escalated and resolved in a timely fashion</p> <p>There is a risk it may not be possible to restore from backup as backups may not be copied correctly or backup media has been corrupted.</p>	<ul style="list-style-type: none"> Enforce consistent call logging with the central IT help desk rather than directly with HP. Periodically review closure of tickets to ensure closure within an appropriate timeframe. Request back up restore tests to be performed at regular intervals by HP. Request HP to include details of institute specific back up success rates and restore test results in monthly reporting. 	<p><u>HP Ticketing System</u> Staff will email HP with server issues and will include the IT department on all future emails. (Immediate – Business Owners)</p> <p><u>Formally Monitor Open Tickets</u> The feasibility of doing this will be examined with a report back by end of March 2017. (IT Manager)</p> <p><u>Back up restore testing</u> Backup and restore testing is conducted on an ongoing basis. HP maintains a pre-production environment and a Disaster Recovery site. Institutes may request that a copy of live data is backed up and restored to the pre-production environment at any time of its choosing. HP are contracted to implement an annual Disaster Recovery exercise. This exercise occurs in December and is simulated using the MIS systems of a single Institution.</p> <p><u>Service Review Report</u> This recommendation has been reported to HP who are considering the request.</p> <p><u>Target Date</u> As above</p> <p><u>Responsible Party</u> IT Manager</p>

5. IT governance weaknesses

Finding	Rating & Implication	Recommendation	Management Action Plan
<p>PwC reviewed the IT governance procedures in place in ITB and noted the following:</p> <ul style="list-style-type: none"> The IT Strategy was drafted in 2012 for a three year period ending October 2015. It has not since been updated. To remain relevant, the IT Strategy needs to be kept up to date and continuously reviewed to assess the ongoing relevance of IT objectives. A formal Service Level Agreement is not in place between IT and the business and hence no formal reporting against such an agreement is performed. The Institute does not have a fully formal process whereby third party performance is reviewed against agreed service levels. ITB rely on third party vendors such as HP, HEAnet and Educampus to provide services and perform key IT control activities. Though service is reviewed for HEAnet, performance versus agreed SLAs is not formally documented for the review. 	<div>Grade 3</div> <p>Without an up to date IT Strategy, the objectives of the IT department may not be aligned with the business objectives. This leads to a risk of the IT department not fully or efficiently supporting the overall business plan.</p> <p>Without formal Service Level Agreements, it is difficult to measure how well the IT function is delivering its service.</p> <p>Without the adequate monitoring of third party performance in relation to IT controls, performance may not be in line with management expectation. Service or control issues may go undetected or rectified.</p>	<ul style="list-style-type: none"> Management should prioritise the updating of the current IT Strategy document. IT should work with the business to define, document and implement a formal service level agreement detailing the services IT will provide to the business. Establish a process whereby IT are responsible for reviewing third party performance against agreed service levels at regular intervals and formally document reviews conducted. 	<p><u>IT Strategy</u> IT Management in ITB and IT Tallaght are collaborating to draft IT Strategy and Cloud policy documents in preparation for the merged entity. These documents are dependent on the final versions of the respective Institutes strategic plans, currently in the final phases of development. (June 2017)</p> <p><u>Formal SLA</u> ITB management have previously considered and subsequently rejected the imposition of inter-department SLA's. This decision will be reviewed in the context of the TU creation and consequent servicing of a multi-campus environment. This will be assessed by 31st March 2017</p> <p><u>Third Party Performance</u> HP produce performance against SLA reports on behalf of Educampus. ITB IT management have advised HP that the reports are not fit for purpose. The HP service contract is coming to an end and the new vendor will be required to supply enhanced performance reports (ref. Educampus). This will be assessed by 31st March 2017</p> <p><u>Responsible Party</u> IT Manager</p>

Appendices

Appendix A – Assigning Ratings for Findings

Appendix B – List of Personnel Interviewed

Appendix A – Assigning Ratings for Findings

Rating	Basis of our classification
Grade 1	<p>A critical weakness which could compromise internal controls potentially resulting in significant loss to IT Blanchardstown or which could be interpreted as a critical weakness in the governance oversight function of IT Blanchardstown and which should be addressed as a matter of urgency.</p> <p>A finding that could have a:</p> <ul style="list-style-type: none"> • Critical impact on operational performance e.g. resulting in major disruption to Institute or inability to provide a quality service to students for more than 3 days, or leading to a loss of the majority of students; <i>or</i> • Critical monetary or financial statement impact; <i>or</i> • Critical breach in laws and regulations e.g. resulting in material fines, penalties being levied on the Institute or funding being withheld; <i>or</i> • Critical impact on IT Blanchardstown's reputation or brand e.g. resulting in sustained adverse national and/ or international media coverage and political reaction
Grade 2	<p>A control weakness which could undermine the system of internal controls and / or operational efficiency and should be addressed within three months.</p> <p>A finding that could have a:</p> <ul style="list-style-type: none"> • Substantial impact on operational performance e.g. resulting in disruption to IT Blanchardstown or inability to provide a quality service to students for up to 3 days, or leading to a loss of a significant number of students <i>or</i> • Substantial monetary or financial statement impact; <i>or</i> • Substantial breach in laws and regulations e.g. resulting in substantial fines and consequences; <i>or</i> • Substantial impact on IT Blanchardstown's reputation or brand e.g. resulting in unfavourable national, or local media coverage, or a significant number of student complaints
Grade 3	<p>A weakness which does not seriously detract from the system of internal controls and / or operational efficiency but which should nevertheless be addressed by management within six to 12 months.</p> <p>A finding that could have a:</p> <ul style="list-style-type: none"> • Moderate impact on operational performance e.g. resulting in limited disruption to Institute or inability to provide a quality service to students for up to 4 hours, or limited impact on students; <i>or</i> • Moderate monetary or financial statement impact; <i>or</i> • Moderate breach in laws and regulations with no fine, and no regulatory investigation; <i>or</i> • Moderate impact on IT Blanchardstown's reputation or brand e.g. resulting in limited media coverage, or some student complaints
Observation	<p>A finding that does not detract from the system of internal controls and / or operational efficiency but which should be addressed by management within 12 to 18 months. Findings in this category can be raised to highlight areas of inefficiencies or suggested good practice.</p> <p>A finding that could have a:</p> <ul style="list-style-type: none"> • Minor impact on operational performance e.g. resulting in disruption of non-core activities for up to 2 hours; <i>or</i> • Minor monetary or financial statement impact; <i>or</i> • Minor breach in laws and regulations; <i>or</i> • Minor impact on IT Blanchardstown's reputation e.g. resulting in no media coverage and no student complaints.

Appendix B – List of Personnel Interviewed

We met with, or obtained information from, the following people throughout the course of our review.

Name	Title
Dave Curran	IT Manager
Tim O'Sullivan	Senior Technical Officer
Cora Bracken	Banner Administrator
Amanda Brennan	Agresso Administrator

www.pwc.com