Grant Thornton

An instinct for growth™

**Paul Rao**
Engagement Lead
T: 016 1953 6303
E: Paul.Rao@uk.gt.com

**Joshua McGee**
Assistant Manager
T: 020 7865 2838
E: Joshua.M.McGee@uk.gt.com

**Riza Unal**
Manager – Subject Matter Expert
T: 020 7383 5100
E: Riza.Unal@uk.gt.com

**Nick Shaw**
Primary Auditor
E: Nick.F.Shaw@uk.gt.com

# The Health and Care Professions Council

## Cyber Security Review

Last updated 22 February 2018

| Distribution | | Timetable | |
|---|---|---|---|
| For action | Guy Gaskins, Director of Information Technology (IT) | Fieldwork completed | 24 January 2018 |
| | Jason Roth, Infrastructure Manager | Draft report issued | 12 February 2018 |
| | Rick Welsby, IT Support Manager | Management comments | 14 February 2018 |
| For information | Andy Gillies, Finance Director | Final report issued | 22 February 2018 |
| | Audit Committee | | |

# Contents

## Sections

## Appendices

## Glossary

The following terms are used in this report:

ATA – Advanced Threat Analytics

CD – Compact Disk

HCPC - Health and Care Professions Council

HR – Human Resources

ISO – International Standards Organisation

IT – Information Technology

SAB – Security Advisory Board

SLA – Service Level Agreement

SMTP – Simple Mail Transfer Protocol

USB – Universal Serial Bus

This report is confidential and is intended for use by the management and Council members of the Health and Care Professions Council only. It forms part of our continuing dialogue with you. It should not be made available, in whole or in part, to any third party without our prior written consent. We do not accept responsibility for any reliance that third parties may place upon this report. Any third party relying on this report does so entirely at its own risk. We accept no liability to any third party for any loss or damage suffered or costs incurred, arising out of or in connection with the use of this report, however such loss or damage is caused.

It is the responsibility solely of the Health and Care Professions Council's management to ensure that there are adequate arrangements in place in relation to risk management, governance and control.

# 1 Executive Summary

## 1.1 Background

The Chair of the Audit Committee at HCPC asked Grant Thornton to review the cyber security arrangements deployed at HCPC. Though not part of the initial 2017/18 Internal Audit Plan, the Audit Committee sought assurance on the arrangements and controls the organisation has deployed for this topic due to the attention that cyber-attacks have gained in the news. Whilst the council was not affected by the most recent ransomware attack that affected several companies worldwide, including the NHS system, there is an internal recognition that cyber security entails more than generic patching within servers.

The IT department is subject to several audits across the year either due to external auditors (performed by the National Audit Office), internal process improvements (in-house), internal audit (Grant Thornton) or by regulation (Professional Standards Authority for Health and Social Care). We have been informed that the last cyber audit was performed in 2012 by the previous internal auditors contracted by HCPC.

HCPC has adopted the ISO27001:2015 standard, which is a framework of policies and procedures that include all legal, physical and technical controls involved in an organisation's information risk management processes. HCPC was certified to ISO27001 in 2016, with the most recent re-certification taking place in April 2017. Several IT controls have been deployed across the organisation such as internal and external regular penetration testing, credit card information not being held on HCPC’s IT environment, double authentication for remote connections and restriction on use of removable media, amongst others. Though not an extensive list of all the information security controls deployed at HCPC, it does provide some context of the extent of work the IT department has incurred so far to ensure that appropriate controls are implemented.

## 1.2 Objective and risk areas

The objective of the review is to assess whether the policies, processes, procedures and controls in relation to Cyber Security are adequate, in place and being adhered to.

Specifically, the review focussed on the following risks:

- There are inadequate user and IT policies and procedures and or governance procedures in place, leading to misunderstanding of appropriate /inappropriate use of IT and inconsistencies in approach and possible security breaches
- System configuration (including logical security controls) are insecure leading to inappropriate access to; and/or amendments to data; or data loss
- There are inadequate preventive controls or monitoring to counter or detect network security threats and events; leading to network access violations or network unavailability
- There are ineffective controls around malware prevention and removable media leading to data theft/loss or corruption.
- Third party services are not subject to effective assurance, leading to security breaches.

## 1.3 Scope

Specifically, the review examined the following:

- **User education and awareness**: security policies have been produced and communicated across the organisation, and employees are made aware of their personal security responsibilities
- **Logical security (include remote access)**: measures deployed to ensure that only authorised users are able to access information in HCPC network
- **Secure platform configuration**: network appliances, hosts and client computers have been security hardened (benchmarked against good practice), an asset inventory exists and automated vulnerability scans are run against all network devices to remedy any vulnerabilities
- **Network security**: multi-layered boundary defences with firewalls and proxies have been deployed between trusted and untrusted networks; intrusion monitoring tools have been deployed across the network; cyber-attack exercises are carried out on a regular basis
- **Malware prevention**: there is a defined approach to manage risks associated with malware in workstations, laptops, servers and across the network
- **Removable media controls**: a removable media acceptable use policy has been produced and communicated, supported by appropriate technology controls
- **Third party assurance (including cloud services)**: assurance on the services provided by suppliers (including security) is achieved at the contractual level, SLA monitoring, the involvement of service owners and others.

The review focused on the areas considered to have the greatest risk, as agreed with management. Therefore, our review did not consider:

- Risk management
- Incident management
- Disaster recovery or business continuity
- Whether the IT Security arrangements in place are compliant with any standards or regulations such as the Data Protection Act or the General Data Protection Regulation
- Data governance arrangements and procedures in respect of data protection, classification, retention and handling is excluded from the scope of this review. We understand as part of the ISO27001 accreditation for information security a full audit of this area will be undertaken in April 2018.

In addition, the performance of any penetration tests or vulnerability assessment of any kind, or running pervasive tools across the network, was out of the scope of this review

Further details on our approach are included in Appendix A.

## 1.4 Overall assessment

The Audit Committee commissioned internal audit to perform a review of the organisation’s cyber security framework and arrangements. This review focused on the technical aspects and configurations of HCPC's cyber security controls. Upon and evaluation, HCPC's cyber security posture appears to be well developed and managed in a risk-based manner. We noted that a well-defined process to manage access to the network, and closely managed the configuration of firewalls, laptops, desktops, and network servers. We also noted that anti-virus is consistently used across the environment and used to screen emails, patching is actively managed, physical and wireless connections to the network are strictly controlled, and that system accounts for vendors are strictly controlled through multi-factor authentication.

Notwithstanding the areas of good practice noted, our review identified areas where the current control framework can be enhanced. Specifically we noted three medium and 5 low findings. We noted that while there is a process in place to review network access to share drives on a monthly basis, there is no process in place to ensure that responses are obtained from department heads to ensure a complete review of users and associated network permissions is conducted. Additionally, we noted that management could improve both their management of removable media that is permitted on the HCPC network, and the expectations that are set with outsourced IT services such as Rackspace, on when they are required to report on outstanding security issues that may have an impact on HCPC's security posture

This review also noted other lower-risk observations relating to network security, emergency patching, and monitoring procedures for user activity monitoring tools.

Below we have included an assessment of each risk area assessed as part of this audit and a summary of the key actions emerging from the audit. See Appendix B for more information regarding our definitions for our issue ratings.

The table below details the key findings from our review.

## 1.5 Key findings

| Risk / Process | High | Medium | Low | Info. |
|---|---|---|---|---|
| User education and awareness | - | - | - | - |
| Logical security | - | 1 | 1 | - |
| Secure platform configuration | - | - | 1 | - |
| Network security | - | - | 3 | - |
| Malware prevention | - | - | - | - |
| Removable media controls | - | 1 | - | - |
| Third party assurance | - | 1 | - | - |
| **Total** | - | **3** | **5** | **-** |

Further details of our findings and recommendations are provided in Section 2 of this report.

## 1.6 Acknowledgment

We would like to take this opportunity to thank the staff involved for their co-operation during this internal audit. Their details can be found at Appendix A.

# 2 Detailed Findings

| 1. | Medium | Monthly user access reviews |
|---|---|---|

| Finding and Implication | Proposed action | Agreed action *(Date / Ownership)* |
|---|---|---|
| Good Practice<br>Access management is a key area within an IT security framework, as it should ensure that data is only accessible to authorised and necessary individuals. It is good practice to implement processes to ensure that all access requests (and changes to existing access rights) are reviewed and approved before being granted, and that access is removed when no longer necessary. In addition, periodically reviewing users' access rights ensures that access remains appropriate and commensurate with job responsibilities.<br><br>Finding<br>We noted that HCPC management has begun to request that department heads revalidate appropriateness of access for users who have access to their respective departments' share drive on a monthly basis. However, not all department heads were revalidating this access as requested. Additionally, there is no documented process in place that provides a path to escalate this non response and ensure that access is ultimately reviewed on the frequency defined by management. Access to organisation-wide assets such as the network is key to ensuring that HCPC can demonstrate that it is appropriately implementing security controls to protect personal data that is held by HCPC. | **R1:** Management should develop policies and procedures to formalise the monthly user access review process, including an escalation process if non response persists from department heads.<br><br>Additionally, management should coordinate with department heads and line managers throughout the organisation to identify opportunities to expand this user access review to include application level access that may be provisioned at the department level such as HCPC's core financial systems, which are provisioned by the finance department. | ***R1:*** *Robust controls for the starters and leavers process enforce access controls to the network infrastructure. The current procedure for managing user access prevents a user from accumulating access rights by enforcing rights that are specific to a single team and role.*<br><br>*Secondary access controls are maintained within business applications and are maintained by each specialist business teams.*<br><br>*A policy and procedure will be developed to clarify the user access revalidation process including the escalation procedure for this secondary control. Owner: Director of IT by April 2018.*<br><br>*The IT team will work with the Business Process Improvement team to support the coordination of the review of access* |

| 1. | Medium | Monthly user access reviews |
|---|---|---|

| Finding and Implication | Proposed action | Agreed action *(Date / Ownership)* |
|---|---|---|
| Implication<br>Responsibilities for access management span across multiple departments (IT, HR, line managers, facilities), requiring coordination. This leads to a greater risk of a user's access not being appropriately removed when necessary. There is a risk that a user with excessive or inappropriate access may retain access to a shared drive for longer than necessary if department heads do not respond to the monthly user access review requests. | | *revalidation for each affected business application by the business owners.*<br>*Owner: Director of IT and Head of Business Process Improvement (BPI)*<br>*Estimated Completion Date (ECD): 30 April 2018.* |

| 2. | Medium | Third party assurance |
|---|---|---|

| Finding and Implication | Proposed action | Agreed action *(Date / Ownership)* |
|---|---|---|
| Good Practice<br>As significant efficiencies and expertise can be gained through the use of third party-managed services, management must ensure that the appropriate protections and requirements are in place to ensure that management has sufficient oversight into the security of the third party service, and an understanding of how the third party may impact the cyber security posture of the organisation.<br>Finding<br>It was noted that HCPC utilises a third party service provider, Rackspace, to provide hosting services primarily for HCPC's external-facing website. Rackspace provides monthly reports disclosing the percentage of time in the past month the service was running (uptime) and a listing of the outstanding service and security issues that require solutions to HCPC. These reports, however, do not detail the age of open tickets, including those that are labelled as security-related. Additionally, there are no defined expectations (for example a Service Level Agreement) between HCPC and Rackspace for their responsiveness to security-related tickets.<br>Implication<br>A lack of reporting of security ticket aging may result in a security-related ticket going unaddressed for an inappropriate length of time without the awareness of HCPC management. Such open tickets would have an impact in HCPC's cyber security posture. | **R2**: Management should consult with Rackspace to determine if the aging of tickets can be reported to HCPC management on a monthly basis in conjunction with the monthly status report.<br>**R3**: Management should request that service levels are agreed, in relation to how responsive Rackspace must be in addressing security-related incidents. | ***R2:*** *Rackspace are currently investigating the feasibility of creating a specific report detailing the aging of security related events; improved reporting will be implemented if feasible.*<br>*Owner: Director of IT*<br>*ECD: 30 April 2018*<br>***R3****: Security related incidents are currently assigned to a standard SLA as Emergency, Urgent or Standard with response times from 15 minutes to 4 hours depending upon the nature of the incident. We will work with Rackspace to clarify the rules that determine which service level is applied to a particular incident type.*<br>*Owner: Director of IT*<br>*ECD: 30 April 2018* |

| 3. | Medium | Policies and procedures for removable media |
|---|---|---|

| Finding and Implication | Proposed action | Agreed action *(Date / Ownership)* |
|---|---|---|
| Good Practice<br>Removable media (such as CDs and USB drives) are used in organisations to fulfil operational purposes, but can pose a risk to security. For example, removable devices can introduce malicious viruses to an organisation's network, or be used to take sensitive data outside of the organisation.<br>Finding<br>HCPC has implemented an automated solution to restrict the usage of removable media to a "whitelisted" set of approved devices that are required to be encrypted, and continuously scanned for malware. However, IT management does not retain documentation related to the (1) owner and (2) justification related to each whitelisted device.<br>Implication<br>Without a record of the personnel responsible for each approved removable device and its associated justification, management is unable to perform reviews of approved devices to ensure that the devices continue to be required, or who is responsible for devices if it is detected that one may have been used to leak sensitive information outside of HCPC's control. Such documentation is critical to allowing management to continuously monitor the appropriate usage of removable media throughout the organisation. | **R4**: Management should revise the provisioning process for removable devices to require that all users requesting removable storage complete documentation noting who is responsible for the safekeeping and proper use of the device, and the justification for the device.<br>**R5:** Management should consider removing all devices that are currently whitelisted using the Symantec Endpoint Protection solution in place. This action would force users to re-request permission for their removable device to access the network and complete the revised process where the devices' owner and justification is retained. | ***R4:*** *A new policy will be created to clarify the management of removable media devices including the requirement for a business justification.*<br>*Owner: Director of IT*<br>*ECD: 30 April 2018*<br>***R5:*** *All existing whitelisted storage devices will be removed and new removable media issued through the new policy.*<br>*Owner: Director of IT*<br>*ECD: 30 April 2018* |

| 4. | Low | Lack of policies to manage user activity monitoring tools |
|---|---|---|

| Finding and Implication | Proposed action | Agreed action *(Date / Ownership)* |
|---|---|---|
| <u>Good Practice</u><br>The implementation of automated IT security monitoring tools can greatly improve an IT department's ability to have a more holistic view of the organisation's security posture. Appropriate processes should be developed by the organisation to manage these tools and the alerts and information that is generated by them so that the full value of their use can be realised.<br><u>Finding</u><br>HCPC management has recently implemented and started to use the Microsoft Advanced Analytics (ATA) package as well as CimTrack to monitor user activity and monitor the integrity of data on perimeter devices, respectively. However, management has not yet developed the processes to manage and escalate relevant alerts to ensure that potential security incidents and anomalies are continuously identified and addressed.<br><u>Implication</u><br>Implementing tools such as Microsoft ATA and CimTrak is an effective first step, and developing processes to manage these tools will assist HCPC in leveraging these tools to a greater extent. With the lack of defined supporting processes, HCPC is at risk of not having a uniform understanding of how the tools are to be used and integrated into day-to-day operations. | **R6**: Management should design and document standardised process to continuously monitor alerts and insights that are developed from IT security monitoring tools. Management should ensure that these processes align with the organisation's ways of working, and that the processes allow management to leverage and disseminate insight gained from these tools to relevant teams and personnel. | ***R6****: The HCPC currently use advanced threat detection tools to monitor and alert against suspicious activity. The process for managing intelligence gathered by these tools will be formalised and documented to standardise the threat response from the IT team.*<br>*Owner: Director of IT*<br>*ECD: Complete* |

| 5. | Low | Use of SMTP protocol |
|---|---|---|

| Finding and Implication | Proposed action | Agreed action *(Date / Ownership)* |
|---|---|---|
| Good Practice<br>The use of secure and encrypted communication across the internet helps ensure that an organisation's communications cannot be intercepted and read by malicious actors.<br>Finding<br>HCPC utilises a bulk email messaging service to send non confidential emails to Registrants. This bulk email service first sends the messages to a service that will scan the messages for any potential viruses, encrypt them, and then send them to Registrants. This messaging service, however, does not encrypt messages when they are first sent to the anti-virus scanning service. The messaging technology that is used during this first step is called Simple Mail Transfer Protocol (SMTP).<br>Confidential emails are sent through separate email services which support encryption.<br>Implication<br>As emails are not encrypted as they are transmitted to the anti-virus provider, there is a risk that these bulk messages sent from HCPC could be intercepted and read by an unauthorised individual. | **R7**: Management should consider utilising alternative email protocols (such as SMTP-Secure) and services that would encrypt email communication, if the risk associated with the current state is determined to be high enough to merit action.<br>Management should consider revising firewall configurations appropriately if an alternative protocol is identified. | ***R7:*** *This delivery mechanism will be replaced with the implementation of the second phase of the Registration Transformation project. It should be noted that the secure delivery of email is also determined by intermediary internet service providers and by the method which the recipient receives their email, for which the HCPC has no control. However, we will investigate with the HCPC email service provider whether an alternative secure email protocol could be used to deliver email securely to their bulk mail service for the period before its replacement.*<br>*Owner: Director of IT*<br>*ECD: June 30 2018* |

| | | |
|---|---|---|
| 6. | Low | Security Advisory Board involvement in emergency patching |

| Finding and Implication | Proposed action | Agreed action *(Date / Ownership)* |
|---|---|---|
| Good Practice<br>Ensuring that IT assets throughout the network are equipped with the latest patches for operating systems and applications helps strengthen an organisation's cyber security posture by ensuring that programs being used are not susceptible to known vulnerabilities. Most patches are released on a periodic cycle, meaning that an organisation can plan in advance to test and apply them when they become available. Testing patches is important in ensuring that the fix that was released by the vendor does not impact the functionality of services in an organisation's unique environment However, from time to time vendors release 'emergency patches', these tend to address critical security flaws, are released with little advance warning, and need to be applied in a short time frame. Having a process in place for addressing emergency patching helps ensure that devices are patched in a timely manner that is commensurate with risk. Organisations will sometimes decide to implement these patches into production without testing them, which adds more risk, as the patch could force a machine or part of the network to stop working due to the organisation's unique IT environment.<br>Finding<br>A process is in place to approve emergency patches in the HCPC IT environment without being formally tested if approved by the IT Director. It was noted, however, that the Security Advisory | **R8**: Management should consider revising the emergency patching process to require that the SAB is consulted and provides final approval for emergency patches via email and during a scheduled meeting. | ***R8:*** *The terms of reference for the Security Advisory Board have been amended to require emergency patches to be authorised through the board.*<br>*Complete* |

| | | |
|---|---|---|
| Board (SAB) (created in October 2017) may be a more appropriate forum to approve emergency patches. While it is common for organisations to implement untested patches, there is risk involved; based on the documented responsibilities of the SAB, it appears that it would be within their responsibilities to provide this final approval.<br><br>Implication<br>There is a risk that the decision to implement critical patches into the production environment is not fully considered if the SAB is not involved in this process. This may result in a lack of proper and defined oversight over the security of the IT environment. | | |

| 7. | Low | Environmental controls for HCPC managed servers and firewalls |
|---|---|---|

| Finding and Implication | Proposed action | Agreed action *(Date / Ownership)* |
|---|---|---|
| Good Practice<br>Physical environment controls are typically necessary when installing IT infrastructure equipment to ensure that availability of the network is not impacted from water damage, overheating, and fire. IT server and equipment stacks should always be on elevated flooring and in a room that is not susceptible to water damage.<br>Finding<br>HCPC's key IT services are hosted on servers which are housed in a server room located in the Kennington office. The equipment stacks, which include network firewalls, are not on elevated flooring. The server room is located near the toilets, increasing the risk of water damage. We did note however that the ground floor was elevated from the road, and thus was protected from low-level flooding from outside the building.<br>Implication<br>There is a risk that in the unexpected event of building water damage or plumbing issues, the network's services and firewalls would not be appropriately protected. There are increased risks to the server being housed next to a toilet, increasing the likelihood of water damage. Server rooms in basements also pose a risk to water damage, as water has a higher chance of leaking from above floors, and basements are more susceptible to flooding damage. | **R9**: Management should assess alternative sites throughout the Kennington office to move the server room and conduct an analysis of alternatives sites within current premises to ensure that the risk of water damage and flooding are kept at an acceptable level.<br>**R10**: Alternatively, management should install raised flooring for the server room to reduce the risk of water damage. | ***R9 & R10:*** *As part of the 186 Kennington Park road building renovation the toilets adjacent to the server room and on the second floor will be removed which will mitigate this risk. However, as part of the budget setting and work planning process for 2018-2019 a project to move the server room will be accessed as part of a larger service improvement plan.*<br>*Owner: Director of IT*<br>*ECD: June 2018* |

| 8. | Low | Firewall policies and procedures |
|---|---|---|

| Finding and Implication | Proposed action | Agreed action *(Date / Ownership)* |
|---|---|---|
| Good Practice<br>Policy and procedural documentation are key to ensuring that an organisation's institutional knowledge is retained and effectively communicated throughout the organisation. Policies and procedures regarding the management of network firewalls helps ensure the continuous and uniform upkeep of network firewalls.<br>Finding<br>It was noted during our review that the firewalls at Rackspace are owned and managed by Rackspace. However, this contradicts the HCPC's 'Perimeter Firewall Policy' which states that all the perimeter firewalls are managed by HCPC IT engineers.<br>Risk<br>Unclear documented roles and responsibilities with HCPC and third party providers may result in a lack of uniform management and understanding of how the HCPC manages firewalls. This could have an impact when sharing, delegating, or passing on IT-security related responsibilities and understanding to new personnel. | **R11**: Management should update The Perimeter Firewall Policy to correctly reflect ownership and management of all firewalls. | ***R11***: *The configuration of the firewalls managed by Rackspace are specified by the HCPC Infrastructure Engineers and a rigorous authorisation process is in place to control changes. The current Perimeter Firewall Policy will be updated to reflect that although HCPC specify the firewall rules the firewalls are maintained through a managed service by Rackspace.*<br>*Owner: Director of IT*<br>*ECD: 31 March 2018* |

# A Internal Audit Approach

## Approach

Our outline approach to this internal audit review was as follows:

- Meeting with key staff to gain an understanding of the arrangements in place, building upon the information we have already gained through our audit planning process;
- Reviewing key documents that support the processes in place and confirming that the risk management activities and controls perform as discussed;
- Where appropriate and relevant, carry out testing to confirm the on-going operation of the risk management activities and controls identified; and
- Comparing existing arrangements with established best practice and other guidance.

## Additional information

### Client staff

The following staff were consulted as part of this review:

- Guy Gaskins, Director of IT
- Bilal Azeem, Infrastructure Engineer
- Kayleigh Birtwistle, Quality Compliance Auditor
- Elandre Potgieter, Senior Support Analyst
- Jason Roth, Infrastructure Manager
- Ali Syed, Infrastructure Engineer
- Rick Welsby, IT Support Manager

### Documents received / examined

The following documents were received or looked at during the course of this audit:

- Access Control Policy
- AD Password Policy
- Applocker, Bitlocker, and Symantec screenshots
- Asset management policy
- Authorisation to test for latest penetration test
- Blocked URL categories for Symantec
- Change Advisory Board (CAB) terms of reference
- Cherwell IT asset management screenshot
- Contractor account lockout screenshot
- Database administrator review
- Deploying windows with System Center Configuration Manager (SCCM)
- Documentation of follow up for leavers identified in Active Directory (AD) listing
- External security testing executive summary from penetration test
- Hardening guidelines
- Human Resources (HR) Security Policy

- Information Security Management System (ISMS) Manual
- Information Security Policy
- Infrastructure build standards policy
- Infrastructure perimeter firewall policy
- ISO27001 security testing policy
- IT policy acknowledgement and agreement Form
- IT Security Advisory Board (SAB) terms of reference
- IT security awareness induction presentation
- Leavers population
- Leavers process document
- Microsoft Azure Cyber Essentials certificate
- Microsoft Azure ISO 27001 Certificate
- Microsoft Dynamics ISO 27001 Certificate
- Microsoft Enterprise Services contract
- Microsoft weekly case management report
- Mobile systems policy
- Netwrix report for "never expire" users
- Password Management Policy (PMP) screenshots
- Password policy
- Privileged accounts review
- Rackspace contract and Service Level Agreement (SLA)
- Rackspace ISO certifications
- Rackspace monthly account review
- Rackspace PCI-DSS certification emails
- Sample of follow up email for IT security awareness compliance
- SCCM scheduled scans screenshots
- SCCM third party scheduled scans screenshots
- Screenshot of IT security awareness compliance tracking
- Screenshot of Ivanti application
- Security patching screenshots
- Server infrastructure patch management policy
- SMTP Bulk email screenshots
- Specific URL exceptions for Symantec
- Starters process document
- Supplier Relationships policy
- User access review email for December 2017
- User access review for December 2017
- Vulnerability scanning weekly summary report
- Web URL policy rules for Symantec
- Weekly case management report

## Locations

The following location was visited during the course of this review:

- Health and Care Professions Council
  Park House
  184 Kennington Park Road
  London SE11 4BU

# B Definition of audit issue ratings

## Audit issue rating

Within each report, every audit issue is given a rating. This is summarised in the table below.

| Rating | Description | Features |
|---|---|---|
| **High** | Findings that are fundamental to the management of risk in the business area, representing a weakness in control that requires the immediate attention of management | • Key control not designed or operating effectively<br>• Potential for fraud identified<br>• Non compliance with key procedures / standards<br>• Non compliance with regulation |
| **Medium** | Important findings that are to be resolved by line management. | • Impact is contained within the department and compensating controls would detect errors<br>• Possibility for fraud exists<br>• Control failures identified but not in key controls<br>• Non compliance with procedures / standards (but not resulting in key control failure) |
| **Low** | Findings that identify non-compliance with established procedures. | • Minor control weakness<br>• Minor non compliance with procedures / standards |
| **Improvement** | Items requiring no action but which may be of interest to management or best practice advice | • Information for department management<br>• Control operating but not necessarily in accordance with best practice |

Grant Thornton

An instinct for growth™

“Grant Thornton” refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires.

Grant Thornton UK LLP is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. 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.

**grant-thornton.co.uk**