Department of Health

Trusted Insider

Final Report

March 2018

pwc

Table of Contents

Limitations

Our Internal Audit work will be limited to that described in the Terms of Reference. It will be performed in accordance with the International Standards for the Professional Practice of Internal Auditing from the Institute of Internal Auditors, and in accordance with the Official Order (Number 127074) dated 29 July 2016, between PricewaterhouseCoopers and the Department of Health. It will not constitute an 'audit' or 'review' in accordance with the standards issued by the Auditing and Assurance Standards Board, and accordingly no such assurance under those standards will be provided.

The Terms of Reference and PricewaterhouseCoopers deliverables are intended solely for the Australian Financial Security Authority's internal use and benefit and may not be relied on by any other party. This scope may not be distributed to, discussed with, or otherwise disclosed to any other party without PricewaterhouseCoopers prior written consent. PricewaterhouseCoopers accepts no liability or responsibility to any other party who gains access to the Terms of Reference.

Report timing and sponsor	
Period of review:	August 2017 – January 2018
Month of final report:	March 2018
Review Sponsor:	Daniel McCabe, First Assistant Secretary, Information Technology Division

1. Executive Summary

1.1 Introduction

The Australian Federal Government's Cyber Security Strategy[1] informs that organisations are hugely impacted by the malicious activities conducted by trusted insiders, causing massive disruption to networks and obtaining confidential information for illegal purposes. Trusted insiders are generally defined as 'potential, current or former employees, contractors or third parties who have legitimate access to information, techniques, technology, assets or premises'[2]. The Australian Signals Directorate (ASD), a commonwealth authority on cyber security, also recommends that government must implement necessary controls to manage, monitor and review privileged accounts so that the risks of cyber intrusions from trusted insiders could be minimised. Privileged system user accounts are a subset of trusted insiders. By design, privileged accounts (such as system administrator accounts) typically provide varying levels of access to trusted personnel so that they can configure, manage and monitor computer systems. While these privileges are necessary for the ongoing administration of a system, if they are not managed, monitored and used correctly, it may introduce a number of potential points of weakness or risks to the system and its data.

The Australian National Audit Office (ANAO) undertakes a number of reviews that have a focus related to the management of privileged accounts. The ANAO Cyber Resilience Report examines the application of the ASD Top 4 mitigating strategies (including Mitigation #4 Minimise Administrative Privileges). While the department has not been subjected to a targeted audit by the ANAO in this area, the findings and recommendations out of these audits are applicable across government entities. The ANAO also undertakes the Audits of the Financial Statements of Australian Government Entities also examines the IT general controls applicable to financial systems, including user access management.

The Department of Health (the department) is responsible for the running of Australia's health system, including supporting universal and affordable access to medical, pharmaceutical and hospital services. To deliver these services, it utilises a large number of information systems and applications that holds a range of sensitive information. To manage and provide ongoing support to these systems and applications, the department has a number of system /application administrators and staff with privileged access. These accounts provide different levels of access to trusted personnel to configure, manage and monitor computer systems. While these privileges are necessary for the ongoing administration of a system or network, they introduce a number of potential points of weakness into that system.

The department defines privileged access in both the *IT Security Policy* and the *Privileged Account Standard*. This definition is consistent with ASD's definition as outlined in the Information Security Manual (ISM), where users who have privileged access are able to perform one or more of the following functions:

- change key system configurations;
- change control parameters (i.e. routing tables, path priorities, addresses on routers, etc.);
- access audit and security monitoring information;
- circumvent security measures;
- access data, files and accounts used by other users, including backups and media;
- access systems for troubleshooting purposes.

The department further defines privileged access roles in the *Privileged Account Standard*. The roles include:

- system or domain administrators;
- database administrators;

[1] Dated 21 April 2016

[2] Australian Government (2016). Managing the insider threat to your business – a personnel security handbook. Accessed at: https://www.protectivesecurity.gov.au/personnelsecurity/Pages/Managingtheinsiderthreattoyourbusiness.aspx

- service desk personnel;
- security personnel;
- application developers;
- testing personnel; and
- users of specialist sub-domains (e.g. the PROTECTED environment).

As part of the Department's Audit Work Plan for 2017-18, PricewaterhouseCoopers (PwC) was engaged to review the Department's approach to manage and reduce the risk posed from trusted insiders and the effectiveness of the approach applied to privileged account management.

1.2 Objective and Scope

The objective of this internal audit was to assess the effectiveness of department's processes and controls that manage the risks associated with "trusted insiders", who as part of their day-to-day duties access the department's information and IT resources. The focus of this audit was on privileged user account management only (for a sample of systems) which included an analysis to determine whether privileged users have access to information that is not commensurate with their roles and responsibilities.

The scope of the internal audit included:

- Reviewing the policies and process implemented in the department, both centrally, and for selected applications, to manage privileged user accounts[3], the access to critical datasets and the lifecycle of a user's account. Of particular focus for this audit are the, business areas responsible for relevant datasets and systems[4]: They include:
    - Pharmaceutical Benefits Scheme (PBS);
    - Shared / Corporate / Grant Services;
    - Medical Benefits Schedule (MBS);
    - Private Health Insurance (PHI); and
    - Financial and Budget Management Systems.

Testing of a sample within the above datasets to determine whether privileged users have access to systems and/or data that is not commensurate with their roles and responsibilities.

1.3 Key Observations and Insights

The following observations are made in relation to the in-scope systems.

1.3.1 Segregated governance responsibilities for privileged access leading to process gaps

Internal Audit reviewed the policies and processes that guide the provision and management of privileged accounts across the critical datasets within scope. As a result of the segregated governance for privileged access between IT Security, IT Operations and various system owners, Internal Audit found the following:

- Even though the department has a set of accessible ICT Security Policies, which comprehensively cover privileged access and ISM requirements, the guidance within the Privileged Account Standard and IT Security Policy were not being fully adhered to. IT Security could not provide evidence (as per the policy guidelines) that all privileged access accounts had been approved by the Information Technology Security Advisor (ITSA). The lack of evidence was due to limitations to retrieve this information in a timely manner from the system where this information is captured and retained. In addition, for the systems in scope, management

[3] This will include policy/process oversight of the provision of access to portfolio staff (if required)

[4] Identified by the Audit Sponsor as part of the audit planning phase

could not provide evidence that that privileged access entitlements were being reviewed periodically (six monthly as per policy).

- IT Security oversee the granting of administrative access[5] for new systems. For all others (i.e. where privileged access is granted without one of these Id's, the system owners are responsible). System owners are then responsible for the ongoing management of privileged access.
- For the three systems reviewed, IT Security do not receive any level of reporting or confirmation from system owners that they are in compliance with the process of reviewing privileged access every six months as required by policy.

If privileged access is not carefully and diligently managed there is an increased risk of the accumulation of access rights, orphaned accounts and user ownership conflicts between system owners, IT Security and Datacom. Privileged access needs to be managed in accordance with the policies and standards in the department. The risk of not adhering to the agreed privileged access policy is that individuals may end up with unauthorised access and be in a position to make system changes and have access to sensitive information that they are not entitled to make.

Without having a complete view of privileged access across the department, it becomes difficult for an organisation to implement the required controls to effectively manage the trusted insider threat.

1.3.2 Sample testing of critical datasets and systems

The following systems were selected to be tested to determine whether privileged users have access that corresponds with their defined roles and responsibilities.

- EDW (to support the MBS/PBS and PHI datasets)
- TM1 (financial forecasting and budgeting system)
- Dynamics 365 (CRM for Shared Services)

For the agreed datasets and systems in scope, Internal Audit selected a sample[6] of users for each system.

All access to the EDW is role-based. All privileged access requests to the EDW requires line manager approval and then ITSA approval, in that order. IT Security made a decision not to provide Internal Audit with evidence of ITSA approval for seven of 16 sampled administrators on the EDW system. This was due to system limitations to retrieve this information in a timely manner from the system where this information (approvals) is captured and retained. This decision was made[7] due to the impact on resources to deliver against competing priorities.

For the TM1 system, privileged user groups have been defined as TM1Admin and TM1PrdPriv. These groups do not have direct TM1 application access. The role of these groups facilitate access to directories on the server to capture feeds from other applications which can subsequently be interrogated by the TM1 application via automated services or processes. For the sampled privileged users on the TM1 system, the applications team provided email evidence of business approval. IT Security did not provide evidence of ITSA approval (due to the decision outlined above to stop the investigation due to higher priorities).

For the Dynamics 365 (CRM) system, Internal Audit noted that privileged access was provided to a number of resources after implementation without having any privileged access procedures in place. Since then, IT Security has developed a set of procedures to manage privileged user access to this system.

[5] Those with a prefix of a_, ida_ and *svc_.

[6] Using the PwC Sample methodology which is based on the IIA internal audit sampling methodology

[7] Decision made by the Director Security, Security and IT Services Branch

Without maintaining accurate and complete records and following the agreed approval procedures for managing privileged user access there is a risk that the department will be unable to determine which users have legitimate access to privileged functions on departmental systems. In the event of a security breach and with incomplete records, the department will not be able to determine who and when the access was authorised.

1.4 Summary of Findings and Recommendations

The following table provides a summary of the audit findings and recommendations (applicable to the systems in scope only):

Ref.	Topic and description	Risk rating	Recommendations
2.1	*Policies and procedure* For some of the systems in scope, the process for approving privileged access by the ITSA is not being adhered to. Privileged access entitlements are not being reviewed on a biannual basis in accordance with the Access Management Policy.	Medium	1. IT Security to further refine their existing IT Systems list by completing the identification of relevant system and business owners. Then apply a prioritisation approach to review access rights provisioned. For example, initial focus on those systems with a high classification (i.e. '1' or 'critical')[8] rating.
2.2	*Results on the sampled datasets and systems* Internal Audit identified three instances where privileged access rights were not commensurate with an individual's roles and responsibilities. Privileged access for these instances was provisioned to Dynamics 365 without any procedures defined, and with no ITSA approval. IT Security have reviewed these instances and removed these access rights, and the users' access now corresponds with their roles and responsibilities.	Medium	2. IT Security to monitor policy adherence[9] with regards to privileged user access reviews undertaken by system owners. In following up on the implementation of this recommendation, verification of the outstanding sample for EDW/TM1 access approvals will also be sought. 3. The Dynamics 365 project team to finalise by 30 June 2018 the system requirements (including those Privileged Access controls outlined in the ASD Information Security Manual) necessary for system accreditation.

1.5 Summary of Ratings

The overall review rating reflects Internal Audit's view of the overall exposure to the department after consideration of all findings highlighted in this report. More detail on the rating scales used throughout this report can be found at Appendix B.

[8] This list contains approximately 60 systems rated as a level '1' (i.e. critical for business continuity/recovery urgency).

[9] In accordance with the Access Management Policy.

Number and rating of findings				Overall Report Priority
Very High	High	Medium	Low	*Medium*
0	0	2	0	

1.6 Positive Observations

IT Security are making improvements to managing privileged access, through setting up a Splunk[10] Privileged User dashboard, as well as reviewing all Datacom policies, and monitoring against Key Performance Indicators (KPIs), such as the number of privileged accounts 'never expiring' and passwords for privileged accounts needing to conform to the Health Password standard.

As an example of the benefit of the use of the Splunk Privileged User dashboard, IT Security was able to identify that some domain administrators had their password setting with 'no change required', meaning that the password would never be required to be renewed. This resulted in IT Security requesting that Datacom improve its privileged access management on a number of criteria and to provide a report on proof that they were in compliance.

IT Operations executed a number of remediation activities in November 2017 for privileged accounts and as a result, across all environments, 513 accounts with Domain Administrator privileges were reduced to 179.

[10] https://www.splunk.com/en_us/solutions/solution-areas/security-and-fraud/use-cases/privileged-user-monitoring.html

2. Detailed Findings and Recommendations

The detailed findings and recommendations section outlines the key audit findings, risks and recommendations. It also captures management actions to address the audit recommendations.

2.1. Segregated governance responsibilities for privileged access leading to process gaps

Background

The department has a set of ICT security policies/standards, all of which contain information and guidance relating to privileged access to systems, applications and information. The relevant policies are:

- IT Security Policy
- Privileged Account Standard
- Management of IT Accounts Policy

According to the policies / standards, privileged access requests can be made using the My Self Service Portal (MSSP) via the Service Desk or by email. Regardless of how access is requested, all access requests generate a ticket within the Service Desk system. All privileged access to systems and information is required to be managed and monitored by using uniquely identifiable accounts and must be approved by the ITSA.

Observations

Internal Audit noted that privileged access management is comprehensively described in the department's policies and standards. The policies and standards closely reflect the privileged access requirements described in ASD's Information Security Manual (ISM). Internal Audit noted that despite the comprehensive nature of the policies and standards, for the systems in scope, they are not being adhered to. As an example, privileged access entitlements are not being periodically reviewed as described in the Draft IT Access Management Policy (i.e. every six months).

Internal Audit also noted that the responsibility for the governance of privileged access is shared between Datacom, IT Security and the various system owners. Datacom manage privileged access for users that support the infrastructure, the network, the databases and domain level administrators. They do not manage user access for application administrators. Individual system owners are responsible for managing application administrator access to their individual systems.

IT Security only provide a high level oversight role for the provision and management of privileged users in the department. They perform independent monitoring and checking of domain administrator accounts only, as a compromise of these accounts attract a high risk because of their broader access privileges than application administration accounts.

In some instances, IT Security do not play any part in managing or monitoring privileged access to application systems. They may leave this task entirely up to the system owners themselves. The only time IT Security get involved with access to systems is during the setup of a new system, where they implement the process for managing user access on the system in question. This means that there is no second line of assurance provided by IT Security regarding the management of privileged access to applications including inadequate periodic reviews of privileged access entitlements.

Datacom informed Internal Audit that they are in the process of developing a Privileged Account Management Plan. This plan will include the definition of privileged access categories together with the entities that are responsible for each management of each category.

Risk

If privileged access is not carefully and diligently managed there is an increased risk of the accumulation of access rights, orphaned accounts and user ownership conflicts between system owners,

IT Security and Datacom. Privileged access needs to be managed in accordance with the policies and standards in the department. The risk of not adhering to the agreed privileged access policy is that individuals may end up with unauthorised access and be in a position to make system changes and have access to sensitive information that they are not entitled to make.

Without having a complete view of privileged access across the department, it becomes difficult for an organisation to implement the required controls to effectively manage the trusted insider threat.

Risk Rating

Likelihood	Consequence	Overall Rating
Possible	Moderate	Medium

Recommendation

1. IT Security to further refine their existing IT Systems list by completing the identification of relevant system and business owners. Then apply a prioritisation approach to review access rights provisioned. For example, initial focus on those systems with a high classification (i.e. '1' or 'critical')[11] rating.

Management Response

1. IT Security will refine the existing IT systems list by utilising the Business Continuity Planning 'Category A' list (priority application systems for recovery). Working with the Business Continuity team, IT Security will identify all relevant system and business owners by 30 June 2018.

IT Security will undertake a review of the access rights provisioned to these systems utilising the necessary investment in the procurement of security software and services to review the access rights provisioned by 30 June 2019.

Accountable Officer	Date of completion
1. Assistant Secretary, Information Technology Division	1. Delivery date by 30 June 2018 for the first stage and 30 June 2019 for the second stage.

[11] This list contains approximately 60 systems rated as a level '1' (i.e. critical for business continuity/recovery urgency).

2.2. Sample testing of critical datasets and systems

Background

In order to test whether the department was following agreed process for managing access to systems, the scope of this audit included testing access to some critical datasets and systems. Access to the department's information and ICT systems must be, irrespective of whether the user is a normal user or privileged user:

- facilitated through defined access management processes;
- limited to a "need-to-know" basis, providing users with the least amount of privileges required to undertake their defined role(s);
- reviewed on a regular basis; and
- is removed when no longer entitled to the defined access (e.g. the user changes role or leaves the department).

The following systems were selected to be tested to determine whether privileged users have access that corresponds with their defined roles and responsibilities.

- EDW (to support the MBS/PBS and PHI datasets)
- TM1 (financial forecasting and budgeting system)
- Dynamics 365 (CRM for Shared Services)

Observations

All access to the EDW that holds the MBS/PBS and PHI datasets is role-based access. All access requests to the EDW requires line manager approval and then ITSA approval, in that order.

IT Security made a decision not to provide Internal Audit with evidence of ITSA approval for seven of 16 sampled administrators on the EDW system. IT Security reported that it would not be possible to provide the evidence as it would be too time consuming to search through all the emails for the records.

As a result Internal Audit is not able to confirm if privileged access was approved by the ITSA for the seven of the 16 sampled administrators.

For the TM1 system privileged user groups have been defined as TM1Admin and TM1PrdPriv. These groups do not have direct TM1 application access. The roles of these groups facilitate access to directories on the server to capture feeds from other applications which can subsequently be interrogated by the TM1 application via automated services or processes.

For the sampled privileged users on the TM1 system, IT Security could only provide email evidence of business approval. They could not provide evidence of ITSA approval (due to the decision outlined above to stop the investigation due to higher priorities).

At the time that this audit was taking place, IT Security in conjunction with the system administrators were in the process of identifying opportunities to implement more granular security controls on these directories. Internal Audit noted that even though there has been no requirement to transfer or remove privileged users from TM1 since its implementation, a procedure describing how to do this exists.

On reviewing the Dynamics 365 (CRM) system, Internal Audit noted that privileged access was provided to a number of resources after implementation without having any privileged access procedures in place. Since then, IT Security has developed a set of privileged access procedures for this system that includes:

- the requirement for a minimum Baseline security clearance;
- a signed confidentiality/non-disclosure agreement form; and
- a monthly review of privileged access in line with users roles.

As a result of this new procedure, the number of users were reduced by four, from nine to five. The Dynamics 365 procedural documentation also covers the lifecycle management of its Global System Administrator and the requirement to remove access within one business day, after notification. Internal Audit noted that the request to remove the four users identified earlier, were actioned the following day.

Risk

Without maintaining accurate and complete records and following the agreed approval procedures for managing privileged user access there is a risk that the department will be unable to determine which users have legitimate access to privileged functions on departmental systems. In the event of security breach and with incomplete records, the department will not be able to determine who and when the access was authorised.

Risk Rating

Likelihood	Consequence	Overall Rating
Unlikely	Moderate	Medium

Recommendation

2. IT Security to monitor policy adherence[12] with regards to privileged user access reviews undertaken by system owners. In following up on the implementation of this recommendation, verification of the outstanding sample for EDW/TM1 access approvals will also be sought.

3. The Dynamics 365 project team to finalise by 30 June 2018 the system requirements (including those Privileged Access controls outlined in the ASD Information Security Manual) necessary for system accreditation.

Management Response

2. The IT Security team will provide verification of the outstanding access approvals for EDW/TM1 by 30 June 2018.

   With the investment in the security software and services in access rights monitoring, the IT Security team will monitor policy adherence for privileged user access against Category A systems (as defined in management response 1) by 30 June 2019.

3. IT Security will work with the Dynamics 365 project team to finalise the system requirements (including those Privileged Access controls outlined in the ASD Information Security Manual) necessary for system accreditation by 30 June 2018.

Accountable Officer	Date of completion
2. Assistant Secretary, Information Technology Division 3. Assistant Secretary, Information Technology Division	2. Delivery date by 30 June 2018 for the first stage and 30 June 2019 for the second stage 3. 30 June 2018

[12] Every 6 months.

Appendix A - Consultations

Appendix A details the staff members consulted throughout the course of the audit.

Stakeholder	Position
Daniel McCabe	Daniel McCabe, First Assistant Secretary, Information Technology Division
Adrian Bugg	Assistant Secretary, Information Knowledge Management Branch
Ian Crittendon	Health Analytics
Craig Boyd	Chief Finance Officer
Charles Wann	Chief Budget Officer
s22	Director Security, Service, Security and Commercial Management Branch
Terry Green	Assistant Secretary, Information Technology Division
s22	Strategic Security Advisor
s22	A/g IT Security Manager
s22	Assistant Director, Enterprise Solutions Branch ITD
s22	Security Advisor, Security and IT Services Branch
s22	Director, IT Solutions Development Branch
s22	IT Operations Security Manager
s22	IT Operations Security
s22	EDW Services and Change Manager
s22	A/g Director, Business Management Section

Appendix B - Internal Audit Risk Ratings

Appendix B provides an overview of the risk matrices outlined in the department's Risk Management Policy. Each individual internal audit finding has been assigned a risk rating, consistent with the department's Assessment Matrix at Figure 1 below. The Department's Risk Tolerance Table at Figure 2 below outlines the required actions against each risk rating.

Figure 1: The Department of Health Risk Assessment Matrix

Australian Government
Department of Health

RISK ASSESSMENT MATRIX

Date Approved:			Likelihood →				
			Rare	**Unlikely**	**Possible**	**Likely**	**Almost Certain**
	General description of Consequences		Exceptional circumstances only	Not expected to occur	Could occur at some time	Will probably occur in most circumstances	Expected in most circumstances
Consequence ↑	Would stop achievement of functional goals/objectives	**Severe**	**High**	**High**	**Extreme**	**Extreme**	**Extreme**
	Would threaten functional goals/objective(s)	**Major**	**Medium**	**Medium**	**High**	**High**	**Extreme**
	Requires significant adjustment to overall function to achieve objective(s)	**Moderate**	**Medium**	**Medium**	**Medium**	**High**	**High**
	Would threaten an element of the function and would require some adjustment to achieve objective(s)	**Minor**	**Low**	**Medium**	**Medium**	**Medium**	**High**
↓	Lower consequence to achievement of objectives.	**Insignificant**	**Low**	**Low**	**Low**	**Medium**	**Medium**

Figure2: The Department of Health Risk Tolerance Table.

Reference	Risk Ratings	Action required
E	Extreme risk	Risk must be given immediate senior management attention. Risk assessment and an approved risk management plan, including treatments must be undertaken.
H	High risk	Risk must have considerable management attention to reduce risk to as low as reasonably possible. Risk assessment and an approved risk management plan, including treatments must be undertaken.
M	Medium risk	Risk should be managed and monitored. Risk assessment and an approved risk management plan required. If controls are working effectively then additional treatments are optional.
L	Low risk	Risk should be managed and controls monitored. Full risk assessment and additional treatments not required.