

This record is not released in accordance with sections 43(1)(d) and 45(a) of the *Freedom of Information Act 2016*, as the record is publicly available on the Directorate's website at [https://www.education.act.gov.au/about-us/policies-and-publications/publications\\_a-z](https://www.education.act.gov.au/about-us/policies-and-publications/publications_a-z) - refer to page G



# Google Apps for Education

## Student Privacy Information

Google Apps for Education provides students with access to twenty-first century learning tools to support their education, including student email. Google Apps for Education will also provide email services to students. This document provides information on the data collected during a student's use of Google Apps and Google's commitment to managing that data.

### What data is collected?

Use of Google Apps will mean that student personal information and data will be collected by Google for the purposes of providing the Google Apps services to students. This personal information will include the student's given name, surname, student ID number and all personal information that is contained in a Google Apps service; such as information or data contained in a student's calendar or email (including text, images, photographs, sound and multimedia).

### How is the data used?

Google stores and processes personal information solely for the purposes of providing the Google Apps service.

Google scans Gmail to keep its customers secure and to improve their product experience. In Gmail for Google Apps, this includes virus and spam protection, spell check, relevant search results and features like Priority Inbox and auto-detection of calendar events. Scanning to provide product features is done on all incoming emails and is 100% automated.

***Google Apps services do not collect or use student personal information and data for advertising purposes or to create advertising profiles.***

As part of providing its services, Google may also collect device information, log and location information as detailed in Google's Privacy Policy.

## *Google will only disclose this data at the direction of the ACT Education and Training Directorate or if compelled to do so by law.*

### **Is the data secure?**

Google is committed to protecting the privacy and security of all of their users, including students. Google has strong security systems in place to keep personal information secure, including an encrypted HTTPS connection.

Google's physical data centre access is restricted to authorised personnel and multiple layers of physical security are implemented. Google personnel are only able to access user data in extremely limited circumstances and subject to rigorous approval and oversight.

### **When is the data deleted?**

Unless required by law, Google will delete Customer-Deleted Data from its systems within 180 days of the ACT Education and Training Directorate deleting a student's account.

### **Where is the data?**

Google holds user data in its data centres that are located around the world.

#### **Google Privacy Information**

Google's approach to privacy, security and transparency with Google Apps for Education is available at <http://www.google.com/edu/privacy>

#### **Further Information:**

[http://www.google.com/apps/intl/en/terms/education\\_terms.html](http://www.google.com/apps/intl/en/terms/education_terms.html)

[https://www.google.com/intx/en/enterprise/apps/terms/dpa\\_terms.html](https://www.google.com/intx/en/enterprise/apps/terms/dpa_terms.html)

<http://www.google.com/policies/privacy/>

#### **ETD Privacy Information**

<http://www.det.act.gov.au/functions/privacy>



[www.det.act.gov.au](http://www.det.act.gov.au)



# Assessment of ETD Information against the PSPF

Enabling Measured Transition to Cloud Services

Version	1.0
Status	Final
Date Saved	Tue 14 Jun 2016

Copyright © 2016 Redcore Pty Limited

This document has been prepared for Education and Training Directorate by Redcore Pty Limited – drawing heavily on material that was developed by Redcore Pty Limited earlier and remains Redcore Pty Limited’s copyright.

Assessment of ETD Information against the PSPF revA.06 DARFT.docx

**DOCUMENT CONTROL**

<b>Date</b>	<b>Version</b>	<b>Primary Author</b>	<b>Reviewed By</b>	<b>Change Reference</b>
8 Dec 2015	0.2	[REDACTED]	N/A	Working draft
13 Dec 2015	0.3	[REDACTED]	[REDACTED]	Working draft
15 Dec 2015	0.4	[REDACTED]	[REDACTED]	Working draft
24 Dec 2015	1.0	[REDACTED]	[REDACTED]	Final release

---

## Table of Contents

<b>Executive Summary</b> .....	<b>5</b>
<b>1 Introduction</b> .....	<b>7</b>
1.1 Background .....	7
1.2 Purpose .....	7
1.3 Scope and Approach .....	7
1.4 Audience.....	9
1.5 Limitations .....	9
1.6 References .....	10
1.7 Glossary .....	10
<b>2 Methodology</b> .....	<b>11</b>
<b>3 Current State of ETD Information Assets</b> .....	<b>13</b>
3.1 Key Regulatory Obligations.....	13
3.1.1 Personally Identifiable Information .....	13
3.2 Information System Summary.....	14
3.3 Data Types .....	14
3.3.1 Category A.....	14
3.3.2 Category B.....	14
3.3.3 Category C .....	15
3.3.4 Category D .....	15
3.3.5 Category E.....	15
3.4 Information Sources.....	15
3.4.1 Category A Applications.....	15
3.4.2 Category B Applications.....	16
3.4.3 Category C Applications .....	17
3.4.4 Category D Applications .....	17
3.4.5 Category E Applications.....	17
3.4.6 File Stores / Share Drives .....	17
3.5 Business Service Lines.....	18
3.6 Current Risk Exposure.....	18
3.6.1 Security Monitoring (#R-01) .....	19
3.6.2 Security risk assessment (#R-03) .....	19
3.6.3 Policy, Governance and non-Technology Risk (#R-03).....	20
3.6.4 Authentication (#R-04).....	20
<b>4 Cloud Migration Considerations</b> .....	<b>21</b>
4.1 Data Profiling Workflow.....	21
4.2 Cloud Migration Workflow .....	23
4.2.1 Service Provider Requirements – Category A.....	23
4.2.2 Service Provider Requirements – Category B.....	24
4.2.3 Service Provider Requirements – Category C.....	24
4.2.4 Service Provider Requirements – Category D.....	25
4.2.5 Service Provider Requirements – Category E.....	26
<b>Appendix A Reference Flowchart</b> .....	<b>27</b>
<b>Appendix B Documentation Reviewed</b> .....	<b>28</b>
<b>Appendix C Current Data Set Analysis</b> .....	<b>29</b>

# Executive Summary

As the use of cloud-based applications allows organisations to improve functionality and user experience, reducing cost of acquisition and maintenance and shortening timeframes. Whilst there are advantages to migrating to cloud applications, there are risk associated with moving sensitive data outside of direct control of ETD or Shared Services.

A risk assessment methodology was selected based on the principles of the PSPF and the ISM, which provides a broad measure of residual risk without a more involved formal risk assessment.

After analysis of the ETD applications and the data contained within, the application data fields can be grouped into 5 categories in order to allow for a streamlined and repeatable cloud consideration workflow.

Category A – No Personally Identifiable Information, but may contain a person’s name without any further information.

Category B – Contains Personally Identifiable Information, which includes a name along with basic personal information such as contact details.

Category C – Contains education records, reports, grades associated with an individual.

Category D – Contains medical/health information associated with an individual, or any information with a DLM attached.

Category E – Ministerial correspondence, information related to protective orders, abuse, or formal complaints that are associated with an individual. Also includes any information with a national security classification.

The current suite of applications was assessed for the sensitivity of information processed and stored.



Figure 1 – Number of Applications by Information Category



Approximately two-thirds of applications are in the low risk category (A or B), making them prime for transition to the cloud without onerous security requirements.

The existing SS ICT environment highlighted several risks:

- The SIEM platform is currently used as a retrospective investigation tool rather than being used proactively. This may provide a false sense of security and allow both externally and internally-originating unauthorised actions to be performed without awareness by administrators.
- At least annually, a broad security risk assessment should be performed to identify and mitigate any risks that may be present in the underlying infrastructure, process or operations, over and above any specific application risk.
- A strong technical security posture is present in the SS ICT environment, through the use of predominately modern and sophisticated products and technology and best practice architecture. Policy and governance, particularly regarding risks people and process may pose is not as well addressed as technology risk.

A number of service provider requirements sets were formulated to reflect the varying sensitivity of information and application criticality. This allowed a cloud migration consideration workflow to be developed:

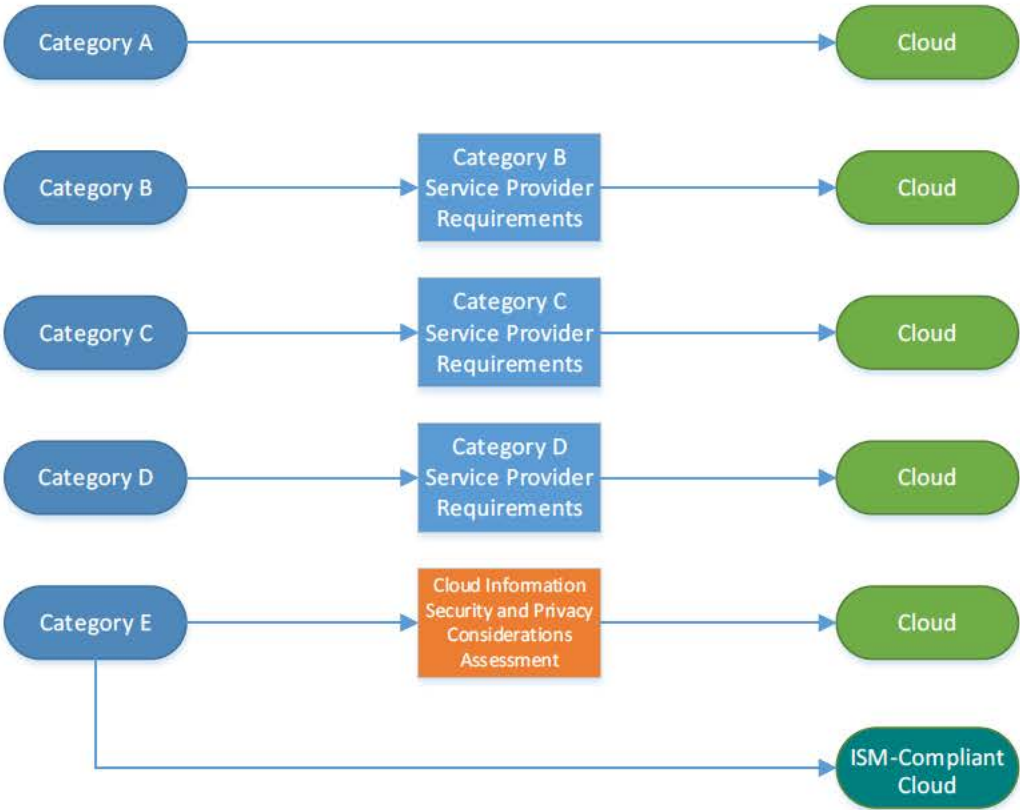


Figure 2 – Cloud Migration Flowchart

---

## 1 Introduction

### 1.1 Background

The ETD is moving towards using online or cloud based applications and tools from a range of providers to improve the efficiencies of business processes.

To ensure that the correct governance and security mechanisms are in place protecting information stored in these cloud-based services, the ETD needs to understand

- What information is stored and used within ETD systems
- The general security posture, in terms of how this complies with the ACT Government's Protective Security Policy Framework (PSPF)
- What other legislative and policy requirements might impact this information

### 1.2 Purpose

The objectives of this review are to assist ETD to:

- Understand the information that is held and used within ETD systems
- Improve ETD's ability to manage and guide the appropriate uptake of ICT services including cloud
- Improve the quality of business administration in ACT ETD, while maintaining compliance with current and emerging legislation and best practice.
- Determine the current level of compliance against the PSPF and other relevant legislation

ETD will use the outcomes of this report to develop appropriate guidance material for use within the Directorate, particularly to explain the policy, process and security considerations when using cloud based services.

### 1.3 Scope and Approach

The engagement was conducted as a mixture of onsite meetings at the ACT Education and Training Directorate, and offsite documentation review and report collation.

The engagement analysed all data stored in ACT ETD systems. Specifically, scope of the report was to

- Outline the classification of current information in relation to security and privacy
- Identify legislative obligations

- Identify current state risks of existing business solutions and hosting arrangements
- Provide advice on controls – e.g. details on how risks posed by different systems can be best managed;
- Provide advice on disclosure and visibility of sensitive or classified information e.g. personal information of students, student immunisation records, parents and staff both internally (across ACT ETD) and externally (e.g. vendor personnel, cloud storage);
- Provide advice on any privacy, security, records or other relevant legislation applying to information in ICT systems
- Provide recommendations on future state options for cloud for hosting key ETD business systems and information assets based on a relative risk assessment (current state versus future state options);
- Provide a business process flow diagram and explanation that indicates how this assessment was undertaken for ETD; and that will allow any Directorate to undertake a similar assessment.

Task/deliverable	Description
Agree stakeholders and tentative timelines	A preliminary exercise to agree the intended stakeholder targets for the exercise, relevant source documents as well as the stakeholders who will be involved in deliverables review and acceptance as well as high level, indicative timelines.
Preliminary Workshop	<p>This was a preliminary workshop with follow-up interviews arranged as required to understand and agree:</p> <ul style="list-style-type: none"> <li>• Core business objectives</li> <li>• Core information assets and systems that are critical to meeting these business objectives, as well as current information classifications</li> <li>• Relevant aspects of legislation</li> <li>• Documentation as in processes, policies, technical specifications etc.</li> <li>• Current state risks of existing business solutions and hosting arrangements</li> </ul>



Documentation review, discovery worksheet and collation	<p>ACT ETD provided the documents listed in Appendix B for review.</p> <p>Based on this a series of questions were drafted and discovery workshop questions were disseminated to critical stakeholders, including:</p> <ul style="list-style-type: none"> <li>• Daniel Bray</li> <li>• Greg Schuhardt</li> <li>• Deb Clayton-Baker</li> <li>• Mark Stirling</li> <li>• Robert Black</li> <li>• Morgan Campbell</li> </ul> <p>More information was collated from a Workshop with Shared Services (Julian &amp; Bryan) to understand systems and security</p> <p>Returned discovery worksheets were analysed to formulate data 'categories'</p>
Preliminary presentation	<p>Preliminary findings in progress based on the collated data were presented to representatives from:</p> <ul style="list-style-type: none"> <li>• the Information and Knowledge Services (IKS)</li> <li>• Enterprise Architecture &amp; Hybrid Cloud and Security teams</li> </ul>
Draft and final reports	<p>These have been collated based on ACT ETD feedback</p>

**1.4 Audience**

This document is intended for application owners, business representatives, users of applications and those considering new applications.

The flowchart in Appendix A is intended for use by anyone with ETD.

**1.5 Limitations**

This report is heavily dependent on a desktop assessment of ETD applications and information, as well as SS ICT architecture and risk profile. It relies heavily on the accuracy of interviews and reviews of supplied documentation. It is not a comprehensive first-hand audit of the systems within scope.





## 1.6 References

- [1] Territory Records Act 2002
- [2] Standards for Records Management
- [3] Health Records (Privacy and Access) Act 1997 (ACT)
- [4] Public Health Regulations 2000 (ACT)
- [5] Information Privacy Act 2014 (ACT)
- [6] Australian Government Information Security Manual
- [7] The ACT Government Protective Security Policy Framework (PSPF)
- [8] Information Security Management Guidelines – Risk Management of outsourced ICT arrangements (including Cloud)
- [9] ISO 31000 Risk management - Principles and guidelines
- [10] Australian Government Information Security Manual

## 1.7 Glossary

Term	Meaning
Cloud	Use of a multi-tenanted environment to achieve economies of scale in providing technology services. See Software as a Service for specific use in this document.
Identifiable Information	Data or artefacts that are unique to an individual. See Section 3.1.
Information Aggregation	Circumstances where large quantities of information of a particular sensitivity or importance result in the sensitivity or importance rated higher, due to the large quantity.
Personal Information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable; whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not. See Section 3.1.
Personally Identifiable Information	Information about an individual, either directly or inferred, where an individual is identified or reasonably identified or their identity is inferred.
Software as a Service	A software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted.

---

## 2 Methodology

Information either carries no classification/sensitivity, or may contain sensitive and/or personally identifiable information. Whilst the Privacy Act calls for general protection of Personal Information, where information is stored in large quantities, aggregation of that information may dictate more stringent controls that would be otherwise be afforded to individual pieces of information.

This risk assessment considers the requirements of the Australian Government Protective Security Policy Framework (PSPF), which provides the overarching set of requirements for protective security of official or sensitive information. The PSPF requires a risk assessment to be completed for outsourced Cloud-based computing arrangements.

A number of policies and guidance documents make reference to an IRAP Risk Assessment as a preliminary tool to evaluate the suitability of a system for processing and storage of official, Government or sensitive information. It is used as an intermediary assessment, without the rigour of more extensive ISM compliance activities. It assesses the principles of the ISM rather than individual controls and is useful in gauging the overall risk profile of an environment rather than specific compliance.

This risk assessment aims to identify and allocate severity to risks which may apply to the subject of assessment. This allows evaluation of suitability of cloud services for processing Government information, commensurate with the level of sensitivity, and quantity, of the information in question.

In accordance with the PSPF and the ISM, the responsibility to evaluate risk lies within Government. However, general recommendations are presented in response to reducing risks identified.

The type of information that is stored is categorised and the systems it resides on is assessed to determine a risk profile. This is shown in Figure 3

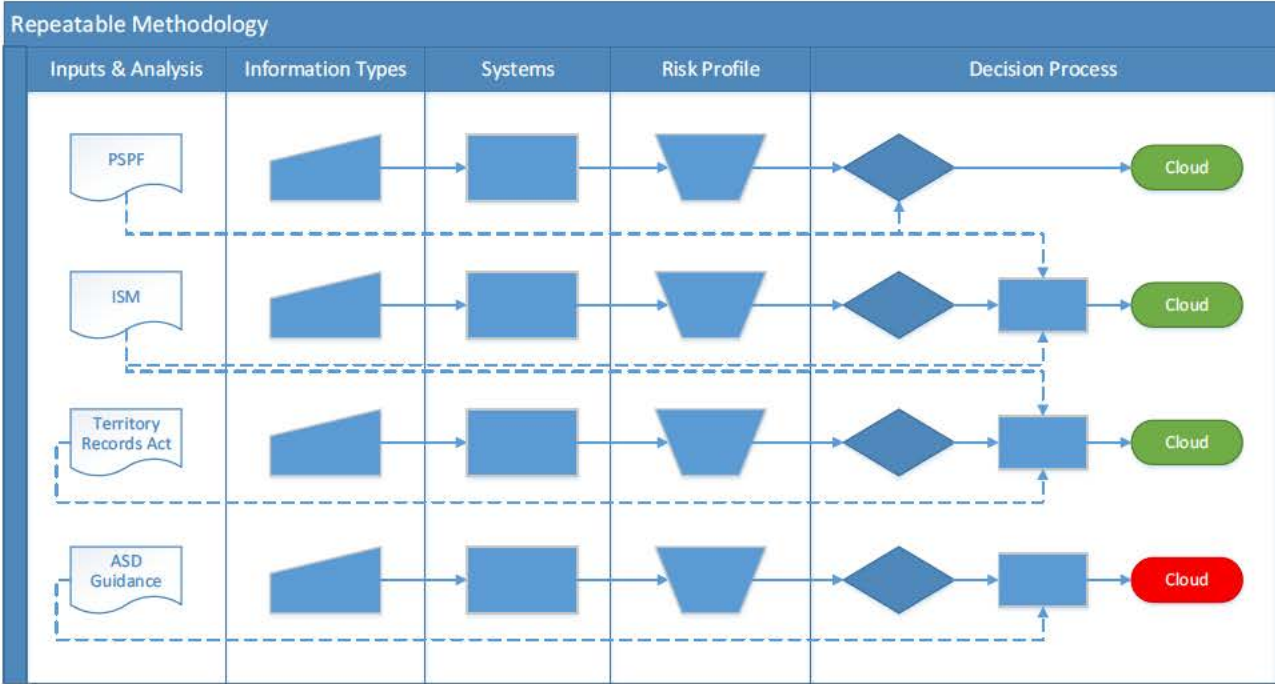


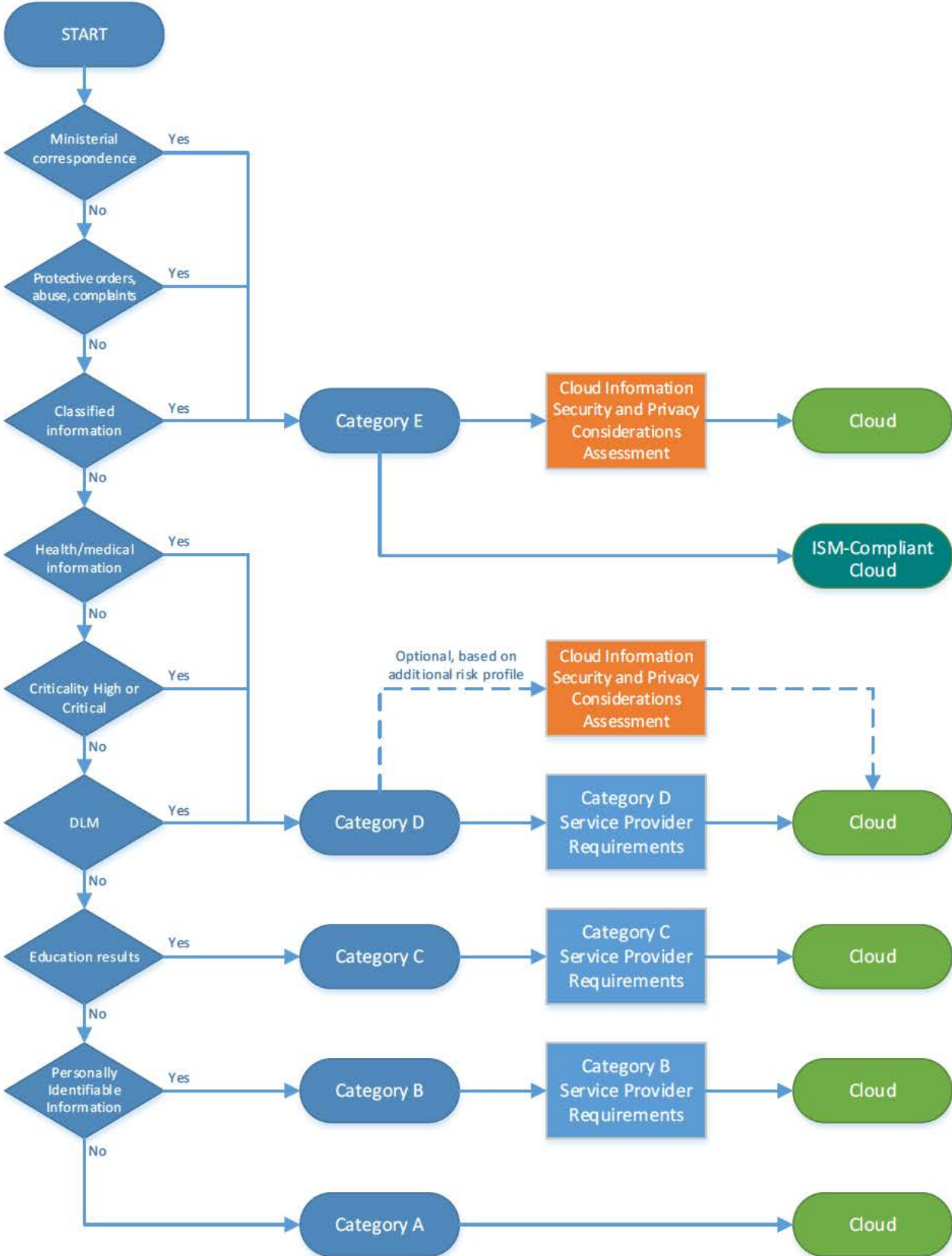
Figure 3 – Repeatable Cloud Transition Methodology

The applicable policies and legislation shape the risk assessment to influence both the risk profile and the decision process. The decision process is a relatively straightforward method of determine if and when a cloud service may be used to hosted the relevant information.

For example, if the legislation, shown in the left-most column, states that particular personal information must be stored onshore, this forms part of the decision process on the right. Likewise, the current risk profile is used to shape the controls that are stipulated in the decision process, for each information category.

The output of this is a decision tree tailored for a specific information and application set.

# Appendix A Reference Flowchart





---

## Appendix B Documentation Reviewed

The following documents were reviews as part of this activity:

- Multiple data discovery worksheets
- ACT PSPF Executive Summary, January 2016
- ETD Business Application Portfolio Data Flows, v5.01
- ETD Corporate Business Applications.xlsx
- File Plan Based on BCS.xlsx
- Generic Administrative Function File Plan.doc
- ACT Government Protective Security Education Guideline
- Risk Management Worksheet - Generic.docx
- ETD Records Management Program 2015
- Part 3 of Attachment 3 - SAS RFT Tenderers Returnable Technical Schedule to the SOR, v1.1
- Attachment 2 - SAS RFT Business and Non-functional Requirements, v1.1
- File Plan 2014 09 01 Compliance\_Report\_Update 2014
- Schedules(ETD).xls
- Cloud Decision Framework Guide
- Cloud Computing Overview
- Cloud Decision Presentation
- Cloud Decision Requirements Chart
- Cloud Endorsement - Cloud Consumer
- Cloud FAQs
- Cloud Information Security and Privacy Considerations Assessment Tool
- Cloud Information Security and Privacy Considerations
- Attachment 4 - Overview of the ACT Government ICT Environment

---

## Appendix C Current Data Set Analysis

{See separate spreadsheet}



**FORESIGHT**

CYBER SECURITY • COMPLIANCE & ASSURANCE

# Maze and Teach Anywhere Current State Security Risk Management Plan

PREPARED FOR

ACT Education and Training



### Document control information

Document title	Maze and Teach Anywhere Current State Security Risk Management Plan
Prepared for	ACT Education and Training
Project name	Maze and Teach Anywhere Current State (ECS)
Document type	Security Risk Management Plan
File name	ACT Education Current State SRMP.docx
Version	2.4
Status	FINAL
Release date	24 January 2017
Prepared by	Foresight

### Revision history

Revision	Author	Date	Comments
1.2	[REDACTED]	2016-11-25	Final.
1.3	[REDACTED]	2016-12-23	Added inherited risks from the broader SSICT environment.
2.1	[REDACTED]	2016-12-12	With minor changes as per feedback from Education and SSICT.
2.3	[REDACTED]	2017-01-24	With updated risk matrix from Education and SSICT.
2.4	[REDACTED]	2017-01-25	Updating wording re. recommended treatments.



## Contents

- 1 Executive summary ..... 6**
- 2 System context ..... 10**
  - 2.1 System description.....10
  - 2.2 System architecture .....10
  - 2.3 Architecture diagrams.....13
  - 2.4 Security architecture .....15
  - 2.5 Component responsibilities.....18
  - 2.1 Interviewed personnel .....19
  - 2.2 Documentation reviewed.....20
- 3 Risk context.....22**
  - 3.1 Threat sources.....22
  - 3.2 Key assets.....25
  - 3.3 Risks .....27
- 4 Risk analysis .....30**
  - 4.1 Current risk levels .....30
- 5 Treatments .....34**
  - 5.1 Recommended treatment strategies.....34
- Annex A: Risk register .....38**
- Annex B: Inherited current state risks.....50**
- Annex C: Risk treatment plan .....70**
- Annex D: Risk criteria .....77**
  - D.1 Likelihood values .....77
  - D.2 Consequences values .....77
  - D.3 Risk rating matrix .....78
- Annex E: Security risk methodology .....79**
  - E.1 Threat, risk and incident.....79
  - E.2 Performing risk assessments .....80
  - E.3 Security controls .....81



E.4 Risk ratings and treatments.....82

E.5 Ongoing review .....82

## Tables

Table 1: Resultant risk.....	8
Table 2: Component responsibilities .....	19
Table 3: Documentation reviewed .....	21
Table 4: Threat sources .....	25
Table 5: Key assets .....	27
Table 6: Risk summary.....	28
Table 7: Inherited risk summary .....	29
Table 8: Current risk levels .....	33
Table 9: Recommended treatments.....	37
Table 10: Risk register.....	49
Table 11: Inherited risk register .....	69
Table 12: Countermeasures.....	75
Table 13: Likelihood criteria .....	77
Table 14: Consequence .....	78
Table 15: Risk matrix .....	78

## Figures

Figure 1: MAZE architecture.....	13
Figure 2: Exchange architecture.....	14
Figure 3: Risk assessment workflow.....	80

## 1 Executive summary

ACT Shared Services provide a variety of ICT services for ACT Education and Training. These include the network, applications, and infrastructure that form the ICT environment of the ACT school system.

As part of an ongoing program to enhance services provided to students, teachers, and parents within the ACT, Education and Training is undertaking several projects to renew and re-architect major components of its ICT services. Projects include:

- a replacement for the current school management system, Maze;
- migration to Office 365 for teachers and students, known as the Teach Anywhere project; and
- the general adoption of a “cloud first” strategy for applications and services.

As part of these activities, Foresight is engaged to produce a risk assessment for current-state ICT services to form a baseline against which future-state services are assessed.

Foresight conducted a threat risk assessment of current systems to identify information security risks and provide recommendations for mitigation strategies, where necessary.

The following risks, and their untreated risk levels, have been identified:





**Table 1: Resultant risk**

Overall, the risk profile of the current state system is **medium**, mainly due to an ageing, unaccredited environment and overly complex infrastructure within the Maze system. Recommended treatment strategies revolve around replacing and modernizing systems, and would be expected to reduce the overall system risk to **medium**.

Foresight conducted this assessment from 17 October 2016 to 11 November 2016. Additional risks relating to broader SSICT systems (those prefixed with "ER", above) were added in December 2016.

This risk assessment should be considered as a point in time reference only. Any changes in the threat landscape or operating environment will require a reassessment of cloud security risks.

## 2 System context

### 2.1 System description

The scope of this current-state assessment included:

- Maze, and its supporting infrastructure, including interfaces with edge systems;
- the current desktop and office productivity suite; and
- in-house Exchange email services.

Services specifically out-of-scope for this assessment included:

- internal (i.e. non-school) Education and Training network;
- Apple OS X and Google Chromebook devices;
- Citrix remote access solution;
- general network and storage infrastructure;
- existing Google Apps for Education platform (“Learn Anywhere”);
- specific architecture of Maze edge systems; and
- broader ACT Shared Services systems and processes.

This record is not released in accordance with section 17 of the *Freedom of Information Act 2016*

Schedule 1, 1.6

**Education Directorate**

UNCLASSIFIED

**To:** Executive Branch Manager, Digital Strategy,  
Services and Transformation Branch

Tracking No.: EDU19/1808

**Date:** 22/10/2019

**CC:** Senior Director, Programmes, Applications & Transformation

**From:** Architect Digital Strategy, Services & Transformation

**Subject:** Gmail eSafety Configuration Update

**Critical Date:** 01/11/2019

**Critical Reason:** To develop a plan to implement recommended configuration changes

**Recommendations**

That you:

1. Agree to the development of an implementation plan by Programmes, Applications & Transformation team (DSST) and deployment of the proposed configuration changes to the Gmail service

**Agreed** / Not Agreed / Please Discuss

.....Kristen Foster..... ...1...../...11...../...2019

**Executive Feedback**

*Thanks – I assume we will be testing the impact on a limited number of users to start with. Could we ensure that a high-level programme of work is provided to the next DSC. I assume these changes will be implemented before the start of Term1 ?*

**Background**

1. DSST engaged Google on 05 July 2019 to perform a ‘Health Check’ on the configuration of the Directorate’s *GSuite for Education* (GSfE) environment.

## UNCLASSIFIED

2. Results were provided by Google on 29 July 2019. This is the first time an assessment on the health of GSfE has been completed.
3. The Health Check rated the environment as 'Healthy'.
4. Google, however recommended that the Digital Strategy, Services & Transformation (DSST) branch review the configuration of security related settings for core services within GSfE to ensure they aligned with the Directorate's desired security posture (particularly for services such as Google Vault (Data Retention and e-Discovery) and external sharing settings).
5. Google were unable to provide any direct guidance around reviewing security settings, however a security checklist for medium and large businesses published by Google was found to be publicly available online.
  - a. The security checklist includes recommended configuration settings to improve the security posture of the GSfE environment; and
  - b. DSST have used this security checklist as a baseline against which the Directorate's current configuration can be assessed.
6. DSST prioritised the Gmail service review with Shared Services ICT (SSICT) on 28 August 2019. The review took into consideration both the Google Health Check and the Google security best practice configuration guide.
7. This joint review by DSST and SSICT recommended nine configuration changes to the Gmail service. These changes fall into one of three categories:
8. A detailed plan for implementing the nine recommended configuration changes will be developed by the Programmes, Applications & Transformation (PAT) team in consultation with the Strategy, Design & Knowledge Management (SDKM) team.

**Issues**

9. Gmail is the primary email platform for students. Whilst the overall risk of the recommend changes is considered low by SSICT, several of the proposed configuration changes are global and would apply to all students with a current Gmail account. Testing will be required to ensure service capability, and this will be incorporated into the implementation plan.

**Financial Implications**

- 10. Nil - configuration changes will be deployed as part of Business As Usual.

**Consultation**

Internal

- 11. Kelly Bartlett | Senior Director, Programmes, Applications & Transformation
- 12. Leigh Pierce | Senior Director, Strategy, Design & Knowledge Management
- 13. Sean Esler | Architect, Strategy, Design & Knowledge Management

Cross Directorate

- 14. Julian Valtas | Director, ICT Security Operations, SSICT
- 15. Daniel Ruecroft | A/g Director, Education ICT Business System Support, SSICT
- 16. Kerrie Stevenson | Exchange Administrator, Technical Services Delivery, SSICT

External

- 17. [REDACTED], Google

**Work Health and Safety**

- 18. N/A

**Benefits/Sensitivities**

- 19. The proposed configuration changes will improve the overall security posture of the Gmail service for students. [REDACTED]

**Communications, media and engagement implications**

- 20. A detailed implementation/communication plan needs to be developed by DSST/SSICT to minimise any disruption to the service and to ensure the desired security outcomes are achieved.

Signatory Name: Leigh Pierce Phone:

Action Officer: Sean Esler Phone:

**Attachments**

Attachment	Title
Attachment A	Gmail Configuration Setting Review

This record is not released in accordance with section 17 of the *Freedom of Information Act 2016*

Schedule 2, 2.2(a)(iii)



Education Directorate

FOR OFFICIAL USE ONLY

<b>To:</b>	Director-General	Tracking No.: EDU19/1923
<b>Date:</b>	26/11/2019	
<b>CC:</b>	Executive Group Manager – Service Design and Delivery	
<b>From:</b>	Executive Branch Manager - Digital Strategy, Services & Transformation	
<b>Subject:</b>	ICT Security Programme Overview	

Recommendations

That you:

1. Note and provide feedback on the programme of work to continue to strengthen Education ICT security controls.

Noted / Please Discuss

...../...../.....

Executive Feedback
--------------------

Purpose

1. The purpose of this brief is to follow up on our meeting of 11 October 2019 and formally advise you of the programme of work being undertaken by DSST to contemporise and strengthen the ICT technical controls that support the use of ICT in schools. These technical controls will be aligned to enable the teaching of Australian Curriculum ICT General Capabilities and Digital Technologies whilst ensuring that we protect students in their use of technology as part of the eSafety programme.

Background

2. ACT Education has successfully implemented a number of leading-edge digital platforms that has transformed the way we teach and enables relevant digital

learnings, that support students to operate in an ever-changing digital world. A full timeline is outlined in **Attachment B**.

3. Some of the significant platforms that have been successfully implemented and adopted include:
  - a. Schools network – [REDACTED]  
[REDACTED] is the shared IT network used to connect all ACT public schools together. It is the medium by which School Staff and Students access a wide range of on-premise and cloud based digital services.
  - b. Digital classrooms and learnings - GSuite for Education (GSfE)  
The Learn Anywhere programme provided the Google for Education G Suite platform and other digital technologies to support the learning needs of today.
  - c. Equitable devices – Technology Enabled Learning (TEL) programme  
All year 7 to year 12 students are provided with a Chromebook to enable equitable access to the digital learning platforms.
  - d. Other programmes such as the Computers for Teachers / Computers for Administrators and the 1:3 device ratio for students in primary schools have provided a modern and resilient technology platform.
4. In the context of an ever-increasing digitalisation of the curriculum and the variety of digital tools being used in our classrooms, management of cybersecurity risks is progressively more complex.
5. The security landscape is constantly evolving, which presents a challenge to ACT Education, however this can be managed by understanding our environment; regularly reviewing technology risks with key partners and implementing controls to treat the risks and manage the eSafety of our users and their information within our environment. This includes Personal Identifiable Information (PII) of our students.
6. DSST will use a Defence in Depth Security Controls approach (**Attachment A**) as a framework for strengthening our security controls which recognising the complexity of implementing security controls. Adapting to cyber security risks and changes to user behaviours requires our internal controls and functions within our environment to be monitored and maintained constantly, some of the key functions within security include:
  - a. Security operations – Monitors and protect against virus's malware, etc. on a daily basis – SSICT Security, provides this support.
  - b. Security Assessments – Threat and Risk Assessments (TRA) are required (as per the ACT Government Protective Security Policy Framework – PSPF) at the

introduction of new or major upgrade of digital tools – SSICT security or external consultant provides this service.

- c. Security Risk Management Plans (SRMP) – Review of security settings of digital tools. It is important to regularly review due to new functions made available through upgrades and the changing nature of cybersecurity challenges – responsibility of DSST to engage consultation from SSICT or external service provider.
- d. Penetration Tests – physical test that highlights where hackers or viruses can enter the environment and outline the business impact – responsibility of DSST to engage consultation from SSICT or external service provider.

### **ACT Education Security Observations**

- 7. DSST have commissioned risk assessments and reviews over the Education technology controls to assess the effectiveness and design of controls for the Education network. These assessments and reviews have been conducted by:
  - a. External service provider - PriceWaterhouseCoopers (PwC)
  - b. External service provider – Google Health Check
  - c. Internal service provider - Shared Services ICT (SSICT)
  - d. Internal configuration and architectural reviews - DSST
- 8. DSST has considered the observations by all parties and have identified key priorities for the security programme (**Attachment C**), assessing each change based on business risk, mitigation impact and complexity to implement. These security changes will be delivered in a manner that ensures they do not adversely impact student learning or impact ICT services provided to teaching staff.

#### PwC Security Review:

- 9. PwC were engaged in April 2019 to undertake a broad review over the maturity of security policies and controls covering the [REDACTED] environment. The scope of the PwC assessment was limited to the [REDACTED] network itself and the users and / or devices that interact directly with it, it did not cover external digital services accessed via it. The Review was completed in June 2019 (**Attachment D**).
- 10. The PwC Review assessed the maturity of seven key security controls across the [REDACTED] environment with the following three controls and processes as in need of immediate attention:

[REDACTED]

[REDACTED]

[REDACTED]

11. The PwC Review made six specific observations to strengthen security controls across the [redacted] environment. The report highlighted that in general, the level of maturity of ICT service management and network controls was low and highlighted improvements were needed across several control areas to mitigate business and security risk.

Google Health Check:

- 12. DSST engaged Google to perform a ‘Health Check’ on the configuration of the Directorate’s *GSuite for Education* (GSfE) environment.
- 13. The Health Check report was provided to DSST on 29<sup>th</sup> July 2019 in **Attachment F** and rated the environment as ‘Healthy’. However, Google recommended that DSST review the configuration of security related settings for core services within GSfE to ensure they aligned with the Directorate’s desired security posture.

SSICT Security Review:

- 14. DSST and the SSICT security team have reviewed several key security threats and risks and identified a range of key actions, as outlined in **Attachment E**, including:
  - a. ContentKeeper web filtering changes
  - b. GSfE environment changes
  - c. Firewall changes
  - d. Group policy changes

DSST Security Review:

- 15. DSST identified that the Directorate needed to implement and adjust a number of pre-existing configuration controls to respond to the rapid changes of the technical landscape of eSafety, privacy and security. This response considered media and community concerns, interjurisdictional policies and standards, shared services security advice, the need to adjust our security posture to support eSafety and digital maturity for students. Various technical improvements were trialled in 2018/19 to support the eSafety agenda and are in the process of being implemented, these include:
  - a. Trialling a Cloud Access Security Broker to identify where schools are using high-risk unsanctioned cloud services.
  - b. [redacted]
  - c. GSfE environment changes to ensure that controls are in line with best practice and appropriate for students and teachers.

- d. Undertaking Security Risk Management Plans (SRMP) on our core systems SAS and O365 (Teach Anywhere).

### Summary of key priorities

- 16. Based on the observations DSST has recommended completing the activities outlined in the Security programme, specifically those outlined in the top two quadrants:
  - a. Top right – Quadrant 1 – High Value Essential Quick Wins
  - b. Top left – Quadrant 2 – High Value Important Changes
- 17. The overall governance of the programme will be through the Digital Strategy Committee, which reports to the Education Governance Committee. These changes will be delivered by:
  - a. Quadrant 1 changes before Term 1 2020
  - b. Quadrant 2 changes by start Term 3 2020
- 18. The remaining activities outlined in quadrant 3 and 4 are operational activities that that will add higher value when high value essential and priority changes are implementing. Completing these activities at this time would represent low business value to the Directorate and do little to reduce the Directorates overall security risks, these include:
  - a. Penetration tests
  - b. Updated Security and Risk Management Plans
- 19. Approval for implementation of all technology and configuration changes will be approved by the EBM DSST following consultation with key stakeholders, including EGM SDD, Principals, ITOs and the eSafety Programme. These changes will be documented and provided in a quarterly report the EGC.

### Financial Implications

- 20. It is anticipated that funding for changes to security controls will be made from within existing resources.

### Consultation

#### Internal

- 21. Trevor Cox (Assistant Director Risk, Security and Emergency Management)

#### Cross Directorate

- 22. Jonathon Owen, Chief Information Security Officer, SS ICT
- 23. Bruce Abdilla, Senior Director, Education ICT, SS ICT

#### External

- 24. [REDACTED], PwC

## Work Health and Safety

25. Nil Response

## Benefits/Sensitivities

26. Implementing the recommendations and security initiatives outlined in the Security programme will increase the effectiveness in the management of our privacy, security and eSafety risks within a defined risk tolerance and ensure security is not a blocker to achieving the benefits of the Future of Education Strategy.

27. Implementation of the initiatives will improve accountability for security of information within schools and the [REDACTED] network. This will enable more effective decisions by the Security and Emergency Management Committee driven by the ACT Protective Security Policy Framework and improve user awareness of data loss and key security risks.

## Communications, media and engagement implications

28. Communications with schools will be required and is included in the draft branch plan for late 2019.

Signatory Name: Kristen Foster Phone: 6205 6749

Action Officer: Leigh Pierce Phone: 6207 2752

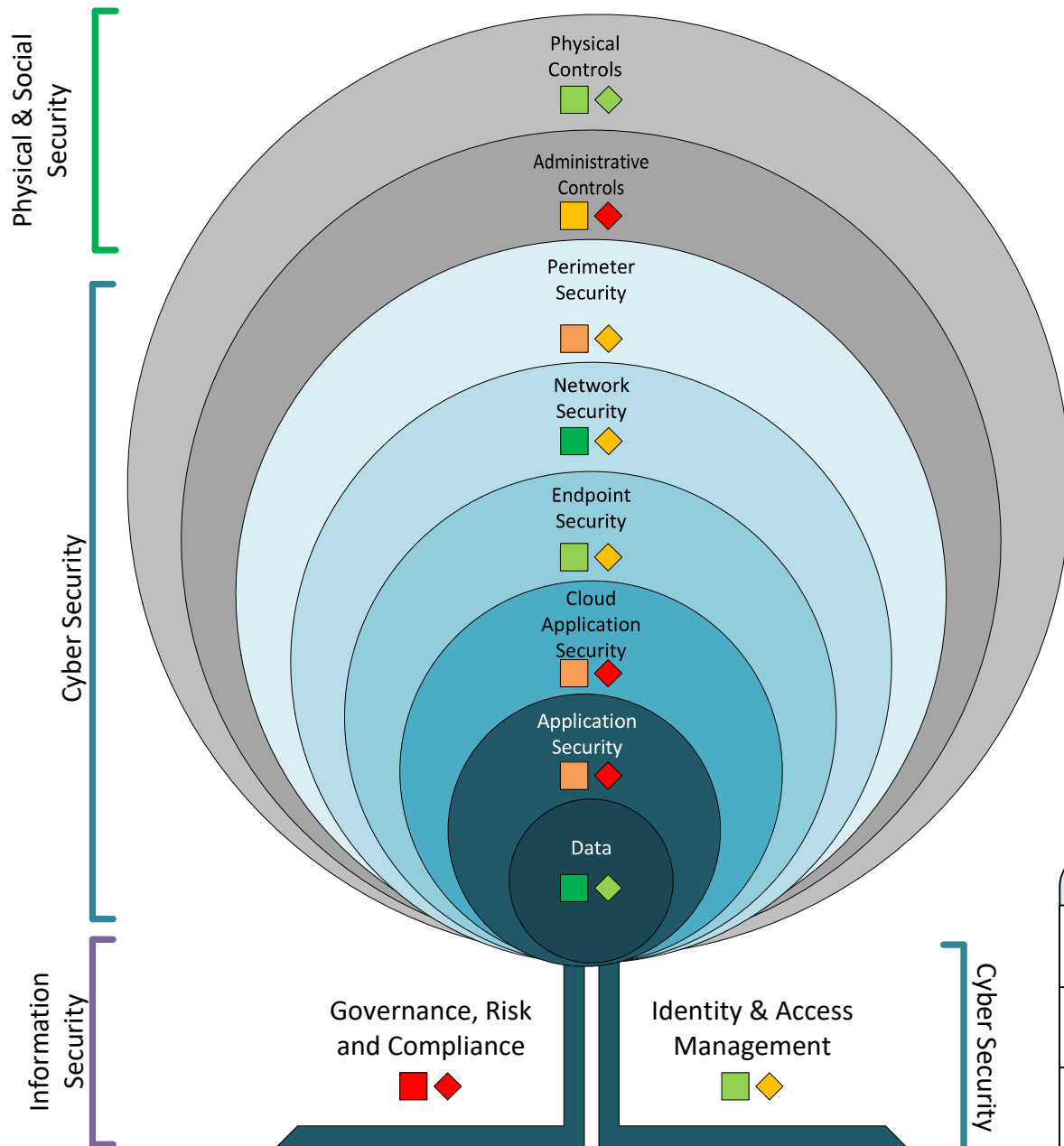
## TRIM References

Type	TRIM Reference
eSafety Programme	EDU19/1321, MIN19/1265
Security related activities	EDU18/720, EDU19/1808

## Attachments

Attachment	Title
Attachment A	Defence in Depth Security Controls Heat Map
Attachment B	Education Security Timeline
Attachment C	Security Programme of IT Security Control remediation and Initiative Descriptors
Attachment D	PwC Draft - [REDACTED] Policy and Security Controls Analysis Addendum
Attachment E	SSICT – EDU security considerations
Attachment F	Google for Education - Environmental Health Check

# Defence-in-Depth Security Controls – Heat Map



Physical Controls, such as key card access to buildings, guards, laptop locks

Administrative Controls for policies, procedures and training & awareness. Including Data classification, Password strength, & Acceptable Usage Policy

Perimeter security, which may include anti-virus and anti-malware programs, DLP solutions, perimeter firewalls, border routers, and other boundaries between the public and private sides of a network such as cloud access security broker (CASB) tool which acts as a gatekeeper between on-premises and cloud-based infrastructures.

Network security such as VoIP protection, proxy content filters (Content Keeper), remote access, and wireless security.

Endpoint security, which secures devices accessing an organization's network remotely or wirelessly, including device firewalls, patch management, content security, antivirus, antispysware, and host intrusion prevention systems.

Cloud Application security, protection of education data assets in cloud environment. Cloud applications such as Office 365, Google Suite, Box.com, Dropbox, Salesforce, ServiceNow, etc. - Software as a Service (SaaS).

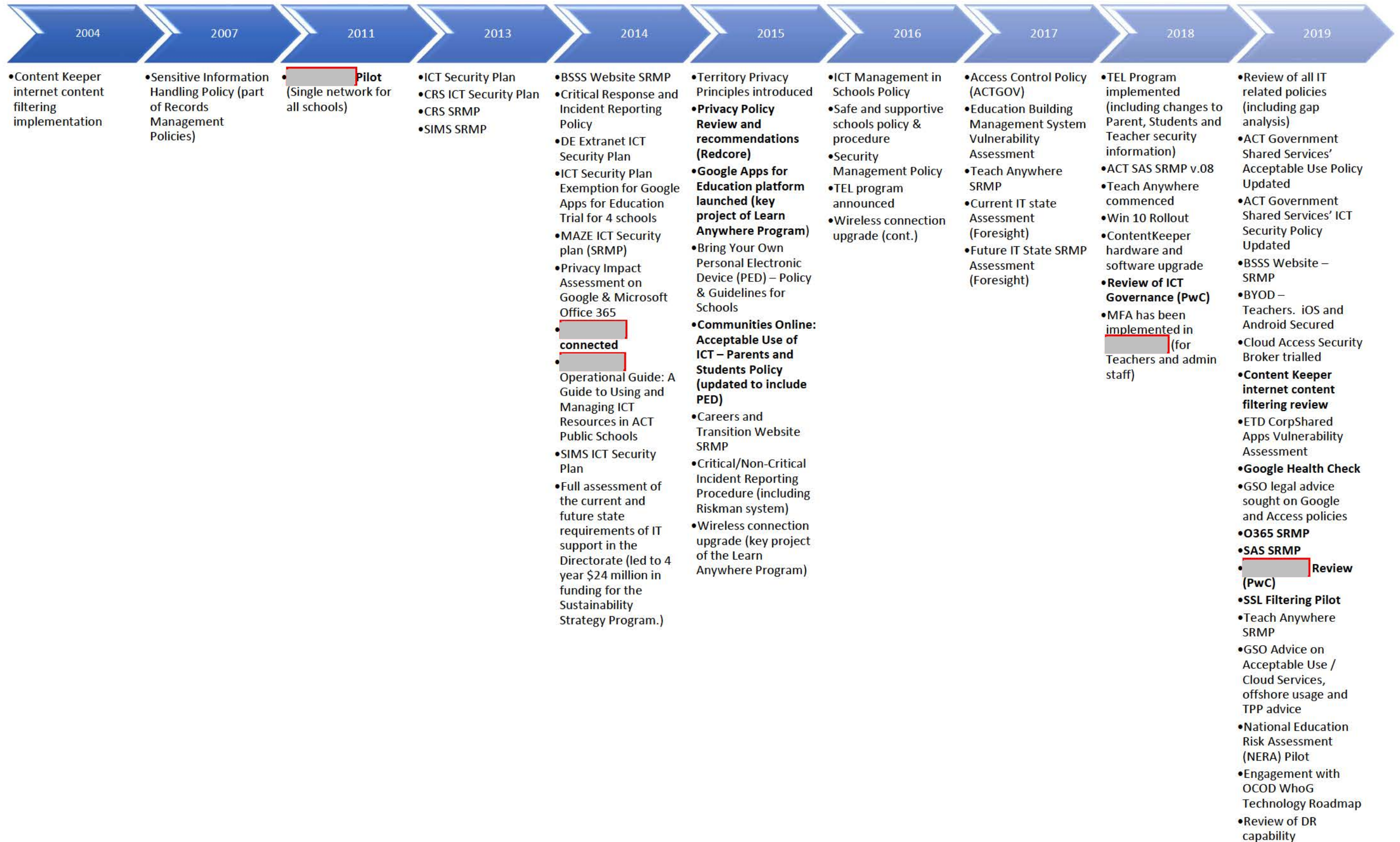
Application security, including user activity monitoring, dynamic app testing, encryption, application firewalls, database monitoring, and runtime application self-protection technology.

Maturity of Controls				
Teacher				
Student				
Maturity	Initial/Ad-Hoc	Developing	Managed	Embedded

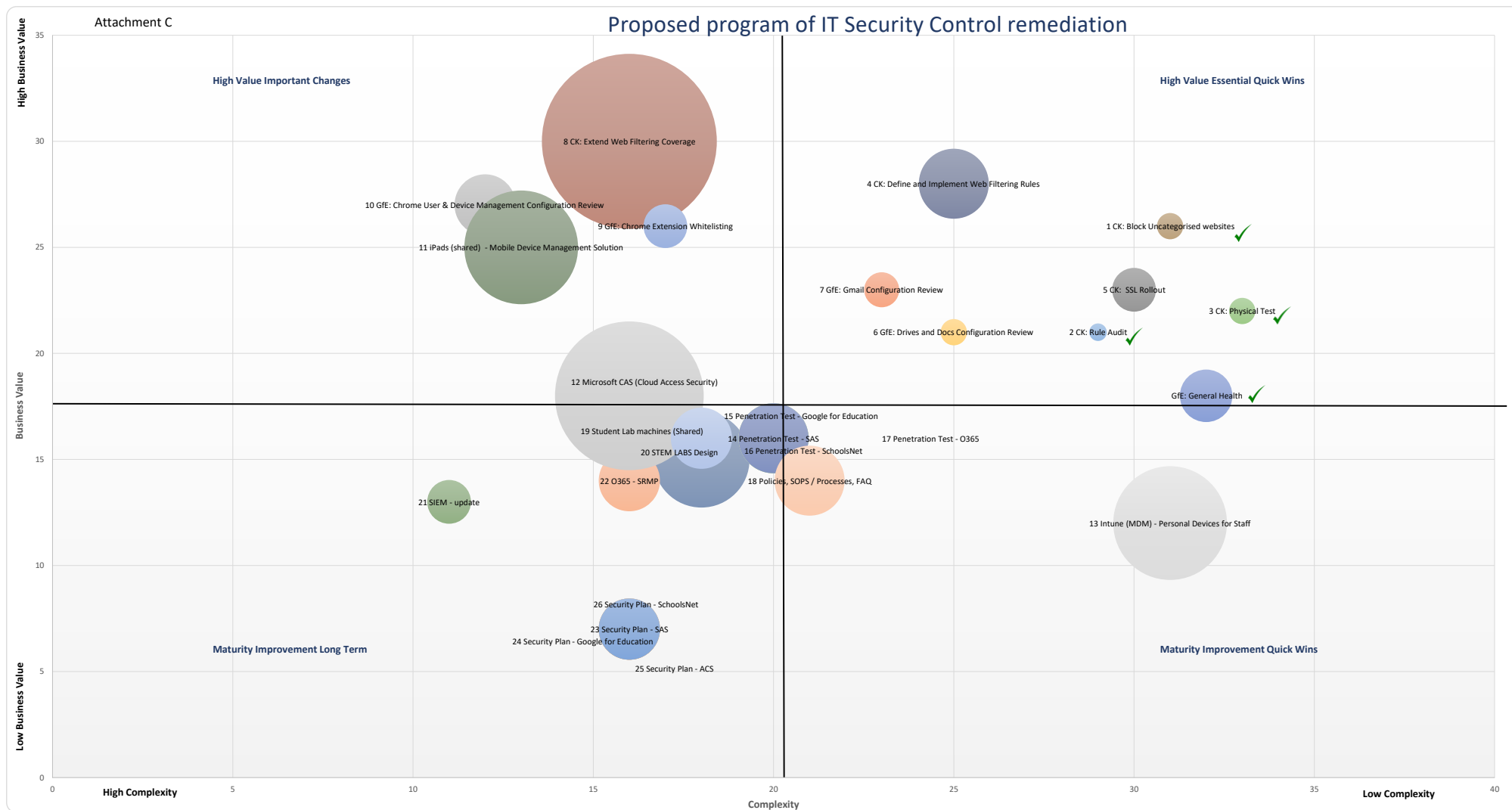


## Attachment B

## Timeline of Key Governance, Risk and Compliance Reviews for Education IT Security







#	Initiative	Description	Business Risk/issue	Estimated Duration / Date
<b>High Value Essential Quick Wins Quadrant</b>				
1	CK: Block Uncategorized websites	Block all uncategorised websites	<p>Uncategorised Websites are sites that have not yet had their content assessed by ContentKeeper. As such they potentially contain content not suitable for consumption by students.</p> <p>Blocking uncategorised websites by default will ensure students are only exposed to content that has already been previously assessed by ContentKeeper and deemed suitable for their consumption.</p>	Completed (11 <sup>th</sup> Oct)
2	CK: Rule Audit	Review the existing CK rules	<p>DSST received feedback indicating inconsistencies in the ContentKeeper rulesets between schools may have resulted in students being exposed to inappropriate web content.</p> <p>An audit of the rules by DSST found sufficient evidence to warrant a physical test (see #3)</p>	Completed (15 <sup>th</sup> Sept)
3	CK: Physical Test	Perform a physical test of contradictory rules at Ainslie and Alfred Deakin	<p>Content Keeper rules which are defined on a school by school basis have grown organically over time. The existing rule sets are complicated and inconsistent between schools and difficult to support.</p> <p>Conflicting and contradictorily rule significantly increase the risk of Students being exposed to inappropriate web content.</p>	Completed (4 <sup>th</sup> Oct)
4	CK: Define and Implement Web Filtering Rules	<p>Implement standard web filtering rules across all ACT public schools based on school years.</p> <p>Develop a support framework to regularly review the standard rule set and allow a mechanism to differentiate between schools who may require greater access than that in the baseline rule set</p>	<p>Responsibility for defining the ContentKeeper ruleset has been decentralised with school principals responsible for defining the school's ruleset.</p> <p>This approach has resulted in each school having an individualised custom ruleset which is difficult to support and often inconsistent between schools. This can result in students being exposed to inappropriate web content.</p>	20 <sup>th</sup> December 2019

#	Initiative	Description	Business Risk/issue	Estimated Duration / Date
			Knowledge of an individual school's ruleset often resides with the principle and is typically lost when they move between schools.	
5	CK: SSL Rollout	Implement Secure Socket Layer (encrypted traffic) inspection	<p>The intention of SSL inspection is to provide enhanced Internet filtering capabilities to help prevent student access to inappropriate content and provide finer grained access and reporting visibility for services such as search engines.</p> <p>Once implemented, it will be possible to review search terms used by students which are often requested as part of investigations performed by the Directorate.</p> <p>Pre-requisite to Reporting Module – At Risk Searches report</p>	<p>Pilot completed (1<sup>st</sup> Sept)</p> <p>Rollout (15<sup>th</sup> Nov)</p>
6	GfE: Drives and Docs Configuration Review	Review configuration of security controls for Google Drives and Docs	<p>Google Drive and Docs is the Directorates primary storage location for learning and teaching material used by both Students and Teachers. Content is created by both Students and Teachers and contains Personally identifiable Information (PII)</p> <p>The service is currently configured to allow students and staff to freely share both files and folders with external anonymous users.</p> <p>Links to this content once shared, never expire putting the Directorate at significant risk of reputational damage through the exposure of confidential information.</p>	1 <sup>st</sup> February 2020
7	GfE: Gmail Configuration Review	Review configuration of security controls for Gmail	Gmail is the primary email platform for Students. Whilst the overall configuration is secure, DSST has proposed several configuration changes that will improve the overall security posture of the service and reduce the possibility this service could be used for cyber bullying between students.	8 <sup>th</sup> November 2019

#	Initiative	Description	Business Risk/issue	Estimated Duration / Date
<b>High Value Important Changes Quadrant</b>				
8	CK: Extend Web Filtering Coverage	Ensure students are protected from being exposed to inappropriate web content when using an Education owned Chromebooks on any network	<p>The existing Content Keeper solution only provides web filtering services for Students using Education provided Chromebook's when they are connected directly to the Education network.</p> <p>This puts students at risk of accessing inappropriate web content on Education provided devices when connected to any network other than the Education network.</p> <p>The Directorate has already received several complaints from parents around this issue resulting in parents banning students from use of TEL device and impacting the students learning experience.</p>	Term 3 2020
9	GfE: Chrome Extension Whitelisting	<p>Develop an approved baseline for Chrome Web Extensions via implementation of Application Whitelisting</p> <p>Implementing scaffolding to assess and implement updates to the Whitelisting rules from schools</p>	<p>Chrome Extensions are 3<sup>rd</sup> party applications which can be installed into a Chromebook to provide additional functionality. They are not subject to the T&amp;C of our G-Suite for Education contract. Over 80% of these applications have no privacy policy, with more than 30% of them able to capture and capture and export content created by students and staff to 3<sup>rd</sup> parties. They are also frequently used by students to bypass Directorate security controls.</p> <p>We do not currently restrict Students use of Chrome Extensions; Students are able to any Chrome Extensions except where that extension has been explicitly blocked at the request of a teacher.</p>	1 <sup>st</sup> February 2020
10	GfE: Chrome User & Device Management Configuration Review	Review configuration of security controls for Chrome User & Device Management settings	The Student experience on Chromebooks is primarily defined by the configuration of Google Chrome User & Device settings within G-Suite for Education.	1 <sup>st</sup> February 2020

#	Initiative	Description	Business Risk/issue	Estimated Duration / Date
			Incorrectly configured, these settings can adversely impact the Student User experience and compromise Student safety.	
11	iPads (Shared) – Mobile Device Management Solution	Implement a centralised management system for shared iPads within Schools.	<p>iPads are used heavily within schools as shared devices to supplement / complement the Schools Chromebook fleet. We do not currently provide schools with access to an enterprise wide management solution. Schools are either configuring iPad individually (taking time away from teaching) or implementing standalone cloud-based solutions managed at the school level (resulting in inconsistent experience and poor economies of scale).</p> <p>This has the potential to put students e-safety at risk through poorly configured security controls on these devices.</p> <p>It is also impacting on School budgets as devices are frequently locked after being associated with a student or teachers personal Apple ID who subsequently leaves resulting in the password being lost.</p>	Term 4 2020
12	Microsoft CASB (Cloud Access Security Broker)	Implement a CASB solution to provide visibility, risk management and policy enforcement of cloud services used by the Directorate	<p>The Directorate is currently unable to monitor the use of 3<sup>rd</sup> Party Web Services by schools. These services are increasingly being used by schools as part of their school curriculum and used to store personally identifiable student data.</p> <p>The lack of effective monitoring puts the Directorate at significant risk of non-compliance with the Territories Privacies Principles (in particular TPP 8) and makes it extremely difficult for the directorate to identify incidents of data leakage.</p>	Term 3 2020

#	Initiative	Description	Business Risk/issue	Estimated Duration / Date
			A CASB once implemented, provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your cloud services.	
<b>Next Maturity Level Quick Wins Quadrant</b>				
13	Intune (MDM) – Personal Devices for Staff	Expand the Directorates Intune based Mobility solution to provide full device-based management.	<p>The Directorates current IOS/Android mobility solution only provides protection for Microsoft based applications, preventing these applications from directly interacting with other Education systems such as Google and SAS which reside outside of the Microsoft Ecosystem i.e. you cannot copy an O365 document into Google drive document within our environment). This can result in a poor user experience for staff.</p> <p>Expanding the existing solution to provide full device-based management will provide a better user experience and allow interaction between the managed Microsoft ecosystem and other Education business systems.</p>	12 months / 2020
14	Penetration Test - SAS	Simulated cyber-attack to actively test security controls and identify vulnerabilities or exploits that may be used to compromise the integrity of the system and / or access Education data	<p>A penetration test provides the next level of security assurance by physically testing that the risks, controls and treatments identified in the SRMP are in place and / or have the desired effect. It will expose actual vulnerabilities in the target environments and help refine the accuracy of the SRMP.</p> <p>Alternatively, where a SRMP has not yet been performed i.e. Google for Education, it can be used to identify high risk vulnerabilities which can be quickly addressed whilst a full SRMP is developed</p>	12 months / 2020
15	Penetration Test - Google for Education	Simulated cyber-attack to actively test security controls and identify vulnerabilities or exploits that may be used to compromise the integrity of the system and / or access Education data	See #14	12 months / 2020

#	Initiative	Description	Business Risk/issue	Estimated Duration / Date
16	Penetration Test - SchoolsNet	Simulated cyber-attack to actively test security controls and identify vulnerabilities or exploits that may be used to compromise the integrity of the system and / or access Education data	See #14	12 months / 2020
17	Penetration Test - O365	Simulated cyber-attack to actively test security controls and identify vulnerabilities or exploits that may be used to compromise the integrity of the system and / or access Education data	See #14	12 months / 2020
18	Policies, SOPS / Processes, FAQ	ICT Policies, Standard Operation Procedures, Process and Frequently Asked Questions	Provides the foundation and rationale used to define the Directorates security posture and justification for the implementation of required security controls.	12 months / 2020
<b>Next Maturity Level Quadrant</b>				
19	Student Lab machines (Shared)	Provide a Windows 10 based learning platform for Students which balances their pedagogical needs against the Directorates broader e-safety requirements	<p>Despite Google being the primary learning platform for students, students within ACT Education use the same SOE build, with the same security controls and dependencies upon Office 365 as that used by Teachers.</p> <p>Note only does this provide a poor user experience for Students as the current SOE does not directly integrate with G-Suite for Education, the security controls designed which are designed to protect the Teachers SOE limit or actively prevent the ability of students to undertake classes in advanced ICT concepts such as program, networking and ethical hacking.</p>	12 months / 2020
20	STEM LABS Design	Provide a pattern for STEM Labs	Ensure future proof design of system and controls for STEM Labs	12 months / 2020
21	SIEM – update	Security Information event management	Without effective controls in place, the following risks exist:	12 months / 2020

#	Initiative	Description	Business Risk/issue	Estimated Duration / Date
			<ul style="list-style-type: none"> <li>● Violation of security policies cannot be attributed to a specific person (i.e. their actions cannot be accounted for).</li> <li>● Security incidents cannot be effectively investigated.</li> </ul> The update is to refine and review the monitoring rules and logs	
22	O365 - SRMP	Security Risk Management Plan (SRMP) - It is a best practice approach to identifying and recommendation controls to reduce potential security risks (Confidentiality, Integrity and Availability)	Identify and manage risks and assist decision-making to apply appropriate controls and improve resilience	12 months / 2020
23	Security Plan - SAS	Security Risk Management Plan (SRMP) - It is a best practice approach to identifying and recommendation controls to reduce potential security risks (Confidentiality, Integrity and Availability)	Identify and manage risks and assist decision-making to apply appropriate controls and improve resilience	12 months / 2020
24	Security Plan - Google for Education	Security Risk Management Plan (SRMP) - It is a best practice approach to identifying and recommendation controls to reduce potential security risks (Confidentiality, Integrity and Availability)	Identify and manage risks and assist decision-making to apply appropriate controls and improve resilience	12 months / 2020
25	Security Plan - ACS	Security Risk Management Plan (SRMP) - It is a best practice approach to identifying and recommendation controls to reduce potential security risks (Confidentiality, Integrity and Availability)	Identify and manage risks and assist decision-making to apply appropriate controls and improve resilience	12 months / 2020
26	Security Plan - SchoolsNet	Security Risk Management Plan (SRMP) - It is a best practice approach to identifying and recommendation controls to reduce potential security risks (Confidentiality, Integrity and Availability)	Identify and manage risks and assist decision-making to apply appropriate controls and improve resilience	12 months / 2020



# *ACT Education Directorate*

## *[Redacted] Policy and Security Controls Analysis*

### Draft Addendum

*ACT Education  
Directorate*

*[Redacted]: Policy and  
Security Controls  
Analysis*

*Draft Addendum*

*October 2019*



# Table of Contents

1	Addendum.....	2
1.1	Mapping of findings to recommendations.....	2

## Disclaimer

This paper has been prepared by PricewaterhouseCoopers in accordance with the agreement with the ACT Education Directorate signed on 01 February 2019 and in accordance with the standards issued by the Auditing and Assurance Standards Board, and accordingly no such assurance under those standards has been provided.

This paper and PricewaterhouseCoopers deliverables are intended solely for the **ACT Education Directorate's** internal use and benefit and may not be relied on by any other party. This paper 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 this paper.

# 1 Addendum

## 1.1 Mapping of findings to recommendations

The following provides a mapping of findings to recommendations.

Finding	Recommendation	Benefits Expected	Suggested Timeframe
<p><b>Finding 1: The existing security policies related to [REDACTED] are outdated, inconsistent and unsupported through a process of continual improvement.</b></p> <ul style="list-style-type: none"> <li>PwC assessed the design effectiveness of security policies covering [REDACTED] and overall found the policy suite was not addressing the current technology-enabled environment. Existing policies are not driven by a shared view over what the 'digital classroom of the future' (or similar statement) may look like or a clear understanding of what the Directorate is looking to achieve.</li> <li>As a result, the policy suite appears to have developed organically over time as opposed to a strategically focused approach. This implies that an understanding of what a</li> </ul>	<p><b>Recommendation 3: The Directorate, based on the ongoing risk and threat assessments, to develop/update a suite of new policies in relation to [REDACTED].</b></p> <p>The Directorate to define 'what a good policy framework looks like' and update existing [REDACTED] policies accordingly.</p> <p>In addition, the following new policies are to be considered:</p> <ul style="list-style-type: none"> <li>The standard operating environment for both Google and Microsoft,</li> <li>The use of 3rd party and cloud applications,</li> <li>User access,</li> <li>Monitoring and event logging, and</li> <li>Security incident management.</li> </ul>	<ul style="list-style-type: none"> <li>Policies will be based on risk assessments, and will therefore be designed to address current risks.</li> <li>Policies will provide stakeholders (school Principals, school staff, students, parents and service providers) with clear rules, principles and guidelines to act upon.</li> <li>Policies help stakeholders know what is expected of them with respect to standards of behaviour and performance.</li> <li>Policies provide clarity and consistency, and set a clear framework for delegation of decision-making.</li> </ul>	<p>Within 6 months Note - This activity is dependent on completion of Recommendation #2, but can commence now.</p>

<p>'good policy framework' looks like is unclear.</p> <ul style="list-style-type: none"> <li>• Other than the Directorate's policy 'Communities Online: Acceptable use of ICT – Parents and Students Policy', no policies have been developed canvassing the controls areas examined in this paper, therefore providing no direct link between policy and controls.</li> <li>• While both the Directorate and SSICT have responsibility for setting security policy, current policies have also enabled schools to retain a level of autonomy in decision making that they held prior to the implementation of [redacted] with each school being able to make its own decisions on security policy. For example, current policy enables school Principals to grant teachers and students access to applications at their discretion, and change settings on ContentKeeper software according to their views on what websites are appropriate to be accessible versus banned.</li> </ul>			
---	--	--	--

<p><b>Finding 2: Security policies do not address current threats and risks.</b></p> <ul style="list-style-type: none"> <li>• Policies and controls that are currently in place were not determined or developed as a result of the undertaking of a strategic threat and risk assessment (TRA) of the complete [redacted] environment. A TRA is a security planning tool, which should be used to identify risks that need mitigating, and to identify the actions that need to be undertaken as a result. These mitigating actions can support the design of policies and controls. It is acknowledged that while TRAs and security risk management plans have been completed for some elements of [redacted] and that that a number of risk workshops were undertaken during the [redacted] network modernisation project, it is clear that these assessments have not provided a holistic risk view from which to make informed decisions related to control requirements.</li> <li>• As a result of the limited initial assessment of risk, and with the parallel</li> </ul>	<p><b>Recommendation 2: The Directorate to undertake a strategic security threat and risk assessment of the [redacted] technology environment.</b></p> <p>The Directorate, to initially and then in an ongoing basis (for example annually) undertake a strategic threat and security risk assessment for the [redacted] environment to determine the adequacy of existing policies and controls; and to identify and manage significant shifts in the risk, threat and operating environment. Steps that could be taken include:</p> <ul style="list-style-type: none"> <li>• Research to identify technical trends (the possible future state) of devices, peripherals and applications.</li> <li>• Research to identify information outlining where students globally have identified control work arounds in schools.</li> <li>• Source information from schools where students have reported knowledge of control work arounds.</li> <li>• Review security incidents that have been reported to identify policy and control weaknesses that have not yet been addressed, and to identify trends.</li> <li>• Research into new information on trends in</li> </ul>	<ul style="list-style-type: none"> <li>• The Directorate is able to identify current threats and risks.</li> <li>• The Directorate is able to identify new threats and risks introduced by the changing threat and risk landscape, and is able to determine appropriate policy and controls.</li> <li>• The Directorate is able to identify weaknesses with existing controls.</li> <li>• Appropriate controls are applied effectively and consistently.</li> <li>• The Directorate is being proactive in staying ahead of the emerging threats to students in regards to online safety.</li> <li>• A reduction in security incidents.</li> <li>• A continuous improvement process is established, and becomes part of ongoing processes.</li> </ul> <p>Best practice security measures and procedures are adopted, increasing the Directorate's security maturity.</p>	<p>Within 3 months</p>
---	--	---	------------------------

<p>evolution of the technological environment, the Directorate has not proactively updated policies according to the current risk environment.</p>	<p>online safety and online risks, for example through scanning the Office of the eSafety Commissioner and Australian Federal Police publications.</p> <ul style="list-style-type: none"> <li>• Source information from SSICT on new and emerging security risks.</li> <li>• Source information from SSICT on recommendations for new security controls, especially in regards to ContentKeeper, the Google for Education Suite, managed devices, peripherals and applications.</li> <li>• Source information from school IT Coordinators and IT Officers on technology trends and new technology that they are investigating for possible use within schools.</li> <li>• Gain and document an updated understanding of the control environment surrounding all control areas in the maturity heat map.</li> </ul>		
<p><b>Finding 3: The maturity of security controls designed, developed and implemented for ██████ is low.</b></p> <ul style="list-style-type: none"> <li>• Existing controls were established during the initial implementation of ██████ Stakeholder</li> </ul>	<p><b>Recommendation 4: The Directorate to develop a Technology Roadmap (based on key services to be provisioned) and from this, identify and implement the desired maturity level of controls for ██████.</b></p>	<ul style="list-style-type: none"> <li>• A program of work will more likely meet its objectives if its goals are agreed and then mapped out with timeframes and milestones for achievement.</li> <li>• A roadmap helps articulate the strategic thinking behind the</li> </ul>	<p>Within 12 months</p>

<p>feedback states that the initial controls design and functionality employed were designed to 'encourage schools to join [redacted] rather than stay on their own networks', that is, controls implemented were a compromise between depth of security and functionality and flexibility allowed. In that context, it could be seen that [redacted] is working as designed, however, the evidence around the design of these controls that is 'good for students' or tailored across the 'stages of schooling' is not as clear to state.</p> <ul style="list-style-type: none"> <li>• Seven specific security controls were assessed and analysed, with most controls rated as either the 'Initial/Ad-hoc' or 'Developing' levels. These levels are on the low end of maturity and reflect that controls are in place, but are not managed in an effective and ongoing manner.</li> <li>• Controls have not been reviewed since implementation. There is no ongoing monitoring approach to maintain the effectiveness of control, nor</li> </ul>	<p>The Directorate to develop a Technology Roadmap of key services to be implemented over the next 3-5 years. From this, develop a program of work to confirm/develop the desired maturity level of controls, in particular:</p> <ul style="list-style-type: none"> <li>• Network security</li> <li>• Content filtering, and</li> <li>• 3rd party applications (including cloud).</li> </ul> <p>Suggested elements for inclusion in the 'Technology Roadmap' are:</p> <ul style="list-style-type: none"> <li>• What technology or services will be required in the future, what the cost will be, and what the timeframe will be for its purchase;</li> <li>• What additional staff resources might be required;</li> <li>• What the ongoing support costs will be, and for how many years into the future;</li> <li>• What training will need to be invested in teachers professional development to learn the technology, and the costs of training; and</li> <li>• What elements of the cost will be funded by the Directorate.</li> </ul>	<p>goals and also serves as a communication tool.</p>	
	<p><b>Recommendation 5 – The Directorate, in consultation with SSICT and Schools, to review and subsequently redesign and</b></p>	<ul style="list-style-type: none"> <li>• Clarity for schools in how to request different types of services.</li> <li>• Efficiency.</li> </ul>	<p>Within 3 months</p>

<p>any structured reporting or continuous improvement process to manage issues/problems identified.</p> <ul style="list-style-type: none"> <li>• There is no clear visibility of the consideration between preventative vs detective controls for [redacted]. There is no strategy or process in place to define the right mix between these control types.</li> </ul>	<p><b>implement new processes for accessing services (i.e. issue and problem management) provided to SSICT and schools.</b></p> <p>The Directorate to design and implement clear and consistent governance and processes to support service requests from the both SSICT and schools.</p>	<ul style="list-style-type: none"> <li>• Ability to identify the type and frequency of services/issues being requested by schools.</li> </ul>	
<ul style="list-style-type: none"> <li>• Schools are endeavouring to teach cyber security and hacking (white hat) to students. They cite that 'students want a programme that develops them and is challenging'. Software is not always able to be installed to facilitate this education, in particular software arrangements that would enable students participate in organised hackathons. Therefore, schools desire more support to teach cyber security courses.</li> <li>• SSICT have stated the benefit that could be derived from a clear 'Technology Roadmap' for the Directorate. This roadmap would serve a greater purpose if it was to be based upon the key services that need to be enabled over the next 3-5</li> </ul>	<p><b>Recommendation 6: Develop and consider a proposal for the undertaking of an 'ACT Education Directorate Hackathon' event where students from all age groups are invited to demonstrate how they circumvent security measures on the school network.</b></p> <p>The Directorate to explore the design and undertaking of an event in which students from all age groups are invited to demonstrate how they circumvent security measures on the school network and then use the outcomes to explore changes to security controls.</p> <p>The event would be run using a simulated [redacted] environment and not the actual 'live' version of the [redacted] network.</p>	<ul style="list-style-type: none"> <li>• Gaining of insight into the techniques used to bypass the ContentKeeper Internet content filter.</li> <li>• Identification of vulnerabilities in current security controls.</li> <li>• Identification of techniques explored by students when bypassing security measures.</li> <li>• Gaining of information on the level of computing expertise possessed by students.</li> <li>• An avenue to promote digital literacy amongst students and convey to them the importance of network security.</li> </ul>	<p>Within 18 months</p>



<p>years (i.e. Google Suite, Schools Administration System (SAS), Smartboards, etc.). From this would flow the details required to inform the controls environment for [redacted] as well as the detail to address a key question for the Directorate on 'how to define the right capability to support students'?</p> <ul style="list-style-type: none"> <li>• The Directorate and SSICT need a scalable capability to support schools. The skills to implement low maturity controls may have existed in the initial rollout of [redacted] but are they adequate now given the changes in technology? Direction provided from the Technology Roadmap will also address this fundamental question.</li> </ul>			
<p><b>Finding 4: Governance over security controls is unclear.</b></p> <ul style="list-style-type: none"> <li>• There are a number of factors impacting upon the control and oversight of controls for [redacted]. As stated, minimal clarity over the purpose and outcomes for [redacted] may be impacting upon the structures in place.</li> </ul>	<p><b>Recommendation 1: The Directorate, in collaboration SSICT and in consultation with schools, to review the current governance structures and provide greater clarity on roles and responsibilities for design, implementation, management and monitoring of controls.</b></p>	<ul style="list-style-type: none"> <li>• Greater clarity on roles and responsibilities.</li> <li>• Clearer accountability.</li> <li>• Clearer line of communication.</li> <li>• Clearer authority to make decisions and take actions.</li> </ul>	<p>Within 3 months</p>

<ul style="list-style-type: none"><li>• This paper found low clarity on accountability and responsibility related to the oversight of the controls framework. Decision making appears distributed across a number of stakeholders and a process to appropriately assess decisions in light of security posture, stakeholder needs and overall objectives is missing. Key stakeholders and points of contact across all levels of the governance layers are not known which also impairs effective communication.</li><li>• Monitoring of the effectiveness of controls is minimal. The Directorate, who should be maintaining oversight of controls, currently has limited line of sight across all control areas and no audit trail in place to support reporting of issues and continual improvement.</li><li>• There is recognition from stakeholders within the Directorate and SSICT of a number of control related issues, but no clear direction on resolution. SSICT acknowledges that they should contact the service desk when reporting an incident, however, state</li></ul>			
--	--	--	--

---

<p>that they do not apply this process as when security related issues are raised and control remediation recommended, they do not receive a response on decisions or actions undertaken from the Directorate.</p>			
--	--	--	--

DRAFT

[pwc.com.au](http://pwc.com.au)

## Background

### ContentKeeper design:

ContentKeeper (CK) is a transparent web filter, which allows users to be provided filtering without having to configure each device to access a specific Proxy. CK is applied in the gateway to all outbound Internet requests over standard web ports (80/443), where it either allows or restricts access to the web content.

### SSL Filtering:

There is active work between SSICT and Education to introduce SSL filtering inspection, which will allow more control and visibility of encrypted web traffic. The need for SSL filtering is at an all-time high after Google and Bing defaulted searching to be via SSL, as the ability to filter and review search terms is required. The new ContentKeeper infrastructure has been sized to meet Education's previously declared intention of targeted inspection of search engines and social media, it will not inspect all traffic, and indeed some inspection is known to break some websites and web applications. This SSL inspection capability is targeted for completion by end of calendar year.

### Firewall Access:

The Education network allows other traffic out directly through to the firewall, this configuration has been made to:

- enable many teaching applications to function without specific network configuration;
- along with supporting non-corporate friendly devices like Androids.

On the ACT Government corporate network, it would usually take a few changes to enable an application to function on the network.

Based on the current network and filtering Education CIO office may wish to reconsider the following to ensure that it complies with their future intentions:

## Policy architecture and 'non-managed' site access.

Currently there is a single policy for all staff. Students however are filtered with separate policies per school, with some larger schools having policies divided between age-groups for primary/secondary/college.

For the Student policies approval for modifications of the allowed/blocked sites are at the principal/deputy principal (or their authorised delegate) level.

The update process is initiated by the School to the Education ICT team, who vets approvals and sends to Security to review and update policies.

### Simplify/collapse policies.

This would be to consolidate student policies so there are no longer school specific policies and filtering policies would be shared territory wide and based on a given year level. All policy management requests would have to be governed and managed by the Education Directorate centrally.

It should be noted that it is not possible to have policies based on classes attended, as a student can only be matched to a single policy.

#### *Advantages:*

- a. much simpler for Education to understand and regularly review policies.

- b. Principals will inherit a known policy the same as any other school when they move into/change schools.
- c. Having a common centralised approval body in Education CIO will likely mean more consistent and acceptable filtering decisions for the directorate.

#### *Disadvantages*

- a. Removes autonomy for principals to make filtering decisions unique to their school or classes.
- b. Likely increased time for changes/approvals as requests from schools would need to go through Education Governance body before being actioned.
- c. Significant policy development and testing will be required to ensure schools are able to access all their required sites with any new consolidated policies.
- d. Transition to simplified policies would be easy to configure on the CK devices however rollback would be difficult unless the device was restored to a point in time.

#### Disallow non-managed web traffic.

'Non-managed' traffic are websites where the web filter does not have a categorisation in place. The current position is that all primary school policies disallow access to non-managed resources. High school/colleges allow this access. Since non-managed is a grey area where the site could be anything from educationally orientated right through to malicious/pornographic, there are considerations in either allowing or rejecting non-managed.

#### *Advantages*

- a. Would prevent this method of bypassing the content filters for web access. As there will always be new malicious and inappropriate sites that are not yet categorised.
- b. Reduce likelihood of accidental student access to inappropriate content at schools. For example, where a student googled a topic, and a search result was to an uncategorised site with inappropriate content.

#### *Disadvantages*

- a) Because non-managed can be legitimate websites, this will introduce delays in high schools/colleges getting access to legitimate content. It would not be accessible until the filters were updated with the new policy. This could be done without through pre-approval where there is a clear idea of the content of the site (for example SSICT can determine a website is 'NEWS' or 'SHOPPING') but there may be sites where the content would need consideration by Education Governance body as to how they would like the site categorised.

Due to the on-going impacts to user experience, the policy design options above are not SSICT recommendations. They are provided as higher assurance models for web filtering. If either of these are to be considered, further analysis should be conducted into the support requirements of either solution.

## Network architecture

Current state is that both the trusted and personal device network is 'proxy-less' and allows a large range of traffic directly out through firewall. This was part of a previous decision by the Education Directorate to enable extra compatibility and ease of use for different types of applications and device types like Android and iOS. This has unfortunate side effect that VPN is very easy to operate and hard to block, including that inappropriate network traffic like torrents can work in certain configurations. This traffic will be encrypted or will not have a signature so that the firewall or web filter can make a policy decision, making it almost futile to block VPN, torrents and other forms of

undesirable traffic. There are known issues where Education has received copyright infringement notices from torrenting, and in the current configuration VPN solutions can function on the network.

Shared Services can restrict the firewall to prevent most types of traffic, however there needs to be consideration about the significant impacts that this will have on legitimate application access. All applications on windows, Chromebooks and mobile devices have been tested in the context of an unrestricted network, so various applications and services will be impacted or cease to function correctly. It would require extensive testing, and likely a lot of labour to make individual applications work in a least privilege context.

*Advantages:*

- a. Much higher assurance of preventing inappropriate and undesirable network traffic, including VPN access and copyright infringement via torrents.
- b. Better security as many types of malware may not operate correctly without open firewall

*Disadvantages*

- a. All testing for apps based on current approach, locking down access will require significant retesting
- b. The environment is currently very simple to support. New apps or web services function with minimal configuration.
- c. Some device types may be more impacted.
- d. There may need to be broad exemptions to make some applications function.
- e. Due to the complexity involved SSICT would need further consultation to scope the resource requirements. It likely such a large and high risk undertaking that it would be best handled as part of a project for network redesign.

Alternatives to a fully restricted firewalling model can be looked at also, for example analysing specific VPNs and trying to lock down, however the effectiveness of this form of lockdown would likely be limited.

## Chromebook application control

Current state is that applications are blocked based on the category, so categories like 'productivity' may be allowed, but other categories can be blocked. The problem is that apps are often, possibly deliberately, miscategorised on the app store, so applications like VPNs can be installed on Chromebooks. It is recommended to centrally manage a whitelist of approved apps.

*Advantages:*

- a. Education would be able to vet all apps centrally and dramatically reduce the risk of nefarious/undesirable apps on the managed Chromebooks.
- b. Help prevent 'shadow ICT' services, where staff are using some apps that are linked to unsanctioned/unassessed cloud services that are not endorsed by the directorate and may not comply with policy

*Disadvantages*

- c. Introducing app approval process will introduce a delay and less flexibility for teachers to determine useful chrome apps for education delivery.

This record is not released in accordance with section 17 of the *Freedom of Information Act 2016*

Schedule 2, 2.2(a)(iii) and 2.2(a)(xi)



# Digital Backpack Red Team Assessment


ACT Education

# 1 Document Details

## 1.1 Assessment

<b>Control classification</b>	OFFICIAL
<b>Project type</b>	Red Team
<b>Report template version</b>	v1.0

## 1.2 Prepared By

Foresight Consulting	
	<b>Address:</b> 11/1 Hobart Street Canberra ACT 2601
	<b>Assessor:</b> [REDACTED]
	<b>Qualifications:</b> [REDACTED]
	<b>Email:</b> [REDACTED]@foresightconsulting.com.au

## 1.3 Prepared For

ACT Education	
	<b>Address:</b> 51 Fremantle Drive, Stirling, ACT 2611
	<b>Contact:</b> an.French
	<b>Email:</b> an.French@act.gov.au

## 1.4 Revision History

Version	Date	Description	Author
0.1	Apr 2021	Initial Draft	[REDACTED]
1.0	Apr 2021	Internal review	[REDACTED]
1.1	Apr 2021	Update based on customer feedback	[REDACTED]

## Table of Contents

1	Document Details .....	2
1.1	Assessment .....	2
1.2	Prepared By.....	2
1.3	Prepared For.....	2
1.4	Revision History .....	2
2	Executive Summary .....	4
2.1	Background .....	4
2.2	Red Team Scenario.....	4
2.3	Trophies.....	4
2.4	Trophy Walkthrough and Recommendations.....	5
2.4.1	Access to another student's email or account (Not Achieved) .....	5
2.4.2	Access to a teacher's email or account (Not Achieved) .....	5
2.4.3	[REDACTED] (Achieved) .....	5
2.4.4	[REDACTED] (Achieved) .....	6
2.4.5	Recommendations .....	8
2.5	Overview of Findings .....	10
3	Open Source Intelligence .....	12
	[REDACTED]	
	[REDACTED]	
	[REDACTED]	
4	Positive Observations .....	15
	PO1: Limited Port Exposure .....	15
	PO2: External File Sharing Not Allowed in OneDrive .....	15
	PO3: Non-ACT Education Users Not Allowed to Join Google Classroom Classes.....	15
5	Findings .....	16
6	Conclusion.....	29
	Annex A: General Observations .....	30
	GO1: Azure Portal Access Allowed .....	30
	GO2: Staff Contact Details via Office 365 Search Function .....	30
	Annex B: Business impact ratings.....	31
	Annex C: Threat matrix.....	32



## 2.4 Trophy Walkthrough and Recommendations

### 2.4.1 Access to another student's email or account (Not Achieved)

During the course of the engagement, Foresight could not gain direct access to another student's email or account. [REDACTED]

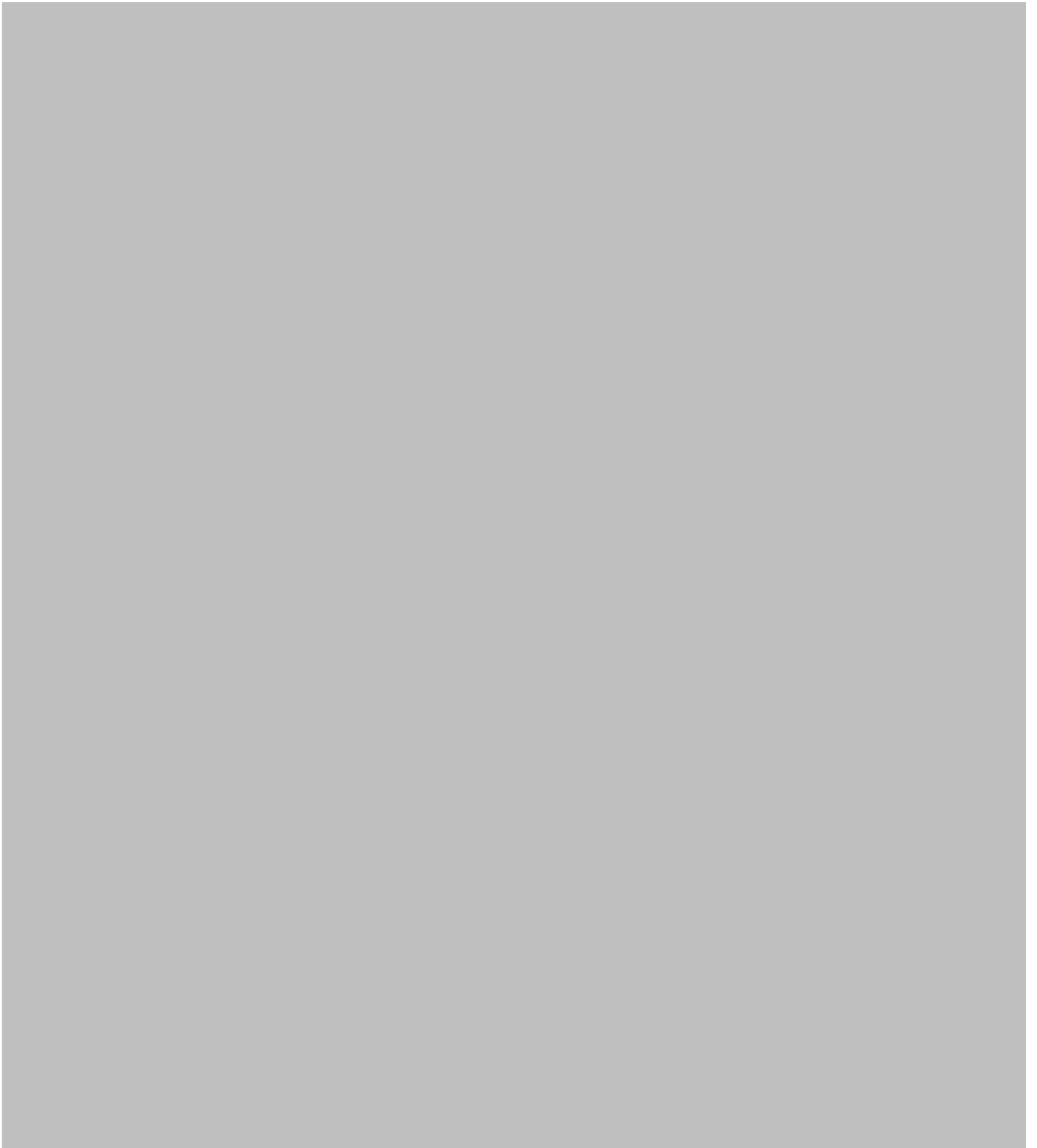
### 2.4.2 Access to a teacher's email or account (Not Achieved)

During the course of the engagement, Foresight could not gain direct access to another teacher's email or account. [REDACTED]

### 2.4.3 [REDACTED] (Achieved)

2.4.4

(Achieved)



### 2.4.5 Recommendations

ID	Recommendation	Implementation Cost	Priority
1	Review Google Groups settings and ensure teacher groups are restricted to teachers only.	Low	High

2	ACT Education staff should avoid posting Personal identifiable information (PII) on public Google Group conversations and public feeds on Google Drive.	Low	High
3	Review Google Drive and OneDrive file sharing settings and ensure files that contain Personal identifiable information (PII), or any other sensitive information are restricted to intended target audience.	Low	High



## 2.5 Overview of Findings



A total of eight vulnerabilities or security issues were identified over the course of this engagement. The significant findings relate to weak password policy and sensitive data exposure in [redacted] search results. Foresight recommends that these issues be given immediate priority for remediation.

Overall, the security posture of the assessed system was average, when compared to organisations of a similar size and complexity.

By validating and actioning the recommendations provided in this report, ACT Education will be in an excellent position to continue the strengthening of their security posture and reduce their overall attack surface.

The following findings section summarises the positive observations noted of the external network and the test findings, including any vulnerabilities detected.

Recommendations and their assigned priorities have been formulated based on Foresight’s understanding of ACT Education’s existing controls, the current threat landscape and vulnerability research. Definitions of priority ratings are:

- **Priority 1** = Immediate attention, actions and/or risk-based decisions required.
- **Priority 2** = Important and relevant actions that should be addressed in the medium term to reduce overall risk exposure.
- **Priority 3** = Minor improvement opportunities for management consideration.

ID	Finding	Business Impact				Remediation Priority
		Critical	High	Medium	Low	
F01	Weak Password Policy		X			1
F02	Sensitive Data Exposure in [redacted] Drive Search Results		X			1
F03	Inadequate External File Sharing Controls [redacted]			X		2
F04	Session Not Invalidated on Logout			X		2
F05	Inufficient Session Expiration			X		2
F06	Lack of Access Controls to Google Classroom via Class Code				X	3
F07	Inadequate TLS Configuration				X	3
F08	Various HTTP Security Setting Improvements				X	3
<b>Total</b>			2	3	3	

Table 1: Findings

Annex A documents the General Observations noted by Foresight when undertaking this assessment. Whilst none of these items are considered findings, ACT Education should ensure that the observed services are expected for the external environment.

### 3 Open Source Intelligence

Prior to and during the red team exercise, Foresight gathered intelligence around ACT Education's external network that is openly available on the Internet. This information can be leveraged by attackers to minimise the detection of their attack and ultimately assist in obtaining their goal.





## 4 Positive Observations

During the engagement, Foresight observed several controls in place that are positively impacting the security posture of Digital Backpack.

### **PO1: Limited Port Exposure**

ACT Education have only exposed the minimum number of ports required for Digital Backpack to operate. This has reduced the attack surface of the Digital Backpack site significantly whereby common ports such as RDP and SMB are not available to attackers to abuse.

### **PO2: External File Sharing Not Allowed in OneDrive**

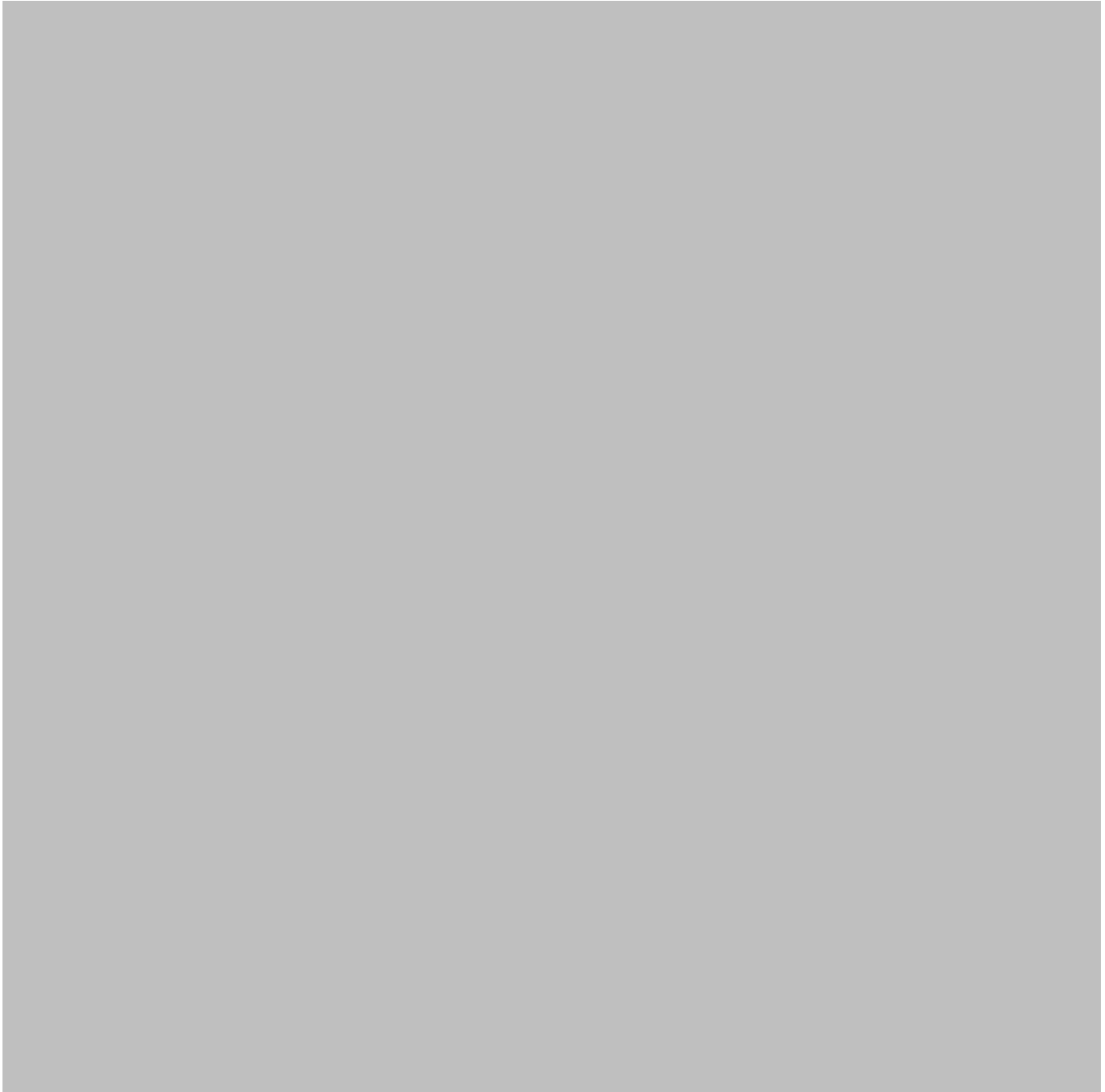
ACT Education have implemented file sharing controls to prevent users from sharing files outside the organisation via OneDrive. During testing, Foresight found that the control had restricted the test user's ability to share files externally. This would restrict a potentially malicious user's ability to share sensitive documents externally.

### **PO3: Non-ACT Education Users Not Allowed to Join Google Classroom Classes**

ACT Education have restricted non-ACT Education users from joining Google Classroom classes despite having a valid class code. This has significantly reduced the attack surface of malicious attackers gaining access to ACT Education student materials from a non-ACT Education user account.

## 5 Findings

A summary of findings including recommendations from the Red Team exercise are presented below. For general observations, please see *Annex A* of this report.



## 6 Conclusion

Overall, Foresight found the security posture of ACT Education's Digital Backpack system to be average when compared to organisations of similar size and complexity. ACT Education should ensure that sensitive content cannot be accessed or shared by students, session management is handled properly, student access to Google Classroom is controlled and appropriate TLS and HTTP security settings are maintained.

Rules of Engagement restrictions prevented DDoS, DoS, social engineering and reverse engineering attacks. ACT Education should be aware that these attack vectors are significant and should take steps to mitigate or test them in the future.

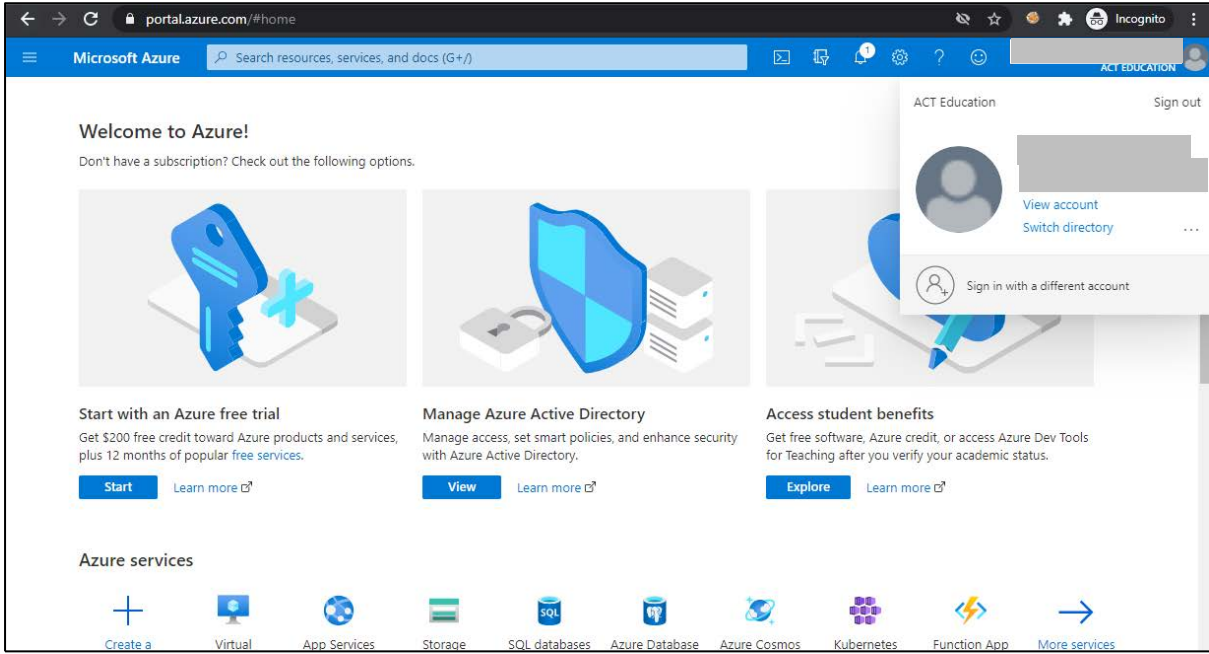
Foresight recommends that ACT Education review the findings detailed in this report and consider the security recommendations provided.

By validating and actioning the recommendations provided in this report, ACT Education will be in an excellent position to continue the strengthening of their security posture and reduce their overall attack surface.

## Annex A: General Observations

### GO1: Azure Portal Access Allowed

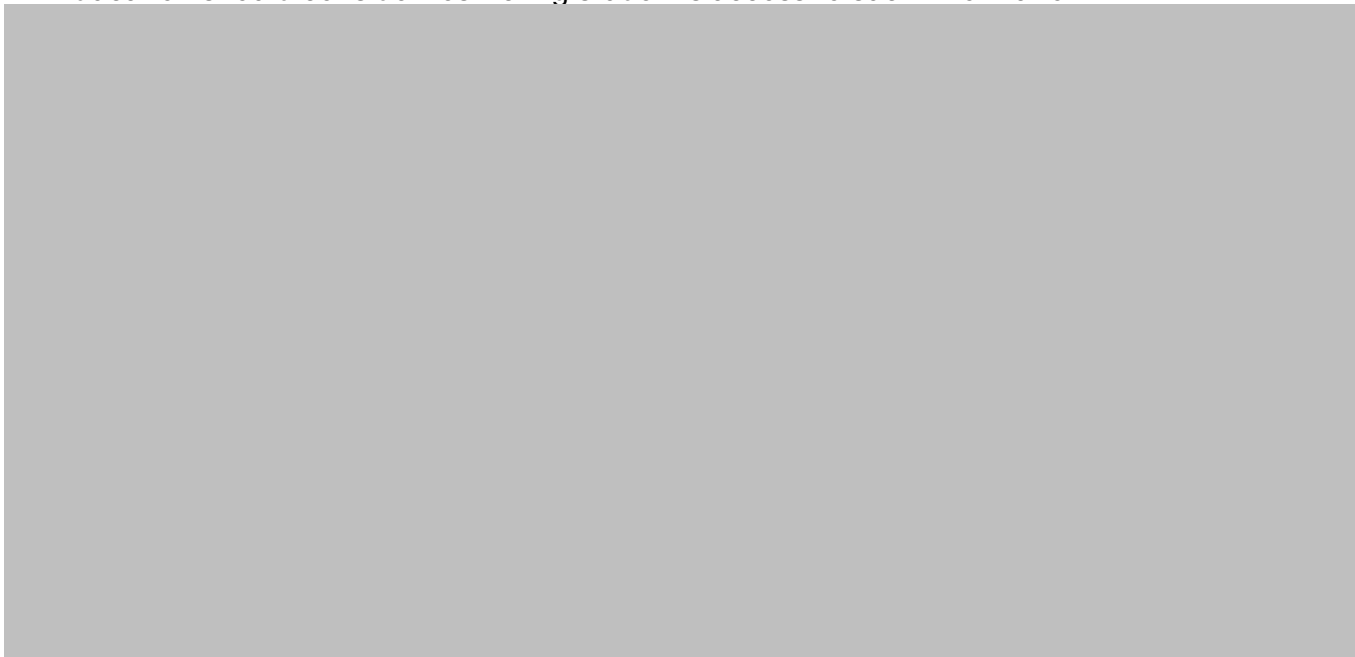
Test student accounts have access to Azure Portal. ACT Education may consider implementing conditional access policies to restrict student’s access to Azure Portal if there is no business requirement for it.



**Figure 9: Student Access to Azure Portal**

### GO2: Staff Contact Details via Office 365 Search Function

Test student accounts could obtain teacher and staff contact details (including phone number and email address) from other schools via the Office 365 search function. ACT Education should consider restricting student’s access to such information.





## Annex B: Business impact ratings

Foresight ranks business impact as being **critical**, **high**, **medium** or **low** based upon the potential damage a vulnerability poses to the business. The metrics used to calculate this impact are:

- **Financial damage:** How much financial damage will result from an exploit? Less than the cost to fix the vulnerability (low); minor impact to annual profit (medium); significant impact to annual profit, up to and including bankruptcy (high).
- **Reputation damage:** Would an exploit result in reputation damage that would harm the business? Minimal damage (low); loss of goodwill or brand damage (medium); loss of major accounts (high).
- **Non-compliance risk:** How much exposure does non-compliance introduce? Minor violation (low); clear violation (medium); high profile violation (high).
- **Information disclosure:** How much personally identifiable or confidential information could be disclosed? One individual or document (low); hundreds of people or documents (medium); thousands to millions of people or documents (high).

The ranking system for exploited vulnerabilities and their possible impacts:

- **Critical:** This vulnerability could have a catastrophic impact on the business, with significant losses to profit and reputation. Such issues pose an immediate threat to business operation and reputation. It may also constitute privacy violations for a large portion of the business and introduce additional exposure to non-compliance violations.
- **High:** This vulnerability could have a major impact on the business, with significant losses to profit and reputation. It may also constitute privacy violations for some portion of the business and introduce additional exposure to non-compliance violations.
- **Medium:** This vulnerability could have a serious impact on the business, with minor losses to reputation and profit. It may also entail smaller amounts of exposure and violations to non-compliance and privacy respectively.
- **Low:** This vulnerability could have a limited effect on the business with smaller losses to profit and reputation being a result. There could also be privacy violations for small groups of employees or customers.

## Annex C: Threat matrix

The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. Its quantitative model ensures repeatable accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability impact scores. Two common uses of CVSS (v2.0 and v3.0) are prioritization of vulnerability remediation activities and in calculating the severity of vulnerabilities discovered on one's systems. Foresight provides CVSS v3.0 'base scores' which represent the innate characteristics of each vulnerability. We do not currently provide 'temporal scores' (metrics that change over time due to events external to the vulnerability) or 'environmental scores' (scores customized to reflect the impact of the vulnerability on your organization). However, Foresight does provide a [CVSS score calculator](#) to allow you to add temporal and environmental score data.

CVSS v3.0 Ratings	
Severity	Base Score Range
Low	0.1 3.9
Medium	4.0 6.9
High	7.0 8.9
Critical	9.0 10.0

End of document.



# **ACT Education – Google (GSUITE-EDU-BS) System Security Plan**

Version 1.0  
13/04/2022

Approved by the Executive Branch Manager  
(Chief Information Officer) DSST Education Directorate

## Contents

<b>1</b>	<b>EXECUTIVE SUMMARY.....</b>	<b>3</b>
<b>2</b>	<b>Introduction.....</b>	<b>4</b>
<b>3</b>	<b>Security Categorisation.....</b>	<b>5</b>
<b>4</b>	<b>Risk Assessment.....</b>	<b>8</b>
<b>5</b>	<b>System Governance.....</b>	<b>11</b>
<b>6</b>	<b>Authentication.....</b>	<b>14</b>
<b>7</b>	<b>Architecture.....</b>	<b>16</b>
<b>7</b>	<b>Personnel Security, Awareness and Training.....</b>	<b>25</b>
<b>8</b>	<b>Identification and Authentication.....</b>	<b>28</b>
<b>9</b>	<b>Access Control.....</b>	<b>30</b>
<b>10</b>	<b>Auditing.....</b>	<b>34</b>
<b>11</b>	<b>Incident Response.....</b>	<b>39</b>
<b>12</b>	<b>Physical, Environment and Media Protection.....</b>	<b>41</b>
<b>13</b>	<b>Contingency Planning.....</b>	<b>45</b>
<b>14</b>	<b>Configuration Management and Maintenance.....</b>	<b>47</b>
<b>15</b>	<b>Vulnerabilities.....</b>	<b>49</b>
<b>16</b>	<b>Essential Eight Compliance.....</b>	<b>54</b>
	<b>Appendix A: Risk Register.....</b>	<b>56</b>
	<b>Appendix B: Risk Treatment Strategy.....</b>	<b>67</b>
	<b>Appendix C: Initial Risk Table - Oct 2015.....</b>	<b>68</b>
	<b>Appendix D: Initial Risk treatment strategies for 2015 Risks.....</b>	<b>74</b>
	<b>Appendix E: Risk Methodology.....</b>	<b>80</b>
	<b>Appendix F: Approvals.....</b>	<b>82</b>



## 1 EXECUTIVE SUMMARY

As part of the Teach Anywhere Initiative in 2015, the Education Directorate enabled Software as a Service (SaaS) based Google Workspace Applications for Education (now known as Google Workspace). The [REDACTED] Google Workspace is the prime environment used for teaching and learning in ACT Government schools. No official information or official records are to be stored in Google Workspace for Education.

This System Security Plan (SSP) identifies and considers the risks to the Education Directorate associated with their use of Google G-Suite and infrastructure.

Google is committed in providing secure products and services that meet the required compliance and reporting needs. Google shares extensive information on best practices and provide easy access to Google's compliance documentation. Google Cloud's industry-leading security, third-party audits and certifications, documentation, and legal commitments help support the required compliance. Google products regularly undergo independent verification of their security, privacy, and compliance controls, achieving certifications, attestations of compliance, or audit reports against standards around the world. As a part of the independent verification process, third-party auditors examine Google's end-to-end security practices, including data centres, infrastructure, and operations, at a regular cadence. Google also created resource documents and mappings against frameworks and laws where formal certifications or attestations may not be required or applied. Google compliance resource centre contains details on Google's compliance documentation and resources.

This 2021 document represents an update to the original SRMP produced in 2015.

## 2 Introduction

### 2.1 Background

The System Security Plan (SSP – formerly called Security Risk Management Plan or SRMP) is a tool developed by DDTS (previously SSICT and is now called Digital Data Technology Solutions or DDTS) to assist Directorates to manage security risk for ICT systems. It is a mandatory requirement of the ACT Government ICT Security Policy for every ICT system including cloud services and systems hosted by outsourced service providers that has a criticality of **Government Critical** or **Business Critical**. The SSP is also recommended for a system that:

- Has a criticality of Government Critical or **Essential Infrastructure**
- Handles information classified with any “Sensitive” Distribution **Limiting Marker** (DLM); or
- Is a **public website** of the ACT Government.

The **System Owner** is responsible for the completion, approval and maintenance of the SSP, in accordance with their legal obligations to protect Territory information assets and to manage security risks as described in the ACT Protective Security Policy Framework.

Approval of the SSP constitutes a **commitment by the System Owner** to the recommended risk treatments and acceptance of the residual risk before using in production or transferring Territory data to the system. The System Owner cannot delegate the signing of this plan.

The SSP must be maintained by the System Owner. The SSP is a live document that must be updated every three years after approval and whenever major changes occur to the business, technology, or threat environment during the life of the system.

The Google infrastructure has a rating of “Business Critical” due to the fact that it is the central IT Learning Management System product for the support of Teaching & Learning in ACT Government Schools.

### 2.2 Purpose

The SSP is used by the business to:

- Describe the business, technology, and security context of the system.
- Define the existing security controls applied to the system.
- Identify the threats to the system.
- Measure “inherent” and “residual” security risks before and after mitigation; and
- Recommend risk treatments to bring Extreme or High risks within the Territory’s **Medium** tolerance for security risk.

The SSP also highlights legislation and policy that Education Directorate (ED) must comply with in its administration and use of GSUITE-EDU-BS.

### 2.3 Assistance

The sample responses in this document illustrate *how* to answer the questions; the sample answers are general and should be modified to suit each business system. It is the responsibility of the System Owner to ensure these responses are accurate.

For advice, contact ICT Security at [cyber.security@act.gov.au](mailto:cyber.security@act.gov.au) or (02) 6205 5196.

### 3 Security Categorisation

#### 3.1 System Information

<b>Directorate/Agency</b>	ACT Education	<b>Branch</b>	Digital Strategy, Services and Transformation
<b>Division</b>	Service Delivery and Design	<b>Business Unit</b>	Business Systems
<b>System Name (as it will appear in CMDB)</b>	GSUITE-EDU-BS	<b>Product Name (given by vendor)</b>	Google Workspace for Education (Formerly known as Google Apps for Education and later G Suite for Education and Google Workspace for Education Plus)
<b>Other names known by</b>	Google, Google Apps for Education, G-Suite, Google Workspace for Education, Google Workspace for Education Plus		
<b>Brief description of the solution</b>	<p>Google Workspace for Education is a set of Google tools and services that are tailored for schools and home schools to collaborate, streamline instruction, and keep learning safe. It is a suite of cloud computing, productivity and collaboration tools, software and products developed by Google. It is the primary ICT Platform for Teaching and Learning activities within the Directorate and is used by both staff and students.</p> <p>The core services are within Google Workspace are Gmail (including Inbox by Gmail), Calendar, Classroom, Jamboard, Contacts, Drive, Docs, Forms, Groups, Sheets, Sites, Slides, Talk/Meet and Vault. These services are provided under the G Suite agreement.</p> <p>Schools can use Google Workspace core services in compliance with COPPA and FERPA. G Suite core services contain no advertising and do not use information in those services for advertising purposes.</p> <p>Please note that there are additional services outside of the Google Workspace core services that Google Workspace users can access. These services are not governed by the Student Privacy Pledge or the G Suite agreement, so we may use information in these services in ways Google would not for Google Workspace core services. For example, additional services may serve ads, and Google may use information in these additional services to improve them.</p> <p>For Google Workspace users in primary/secondary (K-12) schools, Google does not use any user personal information (or any information associated with a Google Account) to target ads.</p> <p>Google contains student assessment data, stored within Google Classroom.</p> <p>Google contains student and teacher generated content in the form of email, chat history, documents and slides which has been generated for teaching and learning purposes.</p> <p>The primary source of the student information containing personal information for Student and Staff including First Name, Last Name, School and Year into Google Workspace comes from the School Administration System (Sentral). Sentral maintains a record of the Teacher, Class, Students and this information is transferred (by API) to Google on a regular basis (daily/when Sentral info changes) to create Google Classrooms. The Google Directory services syncs with Azure Active Directory services enabling the user access and legitimate users can be invited into the environment.</p> <p>Google Workspace may contain student or staff profile photos, where uploaded by an individual user to customise their profile.</p> <p>Google Workspace may contain sensitive personal information for students such as belief systems and /or cultural heritage captured within Google Docs or Slides as part of classwork.</p> <p>The implemented solution comprises of mixed matrix of Google Workspace for Education and Google Workspace for Education Plus version. There are about 5000 of Teachers &amp; School staff users using Education Plus version.</p>		



	<p>Google Workspace core services are guaranteed to be available at least 99.9% of the time. For more information, refer to the Google Workspace Service Level Agreement (<a href="https://workspace.google.com/intl/en/terms/sla.html">https://workspace.google.com/intl/en/terms/sla.html</a>)</p> <p>It is also worth noting that staff have been provided information to remind them that no Official ACT Government Records should be stored in Google Workspace for Education Plus. Official records can be stored in TRIM (paper files for school staff), SAS and other accredited systems.</p>									
<b>Current Status</b>	<input type="checkbox"/> Proposed <input type="checkbox"/> Development <input checked="" type="checkbox"/> Operational									
<b>System Type</b>	<table border="0"> <tr> <td><input checked="" type="checkbox"/> Business</td> <td rowspan="3" style="background-color: #cccccc; vertical-align: middle;"><b>Scope</b></td> <td><input type="checkbox"/> WhoG</td> </tr> <tr> <td><input type="checkbox"/> Technical</td> <td><input checked="" type="checkbox"/> Directorate-wide</td> </tr> <tr> <td></td> <td><input type="checkbox"/> Specific business unit:</td> </tr> </table>	<input checked="" type="checkbox"/> Business	<b>Scope</b>	<input type="checkbox"/> WhoG	<input type="checkbox"/> Technical	<input checked="" type="checkbox"/> Directorate-wide		<input type="checkbox"/> Specific business unit:		
<input checked="" type="checkbox"/> Business	<b>Scope</b>	<input type="checkbox"/> WhoG								
<input type="checkbox"/> Technical		<input checked="" type="checkbox"/> Directorate-wide								
		<input type="checkbox"/> Specific business unit:								
<b>Information Classification</b>	<p><input type="checkbox"/> The client has performed an Information Security Assessment (see <u>Attachment A</u>), and GSUITE-EDU-BS is classified:</p> <table border="0"> <tr> <td><input checked="" type="checkbox"/> Public (Unofficial)</td> <td><input type="checkbox"/> OFFICIAL</td> <td><input type="checkbox"/> CABINET</td> </tr> <tr> <td><input type="checkbox"/> OFFICIAL: Sensitive (was FOUO)</td> <td colspan="2"><input type="checkbox"/> OFFICIAL: Sensitive – Personal Privacy</td> </tr> <tr> <td><input type="checkbox"/> OFFICIAL: Sensitive – Legal Privilege</td> <td colspan="2"><input type="checkbox"/> OFFICIAL: Sensitive – Legislative Secrecy</td> </tr> </table>	<input checked="" type="checkbox"/> Public (Unofficial)	<input type="checkbox"/> OFFICIAL	<input type="checkbox"/> CABINET	<input type="checkbox"/> OFFICIAL: Sensitive (was FOUO)	<input type="checkbox"/> OFFICIAL: Sensitive – Personal Privacy		<input type="checkbox"/> OFFICIAL: Sensitive – Legal Privilege	<input type="checkbox"/> OFFICIAL: Sensitive – Legislative Secrecy	
<input checked="" type="checkbox"/> Public (Unofficial)	<input type="checkbox"/> OFFICIAL	<input type="checkbox"/> CABINET								
<input type="checkbox"/> OFFICIAL: Sensitive (was FOUO)	<input type="checkbox"/> OFFICIAL: Sensitive – Personal Privacy									
<input type="checkbox"/> OFFICIAL: Sensitive – Legal Privilege	<input type="checkbox"/> OFFICIAL: Sensitive – Legislative Secrecy									
<b>Criticality<sup>1</sup></b>	<table border="0"> <tr> <td><input type="checkbox"/> 1 = GOVERNMENT CRITICAL</td> <td><input type="checkbox"/> 3 = BUSINESS OPERATIONAL</td> </tr> <tr> <td><input checked="" type="checkbox"/> 2 = BUSINESS CRITICAL</td> <td><input type="checkbox"/> 4 = ADMINISTRATIVE</td> </tr> </table>	<input type="checkbox"/> 1 = GOVERNMENT CRITICAL	<input type="checkbox"/> 3 = BUSINESS OPERATIONAL	<input checked="" type="checkbox"/> 2 = BUSINESS CRITICAL	<input type="checkbox"/> 4 = ADMINISTRATIVE					
<input type="checkbox"/> 1 = GOVERNMENT CRITICAL	<input type="checkbox"/> 3 = BUSINESS OPERATIONAL									
<input checked="" type="checkbox"/> 2 = BUSINESS CRITICAL	<input type="checkbox"/> 4 = ADMINISTRATIVE									

## 3.2 Compliance Requirements

### 3.2.1 Legislation

<b>Applicable Legislation (select all that apply to this system and the information it handles)</b>	<input type="checkbox"/> Public Sector Management Act 1994 (ACT) <input type="checkbox"/> Territory Records Act 2002 <input checked="" type="checkbox"/> Information Privacy Act 2014 (ACT) <input type="checkbox"/> Health Records (Privacy and Access) Act 1997 <input checked="" type="checkbox"/> Children and Young People Act 2008 (ACT) <input checked="" type="checkbox"/> Freedom of Information Act 2016 (ACT) <input type="checkbox"/> Workplace Privacy Act 2011 (ACT) <input type="checkbox"/> Electronic Transactions Act 1999 (Cth) <input type="checkbox"/> Taxation Administration Act 1953 (Cth) <input type="checkbox"/> Spam Act 2003 (Cth)
---	--

<sup>1</sup> Summary of the [ICT System Criticality Standard](#):

Criticality	Impacts
<b>1=Government Critical</b>	Outage may have impacts including potential risk of loss of life and threat to public safety; damage to the government’s reputation and credibility; and/or potential impact to other critical services.
<b>2=Business Critical</b>	Long term outage may significantly reduce the ability to deliver efficient service to the external customers of the government, and/or significantly impact day to day government and Directorate-based functions and processes.
<b>3=Business Operations</b>	Non-Critical; reduced efficiency and increased cost of operations.
<b>4=Administrative</b>	Non-Critical; Reduced individual and team performance and productivity.

- Crimes Act 1901 (Cth)
- Other (specify):

### 3.2.2 Policy and Standards

**Applicable Policies (select all that apply to this system and the information it handles)**

- Protective Security Policy Framework (ACT)
- Acceptable Use of ICT Resources Policy
- ICT Security Policy
- ICT Security Incident Response Plan
- ICT System Criticality Standard
- Access Control Policy
- ACT Government Gateway Environment Policy
- Security Vetting Policy
- Encryption Policy
- Health Data Release Policy
- ICT Change and Release Management Policy
- Management of Privileged Accounts Policy
- Mobile Device Policy
- Monitoring and Logging Standard
- Password Policy
- Password Standard
- Remote Access Policy
- Smart Device Security Policy
- User Identity Standard
- Website Development and Management Standard
- Other (specify):

## 4 Risk Assessment

☑ A security risk assessment has been performed in accordance with the ACT Government Security Risk Management Standard (Appendix A) and are summarised here.

### 4.1 Risk summary

Without treatments, the inherent security risk of GSUITE-EDU-BS is **MEDIUM**. The risk appetite expressed by the ACT Government was that residual risks of up to **MEDIUM** could be acceptable.

The risk assessment found that the risks identified in the Risk Register (Appendix A) have a residual risk of **MEDIUM**, provided that the treatments (controls and planned controls) identified are put in place.

**Table 1: Risk summary -DSST Risks (with reference to non-availability of information and data)**

ID	Risk	Inherent risk	Advised strategy	Residual risk
R01		High	Updated Solution Architecture Diagram	Medium
R02		High	Recommend for a timely backup	Medium
R03		High	Recommended to integrate in SSO	Medium
R04		High	Recommended documentation of configuration controls – App wise and through testing prior to live in production	Medium

**Table 2: Risk summary -DDTS Risks**

DDTS provide specific infrastructure to support the operation of SAS systems – primarily ADFS for user login credentials and access levels authentication (see Figure 7 and 8) and network firewalls and connections.

ID	Risk	Inherent risk	Advised strategy	Residual risk
AR01		Medium	Accept	Medium
AR02		Medium	Accept	Medium
AR03		Medium	Accept	Medium
AR04		Medium	Accept	Medium
AR05		Medium	Accept	Medium
AR06		Low	Accept	Low
AR07		Medium	Accept	Medium
AR08		Medium	Accept	Medium
AR09		Medium	Accept	Medium
AR10		Medium	Accept	Medium
AR11		Medium	Accept	Medium

**Table 3: Risk summary -Google Risks**

Google Workspace is the main teaching and learning system in ACT Government Schools. It is hosted by Google in Australia and managed by Google Australia Pty Ltd. Google has links to other ACT Government systems including ADFS for login details (see Figure 2).

ID	Risk	Inherent risk	Advised strategy	Residual risk
GR01		Medium	Accept	Medium
GR02		Medium	Accept	Medium
GR03		Medium	Accept	Medium
GR04		Medium	Accept	Medium
GR05		Medium	Accept	Medium
GR06		Medium	Accept	Medium
GR07		Medium	Accept	Medium
GR08		Medium	Accept	Medium
GR09		Low	Accept	Low
GR10		Medium	Accept	Medium
GSR11		Medium	Accept	Medium
GR12		Medium	Accept	Medium
GR13		Medium	Accept	Medium
GR14		Medium	Accept	Medium
GR15		Medium	Accept	Medium
GR16		Medium	Accept	Medium
GR17		Medium	Accept	Medium

## 4.2 Next steps

### 4.2.1 Risk treatments

There are no further Risk Treatment advised in Section Appendix B: Risks will still be monitored at least twice a year by the Cyber Security & Risk Forum (CSRF) to ensure that no risk has moved or changed in any way.

### 4.2.2 Reaccreditation

The risks identified in this SSP will be reviewed at least every three years or whenever a significant change in the business, applications, data and technology architecture or security environment of GSUITE-EDU-BS occurs.

The risks identified in this SSP will be actively monitored for progress on the Treatments through the Education Directorate Cyber Security Risk Forum (CSRF) and the Education Directorate Change Advisory Board.

### 4.2.3 Compliance Auditing

This assessment will proceed to an internally directed compliance audit for independent auditing of the implemented controls that underpin the risk treatments.

Compliance Audits related to Risks and Treatments identified in this SSP will be undertaken on an as-needs basis (possibly 6 months or a year after implementation) to ensure the control is still functioning as expected.

## 5 System Governance

School Administration System has been registered in the WhoG CMDB provided by DDTS, and the information below is accurate for the CMDB **Owner**, **Assigned To** and **Contact** fields.

### 5.1 System Owner

<b>Name</b>	Kelly Bartlett
<b>Title</b>	Executive Branch Manager DSST/CIO
<b>Contact details</b>	Phone: 02 620 75663 <a href="mailto:Kelly.bartlett@act.gov.au">Kelly.bartlett@act.gov.au</a>

For any Critical system, the System Owner must be a person at the Executive level within the directorate with the authority to:

<input checked="" type="checkbox"/>	Accept security risks associated with the system on behalf of the Director General.
<input checked="" type="checkbox"/>	Make binding financial and operational decisions to treat security risk of the system.
<input checked="" type="checkbox"/>	Change business system criticality and approve Business Continuity (BC) processes.
<input checked="" type="checkbox"/>	Approve any data transfers from GSUITE-EDU-BS to other ICT systems or cloud services ("Data Custodian").

### 5.2 System Manager

<b>Name</b>	Mark Sanderson
<b>Title</b>	Senior Director, Education ICT, DDTS
<b>Contact details</b>	Phone: 02 620 75191 Email: <a href="mailto:Mark.Sanderson@act.gov.au">Mark.Sanderson@act.gov.au</a>

The System Manager is a Senior Officer who is responsible for the integrity and operation of the system (data security, development, and testing):

<input checked="" type="checkbox"/>	Change owner for associated changes and/or new features.
<input checked="" type="checkbox"/>	Authorizes access levels, periodically reviews access levels.
<input checked="" type="checkbox"/>	May run the audit log analysis and approves analysis results.

### 5.3 Senior System Administrators

<b>Name</b>	Michael Bayliss
<b>Title</b>	Assistant Director - Education Business Applications, DDTS
<b>Contact details</b>	Phone: 02 620 59451 Email: <a href="mailto:michael.bayliss@act.gov.au">michael.bayliss@act.gov.au</a>
<b>Name</b>	Tresize Dominic
<b>Title</b>	Assistant Director - Education Business Applications, DDTS
<b>Contact details</b>	Phone: 02 6205 0917 Email: <a href="mailto:Dominic.Tresize@act.gov.au">Dominic.Tresize@act.gov.au</a>

The Directorate officer who carries out the day-to-day operational management tasks:

<input checked="" type="checkbox"/>	Sets up user accounts.
-------------------------------------	------------------------

<input type="checkbox"/>	Changes access levels.
<input type="checkbox"/>	May reset passwords (if applicable).
<input checked="" type="checkbox"/>	Runs the audit log analysis.

### 5.4 Exceptions

<input type="checkbox"/>	There are no exceptions to the responsibilities above.
<input checked="" type="checkbox"/>	<p>Document any exceptions to these responsibilities or other governance responsibilities here:</p> <p><b>DDTS Account System Administrators</b></p> <p>DDTS has a number of system administrators (A Accounts) whose role is to manage access for staff in the ACTGOV and Schools Net environments. Their responsibilities are as follows:</p> <ul style="list-style-type: none"> <li>Provisioning of user accounts &amp; profiles (in AD FS). (Staff uses the Exchange email / Students Gmail separately)</li> <li>May reset passwords (if applicable) – Is done through the Single Sign-On (SSO).</li> </ul> <p><b>Google Service Partner</b></p> <p>DDTS and Education have occasionally employed a Google Service Partner to provide expert support in areas such as configuration settings or reporting. The Google Expert Partner is Certified by Google to be able to supply services. Staff of the Google Expert Partner are also qualified and must fill in the “Acceptable Use Policy” documents prior to being allocated a login.</p>

### 5.5 Shared Responsibilities

The following table shows the responsibilities of various organisations with regard to aspects of the implementation of Google Workspace on the Schools network.

Responsibility	Business Unit	DDTS	Service Partner (Google)	Google Expert Partner
Endpoint Devices	✓	✓		✓
Information Security	✓	✓	✓	✓
Data Governance	✓	✓	✓	✓
Access Control	✓	✓		✓
Authentication		✓		✓
Application (Google Workspace for Education)	✓	✓	✓	✓
Network Controls		✓	✓	
Operating System		✓	✓	
Physical Hosts			✓	
Physical Network		✓		
Datacentre Facility			✓	

Table 4 - Google Shared Responsibility Model:

Google Workspace for Education deployed solution is a Software-as-a-Service (SaaS), a software licensing model in which legitimate users access to the software is provided on a subscription basis, with the software located on

Google environment cloud rather than on servers located in-house. This allows each user to access programs via the Internet, instead of having to install the software on the user's computer.

Google Workspace for Education Fundamentals (around 50,000 Student users) includes Gmail, Calendar, Meet, Docs, Sheets, Slides, Forms, Classroom, Assignments, Sites, Groups, Drive, and the Administrator Dashboard. Google Classroom is a collaboration tool for teachers and students that helps organize and streamline the classroom experience.

Google Workspace for Education Plus includes all the features in Education Standard and Teaching and Learning Upgrade with additional features for certain services, such as attendance tracking in Google Meet.

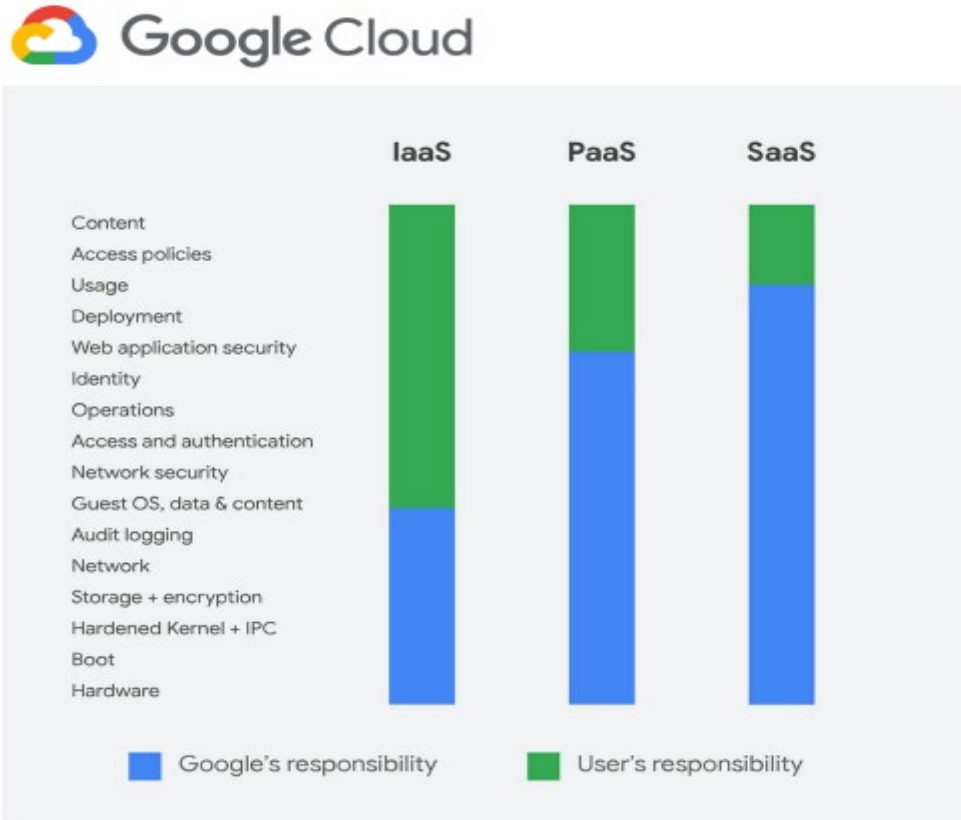


Figure 1 - 3<sup>rd</sup> Party apps that leverage the Google functionality.

Google provides pre-integrated single sign-on (SSO) for many cloud applications. The SSO feature includes OpenID Connect (OIDC) identity provider support and support for Security Assertion Markup Language (SAML) 2.0. The configuration of the users' enterprise cloud applications to use SAML 2.0, they will be able to use their Google Workspace credentials to sign into enterprise cloud applications from a single login.

Google allows the sharing of data safely with third-party apps & services, for more information please refer to - (<https://support.google.com/accounts/answer/10130420#>)



## 6 Authentication

Authentication uses single sign-on (SSO) integration via ADFS using federation to Azure AD. Active Directory and AD FS administration, configuration and support is provided by DDTs Identity Management Services team. They are responsible for ensuring the secure login environment as shown in Figure 2 and Figure 3.

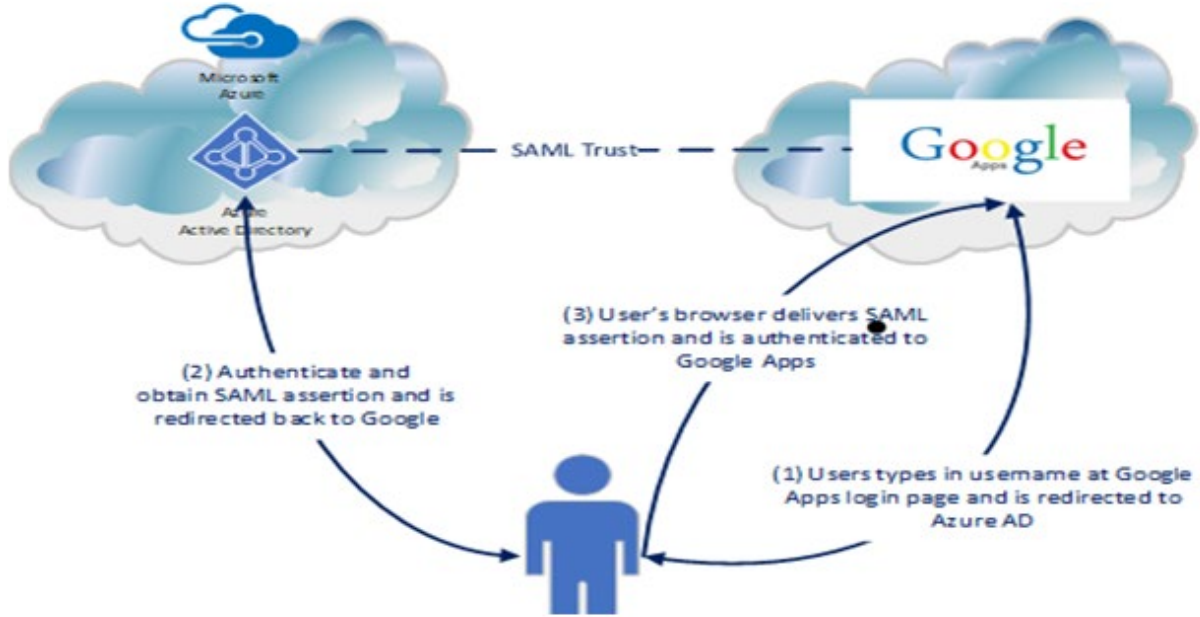


Figure 2 – Secure Login Environment for a Google Workspace user

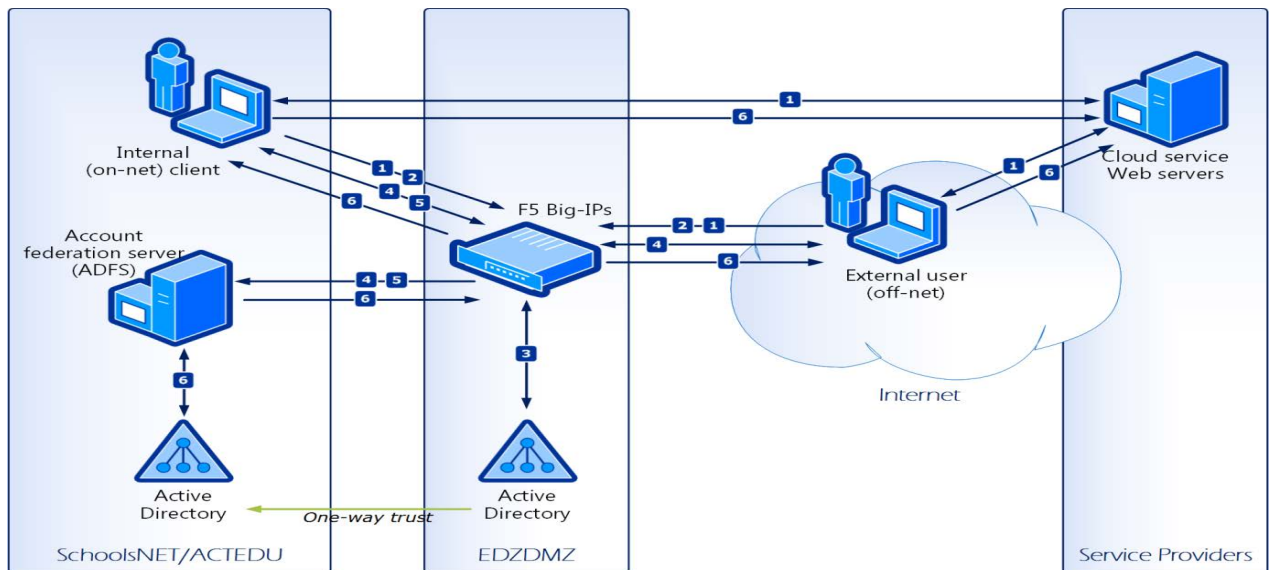


Figure 3 – Physical technology environment for login to Google Workspace (Note: the Cloud Service Provider is Google).

Network configuration and support is performed by DDTs ICT Networks Team. The high-level diagram of the DDTs network configuration is contained in Figure 4.



Figure 4 – High Level [redacted] DDTS network configuration.

## 7 Architecture

☒ A solution design has been prepared for the Google environment that complies with the ACT Government Technical Reference Manual. This document was prepared in 2015 for the original implementation of the Google learning environment.

### 7.1 Solution Design

#### Current Implemented Solution Design

☒	The design documentation describes what interfaces and data flows exist within the system and to other systems (including external systems/cloud services). – Per interface design documentation outside of this scope.
☒	The managed services contract stipulates that ACT Government data and security measures are met.

#### 7.1.1 High level solution overview

Figure 5 identifies the major infrastructure components in the Sentral Azure component managed by Sentral (for Sentral software) and their relationships. Google relies on information provided from Sentral (Class, teacher and students in class details). Figure 5 shows the data flows at a high level between Google and other related systems.



**Figure 5 – High Level Google Solution Design**

## 6.2 Network protection of domains

<input type="checkbox"/>	The system is hosted on-premises in the ACTGOV domain, with no Internet-facing application server.
<input type="checkbox"/>	The system is hosted on-premises in the ACTGOV domain, with external-facing application server(s) in a DMZ ("demilitarised zone").
<input type="checkbox"/>	The system is hosted in DDTS Azure or AWS. Communications between the DDTS Managed Infrastructure-as-a-Service (IaaS) environments of Azure and AWS Cloud over the Internet to on-premises environments is encrypted through an encrypted channel (site-to-site VPN) and no traffic transits an insecure public network "in the clear". Access to Azure and AWS Platform as a Service (PaaS) capabilities are delivered over Transport Layer Security (TLS), except where not supported (exceptions must be described in the Solution Design).
<input type="checkbox"/>	The system is hosted on-premises as a "black box" solution in a private virtual network (VLAN).
<input type="checkbox"/>	The system is hosted externally as a Software-as-a-Service (SaaS) solution by a cloud service provider.
<input checked="" type="checkbox"/>	

## 6.3 System and Domain Interfaces

If two systems or environments are connected for information exchange, then a malicious user could exploit the connection to gain access between the systems and cause harm.

APIs (standing interfaces) between systems are managed using the Mulesoft API Gateway hosted by DDTS.

Batch files are transferred between systems using the Apollo SFTP server hosted by DDTS.

The way in which the system is protected from unauthorised access from other connected systems and networks is shown below.

System / group	Type <sup>2</sup>	Direction <sup>3</sup>	Protection from unauthorised access (ports and protocols)
AD FS	Secure API	In	TLS for encryption
Sentral	HTTPS	Out	TLS for encryption
O365	SAML2/HTTPS	In/Out	TLS for encryption
Google Console	AES	In/Out	Advanced Encryption Standard (AES) for encryption at rest and transit

<sup>2</sup> For example, SFTP, Secure API, HTTPS.

<sup>3</sup> "In" is from the system/group **into** GSUITE-EDU-BS  
 "Out" is from GSUITE-EDU-BS **out to** the system/group

System / group	Type <sup>2</sup>	Direction <sup>3</sup>	Protection from unauthorised access (ports and protocols)
Google supported 3 <sup>rd</sup> Party apps/extensions (Like-Screencastify, Pear Deck etc)	ALTS	In/Out	Protocol Buffer to serialize its certificates and protocol messages.

### 6.3.1 Google interfaces with Edge systems – Sentral

Figure 4 provides the overview of the components that will support the various integrations, including the interactions between these components and levels of responsibility.



Figure 6 provides a conceptual overview of how Google ingests Sentral data and integration.

### 6.3.2 Google Interfaces with Microsoft Azure AD (managed by DDTS)

Figure 7 shows the ADFS Authentication Process for DDTS to provide ADFS information to Google (in the cloud)



Figure 7 – Interface with Microsoft Azure from ACT Government services to the Google cloud



Figure 8 shows the Microsoft Azure ADSync Process from ACT Government servers through to the cloud systems (Sentral)

### 6.3.6 Table - list of attachments containing details of Google Interface integrations

Attachment A	Detailed Design - ED - CLOUDAZURE-EDU v0.5
Attachment B	Interface with Microsoft Azure from ACT Government services to the cloud

Attachment C	Data transactions within Sentral,
Attachment D	SAS Interface integrations with Edge Systems
Attachment E	Google Infrastructure Security Design Overview
Attachment F	School report – ST4S 2020.2 – Google for Education – Google Australia Pty Ltd – Tier 1 v1.0

## 6.4 Data Governance and Trust

Describe the tolerance for data sharing from GSUITE-EDU-BS:

<input type="checkbox"/>	Data in this system is considered Closed.
<input type="checkbox"/>	Data in this system may be shared on a restricted basis to internal users outside the business unit.
<input checked="" type="checkbox"/>	Data in this system may be shared with trusted external users (Parents). This is at the discretion of the Google user (Teacher or student) who can share any document to a known email address
<input checked="" type="checkbox"/>	Data in this system may be shared publicly. This is at the discretion of the Google user (Teacher or student) who can share any document to a known email address within the trusted domains.
<input type="checkbox"/>	Data in this system has been released publicly.

Describe how data handled by GSUITE-EDU-BS is governed:

<input type="checkbox"/>	Data is governed based on a Whole-of Government Data Governance Framework.
<input type="checkbox"/>	Data is governed using a documented EDU data governance framework.
<input checked="" type="checkbox"/>	Data is governed in a bespoke manner for this system (describe): <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Data stewardship has been assigned to appropriate personnel.</li> <li><input type="checkbox"/> Data stewards have been trained in their responsibilities.</li> <li><input checked="" type="checkbox"/> The sources and volume of data handled by GSUITE-EDU-BS is documented.</li> <li><input type="checkbox"/> Official information is handled according to the ACT Records Management Standards.</li> <li><input checked="" type="checkbox"/> Data can be identified, held recalled for legal purposes.</li> <li><input type="checkbox"/> Data is classified according to sensitivity and other categories (describe): None</li> <li><input type="checkbox"/> Transient data is appropriately archived and disposed of when no longer needed.</li> <li><input checked="" type="checkbox"/> Data requests are approved prior to release, and approvals are recorded and audited appropriately.</li> <li><input checked="" type="checkbox"/> Data that is newly ingested by GSUITE-EDU-BS is governed appropriately.</li> </ul>

## 6.5 Data Protection

Describe if and how sensitive information is protected. This is performed by encrypting data at rest (when stored in database) and in transit (when communicated from or to the system). Encryption methods must comply with the ASD Approved Cryptographic Algorithms (AACAs) and Protocols (AACPs), defined in the ACT Government Encryption Standard.

Extra information is contained in Section 6.3.

### 6.5.1 Protection in Transit

<input checked="" type="checkbox"/>	Data is communicated to/from the sub-systems with the following measures to encrypt data in transit -please also refer to Figure 1 for data flows:
-------------------------------------	--

	<ol style="list-style-type: none"> <li>1. Google to /from ADFS; uses TLS. The user’s data is also encrypted at rest when it is stored on Google servers, and encrypted when Google transfer, it between data centres for backup and replication.</li> <li>2. Google to/from Sentral: Data is encrypted using TLS This protection is achieved by encrypting the data before transmission; authenticating the endpoints; and decrypting and verifying the data on arrival. For example, Transport Layer Security (TLS versions 1.0, 1.1, 1.2, and 1.3) is often used to encrypt data in transit for transport security and Secure. See <a href="https://cloud.google.com/security/encryption-in-transit">https://cloud.google.com/security/encryption-in-transit</a></li> </ol>
--	---

### 6.5.2 Protection at Rest

<input type="checkbox"/>	Data in the system is stored in an unencrypted format.
<input type="checkbox"/>	Data stored in the system is protected using cryptographic algorithms recommended by the ACT Government Encryption Standard. Obsolete algorithms are not used.
<input checked="" type="checkbox"/>	<ol style="list-style-type: none"> <li>1. Standard offering in Education Directorate Azure utilises encryption at rest used for Sentral.</li> <li>2. Google protects the user’s data from a system compromise or data exfiltration by encrypting data while stored. The Advanced Encryption Standard (AES) is used to encrypt data at rest. All information temporarily passing on the Microsoft Azure platform uses bank-level SSL technology for secure data transmission. All communications and data flows over the internet use Secure Socket Layer (SSL) thus ensuring that data is encrypted in the process. Independent vulnerability tests are carried out on the full cycle to ensure the application's security levels are of the highest standard.</li> </ol> <p>Layers of encryption at rest</p> <p>The diagram illustrates the layers of encryption at rest, from top to bottom:</p> <ul style="list-style-type: none"> <li><b>Application:</b> Represented by a red bar with a lock icon.</li> <li><b>Platform:</b> Represented by a green bar with a lock icon.</li> <li><b>Infrastructure:</b> Represented by a yellow bar with a lock icon. Description: <b>Distributed file system:</b> data chunks in storage systems protected by AES256 encryption with integrity.</li> <li><b>Block storage:</b> Represented by a yellow bar with a lock icon.</li> <li><b>Hardware:</b> Represented by a blue bar with a lock icon. Description: <b>Storage devices:</b> protected by AES256 or AES128 encryption.</li> </ul>

### 6.6 Capacity and Performance Strategy

A Capacity and Performance Plan for Google has been developed for the system managed by Service Provider through a contract (with Google Pty Ltd).

Google's infrastructure provides a variety of storage services, such as Bigtable and Spanner, and a central key management service. Most applications at Google access physical storage indirectly via these storage services.

The GFE is an HTTP/TCP reverse proxy which is used to serve requests to many Google properties including: Search, Ads, G Suite (Gmail, Chat, Meet, Docs, Drive, etc.), Cloud External HTTP(S) Load Balancing, Proxy/SSL Load Balancing, and many Cloud APIs.

Google visualizes their infrastructure as a three-layer stack:

- Products: search, advertising, email, maps, video, chat, blogger.
- Distributed Systems Infrastructure: GFS, MapReduce, and Bigtable.
- Computing Platforms: a bunch of machines in a bunch of different data centres.

There are two basic types of scalabilities Google cloud computing offers are: vertical and horizontal scaling.

Vertical scaling, also known as “scaling up” or “scaling down,” enables to add or subtract power to an existing cloud server upgrading memory (RAM), storage or processing power (CPU). Usually this means that the scaling



has an upper limit based on the capacity of the server or machine being scaled; scaling beyond that often requires downtime.

- To scale Horizontally (scaling in or out), enables to add more resources like servers to the system to spread out the workload across machines, which in turn increases performance and storage capacity. Horizontal scaling is especially important for businesses with high availability services requiring minimal downtime.
- With the changing business requirements or surging demand, the trigger changes to enable scale their SaaS based solution offerings. But how much storage, memory and processing power are needed - To determine a right-sized solution, ongoing performance testing is essential. IT administrators must continually measure factors such as response time, number of requests, CPU load and memory usage. Scalability testing also enables to measures an application’s performance and ability to scale up or down depending on user requests.

Automation has helped to optimize cloud scalability. Helps to determine thresholds for usage that trigger automatic scaling so that there’s no effect on performance.

### 6.7 Business Architecture

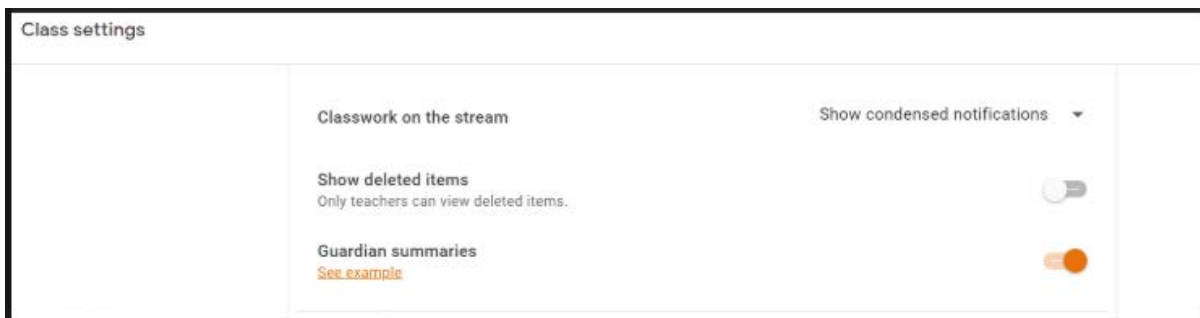
Service	Description	Users
Assignments	It is an application for learning management system (LMS). It helps educators save time grading and guides students to turn in their best work with originality reports.	Students, Staff
Calendar	Spend less time planning and more time doing with shareable calendars that integrate seamlessly with Gmail, Drive, Contacts, Sites and Meet so you always know what's next.	Students, Staff
Classroom	Easy tool helping educators efficiently manage and assess progress, while enhancing connections with learners from school, from home, or on the go.	Students, Staff
Cloud Search	The power of Google to search across the company’s content. From Gmail and Drive to Docs, Sheets, Slides, Calendar, and more, Google Cloud Search answers the questions and delivers relevant suggestions to help the user throughout the day.	Students, Staff
Drive and Docs	Store any and every file. Access files anytime, anywhere from the desktop and mobile devices and also control how files are shared.  Create and edit text documents right in the browser—no dedicated software required. Multiple people can work at the same time, and every change is saved automatically.  In all editions, the school gets 100 TB of pooled storage. For Education Plus and Teaching and Learning Upgrade, the school(s) get additional storage based on the number of licenses that you purchase.  Note: Schools with more than 20,000 students, faculty, and staff can request additional storage.	Students, Staff, External
Gmail	The latest Gmail makes it easier to stay on top of the work that matters. With secure, ad-free email as a foundation, facilitates to chat, make voice or video calls, and stay on top	Students

	of project work with shared files and tasks — all right in Gmail.	
Google Chat and classic Hangouts (Belconnen High School)	From direct messages to group conversations, Google Chat helps teams and businesses collaborate fluidly and efficiently from anywhere. Securely connect with anyone at work and take group work to the next level with shared chat, files and tasks.	Students, Staff
Google Chrome Sync	Range of simple yet powerful devices with built-in accessibility and security features to deepen classroom connections and keep user information safe.	Students, Staff
Google Meet	Meet is a secure, reliable video conferencing solution that helps connect, build, and foster school communities. Host classes, parent-teacher conferences, schoolwide assemblies, and more.	Students, Staff
Google Vault	Keeps track of what matters. Retain, search, and export the organization's data from select apps with Vault for Google Workspace Business and Enterprise editions.	Students, Staff
Groups for Business	Groups for Business is a core service in your Google Admin console that controls how your organization's groups can be used at the Google Groups user app	Students, Staff, External
Jamboard Service	Spark students to learn, collaborate, and engage in active new ways with the Jamboard mobile app or 55-inch cloud-powered whiteboard.	Students, Staff
Keep	Keep organized. Capture inspiration and to-dos effortlessly. Collaborate on notes with teammates and set reminders to stay on track. Everything syncs across your devices, so what's important is always in reach.	Students, Staff
Sites	Collaboratively create engaging, high-quality sites for the team, project or event. The sites look great on every screen, from desktop to smartphone. All without learning design or programming.	Students, Staff
Tasks	Keep track of the user daily tasks, organize multiple lists, and track important deadlines with Google Tasks. Tasks synchronizes across all the user devices, so the user lists and tasks go with the user, wherever they are.	Students, Staff
Google Cloud Console	Is a web-based, graphical user interface that you can use to manage your Google Cloud projects and resources. Enables the users either create a new project or choose an existing project, and then use the resources that are created in the context of that project.	Privileged Users

### 6.7.1 Customer interface (External users)

A teacher or school administrator can invite a guardian to receive email summaries about their student's work in class. To get summaries, the student must use Classroom with a Google Workspace account (looks like  ). Email summaries do not include marks.

For more information, please refer - <https://support.google.com/edu/classroom/answer/6386354?>



## 6.7.2 User interface (ACT staff & Students)

Google is a SaaS based solution accessible from any internet capable device (managed or unmanaged) running a supported browser. Staff and Students will typically access individual Google service via links within the Education Backpack page <https://backpack.ed.act.edu.au/>. Users are however able to access Google services directly if they know the URL i.e., drive.google.com, classroom.google.com, mail.google.com.

Staff and students can access the complete services offered by Google through the icons available in the Digital Backpack or through apps installed in their Chromebook. Any of the users has the privileges of accessing the backpack port using a link can access using browser-based device externally.

## 6.7.3 Administration interface

Technical administrative privileges over the [redacted] Google environment are approved by EBM-DSST and managed by DDTS. These privileged users have access to the Google Console.

The Administrative interface for Google is <https://admin.google.com/?hl=en-GB>. It accessible from any internet capable device (managed or unmanaged) running a supported browser.

## 6.7.4 Reporting and auditing

Audit and reporting is managed by DDTS Administration staff on behalf of EDU.

If an incident occurs, or a request from EDU is received, DDTS provides the information.

Google Workspace audit logs in Google Cloud. access the following types of Google Workspace, Cloud Identity, and Drive Enterprise audit logs in Google Cloud:

- Google Workspace Admin audit - Admin audit logs provide a record of actions performed in Google Workspace Admin Console. For example, you can see when an administrator added a user or turned on a Google Workspace service. For more information about Google Workspace Admin audit logs, see the Admin Activity Report Event Names page.
- Google Workspace Login audit - Login audit logs track user sign-ins to your domain. The login logs only record the login event. They do not record which system was used to perform the login action.
- Google Workspace Enterprise Groups audit - Enterprise Groups audit logs provide a record of actions performed on groups and group memberships. For example, you can see when an administrator added a user or when a group owner deleted their group.

(For more details on Google Workspace audit logs, please refer to - <https://cloud.google.com/logging/docs/audit/configure-gsuite-audit-logs>).

## 7 Personnel Security, Awareness and Training

	Number	Security Clearance Required	Description
External Users/Customers <sup>4</sup>	0	None	Based on audit logs from CASB
Internal Users <sup>5</sup> (Staff)	7500	Police check as per ACTPS on-boarding	All ACT public school teachers
Internal Users (Students)	50,000	None	Students accounts created via enrolment in Sentral
Internal Administrators <sup>6</sup>	5-10	CMTEDD Baseline clearance or equivalent	Senior System Administrator DDTS TSD system administrators Software and Licensing administrators
External Administrators (Google)	Unknown	Education, employment, reference checks. Police Check	System Administrators Help Desk
Google Expert Partner (currently: Geeks on Tap)	01	Police Check	Reporting, System Administration and operational assistance.

---

<sup>4</sup> People who receive data from the system but have no access to it, such as:

- Participating pathology labs (without direct access to the Register)
- Medical Practitioners (without direct access to the Register, and on authorisation from the women clients)
- Federal government entities, accreditation bodies and research project as approved by the Chief Health officer (de-identified data only).

<sup>5</sup> Such as "ACT Government Health Directorate Officers employed within the XXXXXX Section".

<sup>6</sup> Including people designated as deputy or reserve System Administrator.

## 7.1 Service Providers

List the vendors, consultancies and support providers involved with this system below:

Organisation	Contact Details	Role
DDTS	Telephone: 02 6207 9000 Email: <a href="mailto:ServiceDesk@act.gov.au">ServiceDesk@act.gov.au</a>	Provide basic troubleshooting for issues with installation and performance.
Education ICT, DDTS	<b>Michael Bayliss</b> A/g Education Business Applications Telephone: 02 620 59541 Email: <a href="mailto:Michael.Bayliss@act.gov.au">Michael.Bayliss@act.gov.au</a>	L1/L2 Support provider for the application
Google for Education	[Redacted]	Vendor Technical Account Manager
Internal Service Support (DSST)	<b>Shakir Tiruchi</b> Assistant Director, Senior Technical Officer Telephone: 02 620 54209 Email: <a href="mailto:shakir.tiruchi@act.gov.au">shakir.tiruchi@act.gov.au</a>	L1/L2 Support provider for the application
Google Support	Via Admin Portal	Vendor/developer
Google Expert Partner: currently Geeks on Tap	[Redacted]	License Reseller

## 7.2 Training and Education

### 7.2.1 Security Awareness

The following processes are followed to make users aware of their security responsibilities:

<input checked="" type="checkbox"/>	Staff including contractors are required to read and agree to the “ACT Government Acceptable use of ICT Resources Policy” upon engagement, and supervisors scan and email the signed agreements to the directorate Agency Security Advisor.
<input checked="" type="checkbox"/>	The Induction process for new starters to the directorate covers general security responsibilities for people working with the system.
<input checked="" type="checkbox"/>	The Induction process for new starters to the Section identifies each of the applications that the Section uses. The presentation also states the Information Classification of data in the system.
<input type="checkbox"/>	At the monthly Section staff meeting, there is a standing Agenda item “Staff Changes”, and for anyone starting or anyone changing position, the Chairman explicitly confirms what access rights that person has.
<input checked="" type="checkbox"/>	The System Owner enforces a rule that every person leaving their workstation must first lock their computer screen.
<input checked="" type="checkbox"/>	Other (describe): Existing staff have been requested to undertake the online induction training where the security responsibilities of staff are included (this will occur regularly)

### 7.2.2 System Administrators

<input checked="" type="checkbox"/>	System administrators have received formal training from the vendor or from a specialist training company.
<input checked="" type="checkbox"/>	There is adequate technical and system administration documentation.
<input type="checkbox"/>	Other (describe):

### 7.2.3 Internal Users (ACTPS, teachers, students)

<input checked="" type="checkbox"/>	Users have received formal training from the vendor or from a specialist training company.
<input checked="" type="checkbox"/>	There is adequate user documentation.
<input checked="" type="checkbox"/>	Responsibility for keeping business procedure/training material up to date is assigned to (describe): DSST Business Systems Team
<input type="checkbox"/>	Other (describe):

### 7.2.4 External User – Google Expert Partner (Geeks on Tap)

<input checked="" type="checkbox"/>	External users shall be provided with information regarding security and privacy.
<input type="checkbox"/>	There is adequate external user documentation.
<input checked="" type="checkbox"/>	Other (describe): One login with reporting administrator credentials exists to facilitate requested reports.

## 8 Identification and Authentication

### 8.1 Identifying External (Geeks on Tap) Users

<input type="checkbox"/>	External users are identified by evidence supporting the link to their real-life identity by validating matching details, e.g., date of birth, home address, unique government identifier.
<input type="checkbox"/>	External users are identified by evidence supporting the link to their real-life identity by sighting digitally transmitted documents, e.g., birth certificate, drivers’ licence, passport.
<input type="checkbox"/>	Physical presence of applicants is required for identity proofing at time of enrolment.
<input checked="" type="checkbox"/>	Other (describe): <ol style="list-style-type: none"> <li>Only one user account is provided with access on demand to cater to the requirement of any customized reporting or assistance.</li> </ol>

### 8.2 Identifying Internal (ACT staff) Users

<input type="checkbox"/>	Applicants self-assert their identity at time of enrolment with no evidence to link the applicant to their real-life identity is required.
<input checked="" type="checkbox"/>	Applicants are identified by other strong credentials, e.g., a pre-existing ACT Government Active Directory account, prior to enrolment.
<input checked="" type="checkbox"/>	Applicants are identified by evidence supporting the link to their real-life identity by validating matching details, e.g., date of birth, home address, unique government identifier.
<input type="checkbox"/>	Applicants are identified by evidence supporting the link to their real-life identity by sighting digitally transmitted documents, e.g., birth certificate, drivers’ licence, passport.
<input type="checkbox"/>	Physical presence of applicants is required for identity proofing at time of enrolment.
<input checked="" type="checkbox"/>	Other (describe): <p>User accounts are managed via single sign-on (SSO) using SAML 2.0 integration between ACT Gov Active Directory (AD) and the Google Workspace environment.</p> <p>Internal Users will authenticate to the Google service using their Active Directory credentials. Multi-factor authentication has not been enabled for staff or student accounts nor have any IP restrictions been enforced.</p> <p>Internal Users will not have administrative privileges unless explicitly required by their role i.e DSST Support Staff, SSICT &amp; EDU ITO.</p> <p>Internal Users may have access to sensitive information other than their own -</p> <ol style="list-style-type: none"> <li>The data has explicitly been shared with them by the owner of that data</li> <li>The data has been copied or uploaded to a shared or personal Google Drive for which the user has been granted access</li> </ol> <p>Access to Google services is centrally managed by SSICT via policy configured within the Google Administration Console with different policies configured for Students and Teachers. See Appendix F for more detail</p>

### 8.3 Authentication Methods

<input type="checkbox"/>	No logical access control, users can access all data anonymously.
<input type="checkbox"/>	Authentication is provided locally (GSUITE-EDU-BS provides its own Usernames and Passwords). The system enforces password strength that complies with the ACT Government Password Policy <sup>7</sup>

---

<sup>7</sup> At time of writing, the system must comply with the ACT Government Password Standard V2.2:

<input type="checkbox"/>	Single sign-on (SSO) authentication is provided by LDAP.
<input checked="" type="checkbox"/>	SSO authentication is provided for internal staff by Active Directory and AD FS, administered, configured and supported by DDTS Identity Management Services.
<input type="checkbox"/>	Other ():

### 8.4 Multi-factor Authentication (MFA)

<p><b>Confirm whether the system supports Multi-Factor Authentication (MFA) for:</b></p> <p><b>Personal devices</b></p> <p><b>Remote access</b></p> <p><b>System administrators</b></p>	<p>Multi-factor authentication has not been enabled for staff or student accounts nor have any IP restrictions been enforced. _A (administrator accounts) cannot be used outside the network (DDTS Policy).</p>
---	---

- 
1. Minimum 10 characters for standard users, 12 characters for administrators.
  2. Must include at least one character from any *three* of the four-character sets: upper case, lower case, numeric, non-alphabetic
  3. Reset every 180 days (45 days for an application that has data classified as Protected); and
  4. Must not be able to reuse any of the last 10 passwords.

For the latest detailed requirements, refer to the [DDTS website](#).



## 9 Access Control

Access control for use and system administration of GSUITE-EDU-BS has been reviewed by the System Manager for compliance with the ICT Security Policy and Access Control Standard.

### 9.1 Authorisation

Describe how access to GSUITE-EDU-BS is authorised (approved), and how accounts are created, suspended, and removed, and how changes to access rights are made.

<b>Who decides what the appropriate access is for each person (internal users)?</b>	<p>Internal staff users are provided with an ACT Government login account (@ed.act.edu.au) on the school’s network managed by DDTS. Creation of the account is completed on verification of the staff members recruitment to the ACT Government Public Service. Users with (@ed.act.edu.au) access is established for Google through Single Sign-On on the DDTS ADFS system.</p> <p>Privileged users’ access (admin/” all school”/etc) are authorised by EBM-DSST (CIO).</p> <p>A review of staff access levels is conducted in each Term break by ACTEDU to ensure appropriate levels of controls protect enterprise assets, data integrity and aligned with the business overall goals. Staff access is monitored through provisioning of AD Accounts and Admin level access are monitored.</p>
<b>Does the System Administrator keep any record of these decisions?</b>	<p>The requests for application and technical level access are logged through DDTS service desk via ServiceNow tool for action as per the process.</p>
<b>Can anyone apart from the System Administrator change access levels within the application? (If so, how is that controlled?)</b>	<p>Application-level access are determined based on their AD Group policy and can be modified by the system administrator for the requests in the form of tickets logged via ServiceNow by migrating the user account(s) into the AD Group with appropriate level of access requested.</p>
<b>What is the process for someone getting temporarily increased access (to cover for someone on leave etc.)?</b>	<p>Temporary access is not allocated to Google</p>
<b>What is the process for ensuring that temporarily increased access is revoked later?</b>	<p>Temporary access is not allocated to Google.</p>
<b>What is the process for removing access for someone who has left the Section and no longer has a right to use the system? (Especially if he/she still works in the ACT Government)</b>	<p>Deprovisioning processes rely on a combination of DDTS end-date for the accounts to disable (through HR reports), requests initiated by the service provider (for technical access), and manual access reviews (for application-level access).</p> <p>Term Reviews are conducted to compare current user access with staff and enrolled students.</p>
<b>What is the process for identification of Parents (External users) has legitimate access of their children records?</b>	<p>Parents are “invited” to have access to individual documents in Google by the owner of that document.</p> <p>Email address is used and no verification of the email address owner occurs.</p>

## 9.2 Account Management

If the organisational structure is complex and/or there are many users having their access levels changed regularly, we need assurance that users’ access levels are being:

- regularly checked
- effectively controlled

Confirm that these activities for **matching data access levels to job functions** have been carried out:

The School Stewards has analysed the information each user role needs to perform their job	When a new staff member arrives the DDTS account creation procedure defines the access levels required to individual systems by the new staff member and the form is signed (approved) by the principal or manager.
The “Administrator” has set up logical access levels that match those roles	All users of Google are the same access level (students and Teachers) with specific configuration setup for Google Apps based on their functionalities to suit the business requirements. (Eg– In Google Meet, the session to be initiated is provided to Teachers only).
The System Manager, (or a restricted number of staff with defined authority) assign users to appropriate roles / access levels	Formally performed via DDTS as part of Active Directory Group change requests, though see notes regarding local accounts and direct access as described above.
Only the System Administrator (or nominated assistant) implements the assignments in the application  (Alternatively, only the System Administrator raises ServiceNow cases on DDTS Access Control to implement the assignments in the application’s AD groups, if Active Directory group membership is the mechanism used)	As above.
The System Manager (or those staff with defined authority) carry out formal, periodic checks that each user still has appropriate access	An Access list is provided to the Education DSST Team (on request) and in each Term Holiday (quarterly) for manual audit of Google access.
The School Stewards has to analyse the information each External users (Parent) identification and needs to ensure legitimate access.	The Term Audit does check files that have been “allowed access” to external users.

## 9.3 User Roles

Describe the roles and functions available to each user in GSUITE-EDU-BS. Customers, ordinary users, and system administrators are typical starting points. If roles and access is granular, attach a summary table as an appendix.

### 9.3.1 Customers (Parents)

<input type="checkbox"/>	GSUITE-EDU-BS has no public interface.
<input type="checkbox"/>	Public access to GSUITE-EDU-BS will not be available for customers.
<input type="checkbox"/>	GSUITE-EDU-BS has a public interface accessible to customers via the Internet.
<input checked="" type="checkbox"/>	Other (describe): Individual users can authorise external access to individual files

### 9.3.2 Users

<input type="checkbox"/>	GSUITE-EDU-BS has no ACT Government users.
<input checked="" type="checkbox"/>	ACT Government users (Teachers, admin and school Executive staff) on schoolsnet will authenticate to GSUITE-EDU-BS using their Active Directory credentials.
<input type="checkbox"/>	ACT Government users will not have administrative privileges or access to sensitive information other than their own records.
<input type="checkbox"/>	ACT Government users will not have administrative privileges or access to sensitive information other than the records assigned to/shared with them
<input type="checkbox"/>	ACT Government users will have access to sensitive information in aggregate.
<input type="checkbox"/>	ACT Government users will have administrative privileges in GSUITE-EDU-BS.
<input type="checkbox"/>	Other (describe):

### 9.3.3 Administrators

<input type="checkbox"/>	GSUITE-EDU-BS has no ACT Government system administrators.
<input type="checkbox"/>	User access is self-assigned
<input type="checkbox"/>	User access is granted by the Vendor’s system administrators.
<input checked="" type="checkbox"/>	ACT Government system administrators have been assigned to GSUITE-EDU-BS and will authenticate to the administration suite as trusted users using their Active Directory credentials from trusted devices only.
<input type="checkbox"/>	System administrators have access to sensitive information about ACT Government staff or customers.
<input type="checkbox"/>	Other (describe):

### 9.4 Remote Support Access

Staff members from the support provider have access to the system and its data under the following circumstances (select all that apply):

<input type="checkbox"/>	No access to Production or Test, or any Territory data.
<input type="checkbox"/>	No access to Production or Test. Receive printouts/dumps of “de-identified” data
<input type="checkbox"/>	No access to Production. Access to “de-identified” Production data in Test.
<input type="checkbox"/>	Only under direct supervision, without login accounts of their own.
<input type="checkbox"/>	Only under direct supervision, with their own login accounts – with “user-level” access
<input type="checkbox"/>	Only under direct supervision, with their own login accounts – with “application admin-level” access
<input type="checkbox"/>	Remote access or unsupervised access to Test – with “user-level” access
<input type="checkbox"/>	Remote access or unsupervised access to Test – with “application admin-level” access
<input type="checkbox"/>	Remote access or unsupervised access to Production – with “user-level” access
<input type="checkbox"/>	Remote access or unsupervised access to Production – with “application admin-level” access
<input checked="" type="checkbox"/>	Other (describe): Google Support team undergo background checks, are required to execute a confidentiality agreement, and comply with Google’s code of conduct.  In addition, we’ve designed our systems to limit the number of Google Support team that have access to customer data and to actively monitor the activities of those employees. Google Support team are only granted a limited set of default permissions to access resources. Access to internal support tools is controlled via access control lists (ACLs). Google follows a formal process to grant or revoke employee access to Google resources, and access is automatically removed for departing employees.

Access authorization is enforced at all relevant layers of the system. Approvals are managed by workflow tools and logged. An employee's authorization settings are used to control access to all resources, including data and systems for G Suite products. Access is monitored by our dedicated security teams as a check on the effectiveness of our controls. The security teams actively monitor access patterns and investigate unusual events.

As part of Google's long-term commitment to transparency and user trust, Google provide Access Transparency, a feature that enables customers to review logs of actions taken by Google staff when accessing your specific customer data. Access Transparency log entries include the following types of details: the affected resource and action; the time of the action; the reasons for the action (for example, the case number associated with a customer support request); and data about who is acting on the data (such as the Google staff member's location).

Access Transparency logs are produced by the following products:

- Calendar
- Docs
- Drive
- Gmail
- Slides
- Sheets
- Meet recordings stored in Drive

[https://support.google.com/a/answer/9230474?hl=en&ref\\_topic=9230579](https://support.google.com/a/answer/9230474?hl=en&ref_topic=9230579)

## 10 Auditing

Auditing capabilities and procedures for GSUITE-EDU-BS have been reviewed by the System Manager for compliance with the ICT Security Policy and Access Control Standard.

Applications should generate logs to trace user actions. They should contain enough information to establish what events occurred and who caused them. This information is used to ensure Data Integrity and Confidentiality is protected. Application audit logs for business systems belong to the System Owner and are their responsibility to review, protect and retain.

DDTS is responsible for infrastructure audit logging and monitoring. This includes on-premises components like proxy, centralised identity management (active directory) and firewalling. It additionally includes Infrastructure as a Service components like cloud activity logs, Azure active directory logs and other system logs generated by cloud IaaS or PaaS components. For further information on auditing and monitoring, see the *ACT Government Logging and Monitoring Standard*.

Reporting and auditing services within Google can be accessed via the Administration Console at <https://admin.google.com/ac/reporting/home?hl=en-GB>. It is also possible to programmatically generate reports and audit information using the Report APIs available via the G Suite Admin SDK

Google Workspace audit logs in Google Cloud. access the following types of Google Workspace, Cloud Identity, and Drive Enterprise audit logs in Google Cloud:

- Google Workspace Admin audit - Admin audit logs provide a record of actions performed in your Google Workspace Admin Console. For example, you can see when an administrator added a user or turned on a Google Workspace service. For more information about Google Workspace Admin audit logs, see the Admin Activity Report Event Names page.
- Google Workspace Login audit - Login audit logs track user sign-ins to your domain. The login logs only record the login event. They do not record which system was used to perform the login action.
- Google Workspace Enterprise Groups audit - Enterprise Groups audit logs provide a record of actions performed on groups and group memberships. For example, you can see when an administrator added a user or when a group owner deleted their group.

(For more details on Google Workspace audit logs, please refer to - <https://cloud.google.com/logging/docs/audit/configure-gsuite-audit-logs>).

### 10.1 Audit Log

<b>Does the audit log provide information suitable to help detect intrusion?</b>	Yes
<b>Does the audit log capture access rights changes?</b>	Yes

The application provides an audit trail of access/operations on the system that records the following (select all that apply):

<input checked="" type="checkbox"/>	User id log-in: date and time
<input checked="" type="checkbox"/>	User id log-out: date and time
<input type="checkbox"/>	User id and Key of record accessed
<input checked="" type="checkbox"/>	Operation carried out: Create, Change, View, Delete
<input type="checkbox"/>	Other (describe):