Stats NZ Internal Audit

Identity and Access Management Strategy and Roadmap

Author: [redacted]

Date: 2 May 2017

Version 1.0

DOCUMENT HISTORY

Version	Date	Author	Organisation	Description of changes
0.3	23 March 2017	[redacted]	Unify Solutions	Completed draft document
0.4	28 March 2017	[redacted]	Axenic Limited	Quality Assurance review completed
0.5	29 March 2017	[redacted]	Unify Solutions	Incorporate changes from QA review
0.6	29 March 2017	[redacted]	Axenic Limited	Draft document shared with Statistics New Zealand
0.7	18 April 2017	[redacted]	Unify Solutions	Incorporate changes from review [redacted])
0.8	19 April 2017	[redacted]	Axenic Limited	Review of changes from V0.7. Some follow up items from [redacted] to [redacted] pending resolution.
1.0	2 May 2017	[redacted]	Unify Solutions	Final
1.0	2 May 2017	[redacted]	Axenic Limited	Final version QA.

DISTRIBUTION LIST

Name	Role	Organisation	Version
[redacted]	Internal Auditor	Statistics New Zealand	0.6, 0.8, 1.0
[redacted]	Senior Infrastructure Consultant	Statistics New Zealand	0.6, 0.8

TABLE OF CONTENTS

1 INTRODUCTION

Statistics New Zealand (STATS) has set a strategic goal to double the value of the data provided for decision-makers. STATS plan to achieve this by adopting and promoting more efficient and effective data practices, developing their data capability across the government sector, and continuing to meet the needs of key customer groups, suppliers, and stakeholders.

By 2030 STATS aims to create a tenfold increase in the value of data provided to New Zealand.[1]

A key component for delivering to this goal, is the ability for STATS to enable access to data for both internal and external identities in a secure and auditable manner.

The objective of this document is to provide an Identity and Access Management (IAM) Strategy and Roadmap which STATS can use for the following purposes:

1. Identify necessary identity processes to achieve the desired outcome.
2. Identify a single source of truth.
3. Guidance to move to a better identity state with a list of some potential quick wins on the board.
4. Guidance around onboarding for Census staff.

UNIFY has worked together with the AXENIC and STATS teams to identify and understand the high-level business requirements, assess the suitability of the existing product stack to support the IAM desired outcome, and propose a roadmap to progress towards a better identity state.

[1] Statistics New Zealand – Information Systems Strategic Plan 2016 – 1st Edition

2 EXECUTIVE SUMMARY

2.1 BACKGROUND

STATS has previously implemented several mechanisms to automate specific account provisioning and de-provisioning actions and lifecycle management events. While these point solutions function adequately, they do not provide an over-arching solution which is necessary to ensure that end-to-end business processes and requirements are being met.

2.2 ENGAGEMENT OBJECTIVES

STATS has recognised that a whole-of-business perspective towards IAM may deliver significant business benefits to a range of corporate stakeholders and business functions. This engagement was commissioned to conduct a high-level analysis of the business and systems environments within STATS and to identify opportunities for achieving business benefits through the automation of Identity and Access Management.

Leveraging the expertise and experience of a specialist IAM consulting organisation, the task was to present a strategy for IAM, a target IAM architecture and an implementation roadmap that outlines the way in which the proposed IAM strategy should be implemented.

2.3 FINDINGS

[redacted]

In talking with the various stakeholders involved in this engagement, it became clear that a fundamental shift has occurred within STATS regarding the importance of good identity and access management practices. IAM is now seen as being a business enabler for moving the organisation forward, as both a cloud/service consumer and as a service provider of statistical data.

The recent severe Wellington earthquake (14 November 2016), and its aftermath have also provided a catalyst for STATS to review its current state and identify any future needs in order to better align its identity and access management practises with its business strategy. Specifically, in terms of being a leader in the provision of data services to New Zealand.

2.4 RECOMMENDATIONS

[redacted]

- [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]

[redacted]

3 FUTURE STATE REQUIREMENTS

Detailed business requirements for IAM are yet to be defined by STATS, however through discussions with stakeholders a number of high-level requirements have surfaced. These, along with some additional best practice requirements, form the basis for understanding the capabilities that STATS will require from a future IAM solution.

3.1 HIGH-LEVEL FUTURE CAPABILITIES REQUIRED OF IAM

For the purpose of this strategy and roadmap, the capabilities required of IAM for STATS have been split across four towers.

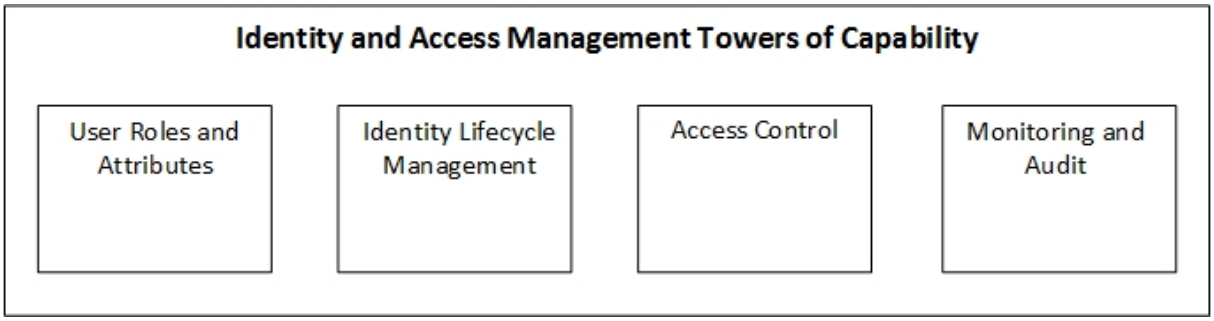


Figure 1 - Identity and Access Management Towers of Capability

3.1.1 User Roles and Attributes

This tower includes all the sources of information that can be used to create a complete picture of an identity and its role and function within the organisation. This will include Human Resources databases and other data sources that may hold relevant user attributes.

3.1.2 Identity Lifecycle Management

Managing the lifecycle of an identity through the organisation should be automated through workflows and predefined processes based on associated attributes and roles assigned to the identity. Identity Lifecycle Management should also provide a means for user self-service where appropriate, including the provision of approval workflows for user requested changes.

Identity Lifecycle Management should include:

- Automated User Provisioning.
- Automated user change based on attribute/role change.
- Automated de-provisioning.

User provisioning must have the ability to provision users in downstream access control systems, other attribute stores, and applications with the appropriate attributes associated with their role and function. The attributes associated to a user must also update in real-time to reflect changes of a user's role or function.

3.1.3 Access Control

Access Control describes the control mechanisms for access to systems and applications across the STATS ecosystem including internal systems, cloud-based systems and externally facing systems.

Access Control should provide the following:

- Ability to map to and enforce system and data classification policies.

- Access Control based on associated security groups.
- Access Control based on other associated identity attributes – role, manager, location, current function, etc.
- Just in time privileged access.
- Multi-factor authentication.
- Multi-factor step-up authorisation.
- Self-service password management.

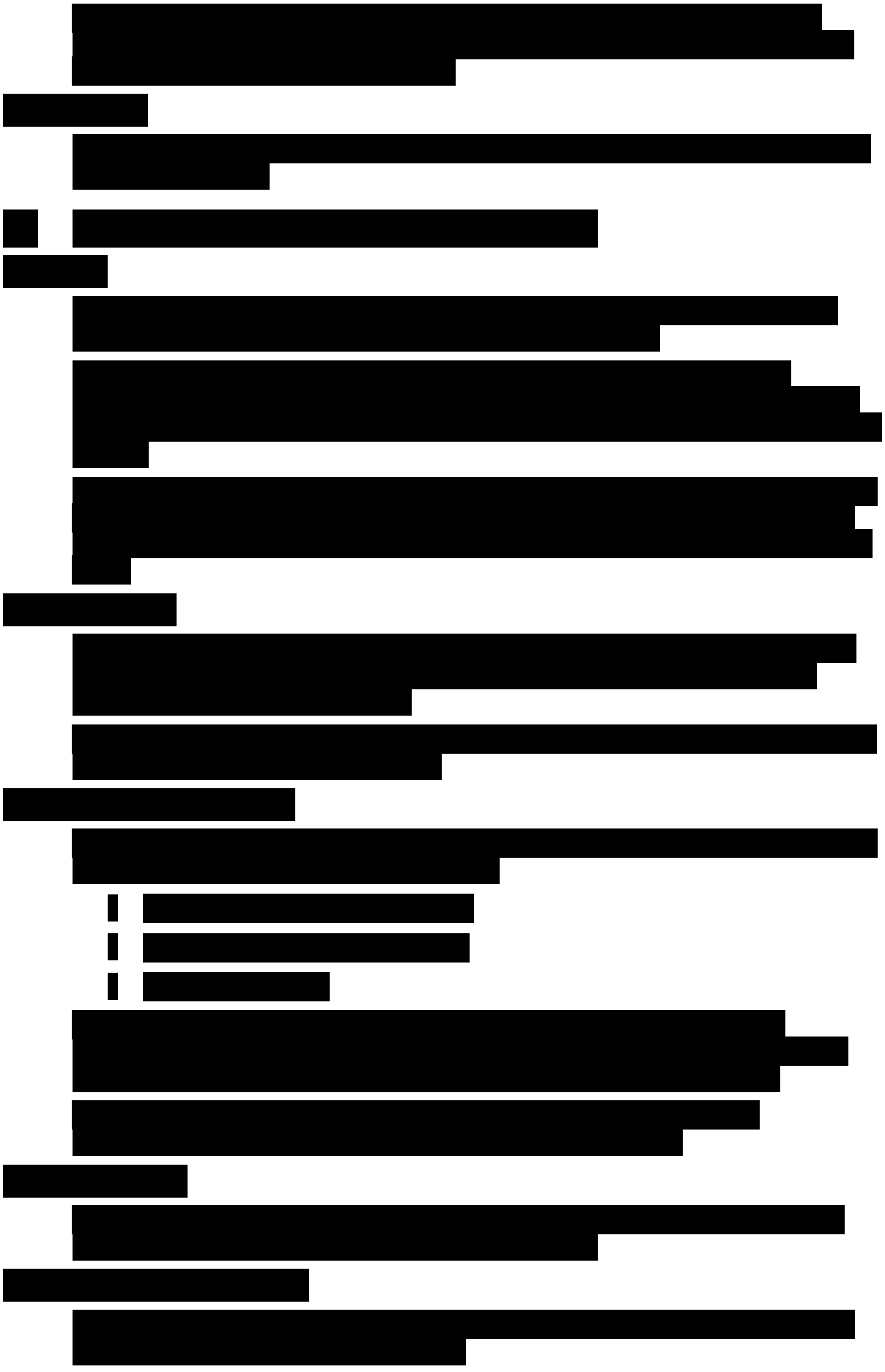
3.1.4 Monitoring and Audit

The IAM platform components must provide means for monitoring and alerting on suspicious access behaviours and should also provide for automated actions to be taken when such behaviour is detected. All access related activities are to be centrally logged.

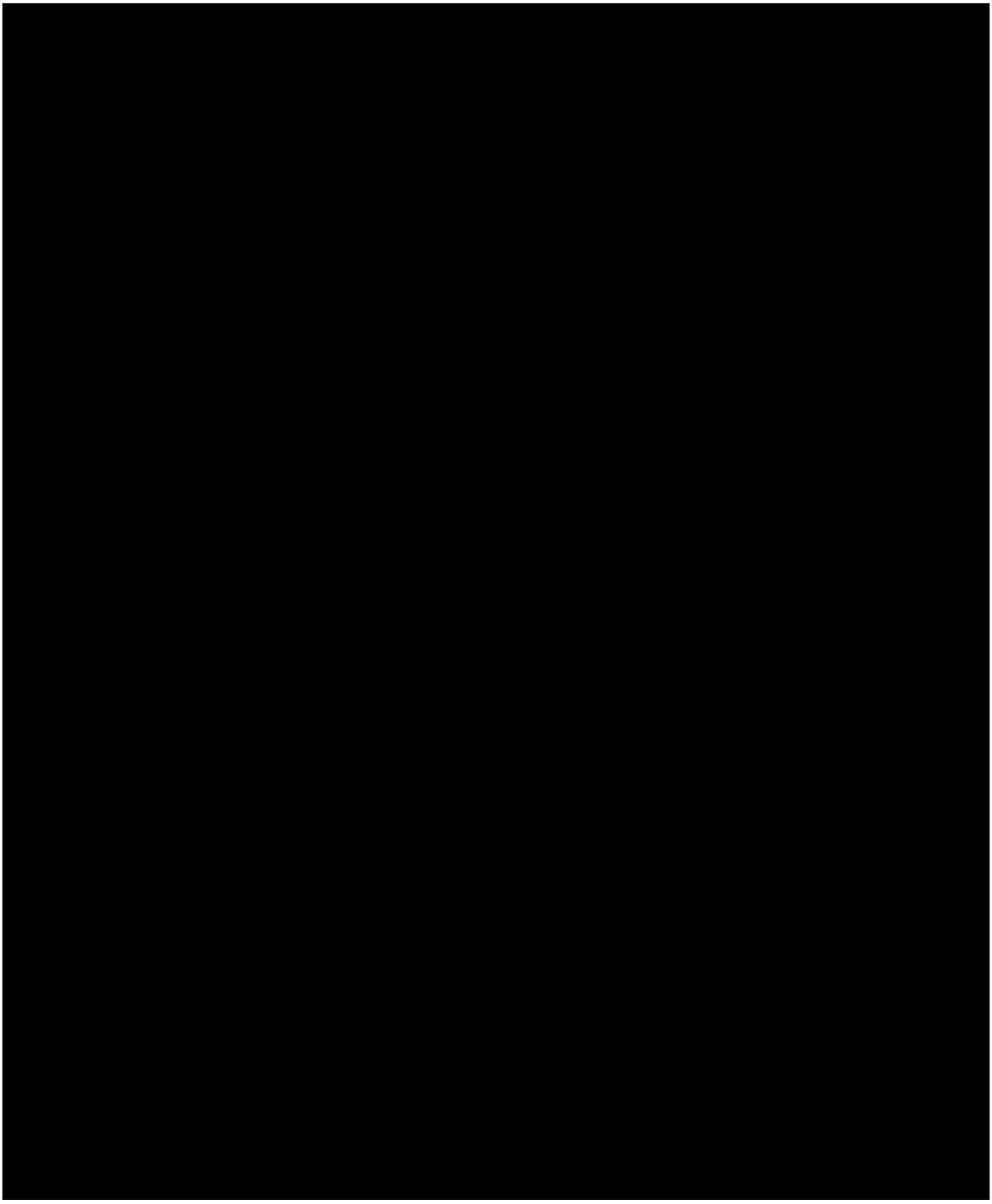
The IAM platform components must provide a full audit trail of all identity changes and provide a means of re-validation of user access.

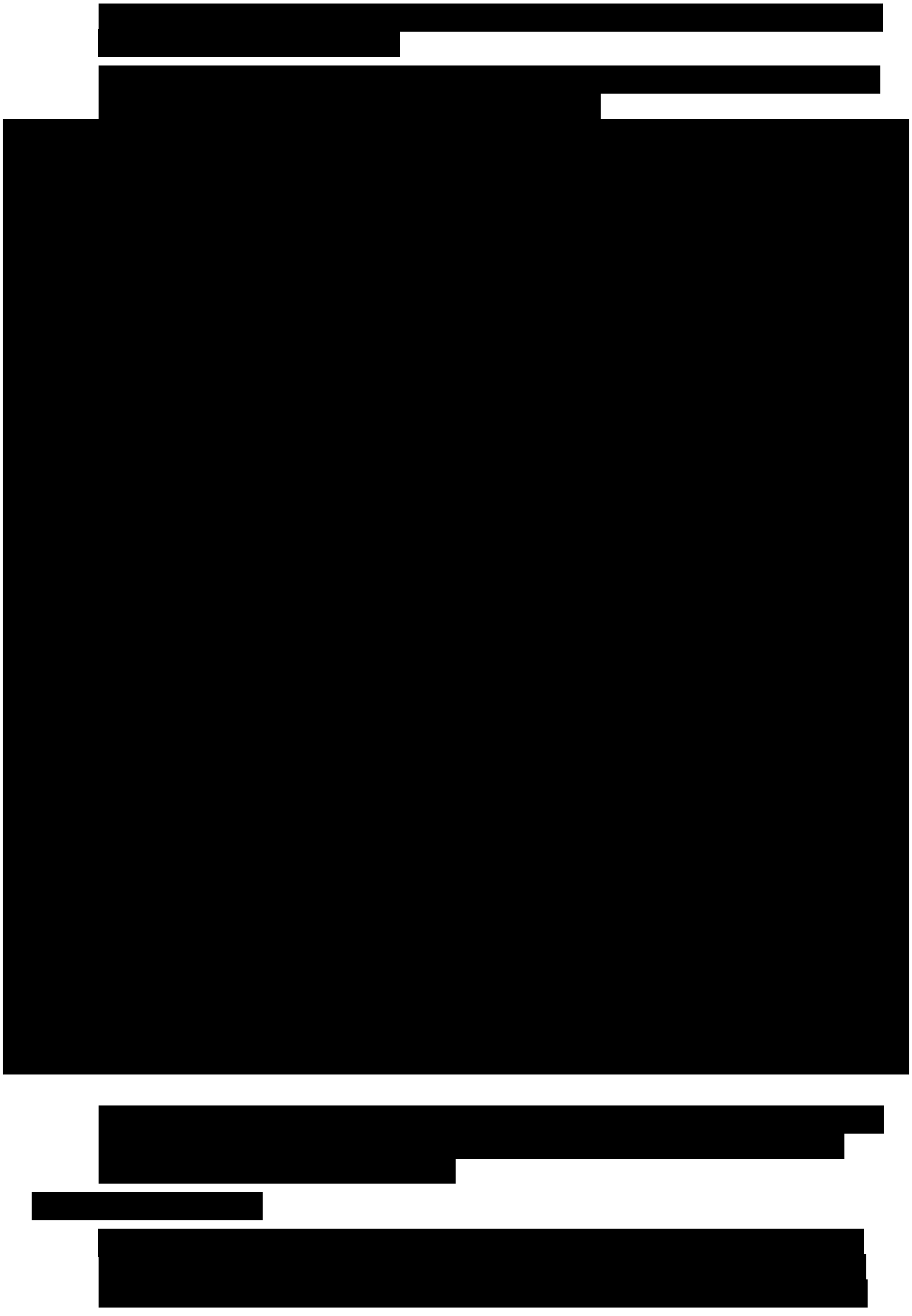
4 CURRENT STATE

The following sections describe the current state of IAM for STATS for all systems and data access.



[redacted]

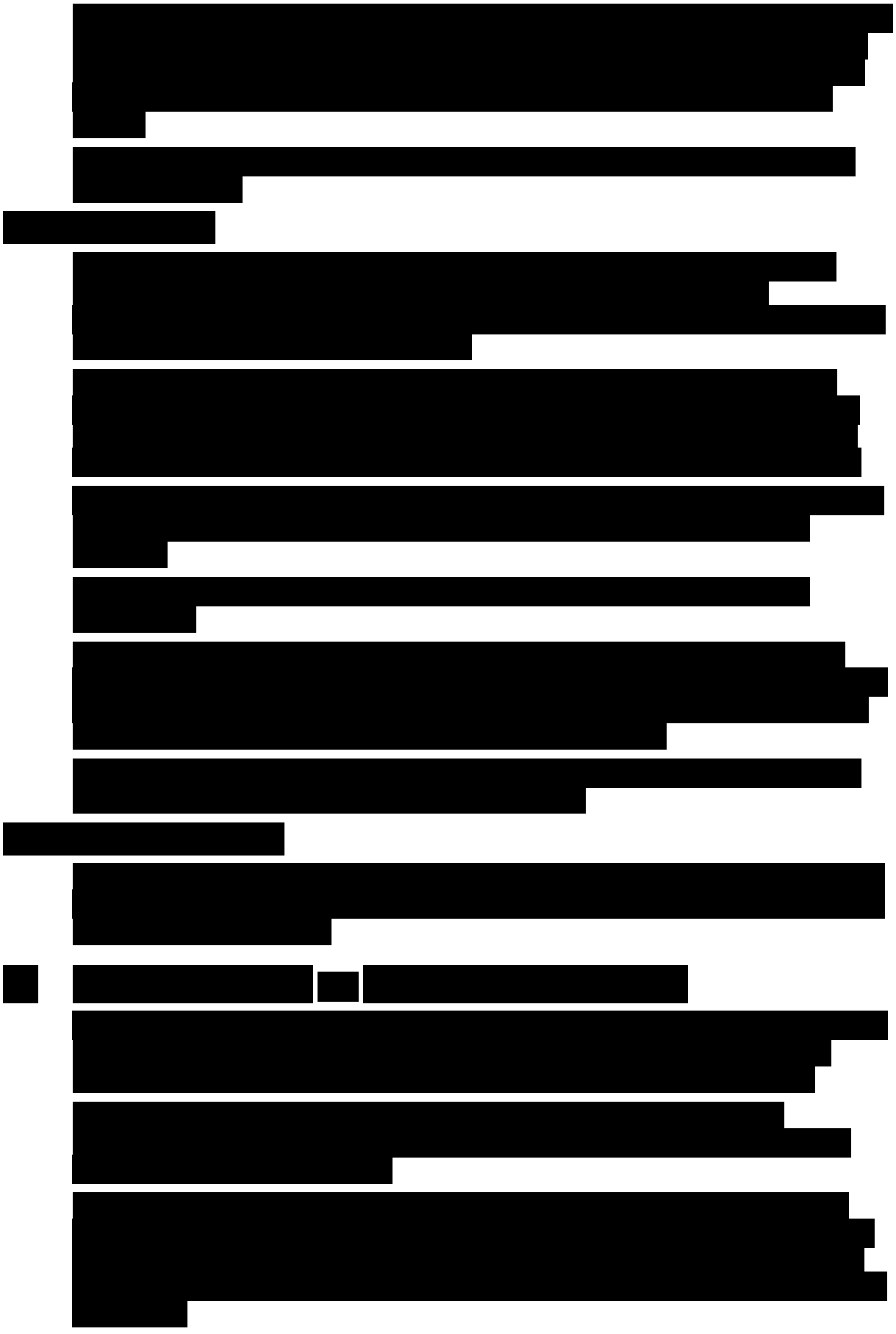




[redacted]

[redacted]

[redacted]



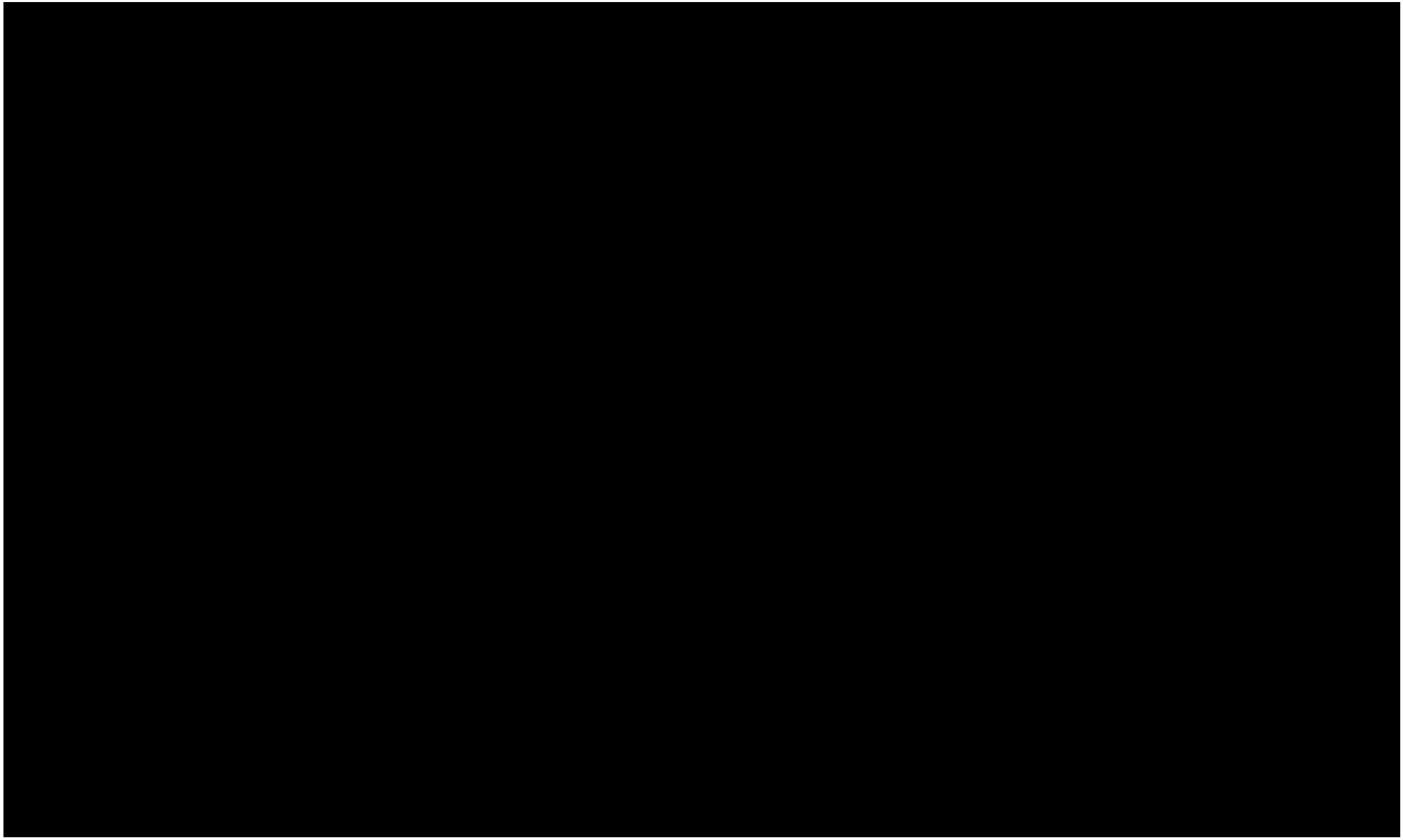
5 RECOMMENDATIONS

This section provides a list of recommendations for the improvement and better utilisation of identity and access management for STATS based on a review of the current state and the future state requirements laid out in section 3 of this document.

[redacted]

[redacted]

[redacted]



6.1 FUTURE STATE REFERENCE ARCHITECTURE OVERVIEW

[redacted]

[redacted]

[redacted]

7 ROADMAP ACTIVITIES

The following provides a sample roadmap based on the outcomes presented in this strategy. Further analysis would be required to complete this roadmap and ensure that it aligns with STATS wider strategic goals, but it should provide a view of the type of work required to implement the proposed outcomes as a starting point, and as an input to future discussion.

All of the tasks can be run in parallel within each of the Phases, unless dependencies on other tasks within the phase have been indicated in the Dependencies column.

It should also be noted that some of these tasks may already be underway so any program of change should take this into consideration.