Change Request

CHANGE REQUEST BRIEF DETAILS

Change Request Number	CR03
Date of Change Request	3 April 2019
Originator of need for Change Request	Customer
Proposed Implementation Date of Change	The date upon which both Parties have signed the Change Request.
Date of expiry of validity of Change Request	Not Applicable
Contractor's estimated time and cost of evaluation	0
Amount agreed to be paid to the Contractor for evaluating the draft Change Request, if any **(This applies only if the Customer is the Party that originated the need for a Change Request; and the Contractor estimates the cost of evaluating and drafting the Change Request exceeds 2 Business Days)**	Not Applicable

CHANGE REQUEST HISTORY LOG

Change Request Version History			
Date	**Issue Version**	**Status/Reason for New Issue**	**Author**
03/04/2019	1	Draft Change Request for additional non-recurring services: • Firewall review and remediation • Delegated access review and remediation • Design phase of Wi-Fi replacement	Alice Yan

DETAILS OF CHANGE REQUEST

Summary

The Contractor must provide additional non-recurring services to the Customer in relation to the migration of the following outsourced IT services to the Contractor:

1) Firewall rule review and remediation
2) Delegated access review and remediation
3) Design phase of Wi-Fi replacement

The Milestones for each service are set out in the following documents comprising Appendix A:

1) Attachment 1: Statement of Work: Firewall rule review and remediation
2) Attachment 2: Statement of Work: Delegated access review and remediation
3) Attachment 3: Statement of Work: Design phase of Wi-Fi replacement

Upon delivery of each Milestone by the Contractor, the Customer will have 3 business days to request modifications, additions or rectification of any defects.

A Milestone is considered complete at the expiry of the 3 days where the Customer has not made further requests, or otherwise, upon written confirmation by the Customer.

The Contractor must make best endeavours to complete all Milestones in the documents comprising Appendix A by 30 June 2019.

If the Contractor has not completed all Milestones by 30 June 2019, the Contractor will issue an invoice to the Customer before 30 June 2019 for all work completed by 30 June 2019, and complete the remaining work necessary to achieve all Milestones by the earliest reasonable date as agreed in good faith between the parties.

SCOPE

As outlined in the documents comprising Appendix A.

EFFECT OF CHANGE ON CONTRACT SPECIFICATION

Not Applicable.

EFFECT OF CHANGE ON PROJECT TIMETABLE

Not Applicable.

New PIPP (annexed)

Not Applicable.

EFFECT OF CHANGE ON CHARGES AND TIMING OF PAYMENT

The following Table 1 details the Milestones and quotations for the additional services included in this Change Request. Any other quotation documents do not form a part of this Change Request.

Table 1: Fees for Additional Services

Item	SKU	Description	Qty	Unit	Unit SELL Ex GST	Extended SELL Ex GST
NON-RECURRING SERVICES						
4	**Firewall review and remediation (one-off)**					
	Milestone 1	Project Kick-off	1	each	$ 4,504.00	$ 4,504.00
	Milestone 2	Firewall Review first pass	1	each	$ 17,432.00	$ 17,432.00
	Milestone 3	Other Firewall Findings Review	1	each	$ 2,404.00	$ 2,404.00
	Milestone 4	Firewall Clean-up preparation and Change First	1	each	$ 9,320.00	$ 9,320.00
	Milestone 5	Firewall Review Second Pass	1	each	$ 9,320.00	$ 9,320.00
	Milestone 6	Firewall Clean-up preparation and Change	1	each	$ 7,064.00	$ 7,064.00
	Milestone 7	Firewall Review Third Pass	1	each	$ 2,968.00	$ 2,968.00
	Milestone 8	Firewall Clean-up preparation and Change	1	each	$ 2,706.00	$ 2,706.00
						$ 57,068.00
5	**Delegated access review and remediation (one-off)**					
	Milestone 1	Concept and Define	1	each	$ 945.00	$ 945.00
	Milestone 2	Plan	1	each	$ 5,326.00	$ 5,326.00
	Milestone 3	Design	1	each	$ 31,335.00	$ 31,335.00
	Milestone 4	Construct	1	each	$ 47,103.00	$ 47,103.00
	Milestone 5	Commission	1	each	$ 18,391.00	$ 18,391.00
						$ 103,100.00
6	**Design phase of Wi-Fi replacement project (one-off)**					
	Milestone 1	Network Architecture Framework – Design	1	each	$ 23,250.00	$ 23,250.00
						$ 23,250.00

CHANGES TO CSI

Not Applicable.

CHANGES TO CUSTOMER PERSONNEL

Not Applicable.

CHANGES TO CUSTOMER ASSISTANCE

Not Applicable.

PLAN FOR IMPLEMENTING THE CHANGE

Not Applicable.

THE RESPONSIBILITIES OF THE PARTIES FOR IMPLEMENTING THE CHANGE

Responsibilities of the Contractor

The Contractor must make best endeavours to complete all Milestones in the documents comprising Appendix A by 30 June 2019. If the Contractor has not completed all Milestones by 30 June 2019, the Contractor will issue an invoice to the Customer before 30 June 2019 for all work completed by 30 June 2019, and complete the remaining work necessary to achieve all Milestones by the earliest reasonable date as agreed in good faith between the parties.

Responsibilities of the Customer

The Customer will support the Contractor where possible to meet the timeframes above.

EFFECT ON ACCEPTANCE TESTING OF ANY DELIVERABLE

Not Applicable.

EFFECT OF CHANGE ON PERFORMANCE OF ANY DELIVERABLE

Not Applicable.

EFFECT ON USERS OF THE SYSTEM/SOLUTION

Not Applicable.

EFFECT OF CHANGE ON DOCUMENTATION DELIVERABLES

Not Applicable.

EFFECT ON TRAINING

Not Applicable.

ANY OTHER MATTERS WHICH THE PARTIES CONSIDER IMPORTANT

In the event of any inconsistency between the documents comprising Appendix A to this Change Request and the remainder of the Customer Contract (including this Change Request), the Customer Contract prevails over the documents comprising Appendix A to the extent of the inconsistency.

ASSUMPTIONS

Not Applicable.

LIST OF DOCUMENTS THAT FORM PART OF THIS CHANGE REQUEST

Appendix A documents:

1) Attachment 1: Statement of Work: Firewall rule review and remediation
2) Attachment 2: Statement of Work: Delegated access review and remediation
3) Attachment 3: Statement of Work: Design phase of Wi-Fi replacement

CUSTOMER CONTRACT CLAUSES, SCHEDULES AFFECTED BY THE PROPOSAL ARE AS FOLLOWS:

The existing Item 11 Common Details of the General Order Form is replaced by the following:

Schedule 1: Item 11 Common Details

The scope of works for the Customer Contract is set out in the document titled QW184320 IPART OITS Programme SOW (version IPART.1) comprising Agreement Document A listed in Schedule 2.

The prices for the Services provided under the Customer Contract are set out in the document titled QW184320 IPART OITS Programme Quote (version IPART.1) comprising Agreement Document B listed in Schedule 2.

The unit price for each Service provided under the Customer Contract is listed in Agreement Document B, in the column titled 'Unit SELL Ex GST'.

The unit price for each Service is fixed for the Contract Period.

The Non-Recurring Services are the items listed in:

- Agreement Document B in the Customer Contract as the 'Non-Recurring Services';
- the documents comprising Appendix A to Change Request CR02 as the 'One Off Services'; and
- the documents comprising Appendix A to Change Request CR03.

All other Services listed in Agreement Document B and the documents comprising Appendix A to Change Request CRO2 are referred to in the Customer Contract as the Recurring Services.

The price for Non-Recurring Services (Non-Recurring Fee) is $548,453.77, excluding GST.

The estimated price for the Recurring Services (Recurring Fee) is $91,500.21, excluding GST. For certainty, while the unit price for each of the Recurring Services is fixed for the duration of the Contract Period, the units of Recurring Services consumed by the Customer may fluctuate from month-to-month.

The estimated Contract Price if the Contract runs for the Initial Term is ~~$4,226,706.46~~ $4,226,707.46 (including GST).

The estimated Contract Price if the Contract runs for the Initial Term and the Renewal Term is $6,642,313.00 (including GST).

AUTHORISATION

The Contractor must not commence work in the Change Request until it is signed by both Parties. Once signed by both Parties, the Customer Contract is updated by this Change Request and any provisions of the Customer Contract that conflict with this Change Request are superseded.

SIGNED AS AN AGREEMENT

Signed for and on behalf of the

Independent Pricing and Regulatory Tribunal of New South Wales
(ABN 49 202 260 878)

By *the Customer's Representative* but not so as to incur personal liability

Signature of Customer Representative

HUGO HARMSTORF

Print name

8.4.19

Date

Signed for and on behalf of

Australian Centre for Advanced Computing and Communication Pty Ltd
(ABN 27 095 046 923)

Signature of Authorised Signatory

Simon Kistouris

Print name

11/4/19

Date

AC3

Australian Centre for Advanced Computing and Communication

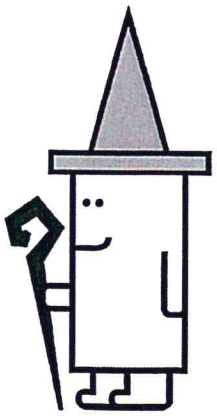
STATEMENT OF WORK

Firewall Review and Remediation Project

For

Independent Pricing and Regulatory Tribunal (IPART)

IPART
Independent Pricing and Regulatory Tribunal
New South Wales



NOTICES

DOCUMENT CREDENTIALS

Client Details

Name:	Mike Webber
Position:	ICT Leader and Chief Procurement Officer
Client:	Independent Pricing and Regulatory Tribunal (IPART)
Email:	Mike_Webber@ipart.nsw.gov.au

AC3 Contact Details

We welcome any enquiries regarding this document, its content, structure or scope. These should be directed to:

Name:	Briant Kareroa
Position:	Sales Manager - NSW Public Sector, Government Sales
Telephone:	02 9199 0856
Mobile:	0420 936 712
Email:	Briant.Kareroa@ac3.com.au

Document Control

Document Reference

Department:	Consulting
Document Name:	IPART - Firewall Review and Remediation Project Schedule

Preparation

Version	Date	Change	By (Name, Position)
1.0	11/02/2019	Initial release	John Seretis

Reviewers

Version	Date	By (Name, Position)
1.0	11/02/2019	Nick Rettenbeck, Consulting Team Lead

Approvals

Version	Date	By (Name, Position)
1.0	11/02/2019	Nick Rettenbeck, Consulting Team Lead

Distribution

Version	Date	To	Position, Organisation
1.0	11/02/2019	Mike Webber	ICT Leader and Chief Procurement Officer, IPART

Classification

Classification	Description
Commercial in Confidence	A document shared with specific customer/s

Related Documents

Document Name	Reference Number	Organisation

Sign-Off

Signed	Name, Position

TABLE OF CONTENTS

1 Executive Summary 6
2 Solution Overview 7
2.1 Firewall Rule Review 7
2.1.1 Approach Overview 7
2.2 Other Firewall Findings Review 7
2.2.1 Project Management 8
2.2.2 AC3 Project Principles & Lifecycle 8
2.2.3 Project Phases 9
2.2.3.1 Project Kick-off – Milestone A 9
2.2.3.2 Firewall review first pass – Milestone B 9
2.2.3.3 Other Firewall Findings Review – Milestone C 9
2.2.3.4 Firewall clean-up preparation and change first pass – Milestone D 9
2.2.3.5 Firewall review second pass – Milestone E 9
2.2.3.6 Firewall clean-up preparation and change second pass – Milestone F 10
2.2.3.7 Firewall review third pass – Milestone G 10
2.2.3.8 Firewall clean-up preparation and third pass – Milestone H 10
2.2.3.9 Project Closure – Milestone I 10
2.3 Work Breakdown Structure 11
2.4 Responsibilities, Assumptions & Constraints 13
2.4.1.1 AC3 Responsibilities 13
2.4.1.2 Client Responsibilities 13
2.4.1.3 Exclusions 13
2.4.1.4 Constraints 13
3 Project Governance Model 15
3.1 Project Execution 15
4 Price and Payment 16
4.1 Pricing 16
5 Recitals 17
5.1 Copyright 17
5.2 Disclaimer 17
5.3 Warranty 17
6 Appendix A – Firewall Audit Findings 18

1 EXECUTIVE SUMMARY

Independent Pricing and Regulatory Tribunal (IPART) is an NSW State Agency company with headquarters based in Sydney CBD. IPART provides independent regulatory decisions and advice to protect the ongoing interests of the consumers, taxpayers and citizens of NSW.

AC3 specialises in the design, implementation and management of information technology focused on meeting constantly evolving user needs and the environment landscape. As a managed services provider, IT consultancy, service delivery and product procurement organisation, AC3 works closely with clients to understand their business and then looks for opportunities to streamline and secure the underlying technology.

IPART have requested AC3 to provide assistance with the remediation of the firewall rules which were recently migrated onto AC3 infrastructure. This proposal is one of six mini projects that are required to address multiple concerns which were identified as part of an external security review prior to the migration to AC3 platform.

Key Requirements Addressed:

- Review firewall rules and remediate any rules which are dormant and not required
- Review any firewall rules and place descriptions on migrated rules

These requirements are covering the following assessment findings:

Scope	Key	Risk	Number	Issue Description	Remedy (Abridged)
Firewall 5520	FW	L	5.1.9	Business requirements of traffic flows are not documented	Ensure that each firewall rule is documented with the business requirements and system owners
Firewall 5520	FW	L	5.1.15	Comments and names are not present for every firewall rule	Appropriate comments and names should be present for every rule defined on the firewall
Firewall 5520	FW	L	5.1.16	There is no explicit deny all rule with logging enabled.	A deny all rule should be placed at the end of each access list
Firewall 550	FW	M	5.2.2	Firewall rules exist that are not configured according to best practice.	All firewall rules should have explicitly defined strict source and destination addresses
Firewall 550	FW	L	5.2.9	Comments and names are not present for every firewall rule	Appropriate comments and names

There are a number of other 26 findings in the Firewalls section of the assessment (see appendix A) which have either been addressed indirectly by the migration to GovDC or are no longer relevant. Appropriate justification, but no remediation activities, will be documented part of this engagement.

2 SOLUTION OVERVIEW

2.1 Firewall Rule Review

AC3 will perform a review of the hosted Palo Alto firewall rules (approx. 450 per site), at both Silverwater and Unanderra GovDC. These rules were migrated as is from firewalls existing IPART firewalls.

2.1.1 Approach Overview

The approach AC3 is proposing is a three staged approach.

First Pass

AC3 will first analyse the rule base, determine "any any" rules and provide a general sanity check. AC3 will then enable detailed logging on the Palo Alto firewalls for 4 weeks, which will show which rules are not being "hit". These rules will be reviewed by both IPART and AC3 to identify source and destination systems. Once all firewall rules have been identified and documented, they will either be removed, updated (description provided) or remain. The updated rules will be created with a higher precedence and will be more specific in terms of source and destination systems.

Second Pass

Once the first pass has been completed and the firewall rules have been remediated, a second pass will be performed. For any rules generic rules that are still being hit, AC3 and IPART will review these and make them even more specific in terms of source and destination endpoints.

Third Pass

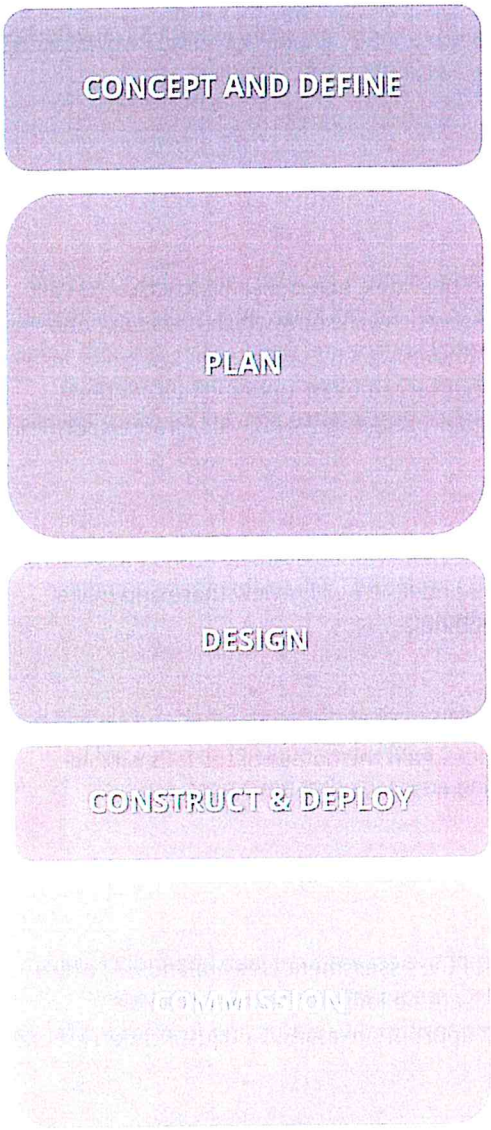
This approach will capture any firewall rules which could have been missed during the first and second pass, this will also capture applications that are used in-frequently. Once again the details of the logs will be reviewed by both IPART and AC3. AC3 will proceed with removing any rules that have not been hit.

2.2 Other Firewall Findings Review

There are a number of other 26 findings in the Firewalls section of the assessment (see appendix A) which have either been addressed indirectly by the migration to GovDC, are no longer relevant or can be exempted. AC3 will go through these findings and will document appropriate status and justification for each finding.

2.2.1 Project Management

2.2.2 AC3 Project Principles & Lifecycle



- Validate Project
- Establish Objectives
- Present Initial Proposal

- Develop Project Scope
- Develop Timeline & Budget (WBS)
- Develop Change Management Plan
- Develop Comms,Training & Doco. Plan
- Develop Risk Management Plan
- Project Document Sign-off
- Procure Staff & Materials
- Resource Review & Execution Kick-off

- Low Level Design
- High Level Design

- Implement Project Plan
- Monitor & Control Project Implementation

- Document Control
- Post Implementation Review
- Report Project Performance
- Final Project Sign-off
- Transition to Operations

Using our qualified understanding of the PRINCE2 as a guide, we have developed a Project Management framework which we feel offers a controlled and measurable lifecycle for our customers. It ensures accountability and visibility for each phase of your program delivery and allows for a continuous focus on quality assurance, cost-benefit analysis, risk management, communication and reporting.

Each of the steps within the project lifecycle contains a carefully constructed range of deliverables which will guide your requirements through to a successful outcome. We pride ourselves on being industry leaders in the development of high quality technical products and services and we also know the importance of robust project management.

2.2.3 Project Phases

In order to ensure that all works performed for IPART are of the highest quality and the proper project management process can be applied; AC3 will perform the work in scope in the **following nine (9) project phases** for remediation, which aligns with our project management framework. These phases are as below.

2.2.3.1 Project Kick-off – Milestone A

During this phase AC3 will create all the required project artefacts that will be used to support the remediation tasks of the firewall rule reviews. These project artefacts will form part of the Project Management Plan (PMP) and will include, at a minimum:

- Project Schedule
- Project Risk, Issue, Action and Change Register
- Communication, Quality and Risk Management Plans

AC3 will also conduct a project kick-off meeting once all the project artefacts have been established, this will be to formally establish the project and for IPART to meet the AC3 project team and discuss any issues or concerns with the project so that they can be flagged and addressed.

2.2.3.2 Firewall review first pass – Milestone B

Firewall Rule Analysis

AC3 will analyse all firewall rules and determine if there are any rules which have had no hits. These rules will be the first rules which will be added to the remediation list.

Firewall Rule Audit

AC3 will then enable detailed logging with retention for a period of 4 weeks, the syslog logs will be storage locally on AC3 infrastructure and retained only for the period of the review. AC3 will then review the syslog output for "any" rules and prepare a remediation list for IPART and AC3 to review.

Firewall Rule Review

AC3 will perform the first pass review of the logs and make notes for attention. AC3 will then work with IPART to identify and document all rules and create a list of rules which will need to be remediated. This will be in preparation for the next phase.

2.2.3.3 Other Firewall Findings Review – Milestone C

To maintain moment during the 4 weeks of syslog data collection, AC3 will review the other, non-ruleset related findings during this time (see appendix A). AC3 will document the treatment or exemption justification for each of these findings.

2.2.3.4 Firewall clean-up preparation and change first pass – Milestone D

Preparation

AC3 will prepare all scripts required for the remediation tasks which were previously identified, AC3 will then prepare the change request for CAB.

Firewall Change

Once the CAB has approved the change AC3 will schedule the change and implement the change outside of business hours.

The following day AC3 will provide a full day of post change support in the unlikely event an issue is identified and requires immediate attention.

2.2.3.5 Firewall review second pass – Milestone E

Firewall Rule Audit

AC3 will clear logs and collect an additional 4 weeks' worth of logging. AC3 will review and detail "any" rules for IPART and AC3 to review.

Firewall Rule Review

AC3 will perform the first pass review of the logs and make notes for attention. AC3 security team will then work with IPART to identify any additional rules and create a list which will need to be remediated. This will be in preparation for the next phase.

2.2.3.6 Firewall clean-up preparation and change second pass – Milestone F

Preparation

AC3 will prepare all scripts required for the remediation tasks which were previously identified, AC3 will then prepare the change request for CAB.

Firewall Change

Once the CAB has approved the change AC3 will schedule the change and implement the change outside of business hours.

The following day AC3 will provide a full day of post change support in the unlikely event an issue is identified and requires immediate attention.

2.2.3.7 Firewall review third pass – Milestone G

Firewall Rule Review

AC3 will review and detail "any" rules that have not been hit.

2.2.3.8 Firewall clean-up preparation and third pass – Milestone H

Preparation

AC3 will prepare all scripts required for the remediation of rules, AC3 will then prepare the change request for CAB.

Firewall Change

Once the CAB has approved the change AC3 will schedule the change and implement the change outside of business hours.

The following day AC3 will provide a ½ a day of post change support in the unlikely event an issue is identified and requires immediate attention.

2.2.3.9 Project Closure – Milestone I

Once all changes have been completed a post implementation a Closure report will be generated and provided to IPART.

N.B. Given this is a live environment, all changes to the IPART network (Firewalls) will be performed outside of business hours and will go through IPART CAB to ensure approval.

2.3 Work Breakdown Structure

The project scope of work defines the tasks, resources, requirements and deliverables that IPART can expect from each and every phase of the project.

Resource Initials:

- **L5-PM** – Level 5 Project Manager
- **L5-SA** – Level 5 Solutions Architect
- **L4-SE-NS** – Level 4 Senior Network Engineer – Business Hours
- **L4-SE-I** – Level 4 Senior Infrastructure Engineer – Business Hours
- **IPART** – Independent Pricing and Regulatory Tribunal NSW

WBS	Task Name	Resource
0	**IPART - Firewall Review and Remediation Project Schedule v1.1**	
1	**Project Kick-off**	
1.1	Project setup	AC3-L5-PM
1.2	Kick-off meeting - AC3	AC3-L4-SE-I,AC3-L4-SE-NS,AC3-L5-PM
1.3	Kick-off meeting - IPART (run through scope and approach)	AC3-L4-SE-I,AC3-L4-SE-NS,AC3-L5-PM,AC3-L5-SA-NS,IPART,IPART-PM
1.4	MILESTONE A	
2	**Firewall Review first pass**	
2.1	**Firewall Rule Analysis**	
2.1.1	Analyse rules, determine "any rules" and "no hit" rules	AC3-L4-SE-NS
2.2	**Firewall rule Audit**	
2.2.1	Setup extended syslog collection (4 weeks)	AC3-L4-SE-NS
2.3	**Firewall rule review**	
2.3.1	Review syslog output for "any" rules	AC3-L4-SE-NS
2.3.2	Work with IPART to review firewall rules	AC3-L4-SE-NS,IPART
2.3.3	Work with AC3 Infrastructure team to review firewall rules	AC3-L4-SE-I,AC3-L4-SE-NS
2.4	Project Management and governance	AC3-L5-PM
2.5	MILESTONE B	
2.6	**Other Firewall Findings Review**	
2.6.1	Review firewall findings x26	AC3-L4-SE-NS
2.6.2	Document treatment or exemption justification for each finding x26	AC3-L4-SE-NS
2.6.3	Project Management and governance	AC3-L5-PM
2.7	MILESTONE C	
3	**Firewall Clean-up preparation and Change First Pass**	
3.1	**Preparation**	
3.1.1	Prepare Change scripts for firewall clean-up (add new rules, remove "no hit" rules)	AC3-L4-SE-NS
3.1.2	Prepare Change for CAB	AC3-L4-SE-NS
3.2	**Firewall Change**	
3.2.1	Implement firewall changes (AH)	AC3-L4-SE-NS
3.2.2	Post Support (1 day)	AC3-L4-SE-NS
3.3	Project Management and governance	AC3-L5-PM
3.4	MILESTONE D	
4	**Firewall Review Second Pass**	
4.1	**Firewall rule Audit**	
4.1.1	Clear logs, collect new logs (4 weeks)	AC3-L4-SE-NS
4.2	**Firewall rule review**	
4.2.1	Review syslog output for "any" rules	AC3-L4-SE-NS

WBS	Task Name	Resource
4.2.2	Work with IPART to review firewall rules	AC3-L4-SE-NS,IPART
4.2.3	Work with AC3 Infrastructure team to review firewall rules	AC3-L4-SE-I,AC3-L4-SE-NS
4.3	Project Management and governance	AC3-L5-PM
4.4	**MILESTONE E**	
5	**Firewall Clean-up preparation and Change Second Pass**	
5.1	**Preparation**	
5.1.1	Prepare Change scripts for firewall clean-up (add new rules, remove "no hit" rules)	AC3-L4-SE-NS
5.1.2	Prepare Change for CAB	AC3-L4-SE-NS
5.2	**Firewall Change**	
5.2.1	Implement firewall changes (AH)	AC3-L4-SE-NS
5.2.2	Post Support (1 day)	AC3-L4-SE-NS
5.3	Project Management and governance	AC3-L5-PM
5.4	**MILESTONE F**	
6	**Firewall Review Third Pass**	
6.1	**Firewall rule review**	
6.1.1	Review syslog output for "any" rules	AC3-L4-SE-NS
6.1.2	Work with IPART to review firewall rules	AC3-L4-SE-NS,IPART
6.1.3	Work with AC3 Infrastructure team to review firewall rules	AC3-L4-SE-I,AC3-L4-SE-NS
6.2	Project Management and governance	AC3-L5-PM
6.3	**MILESTONE G**	
7	**Firewall Clean-up preparation and Change Third Pass**	
7.1	**Preparation**	
7.1.1	Prepare Change scripts for firewall clean-up (remove "no hit" rules)	AC3-L4-SE-NS
7.1.2	Prepare Change for CAB	AC3-L4-SE-NS
7.2	**Firewall Change**	
7.2.1	Implement firewall changes (AH)	AC3-L4-SE-NS
7.2.2	Post Support (1/2 day)	AC3-L4-SE-NS
7.3	Project Management and governance	AC3-L5-PM
7.4	**MILESTONE H**	
8	**Project Closeout**	
8.1	Project Implementation Review	AC3-L5-PM
8.2	Project Closure Report Review	AC3-L5-PM
8.3	Project Closure Acceptance	IPART
8.4	**MILESTONE I**	

2.4 Responsibilities, Assumptions & Constraints

2.4.1.1 AC3 Responsibilities

Item	Descriptions
AR1.	Interview key personnel to respond to the "Statement of Work".
AR2.	Collect and analyse data pursuant to the data defined in the "Project" of this document.
AR3.	Refrain from causing severe network outages.
AR4.	Notify the client in the event the engineer(s) assigned to the project are absent, ill or terminate employment.
AR5.	Provide coordination and management of project resources
AR6.	Provide engineering skills with senior experience in the network and security field.
AR7.	Any reports and information gathered by AC3 staff are the sole property of the Independent Pricing and Regulatory Tribunal (IPART).

2.4.1.2 Client Responsibilities

Item	Descriptions
CR1.	Provide access to key technical IT personnel in order to respond to site-specific requests for information.
CR2.	Provide access to basic office functions; work area, phone, copiers, faxes, etc. while AC3 personnel are on site.
CR3.	Provide administrator access to in-scope systems and devices as required.
CR4.	Provide access to any pertinent documentation that may exist.
CR5.	Provide proper levels of security to AC3 personnel such that access to phone/data areas is not hindered.
CR6.	Responsible to detect any and all suspicious activity and report to AC3 Consultant.
CR7.	Collaborate in timely manner with AC3 staff assigned to this project.
CR8.	IPART will nominate a project manage who will support the deliverables sign-off.

2.4.1.3 Exclusions

Item	Description
E1.	Any firewalls which are not provided by AC3.

2.4.1.4 Constraints

Item	Description
C1.	All work estimated as part of this SOW is calculated at the AC3 standard rates. All service work to be completed during standard business hours (Mon-Fri, 8:00am – 6:00 pm) unless otherwise stated in the Work Breakdown Structure. After hours work occurring on a Sunday or Public holiday will incur additional costs; If it changes to Sun or PH, will be increased to 2.0 and 2.5 respectively.
C2.	Variances between these assumptions and actuality may result in pricing modifications.
C3.	Where recommendations are generated from this engagement, implementation of these changes is not included in the quoted price. These changes can be made available at an extra cost.

Item	Description
C4.	Pricing in this SOW is applicable to services stated only and excludes any hardware not specifically priced in this proposal, products or media.
C5.	Any modifications to the Proposal will need to be in writing and a copy signed by both parties. Changes to this scope may result in additional charges incurred by the client.
C6.	If during the implementation of this SOW there is a product version / model change that results in a requirement for redesign or scope change, a project variance will be initiated. Scope changes will be priced accordingly and agreed by both parties before the continuation of the project.

3 PROJECT GOVERNANCE MODEL

3.1 Project Execution

AC3 will assign an AC3 Project Manager, who will be the primary point of contact for all Project related activities. The Project Manager will:

- Assign AC3 technical resources;
- Organise a project kick-off meeting;
- Circulate the Project Management Plan to stakeholders;
- Agree on implementation schedule with customer and circulate the schedule;
- Ensure that necessary AC3 change requests have been approved.
- Identify and manage variations to the agreed Scope of Work;
- Implement the solution and test to a satisfactory level as agreed by AC3 and the customer;

The following key Project Management artefacts will be developed and actively utilised throughout the project lifecycle to promote informed decision making by all parties involved:

PM Artefacts	Deliverable?
Project Management Plan	✓
Project Schedule	✓
Status Reports	✓
Risk, Issues and Action Registers	✓
Meeting Minutes	✓
Project Closure Report	✓

In this table, × means artefact is not a deliverable; ✓ means artefact is a deliverable

AC3 will provide the following technical document deliverables:

Technical Document Deliverable	Deliverable?
Low Level Design (LLD)	X
As Built Document (ABD)	X
Change Management Content	✓

In this table, × means artefact is not a deliverable; ✓ means artefact is a deliverable

Unless stated above, other project management and technical artefacts are not explicitly in scope of the project management services, but can be negotiated through variations.

4 PRICE AND PAYMENT

4.1 Pricing

- Pricing has been provided in the accompanying quotation to this SOW.
- Pricing is only valid for 30 days from the date this SOW was produced (cover page).
- Services cost will be invoiced upon milestone completion.
- Pricing for the scope of works is commitment between both AC3 and IPART to a fixed price for the complete project unless otherwise specified.

5 RECITALS

5.1 Copyright

The copyright of this document is the property of AC3 Pty Limited.

All information provided by AC3 in this response is provided on a commercial-in-confidence basis. No part of this document may be provided to any other person or organization in any form without the prior written permission of AC3.

5.2 Disclaimer

AC3 will be providing skilled engineers and resources to complete its responsibilities within the project in the timeframe outlined in this proposal. Whilst all due care and consideration has been taken in the preparation AC3 cannot take responsibility for additional products and/or service which may need to be purchased as a result of the any increases in this scope during implementation nor for product being unavailable as a result of a vendor discontinuing a line.

Further, should a product vendor update or modify its product advice after AC3 has acted upon previously current information, AC3 will not be held responsible for the cost of any further modification or update needed to re-comply with the new advice.

The information in this proposal is private and confidential and may not be copied or distributed outside its intended customer without prior permission from AC3.

5.3 Warranty

Following the successful transition of the solution into Client operational support, a warranty period of no more than 30 calendar days will commence. During the warranty period, the Customer will have access to engineering resources via the Service Desk, for any technical issues with the solution that stem from either of the following conditions:

1. *The solution has not been deployed or configured correctly, as agreed within the design documents or as otherwise agreed to during the course of the project.*
2. *The solution does not function as designed (if component has been designed by AC3).*

During the warranty period, we agree to respond and resolve any technical issues with the solution that stems from either of the two conditions described above. Any and all infrastructure and application components that were not deployed by us during the project are not within the scope of the solution warranty.

In order for the warranty to remain valid for the full 30 calendar days, Client must not make any architectural and/or system changes to the solution following the transition, up until the time that the warranty expires. The Customer is expected to utilise the solution and perform regular administrative and management tasks, but these tasks must not alter the solution architecture. Any such changes implemented during the warranty period will immediately void the warranty.

6 APPENDIX A – FIREWALL AUDIT FINDINGS

Scope	Key	Risk	Number	Issue Description	Remedy (Abridged)
Firewall 5520	FW	H	5.1.1	The firewall is soon to be unsupported and end-of-life.	As hardware support for IPART's current firewall is soon to expire,
Firewall 5520	FW	M	5.1.2	Firewall rules exist that are not configured according to best practice.	ll firewall rules should have explicitly defined strict source and destination
Firewall 5520	FW	M	5.1.3	AAA Authentication for HTTP is not configured.	Ensure that AAA authentication is provisioned for all management interfaces.
Firewall 5520	FW	M	5.1.4	Cisco ASA is not configured to use certificate revocation list.	Configure the Cisco ASA device to check the CA's revocation list with the following command:
Firewall 5520	FW	M	5.1.5	SNMP v3 is not configured.	SNMP v3 with authPriv is the only recommended operational mode
Firewall 5520	FW	M	5.1.6	IPsec VPN configuration supports IKE aggressive mode	Disable IKE aggressive mode and configure Main mode instead
Firewall 5520	FW	M	5.1.7	Default Cisco password is in use.	All device passwords should be non-default, long and complex
Firewall 5520	FW	M	5.1.8	Telnet is enabled on the system	Use a more secure alternative such as Secure Shell (SSH)
Firewall 5520	FW	L	5.1.9	Business requirements of traffic flows are not documented	Ensure that each firewall rule is documented with the business requirements and system owners
Firewall 5520	FW	L	5.1.10	Reverse path checking is not enabled.	Unicast RPF verification should be enabled to help prevent IP spoofing attacks.
Firewall 5520	FW	L	5.1.11	Local user account has been assigned privilege level 15.	Create an enable password and modify all accounts to reduce their privilege level.
Firewall 5520	FW	L	5.1.12	Insecure SSH version 1 is enabled.	Ensure that SSH version 2 is only permitted.
Firewall 5520	FW	L	5.1.13	AAA Accounting has not been configured	The following accounting functions should be configured
Firewall 5520	FW	L	5.1.14	SSH is not configured to negotiate a strong shared secret key.	Configure the Cisco ASA SSH daemon to negotiate keys with a larger bit size.
Firewall 5520	FW	L	5.1.15	Comments and names are not present for every firewall rule	Appropriate comments and names should be present for every rule defined on the firewall
Firewall 5520	FW	L	5.1.16	There is no explicit deny all rule with logging enabled.	A deny all rule should be placed at the end of each access list
Firewall 5520	FW	L	5.1.17	TLS/SSL server supports RC4 cipher suites	Disable support for RC4 cipher suites.
Firewall 5520	FW	I	5.1.18	Syslog is configured without encryption	Configure Syslog to send encrypted messages to an internal Syslog server.
Firewall 5520	FW	I	5.1.19	NTP Authentication is not configured.	Enable authentication with multiple NTP servers and set an authentication key.

Scope	Key	Risk	Number	Issue Description	Remedy (Abridged)
Firewall 550	FW	H	5.2.1	The firewall is unsupported and end-of-life.	As hardware support for IPART's current firewall has expired, it is recommended
Firewall 550	FW	M	5.2.2	Firewall rules exist that are not configured according to best practice.	All firewall rules should have explicitly defined strict source and destination addresses
Firewall 550	FW	M	5.2.3	Account policy does not exist.	Define an account policy for local user accounts
Firewall 550	FW	M	5.2.4	IPsec VPN configuration supports IKE aggressive mode	To configure IKE policy mode, include the mode statement and specify main
Firewall 550	FW	M	5.2.5	Telnet is enabled on the system.	Use a more secure alternative such as SSH
Firewall 550	FW	M	5.2.6	Junos screen attack detection and prevention is not configured securely.	It is recommended that the appropriate network level ScreenOS defence mechanisms are enabled
Firewall 550	FW	M	5.2.7	SNMP v3 is not configured	SNMP v3 with authPriv is the only recommended operational mode
Firewall 550	FW	L	5.2.8	Default username is in use.	Rename the default admin account.
Firewall 550	FW	L	5.2.9	Comments and names are not present for every firewall rule	Appropriate comments and names
Firewall 550	FW	L	5.2.10	TLS/SSL server supports RC4 cipher suites.	Disable support for RC4 cipher suites.
Firewall 550	FW	I	5.2.11	NTP authentication is disabled	Enable authentication with an NTP server and set an encrypted authentication key.
Firewall 550	FW	I	5.2.12	Login banner is not configured.	The login banner should be configured

END OF DOCUMENT PAGE

No text to be placed on this page

Activity 2-5: A current issue

Learning outcomes associated with this activity

- Access data, analyse information and synthesise knowledge.
- Think critically.
- Behave ethically.
- Integrate technical knowledge and professional skills.
- Engage in lifelong professional development.

In March 2019, Chartered Accountants Australia and New Zealand released a paper entitled *The future of trust*. The paper includes the results of a survey examining attitudes towards trust.

In this activity you are required to consider the importance of trust in relation to the role and position of Chartered Accountants in society and business.

The paper can be found at www.charteredaccountantsanz.com/news-and-analysis/insights/research-and-insights/the-future-of-trust

The executive summary begins with this statement:

> **Trust is at a record low.** Large-scale data breaches are commonplace. Distrust lies at the heart of many high-profile contemporary global issues such as climate change, globalisation and political disruption. The term "fake news" is everywhere. (page 3)

For accountants the news wasn't all bad:

> Accountants are among the most trusted professional group in Australia and New Zealand, behind doctors, engineers and teachers. (page 7)

Topic 1: Expertise and trust

In workshop 1, activity 1-8, part b, you discussed the possible impacts of artificial intelligence (AI) and changes in technology on the accounting profession. Much of that discussion covered the types of work accountants will perform in the future, and the types that will be automated and/or performed by 'cognitive computing' - technology based on AI. *The future of trust* reports that 77% of survey respondents 'thought new technology would have a significant impact' on the accounting profession. (page 11)

The future of trust outlines the connection between expertise and trust:

> Trust evolves, but trust in expertise is constant. One explanation is that it is not the expert who speaks but his or her expertise. Speaking as an expert allows for greater objectivity in messaging. (page 8)

Question 1: As more and more compliance and technical work is performed by AI, what will be the nature of the expertise provided by accountants?

Question 2: How will expertise be displayed by accountants, and how will expertise be identified by clients?

Topic 2: The trust paradox

> Society faces a trust paradox as people become increasingly dependent on, and simultaneously distrustful of, digital technology. Online information is not always reliable, social media is vulnerable to manipulation and personal data may not be private. Despite compelling evidence to distrust digital technology, people are using it even more intensively in most elements of daily life. (page 11)

Question 3: Do you trust technology in your personal life? In your professional life? Which parts do you trust and which parts do you not trust and why?

Topic 3: Trust in world of new technology

> Artificial intelligence and blockchain technology potentially provide significant opportunities for innovation in the field of audit, enabling the real time extraction and analysis of data, paving the way for 'real-time' auditing. This will create greater trust between an auditor and their client. (page 11)
>
> In simple terms, a blockchain is a centralised ledger. This emerging technology claims to be able to do away with trust as we know it, replacing it with a digital trust via a centralised approach to accounting. This peer-to-peer platform promises to remove the need for trusted intermediaries such as the government or banks, allowing users to transact directly. (page 11)

Question 4: Will audit clients accept this new technology? Does accepting this new technology mean that the users of financial statements trust the outputs of the new system?

Topic 4: Loss of trust

The future of trust discusses behaviours that are most likely to reduce trust in a number of groups, including accountants.

The survey respondents identified 'being dishonest' as the behaviour most likely to reduce trust in accountants, with 'behaving unethically' the second most likely behaviour by accountants that will see trust in accountants decline. (page 10)

Question 5: How is being dishonest different from being unethical?

Topic 5: On trust

Question 6: What does trust look like for you?

Required
1. Review the paper *The future of trust.* 2. Answer each of the above six (6) question – your answers do not need to be long, just well-thought through and considered. 3. Be prepared to discuss your answers in workshop 2.

Note: You are not required to follow the Rubric – analysis and evaluation.

T

Australian Centre for Advanced Computing and Communications

STATEMENT OF WORK

Delegated Access and Password Policies

for

IPART

Document Reference: QW184947
Version Number: 1.0
Published Date: Tuesday, 19 March 2019

Gerald Elizalde

Solutions Architect | AC3 Pty Limited

P +61 2 9199 0875

gerald.elizalde@ac3.com.au

Level 8 East, 8 Central Avenue, Eveleigh NSW 2015 | ABN 27 095 046 923 | 02 9199 0888 | www.AC3.com.au

NOTICES

ABN 27 095 046 923

DOCUMENT CREDENTIALS

Client Details

Name:	Mike Webber
Position:	ICT Leader and Chief Procurement Officer
Client:	IPART
Email:	Mike_Webber@ipart.nsw.gov.au

AC3 Contact Details

We welcome any enquiries regarding this document, its content, structure or scope. These should be directed to:

Name:	Briant Kareroa
Position:	Sales Manager - NSW Public Sector, Government Sales
Telephone:	02 9199 0856
Mobile:	0420 936 712
Email:	Briant.Kareroa@ac3.com.au

Document Control

Document Reference

Department:	Consulting
Document Name:	IPART Network Architecture Framework Statement of Work

Preparation

Version	Date	Change	By (Name, Position)
1.0	18-Mar-2019	Initial release	Gerald Elizalde, Solutions Architect

Revision History

Version	Date	Revision	By
0.1	18-Mar-2019	First Draft	Gerald Elizalde
1.0	18-Mar-2019	Final Approval	John Seretis

Reviewers

Version	Date	Name, Position
0.1	15-Mar-2019	John Seretis, Solutions Architect

Approvals

Version	Date	Name, Position
1.0	15-Mar-2019	John Seretis

Client Distribution

Version	Date	Name, Position
1.0	15-Mar-2019	Mike Webber, ICT Leader and Chief Procurement Officer

Related Documents

Reference	Name
QW194947	IPART - Delegated Access and Password Quote v1.0.pdf

Classification

Classification	Description
Commercial in Confidence	A document shared with specific customer/s

TABLE OF CONTENTS

1 Executive Summary 6
1.1 Document Purpose 7
2 Project Summary 8
2.1 Background 8
2.2 Objectives 8
2.3 Scope 9
2.3.1 In Scope 9
2.3.2 Deliverables 11
2.3.3 Assumptions, Exclusions, Client Responsibilities 11
2.3.3.1 Assumptions 11
2.3.3.2 Exclusions 12
2.3.3.3 Client Responsibilities 12
3 Project Approach 14
3.1 Overview 14
3.2 High Level Solution Design 16
3.2.1 Overview 16
3.2.2 Design Brief 16
3.2.2.1 Requirements Specification 16
3.2.2.2 High Level Design 17
4 Project Management Approach 22
4.1 Project Control Register 22
4.2 Risks 22
4.3 Issues Management 22
4.4 Change Management (Project Variation) 22
4.5 Communications Management 23
5 Schedule and Pricing Summary 24
5.1 High Level Project Schedule 24
5.2 Commencement 25
5.3 Variations 26
6 Recitals 27
6.1 Copyright 27
6.2 Disclaimer 27
6.3 Warranty 27

1 EXECUTIVE SUMMARY

Engagement Name	IPART – Delegated Access and Password Policies
Engagement Number	QW194947
Summary of Scope and Objectives	**Scope Summary:** 1. Design and Implement Delegated Access 2. Design and Implement Password Policies **The primary objectives of this project are to:** • Resolve the current issues on Access Delegation • Resolve the current issues on Password Policies • Adopt best practices on Access Delegation • Adopt best practices on Password Policies
Summary of Deliverables	• Design and Implement best practices Access Delegation • Design and Implement best practices on Password Policies • Document how security audit items have been addressed • Handover to BAU • Project Implementation Review
Planned Start Date	TBA
Planned Completion Date	TBA
Project Sponsor	Mike Webber
AC3 Project Manager	TBA

Table 1 Executive Summary

1.1 Document Purpose

This Statement of Work (SOW) has been prepared with the purpose of defining a solution that meets defined requirements and describing the scope of work proposed to implement that solution.

Further information regarding any aspect of this scope of work details will be within the Project Documentation or equivalent documentation upon sign-off of the Scope of Work.

2 PROJECT SUMMARY

2.1 Background

IPART has sought a proposal for a Delegated Access and Password Policy design and implementation. This is to help address the compliance requirement from an external audit conducted in the current systems and infrastructure.

The following requested items are to be included as part of the requirement(s):

- Delegated Access to Systems
- Best Practice on Access Delegation
- Best Practice on Password Policy

2.2 Objectives

The primary objectives of this project will be to:

- Resolve the current issues on Access Delegation:
  a. Domain User Account used as Service Accounts
  b. Domain Administrators logon to any workstation
- Resolve the current issues on Password Policies:
  c. Local Administrator password used across multiple systems
  d. Weak passwords on Privileged Accounts
  e. Use of default passwords
  f. Passwords unchanged for more than 5 years
  g. Reversibly encrypted plain text passwords in memory is enabled
  h. Password based authentication is in use for SSH
- Design and Implement a solution to resolve the issues
- Adopt best practices on Access Delegation
- Adopt best practices on Password Policies

Specifically addressing the following items from the security audit:

Ref. No	Subject	Requirement
5.1.2	Privileged account passwords are weak and shared.	All users should understand password reuse issues and the risk to the organisation
5.1.3	Default and weak application passwords are in use.	All user accounts should have strong passwords assigned which is reinforced by a strong account policy.
5.1.4	IPART network is susceptible to the Pass-the-Hash (PtH) attack.	To effectively mitigate PtH and similar attacks, any change must deny attackers the ability to perform
5.1.5	Account, password and privilege management is inadequate.	All accounts should have passwords which are enforced by a strict password policy.
5.1.12	KRBTGT user account password has not been changed since 2010.	Raising the Domain Functional Level (DFL) from Windows 2003 to higher (2008, 2008 R2, 2012 or 2012 R2) changes the KRBTGT account password.
5.1.14	Common Local Administrator password is in use across numerous systems.	Local 'Administrator' (SID 500) accounts should be renamed and disabled

Ref. No	Subject	Requirement
5.1.15	Domain administrators can logon to any workstation	DA accounts must be restricted to only be able to login to Domain Controllers.
5.1.29	Service accounts are running through a domain user account.	Wherever possible, the following best practices should be followed:
5.1.33	Domain Administrators do not have a separate password policy.	Configure an independent password policy for higher privileged accounts
5.1.34	Reversibly encrypted plain-text passwords in memory is enabled.	Ensure users always close the session (log off).
5.1.37	Password based authentication is in use for SSH	It is recommended to only allow SSH authentication using keys.

2.3 Scope

2.3.1 In Scope

The following considered items which are required for this project:

Concept and Define

- Project Initiation
- Project Brief with SA

Plan

- Prepare Project Artefacts
- Prepare Draft PMP
- Develop Draft Schedule
- Kick Off Meeting

Design

- Customer Design Workshops
- Develop Low Level Design
- Internal Design Workshop
- Draft Low Level Design Document
- Internal Review of Low Level Design
- Amendment of Low Level Design
- Deliverables Sign Off

Construct

- Delegated Access
    - Creating of Roles for Active Directory
    - Creating of Roles for Network Devices
    - Creating of Roles for Applications
    - Configure defined Role Responsibility and assigning of Access by Function - Active Directory
    - Configure defined Role Responsibility and assigning of Access by Function - Network Devices
    - Configure defined Role Responsibility and assigning of Access by Function - Database
    - Configure defined Role Responsibility and assigning of Access by Function - Web Services
    - Configure defined Role Responsibility and assigning of Access by Function - File Services
    - Configure defined Role Responsibility and assigning of Access by Function - Sharepoint and other Applications
- Renaming of Local Administrator Accounts
    - Per Server Role / Local Administrators
    - End User Device / Local Administrators
- Establish Delegation Model
- Establish Audit Policy by Operating System
- Organisation Unit Security Model
    - Reorganisation of OU's
    - Create OU's based on defined Security Model
    - Reorganise OU's and GPO Re-assignment
- Create Least Privilege Administrative Model
- Domain Functional Level - Raise
    - Verify all Domain Controllers comply to the minimum Domain Functional Level prerequisites
    - Verify all applications can work with the target Domain Functional Level
    - Execute the Raising of the Domain Functional Level
- Password Policies
    - Implement Fine Grain Password Policy for Identified Security Groups
    - Implement GPO based Password Policy for identified GPO's
- UAT
- AC3 Support
- UAT Acceptance

Commission

- As Built documentation
- Post Implementation review
- Transition to BAU

- Deliverables Sign Off
- Project Closure Report

2.3.2 Deliverables

Deliverable	Description	Due Date
Project Management Plan	A document outlining how the project will be managed throughout the project lifecycle from execution, monitoring, and controlling through to closure.	Phase 2, during Plan Phase
SOW Creation	Creation of SOW which will define all the work that is required to complete the project.	Initial Phase
Project Schedule	Gantt chart outlining work breakdown structure, timeline, dependencies and resources.	Phase 2, during Plan Phase
Technical Infrastructure Design	Detailed Design document outlining the proposed technical solution.	Phase 3, during Design Phase
As Built Documentation	A revised design provided by AC3 based on the implemented solution that reflects the technical configurations and installed components.	At conclusion of project, Phase 5
Post Implementation Review (PIR)	A document to facilitate the evaluation of the project against the defined objectives. It determines how effective the project was managed with the view to capture improvements from lessons learnt for future use.	At conclusion of project, Phase 5
Acceptance Certificate	Document providing approval from the IPART which signifies completion of project and acceptance of all deliverables.	At conclusion of project, Phase 5

Table 2 Deliverables

Actual due dates for deliverables will be provided upon Project Kick Off where the Project Schedule will be presented for the client to review and accept as the first baseline.

2.3.3 Assumptions, Exclusions, Client Responsibilities

2.3.3.1 Assumptions

Item	Description
A1	The resources required to complete the project as defined in this document will be provided during normal business hours only, unless explicitly defined in the work breakdown;
A4.	Any infrastructure requirements change will be a subject of variation;
A5.	All Domain Controllers must meet the minimum requirements of the target Domain Functional Level;
A6.	Application compatibility with the target Domain Functional Level must be verified by the customer;
A7.	Remediation or Upgrade or Application to comply with the target Domain Functional Level is to be conducted by IPART.

Item	Description
A8.	AC3 will not be responsible for Application failure which AC3 does not support as part of the managed services agreement

Table 3 Assumptions

2.3.3.2 Exclusions

Item	Inclusion Descriptions
E1.	Any operating system / application configuration not listed explicitly in the above Inclusions or scope of work
E2.	Any configuration or functionality not explicitly listed in the Inclusions
E3.	Any activity not listed in the Inclusions
E4.	In-depth user training, unless explicitly noted otherwise
E5.	Any client workstation or server application configuration is out of scope of work.
E6.	Any application installation or packaging is out of scope of work.
E7.	Any application testing is a responsibility of the client.
E8.	Installation and configuration of any hardware not stated to be in scope.
E9.	Troubleshoot any existing issues with user accounts, domain accounts, service accounts, device accounts. If any issues are encountered, the account in question will be replaced.

Table 4 Exclusions

2.3.3.3 Client Responsibilities

Item	Inclusion Descriptions
C1.	The client retain responsibility for carrying out all Application related activities (Discovery, Assessment, Re-configuration and Testing), as required.
C2.	Log any required change requests into the appropriate customer change request system(s)
C3.	Provide access to key technical personnel in order to respond to requests for information or access to systems
C4.	All configuration changes on the applications;
C5.	Run the change and release management process
C6.	Prepare and Execute User Acceptance Testing plans;
C7.	Manage third party vendors;
C8.	Provide any licences not covered under AC3's service offering;
C9.	Facilitate and Coordinate communications to the client's business and customers:
C10.	Coordinate functional testing and user acceptance testing
C11	The client retains responsibility for all communications with its End Users;
C12	The client retains responsibility for all software that is not explicitly included within the accompanying quotation;

Item	Inclusion Descriptions
C13	The client will coordinate vendor engagement for any published application issue, if required;
C14	AC3 will be provided the necessary access to accommodate AC3's responsibilities for management and support of the client's platform;

Table 5 Client Responsibility

3 PROJECT APPROACH

3.1 Overview

The high level approach for delivering this project will be via the initiate phase and the four execution phases.

The following activities will be completed in the following order:-

Phase 1 and 2	• Project Initiation • Discovery of requirements led by IPART Project Manager • Planning and Scheduling
Client Responsibilities	• Work with AC3 to identify key technical stakeholders to be present at the Requirements Confirmation and Design Workshop. • Identify dates and a meeting location for the Requirements Confirmation and Design Workshop
AC3 Deliverables	• Project Management Plan • Project Schedule

Table 6 Phase 1 and 2

Phase 3	• Solution Design • Design Workshops
Client Responsibilities	• Provide necessary information such as relevant as built documentation, policies, standards and requirements. • Supply feedback on the draft Design document within five (5) business days of reception. • Allocate resources for the Design Workshops • List of identified issues identified and tracked
AC3 Deliverables	• Design Document • List of identified issues identified and tracked

Table 7 Phase 3

Phase 4	• Implement Delegated Access Best Practices • Implement Password Policy Best Practices
Client Responsibilities	• Supply any access required to the environment • Supply accounts required to the current domain • Coordinate and supply key technical stakeholders to be available for the Construct Phase • Communicate with End-users for any scheduled downtime • List of identified issues identified and tracked
AC3 Deliverables	• Complete implementation of Delegated Access • Complete implementation of Password Policies • Complete UAT • List of identified issues identified and tracked

Table 8 Phase 4

Phase 5	• ABD Documentation • Handover to Support • Project Closure
Client Responsibilities	• Coordinate and supply key technical stakeholders to be available for Sign Off
AC3 Deliverables	• Complete UAT • ABD Documentation • Post Implementation Review • Acceptance Certificate for Sign Off

Table 9 Phase 5

3.2 High Level Solution Design

3.2.1 Overview

AC3 will conduct this scope of work in accordance with IPART's defined requirements. IPART requested for professional services to implement an access delegation model and password policies within the existing ICT environment, in order to ensure that all administrative staff has the appropriate level of access to perform their assigned tasks, whilst restricting privileged access where it is not required.

3.2.2 Design Brief

3.2.2.1 Requirements Specification

IPART and AC3 have worked closely to define the required service specifications for the Delegated Access and Password Policies.

The services are reflected in the high-level design provided below. The solution will be provided to IPART with the Services obligation of AC3 as defined in this Statement of Work.

The requirements that will be addressed by the design are the following:

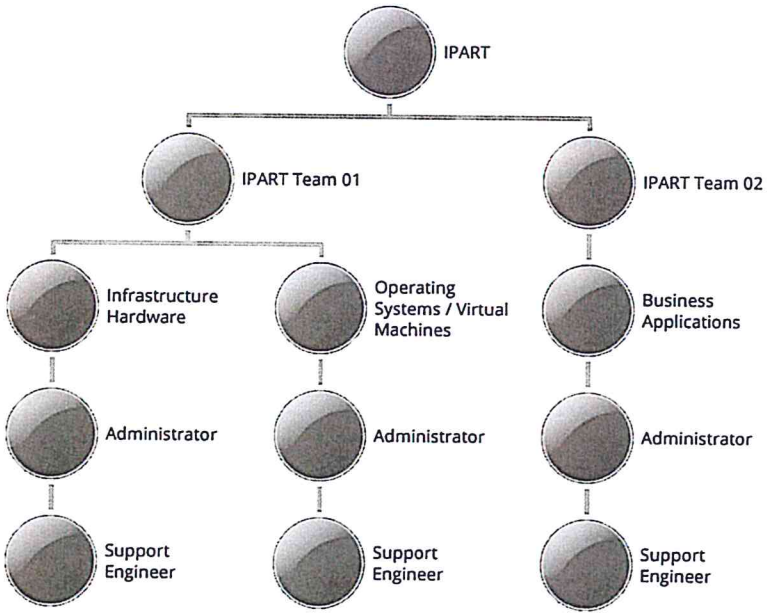
i. Access Delegation Best Practices
j. Password Policy Best Practices

3.2.2.2 High Level Design

An Access Delegation best practices model will be adopted in the IPART environment. The goal is to provide privileged access only to systems that the account needs access to. Otherwise, it will be limited or prevented access to systems or devices that is not required.

Hierarchy Definition

AC3 will work with IPART to define the hierarchy for the IT Systems, Projects, and Teams that are within the organisation. This will help to define how the access control and permissions will be managed. The following diagram is a proposed model which will be updated and defined during the design phase.



Delegated Access

AC3 will work with IPART to define roles, purpose, responsibilities and access provided. This will facilitate in a delegated access model to identify which type of roles would have what type of access.

This is a high-level design example which will be updated based on the workshop and design agreement between AC3 and IPART.

The model will follow Least Privilege Administrative access. Additional account names may be added which is to be defined in the design phase.

Role	Purpose / Responsibilities	Access	Owner
Enterprise Administrator	Forest Top Level Administrator	Top Level Access	TBC (ie. Head of IT, CIO) Two individuals will be assigned to this account.
Domain Administrators	Domain Level Administrator	Domain Level Access	Owner to be defined in the Design Workshop
Backup Operators	Run Backup Jobs / Service in Systems	Backup Operator	Owner to be defined in the Design Workshop
Local Administrators	Local Machine Administrator	Local Machine Administrative Access	Owner to be defined in the Design Workshop
Service Account	Used to run services for specific systems or applications	Application service	Owner to be defined in the Design Workshop
Device Administrator	To administer physical devices	Physical Devices	Owner to be defined in the Design Workshop
Custom Role 01	Responsibilities to be defined in the Design Workshop	Access to be defined in the Design Workshop	Owner to be defined in the Design Workshop
Custom Role 02	Responsibilities to be defined in the Design Workshop	Access to be defined in the Design Workshop	Owner to be defined in the Design Workshop
Custom Role 03	Responsibilities to be defined in the Design Workshop	Access to be defined in the Design Workshop	Owner to be defined in the Design Workshop
KRBTGT			

Table 10 Role Definition and Access

Organisation Unit Security Modelling will also be adopted as part of the design for IPART's Delegated Access requirement. There will be creation of new OU's and restructuring of organisational units. Below are required in this process:

- Creation of new Organisation Units in Active Directory
- Creation of new Security Groups in Active Directory
- Creation of new GPO for Delegated Access
- GPO re-assignment

Additional local administrator account names may be added which is to be defined in the design phase.

Part of the Delegated Access design will be the "Renaming of Local Administrator Accounts". This will be done based on the following:

Machine Type	Definition	Local Administrator Name
Core Servers	The Local Administrator for Core Servers will be provided a new name. This will only allow the Local Administrator access to its own local machine. It will have a different set of passwords from the end-user devices and network devices.	This will be defined in the Design phase of the project.
Network Devices	The Local Administrator for Network Devices will be provided a new name. This will only allow the Local Administrator access to its own device. It will have a different set of passwords from the end-user devices and Core Servers.	This will be defined in the Design phase of the project.
End-User Devices	The Local Administrator for End-User Devices will be provided a new name. This will only allow the Local Administrator access to its own device. It will have a different set of passwords from the Network Devices and Core Servers. Laptops and Desktops are defined as End-User devices in this project.	This will be defined in the Design phase of the project.

Table 11 Local Administrator

Service Accounts will be created per application, device, or system that requires a service account. Service accounts will not be allowed to be used for systems that is not under its defined access.

It is very common for applications and services to have an in-built requirement to run under the context of a privileged account. These accounts are typically provisioned within the core directory service of the

organization (eg Active Directory), and then configured within the application and/or Service. Accounts used for this purpose are generally referred to as 'Service Accounts'.

Additional service account names may be added which will be defined in the design phase.

Service Account Name	Definition	Access
SVC_Database	The account will only be used to run a Database Service.	Database Servers
SVC_Webservice	The account will only be used to run a web service	Web Servers
SVC_Middleware	The account will only be used to run a middleware	Middleware
SVC_FileServer	The account will only be used to run a File Server	File Servers
SVC_Sharepoint	The account will only be used to run a Sharepoint	Sharepoint Servers
SVC_App01	The account will only be used to run Custom Application 01	Custom Application 01
SVC_App02	The account will only be used to run Custom Application 02	Custom Application 02
SVC_App03	The account will only be used to run Custom Application 03	Custom Application 03

Table 12 Service Account

To help detect a compromise/breach on systems and user accounts, Audit Policies will be implemented. The recommendation and best practice is to create an audit policy for each Operating System.

The following will be defined per Operating System:

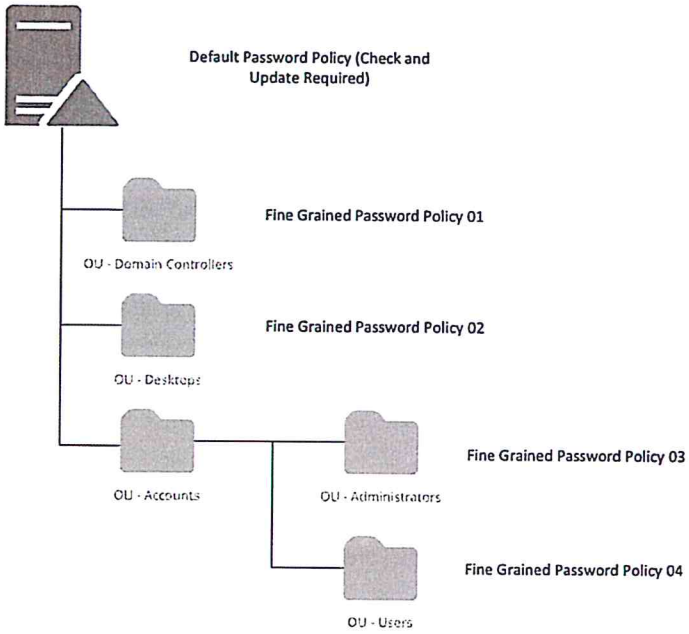
- Account Logon
- Account Management
- Detailed Tracking
- DS Access
- Logon and Logoff
- Object Access
- Policy Change
- Privilege Use
- System
- Global Object Access Auditing

Password Policies

In most environments, Password policies are often left with the default configuration (ie. Active Directory, Devices). As part of this project, AC3 will work with IPART to define new Password Policies that would help support IPART in its compliance requirement(s).

The approach for the password policies will be based on the best practices in Enterprise environments to help secure the environment and lower the risk of compromised accounts and passwords. The Fine Grained

Password Policy will be adopted. This however has a minimum requirement for Operating Systems and the Domain Functional Level.



4 PROJECT MANAGEMENT APPROACH

4.1 Project Control Register

The AC3 project manager will use a project control register along with a WBS Schedule to manage the day to day activities of the project. The project control register includes the following registers:

- Actions register - Tracks actions that have been assigned within the project
- Risk registers – Contains risks associated with this project and estimates the impact to the project should it occur
- Issues register – Collects information about Issues (actualised risk) that have occurred in the project
- Configuration Management & Version Control –Contains details about current document including the most recent version.
- Change Log – Cover variations to the project such as scope change, additional works, and change in requirements
- Leave register – Tracks the leave of project staff, along with their replacements for the duration of the leave.
- Project Notes – General information around the project

4.2 Risks

All risks will be managed according to Services' risk management policies and procedures. Where necessary, AC3 will employ its own risk management policies and procedures.

Any risks identified will be documented in the Risk register as part of the Project Control Register held by the AC3 Project Manager. All risks will be continually monitored throughout the project and their status updated in the risk log as appropriate. Any changes made in the risk log will be raised to the IPART Project Manager as agreed.

4.3 Issues Management

All issues will be managed according to the established issue management process for the project.
An Issues Register will be maintained by the AC3 Project Manager as part of the Project Control Register. All recorded issues will be assigned for resolution, tracked and reported on during the engagement as agreed between IPART and AC3.

4.4 Change Management (Project Variation)

Changes to scope, cost, time and quality will be managed through formal change control.
All Change Requests will be submitted to the IPART for approval and adjustment of baseline where applicable.

The Change Request will:

- Identify the proposed changes to the project scope, design, budget or schedule or any combination of these.
- Allow distribution to affected parties for evaluation, review, comment and approval or rejection.
- Identify reasons or justification for change request, and provide opportunity for comment, financial and schedule impacts, and identify responsibility for implementing the change.

Where the change has an additional financial impact (i.e. increase in price), client approval must be given in the form of a purchase order.

IPART approval of change requests is to be done by a nominated IPART representative, or Change Sponsor, and final acceptance / approval will be deemed to be received when issues have been resolved, and the change request form has been approved by the IPART.

4.5 Communications Management

The AC3 Project Manager will prepare and deliver the following communications during the engagement – these communications will be integrated as part of the IPART Practice Management System project (except kick-off):

Communication	Schedule	Audience	Agenda
Kick Off Meeting	Project Start	Project Team, Vendors and Stakeholders	Objectives Deliverables Schedule Risks Issues
Project Status Meeting	Weekly	Project Team, Vendors and Key Customer	Objectives Deliverables Schedule Risks Issues
Project Status Meeting Minutes	Weekly	Project Team, Vendors and Key Customer	N/A
Project Status Reports	Weekly	Project Team, Vendors and Key Customer	N/A

Table 13 Communication Management

5 SCHEDULE AND PRICING SUMMARY

5.1 High Level Project Schedule

A detailed Project Plan and Schedule will be established, however, the broad strategy for the implementation comprises the following activities within the indicative schedule provided.

Task Name	Resource Initials
IPART_Delegated Access and Password	
Concept and Define	
Project Initiation	
Quote Received	Customer
SoW Received	Customer
Purchased Order Received	P-5-PMO
Client Contacted	P-5-PMO
Project Brief with SA	P-5-PMO,P-5-SA
Milestone - Concept and Define Complete	
Plan	
Prepare Project Artefacts	P-5-PMO
Prepare Draft PMP	P-5-PMO
Develop Draft Schedule	P-5-PMO
Draft Plan Complete	P-5-PMO
Kick Off Meeting	Customer,P-4-SIE,P-5-PMO
Milestone - Planning Complete	
Design	
Customer Design Workshop (3 x Sessions)	Customer,P-4-SIE
Develop Low Level Design	
Internal Design Workshop	P-4-SIE,P-5-PMO
Draft Low Level Design Document	P-4-SIE
Internal Review of Low Level Design	P-5-SA
Amendment of Low Level Design	P-4-SIE
Deliverables Review	
Deliverables Review	P-5-PMO
Deliverables Amendments	P-4-SIE,P-5-PMO
Deliverables Sign Off	
Low Level Design	Customer
Milestone - Design Complete	
Construct	
Build	
Delegated Access	
Creating of Roles for Active Directory	P-4-SIE
Creating of Roles for Network Devices	P-4-SNE
Creating of Roles for Applications	P-4-SIE
Configure defined Role Responsibility and assigning of Access by Function - Active Directory	P-4-SIE
Configure defined Role Responsibility and assigning of Access by Function - Network Devices	P-4-SNE
Configure defined Role Responsibility and assigning of Access by Function - Database	P-4-DBA

Task Name	Resource Initials
Configure defined Role Responsibility and assigning of Access by Function - Web Services	P-4-SIE
Configure defined Role Responsibility and assigning of Access by Function - File Services	P-4-SIE
Configure defined Role Responsibility and assigning of Access by Function - Sharepoint and other Applications	P-4-SIE
Renaming of Local Administrator Accounts	
Per Server Role / Local Administrators	P-4-SIE-AA
End User Device / Local Administrators	P-4-SIE-AA
Establish Delegation Model	P-4-SIE
Establish Audit Policy by Operating System	P-4-SIE
Organisation Unit Security Model	
Reorganisation of OU's	
Create OU's based on defined Security Model	P-4-SIE
Reorganise OU's and GPO Re-assignment	P-4-SIE-AA
Create Least Privilege Administrative Model	P-4-SIE
Domain Functional Level - Raise	
Verify all Domain Controllers comply to the minimum Domain Functional Level prerequisites	Customer,P-4-SIE
Verify all applications can work with the target Domain Functional Level	Customer,P-4-SIE
Execute the Raising of the Domain Functional Level	Customer,P-4-SIE-AA
Password Policies	
Implement Fine Grain Password Policy for Identified Security Groups	P-4-SIE
Implement GPO based Password Policy for identified GPO's	P-4-SIE
Customer UAT Environment	
UAT	Customer,P-4-SIE
AC3 Support	P-4-SIE
UAT Acceptance	Customer
Milestone - Construct Complete	
Commission	
Finalise As Built documentation	P-4-SIE
Post Implementation review	P-5-PMO
Develop Project Closure Report	P-5-PMO
Transition to BAU	P-4-SIE
Deliverables Review	
Deliverables Review	Customer,P-5-PMO
Deliverables Amendments	P-4-SIE
Deliverables Sign Off	
As Built	Customer
Project Closure Report	Customer
Milestone - Commission Complete	

Table 14 Draft Project Schedule

5.2 Commencement

Commencement of this work is subject to provision of a Customer Purchase Order for the One-Off Fee contained in the accompanying Quotation and Customer approval of the Contract Services Variation indicated by the quoted on-going services. In providing the Purchase Order and/or approved Contract Services Variation the Customer approves the commencement of work and acknowledges its liability for the charges detailed in the accompanying quotation.

5.3 Variations

Variations to this Statement of Work will not be recognised and cannot be made without written approval of both the Customer Owner and the AC3 Approver.

6 RECITALS

6.1 Copyright

The copyright of this document is the property of AC3 Pty Limited.

All information provided by AC3 in this response is provided on a commercial-in-confidence basis. No part of this document may be provided to any other person or organization in any form without the prior written permission of AC3.

6.2 Disclaimer

AC3 will be providing skilled engineers and resources to complete its responsibilities within the project in the timeframe outlined in this proposal. Whilst all due care and consideration has been taken in the preparation AC3 cannot take responsibility for additional products and/or service which may need to be purchased as a result of the any increases in this scope during implementation nor for product being unavailable as a result of a vendor discontinuing a line.

Further, should a product vendor update or modify its product advice after AC3 has acted upon previously current information, AC3 will not be held responsible for the cost of any further modification or update needed to re-comply with the new advice.

The information in this proposal is private and confidential and may not be copied or distributed outside its intended customer without prior permission from AC3.

6.3 Warranty

Following the successful transition of the solution into Client operational support, a warranty period of no more than 30 calendar days will commence. During the warranty period, the Customer will have access to engineering resources via the Service Desk, for any technical issues with the solution that stem from either of the following conditions:

1. *The solution has not been deployed or configured correctly, as agreed within the design documents or as otherwise agreed to during the course of the project.*
2. *The solution does not function as designed.*

During the warranty period, we agree to respond and resolve any technical issues with the solution that stems from either of the two conditions described above. Any and all infrastructure and application components that were not deployed by us during the project are not within the scope of the solution warranty.

In order for the warranty to remain valid for the full 30 calendar days, Client must not make any architectural and/or system changes to the solution following the transition, up until the time that the warranty expires. The Customer is expected to utilise the solution and perform regular administrative and management tasks, but these tasks must not alter the solution architecture. Any such changes implemented during the warranty period will immediately void the warranty.

END OF DOCUMENT PAGE

No text to be placed on this page

AC3

Australian Centre for Advanced Computing and Communication

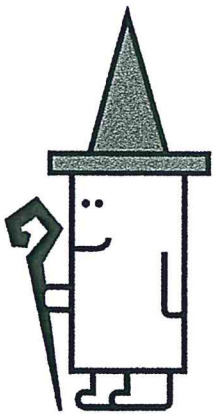
STATEMENT OF WORK

Network Architecture Framework

For

Independent Pricing and Regulatory Tribunal (IPART)

IPART
Independent Pricing and Regulatory Tribunal
New South Wales



NOTICES

DOCUMENT CREDENTIALS

Client Details

Name:	Mike Webber
Position:	ICT Leader and Chief Procurement Officer
Client:	Independent Pricing and Regulatory Tribunal (IPART)
Email:	Mike_Webber@ipart.nsw.gov.au

AC3 Contact Details

We welcome any enquiries regarding this document, its content, structure or scope. These should be directed to:

Name:	Briant Kareroa
Position:	Sales Manager - NSW Public Sector, Government Sales
Telephone:	02 9199 0856
Mobile:	0420 936 712
Email:	Briant.Kareroa@ac3.com.au

Document Control

Document Reference

Department:	Consulting
Document Name:	IPART Network Architecture Framework Statement of Work

Preparation

Version	Date	Change	By (Name, Position)
1.0	15-Mar-2019	Initial release	Sergey Nasonov, Solutions Architect

Reviewers

Version	Date	By (Name, Position)
1.0	15-Mar-2019	John Seretis, Solutions Architect

Approvals

Version	Date	By (Name, Position)
1.0	15-Mar-2019	John Seretis, Solutions Architect

Distribution

Version	Date	To	Position, Organisation
1.0	15-Mar-2019	Mike Webber	ICT Leader and Chief Procurement Officer, IPART

Classification

Classification	Description
Commercial in Confidence	A document shared with specific customer/s

Related Documents

Document Name	Reference Number	Organisation
IPART Network Architecture Framework QUOTE v1.0.pdf	QW194948	AC3

Sign-Off

Signed	Name, Position

TABLE OF CONTENTS

1 Executive Summary 6
2 Solution Overview 7
2.1 Floor Switches Replacement 7
2.1.1 Floor Switching Network Refresh Design 7
2.1.1.1 Solution Overview 7
2.1.1.2 Cisco Catalyst 9300 Capability Overview 8
2.1.2 Floor Wireless Network Refresh Design 10
2.1.3 Project Management 11
2.1.4 AC3 Project Principles & Lifecycle 11
2.1.5 Project Phases 12
2.1.5.1 PHASE 1 – DESIGN – Milestone A 12
2.2 Work Breakdown Structure 13
2.3 Responsibilities, Assumptions & Constraints 13
2.3.1.1 AC3 Responsibilities 13
2.3.1.2 Client Responsibilities 14
2.3.1.3 Exclusions 14
2.3.1.4 Assumptions 14
3 Project Governance Model 16
3.1 Project Execution 16
4 Price and Payment 18
4.1 Pricing 18
5 Recitals 19
5.1 Copyright 19
5.2 Disclaimer 19
5.3 Warranty 19

1 EXECUTIVE SUMMARY

Independent Pricing and Regulatory Tribunal (IPART) is an NSW State Agency company with headquarters based in Sydney CBD. IPART provides independent regulatory decisions and advice to protect the ongoing interests of the consumers, taxpayers and citizens of NSW.

AC3 specialises in the design, implementation and management of information technology focused on meeting constantly evolving user needs and the environment landscape. As a managed services provider, IT consultancy, service delivery and product procurement organisation, AC3 works closely with clients to understand their business and then looks for opportunities to streamline and secure the underlying technology.

IPART have undertaken an initiative to refresh their ageing Local Area Network (LAN) and Wireless Local Area Network (WLAN) and perform associated migration activities. As part of new network solution development, IPART requested AC3 to develop new LAN and WLAN design for IPART office at 2-24 Rawson Pl, Sydney NSW 2000, addressing the requirements below:

Key IPART Requirements:

- Develop high-density WLAN design aimed to enable wire-free operation for all IPART staff, contractors and guests
- WLAN should be able to support up to 450 devices at the same time
- WLAN should be able to support Voice and Video over WLAN
- Produce LAN and WLAN Bill of Materials to support intended deployment
- Produce WAP placement map to ensure optimal coverage and performance
- Replace all floor switches IPART have located on Level 16, including the switch that links Audio Visual systems to IPART network. The number of switches should be reduced with the aim to support wired-only clients (desk IP phones, WAPs, printers)

AC3 are proposing to use a structured process based on the following two (2) phases in order to efficiently address the requirements identified above.

Phase 1 - Design - Network Architecture Framework:

Creation of a Network Architecture Framework document which will outline the proposed end-state for a consolidated and upgraded environment LAN and WLAN (with the latest supported software recipe), paired with a solid migration plan which can immediately be implemented. The final document set will include Low Level Wired and Wireless Network Design, accompanying network hardware BOM, cabling costs and SOW to implement updated network as per LLD.

This framework document will be created in consultation with IPART through design workshops and will also seek to capture any potential software or hardware expenditure that will be required by IPART. **This SOW covers the implementation of this phase of the proposed process.**

Phase 2 - Implementation - LAN and WLAN Upgrade:

In the second phase, the core components of the Network Architecture Framework would be implemented:

1. LAN refresh
2. WLAN refresh
3. SOE tuning to support new wireless-only environment

2 SOLUTION OVERVIEW

2.1 Floor Switches Replacement

IPART has made a decision to modernise its access switching to migrate away from legacy switching and support Multi-Gigabit Ethernet (mGig) speeds for newly deployed access points. The current switching infrastructure is comprised of 6 Meraki MS320-48FP access switches as well as number of legacy Cisco Catalyst 3560 switches which will be replaced by Cisco Catalyst 9300 switches

2.1.1 Floor Switching Network Refresh Design

2.1.1.1 Solution Overview

The following diagram illustrates the intended deployment.

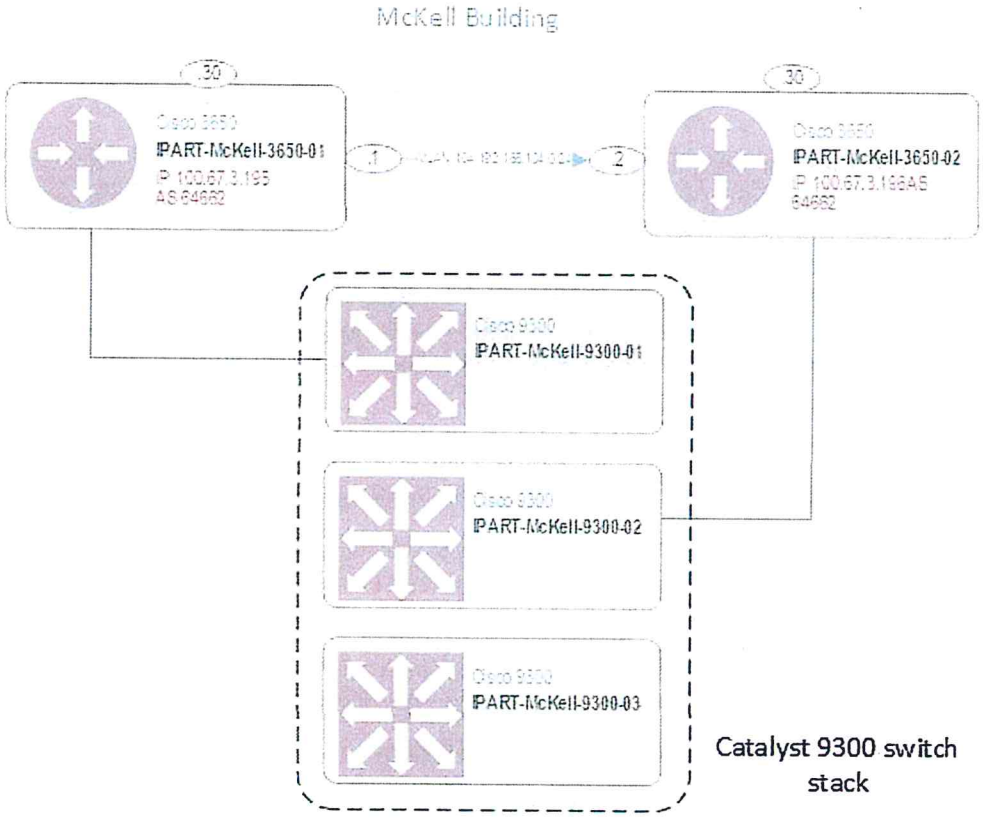


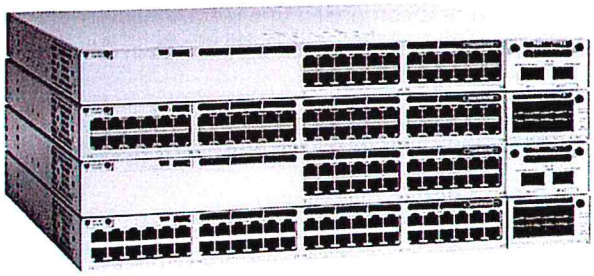
Figure 1 IPART LAN Network - Proposed State

The solution takes into account the following considerations:

- Replace all Floor 16 switches (providing connectivity to Floors 15 and 16).

- Supply two mGiG switches with the view of using it as a base for next-gen wireless access points.
- Network redesign with the aim to simplify existing network and provide higher resiliency.
- Move network inter-VLAN routing to Catalyst 9300 stack.
- Decommission AV switches and move AV ports to Catalyst 9300 stack.
- Reduce total count of switch ports with the aim to support wireless-only deployment for users.

2.1.1.2 Cisco Catalyst 9300 Capability Overview



The Cisco Catalyst 9300 Series Switches are Cisco's lead stackable enterprise switching platform built for security, IoT, mobility, and cloud. They are the next generation of the industry's most widely deployed switching platform. The Catalyst 9300 Series switches form the foundational building block for Software-Defined Access (SD-Access), Cisco's lead enterprise architecture. At 480 Gbps, they are the industry's highest-density stacking bandwidth solution with the most flexible uplink architecture. The Catalyst 9300 Series is the first optimized platform for high-density 802.11ac Wave2. It sets new maximums for network scale. These switches are also ready for the future, with an x86 CPU architecture and more memory, enabling them to host containers and run third-party applications and scripts natively within the switch.

The Catalyst 9300 Series is designed for Cisco StackWise technology, providing flexible deployment with support for nonstop forwarding with Stateful Switchover (NSF/SSO), for the most resilient architecture in a stackable (sub-50-ms) solution. The highly resilient and efficient power architecture features Cisco StackPower, which delivers high-density Cisco Universal Power Over Ethernet (Cisco UPOE) and Power over Ethernet Plus (PoE+) ports. The switches are based on the Cisco Unified Access Data Plane 2.0 (UADP) 2.0 architecture which not only protects your investment but also allows a larger scale and higher throughput. A modern operating system, Cisco IOS XE with programmability offers advanced security capabilities and Internet of Things (IoT) convergence.

Product Highlights

- Highest wireless scale with Wave 2 access points supported on a single switch with select models
- UADP 2.0 Application-Specific Integrated Circuit (ASIC) with programmable pipeline and micro engine capabilities, along with template-based, configurable allocation of Layer 2 and Layer 3 forwarding, Access Control Lists (ACLs), and Quality of Service (QoS) entries
- x86 CPU complex with 8-GB memory, and 16 GB of flash and external USB 3.0 SSD pluggable storage slot (delivering 120GB of storage with an option SSD drive) to host containers
- USB 2.0 slot to load system images and set configurations
- Up to 480 Gbps of local stackable switching bandwidth
- Flexible and dense uplink offerings with 1G, Multigigabit, 10G, 25G, and 40G
- Flexible downlink options with 1G and Multigigabit links
- Leading PoE capabilities with up to 384 ports of PoE per stack, 60W Cisco UPOE, and PoE+
- Intelligent Power Management with Cisco StackPower technology, providing power stacking among members for power redundancy
- Line-rate, hardware-based Flexible NetFlow (FNF), delivering flow collection of up to 64,000 flows
- IPv6 support in hardware, providing wire-rate forwarding for IPv6 networks

- Dual-stack support for IPv4/IPv6 and dynamic hardware forwarding table allocations, for ease of IPv4-to-IPv6 migration
- IEEE 802.1ba AV Bridging (AVB) built in to provide a better audio and video experience through improved time synchronization and QoS
- Precision Time Protocol (PTP; IEEE 1588v2) provides accurate clock synchronization with sub-microsecond accuracy making it suitable for distribution and synchronization of time and frequency over network
- Cisco IOS XE, a modern operating system for the enterprise with support for model-driven programmability including NETCONF, RESTCONF, YANG, on-box Python scripting, streaming telemetry, container-based application hosting, and patching for critical bug fixes. The OS also has built-in defenses to protect against runtime attacks

Exact number of deployed switches will be determined after Network Architecture Framework SOW is delivered.

2.1.2 Floor Wireless Network Refresh Design

IPART has made a decision to modernise its access wireless network in order to enable wireless-only office. It is understood that IPART requirement is to keep wired-only endpoints on LAN (WAPs, IP phones, printers, meeting room screens, etc) and move all user laptops to wireless network.

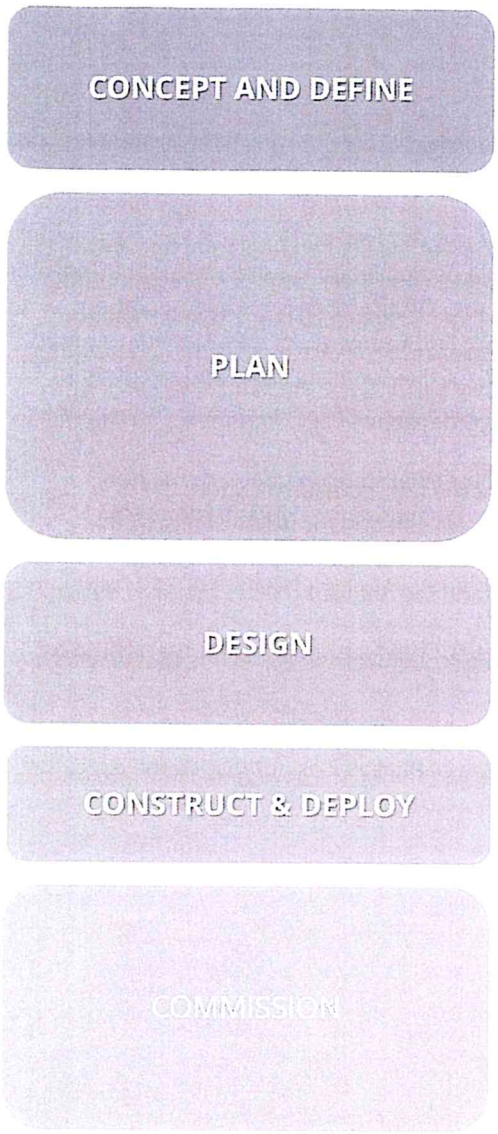
In order to address this requirement, AC3 proposes the following phases:

1. Wireless workshop in order to formalise and lock down IPART WiFi requirements (number of users/devices per floor/area, floor coverage, SSIDs, authentication workflows, security enforcement, wireless QoS, wireless integration with Lync/SFB)
2. Site survey to understand and record real-time RF environment across IPART offices, considering existing IPART laptop fleet of 802.11ac-enabled laptops
3. Develop RF design and WAP placement map considering sections 1 and 2
4. Validate RF design using predictive site survey tools
5. Finalise Wireless BOM and provide cabling contractor quotation for extra WAP deployment / relocation of existing WAPs

Exact number of WAP and the WAP placements will be determined after Network Architecture Framework SOW is delivered.

2.1.3 Project Management

2.1.4 AC3 Project Principles & Lifecycle



- Validate Project
- Establish Objectives
- Present Initial Proposal

- Develop Project Scope
- Develop Timeline & Budget (WBS)
- Develop Change Management Plan
- Develop Comms,Training & Doco. Plan
- Develop Risk Management Plan
- Project Document Sign-off
- Procure Staff & Materials
- Resource Review & Execution Kick-off

- Low Level Design
- High Level Design

- Implement Project Plan
- Monitor & Control Project Implementation

- Document Control
- Post Implementation Review
- Report Project Performance
- Final Project Sign-off
- Transition to Operations

Using our qualified understanding of the PRINCE2 as a guide, we have developed a Project Management framework which we feel offers a controlled and measurable lifecycle for our customers. It ensures accountability and visibility for each phase of your program delivery and allows for a continuous focus on quality assurance, cost-benefit analysis, risk management, communication and reporting.

Each of the steps within the project lifecycle contains a carefully constructed range of deliverables which will guide your requirements through to a successful outcome. We pride ourselves on being industry leaders in the development of high quality technical products and services and we also know the importance of robust project management.

2.1.5 Project Phases

This Statement of Work (SOW) covers a single milestone where AC3 will prepare a Network Architecture Framework for IPART.

2.1.5.1 PHASE 1 – DESIGN – Milestone A

The framework will consist of the following AC3 deliverables:

1. **Discovery and Workshops:** AC3 will perform a deep investigation of the current environment, and run design workshops with IPART to confirm the current state as well as confirm that the proposed final state will be in line with IPART's expectations.
2. **Final State Architecture:** The framework will outline not just the final architecture, but also all the configuration detail (IP addressing, hostnames) that would be applied to the environment during implementation. IPART will be able to use this as a Low-Level Design (LLD) for implementation.
3. **Dependency Mapping:** AC3 will outline the exact software and firmware recipes that are required between the various components of the solution (APs, WLCs, ISE, Switches, SOE) and document these in the framework. There will likely be multiple upgrade steps of all components during the consolidation and upgrade of the solution.
4. **Authentication architecture**: AC3 will design as part of the final state architecture the new methods to streamline the Corporate / BYOD / Guest access solution for IPART (if required).
5. **Migration Plan**: AC3 will formulate a migrate plan in order to transition from the current environment to the proposed architecture. This will include the detailed phases required during the transition of the environment.
6. **Licenses, Software or Hardware**: AC3 will list any Licenses, Software or Hardware that would be required to provide the final solution.

Upon completion of the framework document, AC3 will perform a walkthrough of the document with IPART and will provide Statements of Work (SOW) for the implementation of Phases 2 as outlined in the executive summary of this document.

2.2 Work Breakdown Structure

The project scope of work defines the tasks, resources, requirements and deliverables that IPART can expect from each and every phase of the project.

Resource Initials:

- **L5-PM** – Level 5 Project Manager
- **L5-SA** – Level 5 Solutions Architect
- **L4-SE-NS** – Level 4 Senior Network Engineer – Business Hours
- **L4-SE-NS-AA** – Level 4 Senior Network Engineer – After Hours
- **L4-SE-I** – Level 4 Senior Infrastructure Engineer – Business Hours
- **L4-SE-I-AA** – Level 4 Senior Infrastructure Engineer – After Hours
- **IPART** – Independent Pricing and Regulatory Tribunal NSW

Task Name	Resource Initials
PHASE 2 - DESIGN	
Discovery and workshops	L4-SE-NS
Onsite wireless survey	L4-SE-NS
Document final state architecture	L4-SE-NS
Document dependency mapping and SOE changes	L4-SE-NS
Document Corp / BYOD / Guest architecture	L4-SE-NS
Document Migration Plan	L4-SE-NS
Document BOM	L4-SE-NS
Walkthrough	L4-SE-NS
Document updates	L4-SE-NS
Project Management	L5-PM
MILESTONE A	

2.3 Responsibilities, Assumptions & Constraints

2.3.1.1 AC3 Responsibilities

Item	Descriptions
AR1.	Interview key personnel to respond to the "Statement of Work".
AR2.	Collect and analyse data pursuant to the data defined in the "Project" of this document.
AR3.	Refrain from causing severe network outages.
AR4.	Notify the client in the event the engineer(s) assigned to the project are absent, ill or terminate employment.
AR5.	Provide coordination and management of project resources
AR6.	Provide engineering skills with senior experience in the network and security field.
AR7.	Any reports and information gathered by AC3 staff are the sole property of the Independent Pricing and Regulatory Tribunal (IPART).

2.3.1.2 Client Responsibilities

Item	Descriptions
C1.	Provide access to key technical IT personnel in order to respond to site-specific requests for information.
C2.	Provide access to basic office functions; work area, phone, copiers, faxes, etc. while AC3 personnel are on site.
C3.	Provide administrator access to in-scope systems and devices as required.
C4.	Provide access to any pertinent documentation that may exist.
C5.	Provide proper levels of security to AC3 personnel such that access to phone/data areas is not hindered.
C6.	Responsible to detect any and all suspicious activity and report to AC3 Consultant.
C7.	Accurate, up-to-date documentation of network and topology must be made available to AC3 consultant(s) prior to engagement.
C9.	Collaborate in timely manner with AC3 staff assigned to this project.

2.3.1.3 Exclusions

Item	Description
E1.	Review of any network infrastructure not related to 2-24 Rawson Pl site LAN and WLAN.

2.3.1.4 Assumptions

Item	Description
A1.	All work estimated as part of this SOW is calculated at the AC3 standard rates. All service work to be completed during standard business hours (Mon-Fri, 8:00am – 6:00 pm) unless otherwise stated in the Work Breakdown Structure. After hours work occurring on a Sunday or Public holiday will incur additional costs; If it changes to Sun or PH, will be increased to 2.0 and 2.5 respectively.
A2.	Variances between these assumptions and actuality may result in pricing modifications.
A3.	Where recommendations are generated from this engagement, implementation of these changes is not included in the quoted price. These changes can be made available at an extra cost.
A4.	Pricing in this SOW is applicable to services stated only and excludes any hardware not specifically priced in this proposal, products or media.
A5.	The site contact nominated is responsible for signoff of deliverables.
A6.	Any modifications to the Proposal will need to be in writing and a copy signed by both parties. Changes to this scope may result in additional charges incurred by the client.
A7.	If during the implementation of this SOW there is a product version / model change that results in a requirement for redesign or scope change, a project variance will be initiated. Scope changes will be priced accordingly and agreed by both parties before the continuation of the project.
A8.	While onsite, AC3 resources will be expected to work towards the completion of project deliverables. It is expected that Independent Pricing and Regulatory Tribunal (IPART)may use a limited amount of time from them to assist with questions and items of an advisory nature regarding the existing environment. AC3 resources will cooperate in these matters provided it does not result in a significant deviation from the project plan. In the event that issues arise

Item	Description
	requiring an increased time commitment from AC3, AC3 will discuss any fee and schedule impact with the appropriate Independent Pricing and Regulatory Tribunal (IPART) representative prior to proceeding with the work.
A9.	IPART will manage all end user communication.

3 PROJECT GOVERNANCE MODEL

3.1 Project Execution

AC3 will assign an AC3 Project Manager, who will be the primary point of contact for all Project related activities. The Project Manager will:

- Assign AC3 technical resources;
- Organise a project kick-off meeting;
- Circulate the Project Management Plan to stakeholders;
- Agree on implementation schedule with customer and circulate the schedule;
- Ensure that necessary AC3 change requests have been approved.
- Identify and manage variations to the agreed Scope of Work;
- Implement the solution and test to a satisfactory level as agreed by AC3 and the customer;

The following key Project Management artefacts will be developed and actively utilised throughout the project lifecycle to promote informed decision making by all parties involved:

PM Artefacts	Deliverable?
Project Management Plan	✓
Project Schedule	✓
Status Reports	✓
Risk, Issues and Action Registers	✓
Meeting Minutes	✓
Project Closure Report	✓

In this table, × means artefact is not a deliverable; ✓ means artefact is a deliverable

AC3 will provide the following technical document deliverables:

Technical Document Deliverable	Deliverable?
Network Architecture Framework Design Document	✓
Network Architecture Framework – Implementation SOW	✓
Network Architecture Framework – Implementation BOM	✓

In this table, × means artefact is not a deliverable; ✓ means artefact is a deliverable

Unless stated above, other project management and technical artefacts are not explicitly in scope of the project management services, but can be negotiated through variations.

4 PRICE AND PAYMENT

4.1 Pricing

- Pricing has been provided in the accompanying quotation to this SOW.
- Pricing is only valid for 30 days from the date this SOW was produced (cover page).
- Services cost will be invoiced upon milestone completion.
- Pricing for the scope of works is commitment between both AC3 and IPART to a fixed price for the complete project unless otherwise specified.

5 RECITALS

5.1 Copyright

The copyright of this document is the property of AC3 Pty Limited.

All information provided by AC3 in this response is provided on a commercial-in-confidence basis. No part of this document may be provided to any other person or organization in any form without the prior written permission of AC3.

5.2 Disclaimer

AC3 will be providing skilled engineers and resources to complete its responsibilities within the project in the timeframe outlined in this proposal. Whilst all due care and consideration has been taken in the preparation AC3 cannot take responsibility for additional products and/or service which may need to be purchased as a result of the any increases in this scope during implementation nor for product being unavailable as a result of a vendor discontinuing a line.

Further, should a product vendor update or modify its product advice after AC3 has acted upon previously current information, AC3 will not be held responsible for the cost of any further modification or update needed to re-comply with the new advice.

The information in this proposal is private and confidential and may not be copied or distributed outside its intended customer without prior permission from AC3.

5.3 Warranty

Following the successful transition of the solution into Client operational support, a warranty period of no more than 30 calendar days will commence. During the warranty period, the Customer will have access to engineering resources via the Service Desk, for any technical issues with the solution that stem from either of the following conditions:

1. *The solution has not been deployed or configured correctly, as agreed within the design documents or as otherwise agreed to during the course of the project.*
2. *The solution does not function as designed (if component has been designed by AC3).*

During the warranty period, we agree to respond and resolve any technical issues with the solution that stems from either of the two conditions described above. Any and all infrastructure and application components that were not deployed by us during the project are not within the scope of the solution warranty.

In order for the warranty to remain valid for the full 30 calendar days, Client must not make any architectural and/or system changes to the solution following the transition, up until the time that the warranty expires. The Customer is expected to utilise the solution and perform regular administrative and management tasks, but these tasks must not alter the solution architecture. Any such changes implemented during the warranty period will immediately void the warranty.

END OF DOCUMENT PAGE

No text to be placed on this page