
Microsoft Customer Success
Department of Police, Fire and Emergency Management
Power Platform Solution Review
Findings & Recommendations Report - v1.0
By Microsoft
May 2025

Table of Contents

- Purpose & Executive Summary
- Engagement Approach
- Review Summary
- Assessment Findings
  - Details
  - Recommendation
  - Resources

Solution Review - Purpose

What is the purpose of the Power Platform Solution Review

- This review provides recommendations for enhancing the strategy, operations or support of the department's Power Platform solution, primarily the **Project Link** application built via **Power Pages** framework.
- It aims to review the solution and architecture, identify potential misconfiguration, explore configuration options, advise on implementing recommended practices and a guide for enhancement strategies.
- It is based on learnings from many international projects and from observations, discussions and learnings from the department's current implementation.
- It can be used during current Power Platform projects but can also be used when planning a future projects.
- Recommendations and comments capture Microsoft's suggestions for learning or for addressing findings as well as links to documentation if the team needs to research a recommended topic. Microsoft is not liable for the implementation of such recommendations.

How should you incorporate the recommendations within your programme?

- Findings and recommendations can be used as checklists to guide either a new project or for operational enhancements and to verify if/how those areas are already covered. Some findings may not have been fully considered by the team yet but will be important for later testing, deployment or operational phases.
- Findings also provide an opportunity for discussion with your implementation or support partner, stakeholders, SME or product owners to identify if the specific requirements of the project justify the existing approach or if changes should be made based on the findings.
- Use this report as a starting point to formulate your own plan to address the findings and recommendations based on your business needs.

Classified as Microsoft Confidential

Executive Summary

A Microsoft Cloud Solution Architect (CSA) conducted a five-day review of DPFEM's Project Link solution, initially focused on Power Platform low-code components but extended to include architectural and pro-code elements, with an emphasis on best practices and standards. The review involved multiple workshops with DPFEM and their implementation partner.

S30

The solution features a low-complexity design and primarily uses standard out-of-the-box design features. The solution was assessed at the 'pre-deployment' stage.

Relating to the forms, there were no major design or configuration issues identified that would prevent the solution from being deployed to production and go-live.



Classified as Microsoft Confidential

Executive Summary (cont'd)

[redacted]

S30

To move forward effectively, DPFEM should consider developing a recovery and optimisation plan that prioritises these improvements in alignment with broader business goals, resource availability, and project timelines.

Classified as Microsoft Confidential

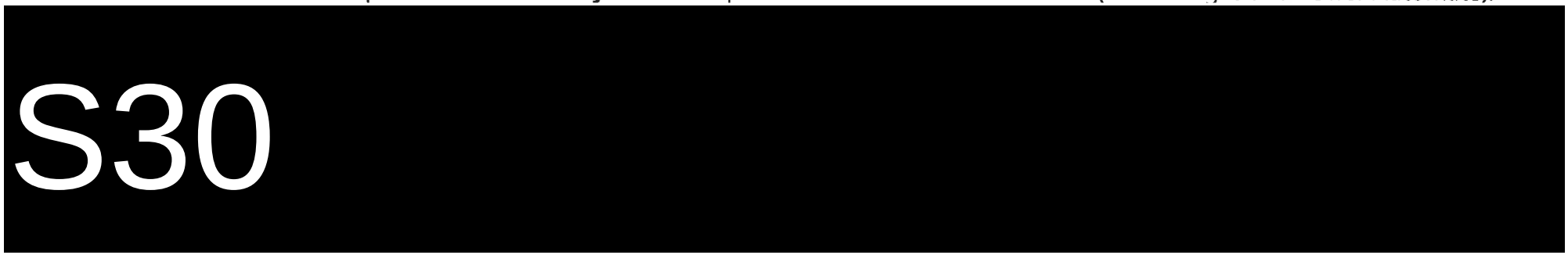
Engagement Approach

Delivery Method

- A series of daily sync up calls and 2 workshops (check next slide for plan and schedule details) were conducted between Microsoft and DPFEM team including the implementation partner's representatives covering various topics including:
  - Overall **solution architecture** with primary focus on Power Platform (i.e. Power Pages) and Dynamics interrelated interfaces
  - **Solution design** and main solution building blocks and configurations
  - **Environment strategy** and management
  - **Security** practices and management through the various layers
  - Application Lifecycle Management (**ALM**) with focus on solution management, build and release pipelines and deployment practices
- The department shared project related documentations in SharePoint folder here.

Scope of this Review Engagement

- The solution review was scoped to cover the **Project Link** implementation in **Power Platform** (Power Pages and Power Automate).



- The online offence reports covered were: Fuel Drive Off; Make Off Without Payment; Mark Graffiti; Property Damage; Retail Theft; and Theft.

Classified as Microsoft Confidential

Engagement Cadence – Week starting 22nd of May 2025

Planned

AEDT/ SYD	Thu 22nd	Fri 23rd	Mon 26th	Tue 27th	Wed 28th
9 am	Kick-off & Alignment. Architecture Discussion	Daily Sync & Update	Daily Sync & Update	Daily Sync & Update	
10 am					
11 am					
12 pm				Workshop: Performance Review	
1 pm					
2 pm		Workshop: Application Lifecycle Management	Workshop: Power Page Design		
3 pm					Present findings & recommendations
4 pm					
5 pm					

Classified as Microsoft Confidential

Key Definitions

The findings in this report will have the following classifications or priorities:

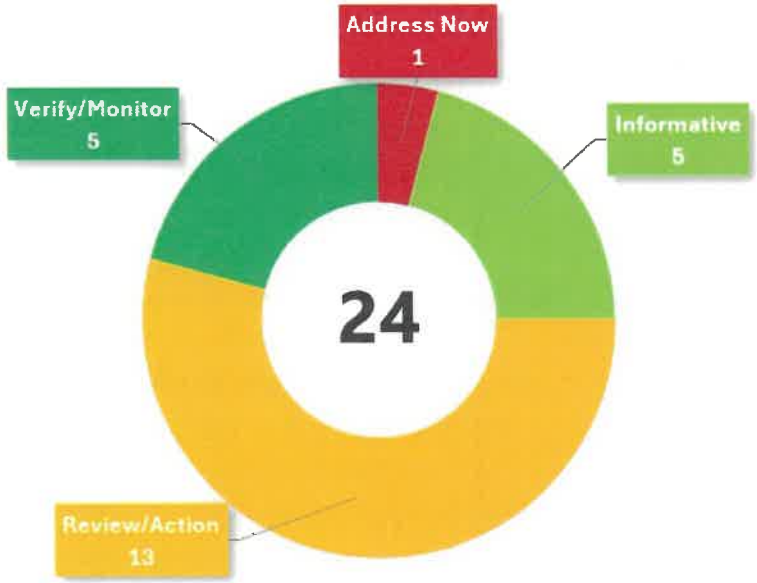
Address Now	You should consider this finding with highest priority. The finding in this category will likely improve the overall solution or address a critical gap in the current implementation or operation processes. It is recommended to address such items before other categories if applicable.	**Level 1**
Review/Action	You should consider this finding with higher priority as it can help to improve stability, security or governance adoption of DPFEM's environment/solution. It is recommended to promptly review and address the recommendations listed for them.	**Level 2**
Verify/Monitor	The finding doesn't require an immediate or urgent attention but rather can be considered based on business priorities or for ongoing monitoring and considerations. It is recommended to check such items to make sure DPFEM still adheres to the recommendations listed for them.	**Level 3**
Informative	The finding is listed for awareness and future consideration. There isn't an immediate need to take any action but good to track and understand such item.	**Level 4**

Adoption Plan

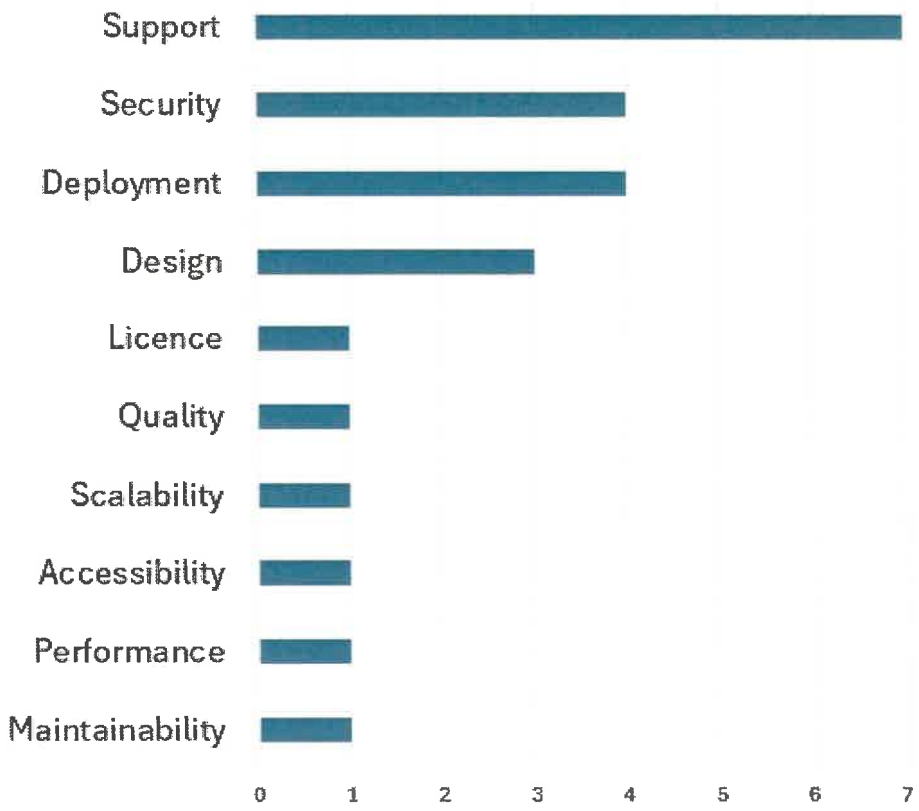
Work with the IT and infrastructure team to establish a **solution review adoption plan** to prioritise some of the recommendations and ensure you have a clear schedule on implementing them. Also establish some practices for **proactive monitoring** of your environment's health on regular basis. Adopt a Zero-Trust principal when dealing with security related activities.

Findings Summary Reports

Findings Count by Category



Findings Count by Area



Microsoft

Findings Summary

⭐ Important | Address Now | Review/Action | Verify/Monitor | Informative



Classified as Microsoft Confidential


Review Details

01 Empty Site's Home Page in Power Pages

Review/Action

Accessibility

Finding

The home page or site root for the current Power Pages portal is an empty blank page. It is well understood that the portal will act as a digital form host for 6 of the current's departments common reported offences and visitors will reach to these specific forms directly from the main official police site (i.e. police.clients.ionate.com.au). However, customers might bookmark their links or alter the URL address in the browser address bar to only include the root page which is currently a blank page.

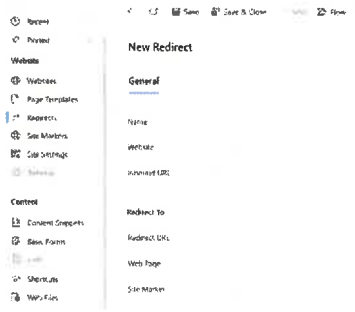


Recommendation

It is best practice not to have a blank page in your site. Ensure to:

- Either redirect visitors from the root site page back to the public police site in which they can report a crime. You can achieve this with configuration or add a JavaScript at root page header.
- Or implement some content that will surface and showcase the various 6 offence reports with information/link about each one and the ability to initiate the reporting process if needed.

Implementing the root page will help with accessibility and user experience of the site in general.





Resources

- Add a redirect URL to a new URL on a website | Microsoft Learn

Microsoft

S30

S30

04 WAF Rules Were Not Found in TEST Environment

Verify/Monitor

Deployment

Finding

S30

Recommendation

The recommendation is to consider implementing WAF rules as per business requirements and context of the application. These rules are meant to provide an added security layer from the portal site networking side. The implementation team has already configured a rule to prevent bots or scripted attacks from simulating high-volume transactional access to the platform but it seems that the rule was not configured in the TEST environment.

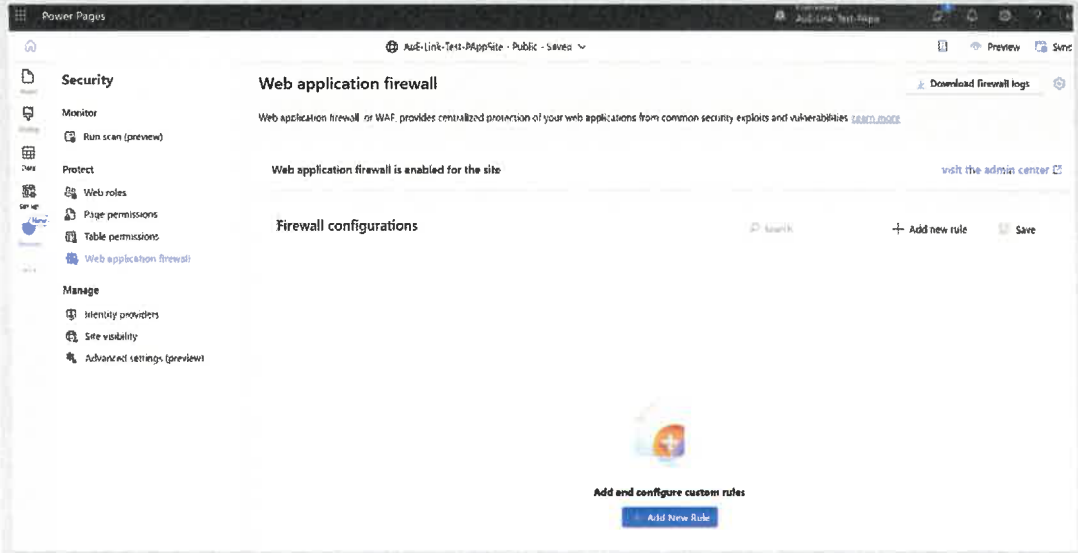
This finding is not about a security gap but rather is related to a gap in the Deployment Guide. Thus, ensure to add a section on the configuration and checking of the WAF rule post the deployment procedure of the solution.

There was a question raised whether it is possible to automate the deployment of the WAF rules. Unfortunately, it is not available as of now to automate them via the platform build tools.

S30

Resources

- Consider some common WAF custom rules that frequently configured by customers for various scenarios here: FAQ for configuring Web Application Firewall in Power Pages | Microsoft Learn





Microsoft

05 S30

Informative

Licence

Finding

S30

Recommendation

S30

If the Project Link solution doesn't interfere or interact with the 1st party business applications' tables and components (i.e. Case table, routing, Lead/Opportunity...etc.) then there's no risk of keeping the current configuration as is. This recommendation is raised as **informative** level just to bring this area to the department's attention and for future considerations.

Note: once the Dynamics 365 business applications are installed, they cannot be uninstalled or removed. It is possible to hide them via security role assignment. However, System Administrators will always be able to access them.

Resources

- What is Dynamics 365? - Dynamics 365 | Microsoft Learn

S30

t


S30

07 Consider Adding CAPTCHA to Form Submissions

Review/Action

Security

Finding

[redacted]

Recommendation

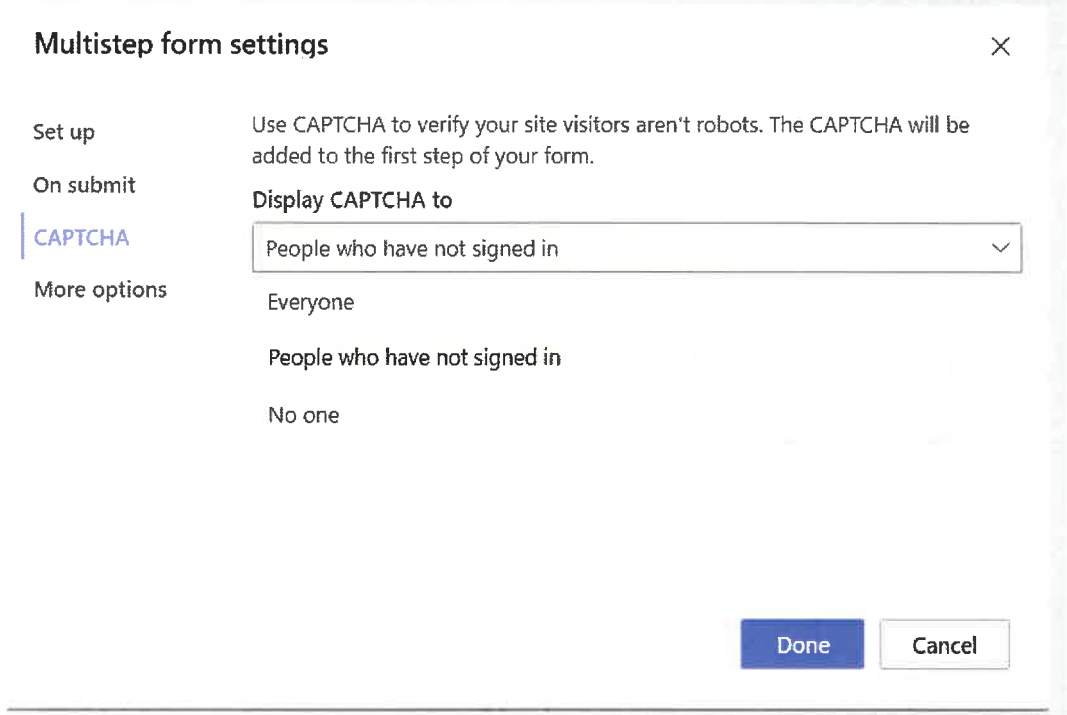
Consider implementing CAPTCHA as part of your form submissions. Power Pages has this feature out-of-the box available when configuring Multi-step forms. This is important in order

[redacted]

We identified this finding with a mid level since the WAF rule is still available for the time being. While this finding is not critical for go live, it is still important to give it a priority and address when time allows.

Resources

- Multistep forms | Microsoft Learn



Microsoft

08 Do Not Set Default Value for Environment Variable

Verify/Monitor

Deployment

Finding

[redacted]

Recommendation

In TEST, UAT, PRODUCTION or higher environments in general, it is recommended that you use "Current Value" when configuring the Environment Variables. The Default Value is not reliable as it can be overridden with solution import/deployment if it meant to have a different value in the lower environments (i.e. DEV).

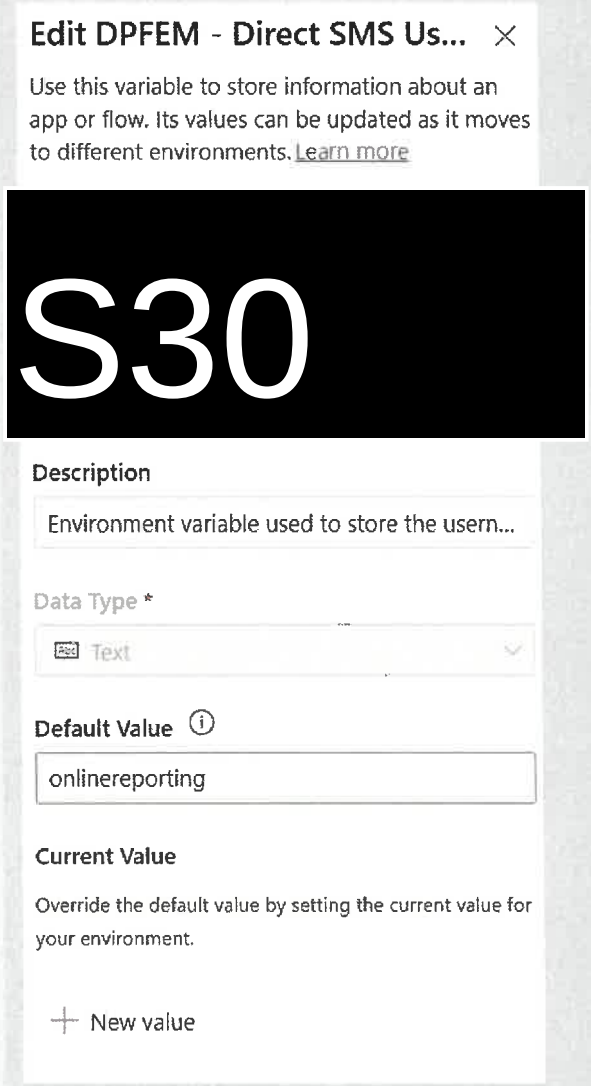
This finding was only observed for the following Environment Variables:

- DPFEM – Direct SMS Password
- DPFEM – Direct SMS Username

Action: try to add the Current Value for the affected Environment Variables and ensue to rely on it moving forward because they'll not be overridden when there's a solution deployment in the future. The benefit of Current Value is it will take precedence over the default value. Remove the value from your solution if you don't want to use it in the next environment. The values are also separated into separate JSON files within the exported solution.zip file and can be edited offline

Resources

- Use environment variables in Power Platform solutions - Power Apps | Microsoft Learn



Microsoft

S30

S30

11 Deployment Guide Improvements

Review/Action

Deployment

Finding

The current Deployment Guide is very rich document and contains over 140 pages with screen shots and procedure that defines the deployment and post-deployment steps of the solution. This is a great artefact and implementation team should be praised for documenting such level of details. Still, there are few gaps identified which can add further strength and completeness factors to the guide.

Recommendation

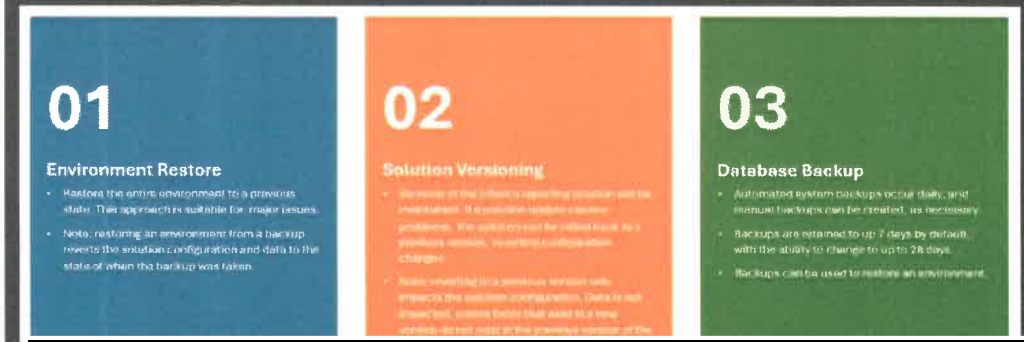
It should be made clear that the Deployment Guide shouldn't belong to a single party. The guide interest is to deploy the solution, and it will likely involve multiple stakeholders to fully complete all procedures. Thus, the guide should be written and reviewed by all required parties and endorsed through Architect Review Board (ARB). It should be made available for all parties during the cutover procedure and go live deployment.

Consider improving the Deployment Guide with the following notes or comments:

- The guide needs to be **instructive** rather than informative. It should clearly illustrate the procedure as instruction without the need to give options or leave it up to the reader to decide.
- Add a **pre-requisites** section that clearly list all the items that should occur ahead of the main night of the cutover window. It would include setting up Environment and its settings, service accounts, obtaining SSL certificate for the site, checking message centre for platform updates/releases...etc.
- [redacted]
- The **mailbox** approval will require a Global or Exchange Administrator. It seems that this will not be an issue as the implementing party will have such roles, but it shouldn't be assumed and rather, it should be added as a clear statement and in the pre-requisites section. You can delegate this role as well: Connect to Exchange Online - Power Platform | Microsoft Learn
- The WAF custom rule was not mentioned in the deployment guide.
- [redacted]
- [redacted]

7.1 Rollback

Power Platform provides the ability to revert changes to manage exception scenarios where errors or unexpected behaviour is introduced to the environment. The diagram below illustrates the common rollback capabilities:



[redacted]

12 ORS Integration Performance Optimisation

Review/Action

Performance

Finding

There are 2 power automate flows that are responsible for ORS integration orchestration:

- [redacted]
- [redacted]



The combined average of the above 2 flows is equal to 8 seconds. Sometimes the ORS number is already available on Dataverse database but the second flow is still waiting for the 2 seconds to finish before checking again. While decreasing the pulling window may sound an easier task, it can have throttling consequences if we have large volume of reports pulling frequently at the same time.

Recommendation

After analysing the design of both flow jobs, it seems that they should be designed as one unit. In another word, the recommendation is to combine these 2 jobs into one single Power Automate job and eliminate the need for the pulling mechanism. This new single job will trigger from Power Pages form submission event and will collect data and push to ORS via same HTTP mechanism we have today and once it gets the number, it stores it back into Dataverse but also return it to the Power Page response/screen.

Additionally, you can consider segmenting some repetitive parts into a Child flow to avoid logic duplication. This might be desired when constructing the payload before sending it to ORS



13 Solution Scalability

Informative

Scalability

Finding

The current Project Link supports 6 online crime reports/forms. The department raised a question whether the solution can be scaled to support much larger number of other forms and up to 60 in total. While it is unlikely that such scale would hit a technical or physical blocker, it will add a huge overhead and maintenance due to the current static design approach of the site.

Observation

The current solution design is considered **Static** in nature. All the 6 forms were crafted manually by platform developers using native features such as Advanced Multi-Step forms, Model-Driven App forms, Online Crime Report table to store questionnaires and any supporting site configurations. This is a **correct form design pattern in Power Pages and endorsed and documented publicly**. There's nothing wrong with this approach. However, this approach is more recommended if we have a small number of forms to be digitalised due to the manual and **labour-intensive** approach. In order to scale the solution to support future business forms, the department will need consultation from a Power Pages developer as the work required to build such forms cannot be done by regular super users/admins. While the solution can support such implementation, we'd recommend not to exceed 10 15 forms using such approach.

S30

S30

In summary, there isn't anything wrong with current Static nature of the form design. However, the department needs to plan maintenance and support effectively and engagement a Power Pages developer shall there is a need for changes or new forms in the future.

S30

Microsoft

14 Remove Redundant Duplicate Submission Pages

Review/Action

Design

Finding

There are currently 6 Online Crime Report forms, but they all tend to end with same confirmation logic and notice. The solution can use a single Submission Page for all these 6 forms. However, currently we have 6 duplicate Submission Pages used (one per each form). This can lead to maintainability and scalability issues.

It was understood that original design had an intention to handle confirmation page and notice differently per each form. If that's the case, then the current design can be justified. However, it seems that the requirement moved on to consolidate the confirmation page's functionality or logic but the design remained following the original view.

Recommendation

Attempt to delete the other 5 Submission Pages and have all the current 6 forms redirect to a single Submission Page.

Resources

- Add a redirect step type | Microsoft Learn

S30

S30

Review/Action

Quality

Finding

S30

Recommendation

S30

S30

Such content might need to change if the compliance or business processes changes in the future. The goal is to be able to make such changes without the need to involve a developer (i.e. to modifying code) or even go through the full release lifecycle. They should be made configurable enough to allow Super Admin business persona to make modification when needed.

S30


S30

S30

Microsoft

17 Address Lookup as PCF

Informative

Design

Observation

This finding is just to present an alternate view. **There's nothing wrong with current implementation**. The department has enquired about other configuration means that are commonly used and hence this finding will attempt to explore the other means.

The current Project Link solution integrates with Google Maps API to show a list of address suggestions. The code is currently written as JavaScript against each Multi-Step form under each step that needs such integration logic. We have already flagged a code duplication issue in a previous finding, so we'll not revisit the duplication issue again here. Instead, We want to present an alternative design which is using a **PowerApps Component Framework** (**PCF**) to implement such logic.

PCF components are the recommended way to extend the various form controls outside the available out-of-the box controls. With PCF components, the framework better handles the control as if it was a native control. In fact, all other out-of-the box controls were developed internally by Microsoft product group as a PCF component from the start.

There are lots of community-based PCF solutions that also attempt to provide address lookup and mapping integration with Google Maps API. This can make the development much faster for such controls as opposed to starting from scratch. They do provide a good configuration wizard to allow the configurator to pass in parameters in order to control some logic instead of hardcoding them (i.e. limiting the address mapping scope to Tasmania only). Also PCF components can be added in Model-Drive Apps, Canvas Apps and also Power Pages to provide a more universal support across all various app types.

In summary, current address mapping design is embedded in Power Pages site code and that's one correct way to do it. Alternative approach is to consider standardising the logic as a PCF control to provide more flexibility to extend the coverage even outside Power Pages scope. Since the code is written already, there's no need to change it apart from fixing the code duplication issue raised in a previous finding.

Resources

- Home | PCF Gallery
- Power Apps component framework overview in Microsoft Dataverse - Power Apps | Microsoft Learn

S30

S30

Microsoft

19 Implement Power Platform Governance Practices

Verify/Monitor

Support

Finding

Although DPFEM demonstrated a good level of solution management for Project Link application, we extended the review outside the solution and more at the environment and tenant scope. We identified a room for improving platform governance overall. This can range from environment strategy and request processes, managing applications/flows, tenant wide settings (i.e. Tenant Isolation feature), security measures, monitoring and more...etc.

Recommendation

Establishing such governance layer takes years. It requires a strong orchestration between three main parties: People, Process and Technology. Having a governance process (even if very simple) is better than nothing. Try to establish clear governance policies for Power Platform usage; implement regular audits to ensure compliance with governance standards; Review and implement the guidance published under **Success by Design** framework; Utilise a **Center of Excellence (CoE) Starter Kit** to oversee governance efforts; and finally engage stakeholders (IT, business, partners.. etc.) in governance discussions for better alignment.

When it comes to Power Platform governance, there are several key areas you should focus on to ensure effective management and control of your environment:

- **Admin and Governance Best Practices**: Establishing best practices for managing users, licenses, capacity, data, security, and reporting is essential. This includes designating the Microsoft Power Platform admin role, managing users, planning and managing license and capacity, and establishing an ALM strategy.
- **Security and Governance Considerations**: Governance aims to enable business groups to focus on solving business problems efficiently while complying with IT and business compliance standards. This includes setting up Microsoft Entra conditional access, enabling cross-tenant isolation, and monitoring and alerting on resource usage.
- **Environment Strategy**: It's important to have a clear strategy for managing different environments (e.g., development, testing, production, support). This includes understanding the types of environments, their purposes, and how they are managed. Environment request procedure should be explored with approval layer and access control.
- **User and Role Management**: Assigning appropriate roles and permissions is vital. The Power Platform administrator role is separate from the Microsoft 365 admin role and is essential for managing and monitoring environments.
- **Documentation and Standards**: Having a well-documented process for governance, including naming standards, operational documentation, and knowledge base articles, helps maintain consistency and control.

Success by Design Framework

Success by Design is a framework and practice created by Microsoft to help project teams implement Dynamics 365. Based on thousands of real-world customer projects, Success by Design is the sum of our Dynamics 365 implementation experience. It offers topic-specific reviews and prescriptive guidance (approaches and recommended practices), which provide a reliable path to project success.

We recommend DPFEM to check the content published under this framework and use it to enrich its current governance capabilities.

Introduction to the Success by Design framework - Dynamics 365 | Microsoft Learn

Power Platform Well-Architected Framework

Microsoft Power Platform Well-Architected is a set of best practices, architecture guidance, and review tools to help you make informed decisions about the design, planning, and implementation of modern application workloads with Microsoft Power Platform.

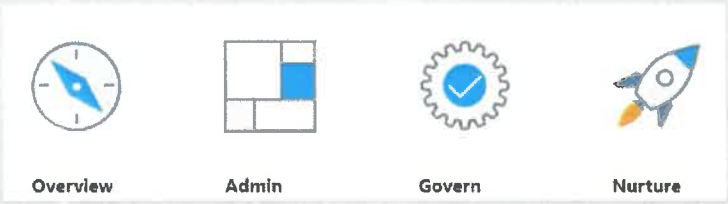
How to use the Power Platform Well-Architected documentation - Power Platform | Microsoft Learn

Center of Excellence (CoE) Starter Kit

A Center of Excellence (CoE) in an organisation drives innovation and improvement and brings together like-minded people with similar business goals to share knowledge and success, while at the same time providing standards, consistency, and governance to the organisation.

The Microsoft Power Platform CoE Starter Kit is a collection of components and tools that are designed to help you get started with developing a strategy for adopting and supporting Microsoft Power Platform, with a focus on Power Apps, Power Automate, and Microsoft Copilot Studio.

Microsoft Power Platform Center of Excellence Kit - Power Platform | Microsoft Learn



Microsoft

S30

21 Implement Regular Proactive Health-Check Hygiene

Review/Action

Support

Finding

There are several areas that should be regularly checked to maintain a healthy solution/platform overall. DPFEM should document such areas that are relevant to their Project Link solution but also should have a tenant wide strategy for proactive operational support.

Recommendation

Improve the internal operational support of the platform by adding a layer of **proactive checks and monitoring** of the various production solutions. This can help in detecting early signs of issues ahead of an escalation or business impacted incident. Proactive measures requires investment by the IT team to dedicate time for monitoring but also implement technical solutions that can automate, detect and alert when there are abnormal activities.

Some of the areas to regularly check are:



Resources

- Management and monitoring - Power Platform | Microsoft Learn
- Monitor the health of your resources (preview) - Power Platform | Microsoft Learn
- Overview of integration with Application Insights - Power Platform | Microsoft Learn
- Monitor and optimize your Dynamics 365 environments - Dynamics 365 | Microsoft Learn



Microsoft

S30

Informative

Security

Finding

S30

Observation

S30

S30

23 Invent new Super User or Admin Security Role

Review/Action

Design

Finding

There's only one security role configured and shipped with the Project Link solution which is **DPFEM – Business Administrator**. This security role will only give **Read** access to the various tables of the solution. Despite the name implies the administration nature, this security role is intended for the regular user to access and check records. The problem is, there's no other custom built security role with any higher level that provide **Create/Update** permissions to master and reference tables. It means business users who'd need to administer these master or configuration data will need to have the System Administrator security role which is a global role that provide access to all areas of the solution, and it can be dangerous to be assigned to a regular business user without training or consideration (i.e. they can easily delete records including master records or configurations intentionally or accidentally for instance)

Recommendation

The system should clearly define the persona that will use the system. At least, there'll be following type of personas (at a minimum):

1. Regular business user who will perform basic operations and might need the lowest privileges
2. Super role or business administrator who will be responsible for maintaining the master and configuration data of the system and provide basic administration from the business side
3. System administrators/customisers who are usually the developers or platform IT admins that are responsible for the overall health of the solution and can have a wide access to all the components of the application.

Currently, the Project Link solution is shipped with one security role that addresses first type of persona mentioned above. For the third type, this is usually provided out of the box by **System Administrator** or **System Customizer** security roles. There's a gap with the second persona as there's no custom security role currently available to be assigned to them.

Ensure to rename the current security role to align with the role of basic business user. Create a new custom security role for business administrator that provide Create and Update permissions to various master tables appropriately. Do not give Delete permission to this role. Users with System Administrator security role should be made limited and restricted.

Resources

- Role-based security roles - Power Platform | Microsoft Learn
- Security roles and privileges - Power Platform | Microsoft Learn



Microsoft

24 Solution Checker Findings

Verify/Monitor

Quality

Finding

We ran Solution Checker assessment in DEV environment against the Offence Reporting main solution. All findings were medium. There's no immediate need to address them, but it is good to review these and address them appropriately in the long term. Some of these can be False-Positive so you can review the rule or document the findings if needed.

Recommendation

Always aim to run Solution Checker regularly and address the findings. These are common rules that built by Product Group engineers following recommended standards and best practices. In fact, when ALM is fully configured and automated, the Solution Checker step should be configured as part of the Build routine and should stop the build if there are failed checks.

There are number of findings observed but they are all under **Medium** category. The are minor in nature and wouldn't pose a big concern on the solution. They can be categorised as follows:

-
-
-

S30

Ensure to review the Solution Checker report and try to address these findings to improve the overall quality of the solution.

Resources

- Improve component performance, stability, and reliability with solution checker - Power Apps | Microsoft Learn

S30

Microsoft


Microsoft
End of Report

Garth, Rhiannon

From: Brumby, Eric
Sent: Friday, 21 March 2025 10:05 AM
To: Lyons, Matthew; Hughes, Matthew; DeSchipper, Ben
Cc: Macleod, Ellie
Subject: RE: Remediation Plan

S35

ERIC BRUMBY

S36

From: Lyons, Matthew
Sent: Thursday, 20 March 2025 4:10 PM
To: Brumby, Eric ; Hughes, Matthew ; DeSchipper, Ben
Cc: Macleod, Ellie
Subject: RE: Remediation Plan

S35

From: Brumby, Eric S36
Sent: Thursday, 20 March 2025 3:17 PM
To: Lyons, Matthew S36 Hughes, Matthew
S36 DeSchipper, Ben S36
Cc: Macleod, Ellie S36
Subject: RE: Remediation Plan

Hi all,

S35

Cheers,
Eric.

ERIC BRUMBY

S36

From: Lyons, Matthew S36
Sent: Wednesday, 19 March 2025 3:02 PM
To: Brumby, Eric S36 Hughes, Matthew S36
DeSchipper, Ben S36
Cc: Macleod, Ellie S36
Subject: RE: Remediation Plan

S35

Cheers,

Matt

From: Brumby, Eric S36
Sent: Wednesday, 19 March 2025 2:47 PM
To: Hughes, Matthew S36 Lyons, Matthew
S36 DeSchipper, Ben S36
Cc: Macleod, Ellie S36
Subject: FW: Remediation Plan

Hi all,

KPMG are currently addressing the security issues that they identified in their report. One of these was S30

S35

That may not be a real risk, of course.

Anyway, any feedback would be greatly appreciated!

Thanks,
Eric.

ERIC BRUMBY
S36

From: S36
Sent: Wednesday, 19 March 2025 2:31 PM
To: Williams, Jeremy S36 McCreadie, Matthew
S36 Brumby, S36
Cc: Brown, Clare S36 Macleod, Ellie S36 Turner, Ben

S36 S36

Subject: RE: Remediation Plan

Hi all,

S35

S38

Additional testing required
Due to the minimal configuration change, standard automated regression testing to validate the key scenarios and workflows would be sufficient.

Can you please confirm if you would like to proceed?

Thank you.

Best regards,

S36

From: S36
Sent: Monday, 17 March 2025 4:38 PM
To: Williams, Jeremy S36 McCreadie, Matthew S36 Brumby, Eric S36
Cc: Brown, Clare S36 Macleod, Ellie S36 Turner, Ben S36 S36
Subject: RE: Remediation Plan

Hi all,

We would like to provide an update regarding security remediation item 3.2 - S30
We investigated the options to mitigate this risk, please see the summary of our findings below:

Option	Description	Recommendation

S35

S35

Proposed next steps:

- KPMG to share the option 1 issue details with DPFEM
  - DPFEM to log a support ticket with Microsoft
- DPFEM to enable URL re-write via WAF in dev environment to validate this approach. Note: KPMG will be available to support, as necessary.

Thank you.

Best regards,

S36

From S36
Sent: Friday, 14 March 2025 8:30 AM
To: Williams, Jeremy S36 McCreadie, Matthew S36 Brumby, Eric S36
Cc: Brown, Clare S36 Macleod, Ellie S36 Turner, Ben S36 Covington, Darren S36
Subject: RE: Remediation Plan

Good morning, Jeremy,

The latest version was published on Wednesday, also attached.

Best regards,

S36

From: Williams, Jeremy S36
Sent: Thursday, 13 March 2025 7:09 PM
To: S36 McCreadie, Matthew S36 Brumby, Eric S36
Cc: Brown, Clare S36 Macleod, Ellie S36 Turner, Ben S36 Covington, Darren S36
Subject: RE: Remediation Plan

Hi S36

Has there been any changes to the Remediation Plan sent to me at 7:06pm yesterday? If so, please provide the most up-to-date version.

Jeremy

Regards,

Jeremy Williams

Program Director
Project Unify

Department of Police, Fire and Emergency Management
S36



From: S36
Sent: Thursday, 13 March 2025 7:00 PM
To: McCreadie, Matthew S36 Brumby, Eric S36
Cc: Brown, Clare S36 Macleod, Ellie S36 Williams, Jeremy S36 Turner, Ben S36 S36 S36
Subject: RE: Microsoft Ticket - Project Link

Hi all,

We are still investigating and collaborating with Microsoft to explore potential solutions for addressing item 3.2 S30
In the interim, we request approval to proceed with the remediation plan as it currently stands, acknowledging the outstanding item.

Thank you.

Best regards,

S36

From: Turner, Ben S36
Sent: Thursday, 13 March 2025 4:26 PM
To: McCreadie, Matthew S36 S36 S36
Cc: S36 Brown, Clare S36 Macleod, Ellie S36 Brumby, Eric S36 Williams, Jeremy S36
Subject: RE: Microsoft Ticket - Project Link

+ The team on later email

From: Turner, Ben
Sent: Thursday, March 13, 2025 4:11 PM
To: McCreadie, Matthew S36 S36 S36

Cc: S36 [redacted]
Subject: RE: Microsoft Ticket - Project Link

Hi Matt,

As discussed with Jeremy raising a case with MSFT is a good pathway as a backup as we troubleshoot this remediation further.

Appreciate the opportunity to do so. In my experience it's often the combination of specific use case/incident context and collaboration between teams that help facilitate the fix.

I 'll sort my credentials to raise a support ticket accordingly.

Thanks for your support,

Ben

From: McCreadie, Matthev S36 [redacted]
Sent: Wednesday, March 12, 2025 4:41 PM
To: S36 [redacted] Turner, Ber S36 [redacted]
Cc: S36 [redacted]
Subject: [redacted]

Hi Ben & Darren,

I have just spoken with Jeremy, following a conversation with Ben about lodging a Microsoft ticket for the Link security remediation. To ensure we are all on the same page, can I confirm this is the issue being referred to ?

Security remediation 3.2

35335

S30 [redacted]

S35 [redacted]

Feel free to let me know if this is no longer required.

Matt

Matthew McCreadie

Inspector
Tasmania Police
Project Unify

S36

PROJECT UNIFY

PROJECT LINK

KPMG

Project Link Monthly Status Report

March 2025

Summary of KPMG delivery to the Department of Police, Fire and Emergency Management

—

10 April 2025

Summary of KPMG delivery

Project Month	March 2025	Overall Status	
Prepared By	Darren Covington		Attention Required

Summary

During March, the primary focus areas included finalising the security remediation build to address the issues identified through penetration testing, completing the testing phase, and preparing for the approval gates.

- **Security remediation build** – the supplier finalised the build of the security remediation changes. This consisted of site setting configurations and the implementation of server-side logic to reinforce validations already applied via the front end. Only one item identified in the supplier's cyber security report remains outstanding, relating to the [redacted] The proposed solution available in Power Pages was rejected by the State due to the potential privacy concern [redacted] We understand the State accepted to proceed with the known security issue given the low risk.
- **System Integration Testing** – the supplier executed regression testing and system integration testing following the release of the latest solution containing the security remediation changes. The SIT exit criteria was not met initially due to 1 outstanding high severity issue relating to the [redacted] ntegration. The issue has since been resolved and the SIT Closure Report is now completed.
- **User Acceptance Testing** – user acceptance testing has been undertaken following the release of the latest solution containing the security remediation changes. Issues and feedback identified during UAT were promptly resolved and re-tested. The UAT has been completed and the resolution plan to address outstanding issues post-go-live will be published on 10/04.
- **Penetration testing** – Cyber CX executed a final round of testing and identified 3 issues that will require further investigation by the supplier. The issues are not of a risk level to preclude Go-Live.
- **Approval preparation** – Meetings were held with T&I to align on the requirements for CAB approval and the necessary documentation has been prepared for the CAB meeting.

The following change requests were issued:

- Link_CR_14 - Postponement of the go-live date from the 18th of November to the 28th of April.
- Link_CR_15 - Acceptance of current solution performance which does not meet the contractual requirements (5-6 seconds submission, instead of up to 3 seconds).

ACHIEVEMENTS THIS PERIOD (March 25)

- Security remediation build completed
- SIT completed
- Performance testing completed
- UAT completed
- Outstanding issues post-go-live
- Penetration testing completed
- Dress rehearsal completed
- CAB approval granted (8/04)
- Solution deployed to production (9-10/04)

KEY ACTIVITIES PLANNED NEXT PERIOD

April sees the delivery of several critical milestones including:

- SIT, Performance Testing and UAT Closure sign off
- Go Live Plan sign off
- Administrator guide sign off
- SteerCo sign off
- Commissioner sign off of go-live process
- BVT sign off
- DCoP, CoP and Ministerial Approval to Go Live
- Go-Live

KEY DELIVERABLES (March)

Ref	Milestone	Due Date	Status
LDA-010a	SIT Closure Report	21/03	Completed on 10/04
LDA-010b	NFT Closure Report	21/03	Completed on 10/04
LDA-010c	UAT Closure Report	03/04	Completed on 10/04

KPMG

©2025 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization. Document Classification: KPMG Confidential

Liability limited by a scheme approved under Professional Standards Legislation

Summary of KPMG delivery

AREAS OF OPPORTUNITY

Lessons Learned:

- Relying too heavily on a few key individuals creates vulnerabilities

Solutions:

- Create and maintain comprehensive documentation to support knowledge transfer (i.e., administrator guide)
- Identify and train individuals to fill critical roles in case of departures
- Record KT sessions

EMERGING CHALLENGES

- N/A

RISKS & ISSUES

RISKS: Current risk status for **high** and/or **severe** risks as follows:

- 1- Knowledge gaps in platform design and configuration S30 [redacted] will limit T&Is ability to support the solution following completion of the project.
- 2 - The repeated changeover of key KPMG staff during the Project may reduce knowledge of the product, resulting in delays to issue resolution during launch and Hypercare. support.
- **ISSUES:**
- Due to the additional work required to improve the security of the solution as per the cyber security testing findings, the go-live date was further postponed.
- 5 issues remain outstanding for resolution post-go-live:
    - 2 low severity Microsoft product bugs with an estimated resolution timeframe of June 2025 (reference #: 32166 and 31734).
    - 3 low severity issues reported by CyberCX during the final round of penetration testing (reference #: 36952, 36955 and 36956).

REQUIRED DECISIONS

DECISIONS: N/A.

KPMG

©2025 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation. Document Classification: KPMG Confidential

Liability limited by a scheme approved under Professional Standards Legislation.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

KPMG.com.au

©2024 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.

The information contained in this document is of a general nature and is not intended to address the objectives, financial situation or needs of any particular individual or entity. It is provided for information purposes only and does not constitute, nor should it be regarded in any manner whatsoever, as advice and is not intended to influence a person in making a decision, including, if applicable, in relation to any financial product or an interest in a financial product. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

To the extent permissible by law, KPMG and its associated entities shall not be liable for any errors, omissions, defects or misrepresentations in the information or for any loss or damage suffered by persons who use or rely on such information (including for reasons of negligence, negligent misstatement or otherwise).

Liability limited by a scheme approved under Professional Standards Legislation.

Document Classification: KPMG Confidential

Ref:

BUSINESS AND EXECUTIVE SERVICES

BRIEFING NOTE

TO: **Policing and Justice Solutions Steering Committee**

FROM: **Program Director, Project Unify**

SUBJECT: **Project Link - KPMG Request to Change Go-Live Date**

☐ APPROVED ☐ NOT APPROVED ☐ SUPPORTED ☐ NOT SUPPORTED ☐ NOTED Dated: / / 20	RETURN TO:

RECOMMENDATION:

- [redacted]

BACKGROUND:

- In August 2024, an acceptable contract position was agreed with KPMG for the design, build and implementation of a public facing service (Project Link) for the Tasmanian Community to report crime online to Tasmania Police.
- The agreed Project Plan for Project Link set a contractually agreed Go-Live date of 18 November 2024 for the online crime reporting solution.
- [redacted]
- [redacted]
- At the last Policing and Justice Solutions Steering Committee meeting, held on 20 March 2025, a revised forecast Go-Live date of 28 April 2025 was communicated.

CURRENT SITUATION:

- KPMG has provided DPFEM with a draft Change Request to formally move the Go-Live date from 18 November 2024 to 28 April 2025.
- [redacted]

- As tabled at the last Policing and Justice Solutions Steering Committee meeting, the Project is currently working to meet Go Live on 28th April 2025, with a Ministerial launch at Eastlands on 5th May 2025.
- S35

FINANCIAL CONSIDERATIONS:

- S38
- S38
- It should be noted that the above Estimates at Completion does not include the time expended by the Program Director, Business Lead, Atlas Project Manager, Atlas PMO Lead, Atlas Training Manager, and the Atlas Training Analyst to ensure the delivered solution meets the requirements. This amount still needs to be journaled from the Link Project to the Atlas Project and is estimated to be approximately $200,000.
- S37, S38

WORK, HEALTH, SAFETY CONSIDERATIONS:

- None.

INFORMATION DISCLOSURE CONSIDERATIONS:

- Guidance on Information Disclosure requirements are available here.

AUTHOR: **Jeremy Williams** Date: 10/04/2025
Program Director, Project Unify

CLEARED BY: **Matt McCreadie** Date: 10/04/2025
Business Lead, Project Unify

Briefing Note should be CLEARED electronically in RM8/TRIM by using the Workflow process (1) Save document in RM8/TRIM (2) Update the NOTES FIELD with CLEARED BY details and apply your USER STAMP (3) Assign document to the Addressee (4) Electronic clearing process should be continued/repeated for each/next person in the approval process, updating the notes field at each stage until final approval is received.

TECHNOLOGY GOVERNANCE COMMITTEE

Matter for Decision

Agenda No x.x – Additional Projects within Project Unify

Recommendation

That the Technology Governance Committee:

- Notes, that on the 2nd of December 2024, the Commissioner of Police approved the direct sourcing of KPMG to build:
    - A thin client (front end) for NicheRMS (Atlas)
    - A system for the online reporting of sexual offences (OSOR), in response to the Commission of Inquiry's recommendations
    - A new Police Infringement Notice system (PINS); and,
- These projects will fall under Unify; and,
- Notes, the Atlas front end and PINS will be deployed to frontline officers in line with the existing Atlas schedule, with simultaneous testing, training, and go live periods; and,
- Notes and supports the future use of additional T&I resources required to support these projects.

Background

- The Tasmania Police technology strategy highlights the need to reduce complexity, through standardising and simplifying the solutions that are used by Tasmania Police daily to:
    - Provide a consistent and engaging user experience.
    - Leverage single technology solutions where possible to minimise support costs and licence fees in line with Tasmanian whole of government agreements (e.g. Microsoft).
    - Reduce the technical debt within the DPFEM technology stack from aging unsupported systems and security vulnerabilities.

- Project Unify is currently comprised of a number of projects including:
    - Project Atlas which will replace multiple unsupported policing applications with a single Commercial-Off-The-Shelf (CoTs) records management solution (NicheRMS).
    - Project Link to enable online reporting of crime to Tasmania Police via an online portal. This online portal has been built on the Microsoft Power Platform, similarly to the Service Tasmania online portal.
- S38

S38

- In commencing Project Unify, and undertaking significant user experience validation across Tasmania Police, Project Unify has identified considerable limitations in both the user experience and efficiency of the NicheRMS platform which places at risk the user adoption of the NicheRMS platform if it were to be implemented as-is. For example, users having to jump between multiple screens within NicheRMS to enter data on a single incident and in some cases re-enter data about an incident multiple times.
- There is a need to develop a NicheRMS front end that provides both a user centric experience as well as providing for automation and pre-population of data across multiple business processes.
- During consideration of the Unify user adoption strategy, it was highlighted that a single-entry point to policing systems through a front end was the best approach, whereby the highest usage and the highest risk activities undertaken by frontline police were to be incorporated, which included PINS.
- S38

Current Situation

- Exploration of potential efficiencies across the projects and refinement of requirements is underway.
- Financial negotiations with KPMG are underway and due to be finalised within the month.
- Contract amendments are being overseen by Minter Ellison with consultation from the Office of the Crown Solicitors. This is expected to be finalised within the next 12 weeks.
- Atlas front end and PINS will be incorporated under Project Unify, as the singular governance structure will facilitate the utilisation of a common technical platform and alignment of schedules. This is crucial to preventing a technical sprawl whereby duplicate or inelegant interfaces are developed, leading to additional timescales and cost, and policing systems

that are more complex to operate, manage and extend. And is expected to have the following benefits:

- Delivery of a better technology system that provides a consistent, enhanced, and user centric experience for all members.
- A core policing platform for Tasmania Police that provides improved data quality and timeliness of data for policing.
- Significant improvements in employee satisfaction, engagement and use of core policing platforms.
- Increased productivity with timely and efficient processing of information in the field, leading to increased frontline policing availability for other matters.
- The ability to submit information and complete reports more easily means flags and warnings are applied much sooner, this means increased safety for officers and community members.
- Through the user centric front end, officers will be able to provide each other with near real time intelligence and information sharing, better informing officers and increasing their situational awareness.
- The funding for the relevant projects is consolidated under Project Unify and provides savings through the use of a consistent platform, third party providers as well as significantly reducing the time and cost of the procurement process.
- By significantly reducing the time and cost of the procurement process, DPFEM will see financial savings, which can be re-invested into the development of the applications.

- The current PINS steering committee will disband and the PINS project will report to the Police and Justice Steering Committee.
- PINS will be resourced separately to Project Unify, with recruitment due to commence shortly. Peter Shearer is the Project Manager for PINS.
- Peter Shearer will also project manage the user interface aspect of the Atlas front end, with the Atlas project manager and team responsible for the integration and back-end data repository.
- Atlas, the Atlas front end and PINS are expected to go live simultaneously. The aim is to consolidate the testing and training periods and change management activities. Due to a few Atlas modules already built and ready for testing, additional testing will be required for the front end. This will have an impact to the T&I workplan.
- Online Sexual Offence Reporting will leverage Project Link, utilising the same technology, reducing build and testing timeframes.

- Expected impact on Technology and Innovation include:

- Additional resourcing requirements for testing – timeframes to be determined.
- Additional resourcing requirements for security testing oversight - timeframes to be determined.
- Additional application development resourcing requirements for SME consultation – FTE to be determined.
- Additional resourcing for deployment.
- The Business Systems Support team will attend training on the additional systems.

Next Steps

- Finalisation of contract.
- Development of project plan.
- Consolidation of project schedules. PINS, Atlas front end and Atlas will go live simultaneously.
- Communication will be distributed to the broader Unify project team, the Project Management Office, and the whole of DPFEM once the contract is finalised.
- Project Unify to further consider T&I project resourcing requirements. An update will be provided to the Technology Governance Committee once known.

Clearance

Tim Rutherford
Chief Information and Technology Officer

Date: 12 March 2025

Garth, Rhiannon

From: S36
Sent: Thursday, 20 March 2025 2:18 PM
To: McCreadie, Matthew; Brumby, Eric
Cc: Macleod, Ellie; S36 Brown, Clare; S36 Williams, Jeremy
Subject: Updated security remediation plan with the performance results
Attachments: Security Remediation Plan v2.2.xlsx

Hi Eric and Inspector McCreadie,

As requested during the standup, we updated the security remediation plan to include the performance results after the security remediation release.
Please refer to the "Performance Results" worksheet. We also updated column M on the "Remediation Overview" worksheet to reflect the performance testing findings.

Please let us know if you have any questions or feedback.

Best regards,

S36

Garth, Rhiannon

From: Haynes, Michael
Sent: Thursday, 20 February 2025 11:02 AM
To: McCreadie, Matthew; Giles, Ben; Williams, Jeremy; Brown, Matt; Macleod, Ellie
Subject: RE: Security Testing

Hi everyone,

S35

Cheers
Michael

From: McCreadie, Matthew S36
Sent: Wednesday, 19 February 2025 11:43 AM
To: Giles, Ber S36 Villiams, Jeremy S36 Brown, Matt S36 Macleod, Ellie S36 laynes, Michael S36
Subject: RE: Security Testing

Hi all,

Yes, Evidence.Com is currently used identically to how we propose to use it in Link – via the online traffic crash reporting.

Eric was involved in these discussions with Axon, and I have asked him to provide the details of the engagement and approval and security inherent to Evidence.Com. and to answer any other questions you have.

Cheers

Matt

Matthew McCreadie
Inspector
Tasmania Police
Project Unify

S36

From: Giles, Ben S36
Sent: 19 February 2025 10:36
To: Williams, Jeremy S36 Brown, Matt S36
Macleod, Ellie S36 Haynes, Michael S36
Cc: McCreadie, Matthew S36
Subject: RE: Security Testing

S35

Do we currently use evidence.com for other external links to the public?

From: Williams, Jeremy S36
Sent: Wednesday, 19 February 2025 8:06 AM
To: Brown, Matt S36 ; Macleod, Elli S36 Giles, Ben
S36 Haynes, Michael S36
Cc: McCreadie, Matthew S36
Subject: RE: Security Testing

Team

When you have completed your review of the KPMG penetration test report I would like to understand if there are any security issues that would a showstopper for a Link Go-Live if they remain unresolved.

Many thanks

Regards,

Jeremy Williams

Program Director
Project Unify

Department of Police, Fire and Emergency Management
S36

From: Brown, Matt S36
Sent: Tuesday, 18 February 2025 3:00 PM
To: Macleod, Ellie S36 Giles, Ben S36 Haynes, Michael
S36
Cc: Williams, Jeremy S36 McCreadie, Matthew

S36

Subject: Re: Security Testing

Hi Team,

S35

Matt

Matt Brown

Manager ICT Infrastructure

S36

From: Macleod, Ellie S36
Sent: Tuesday, February 18, 2025 2:24 PM
To: Giles, Ben S36 Brown, Matt S36 Haynes, Michael S36
Cc: Williams, Jeremy S36 McCreadie, Matthew S36
Subject: Security Testing

Good afternoon,

As per the meeting, both the CyberCX and KPMG report can be found in the following folder: 11.08 Security Testing

Please review and provide relevant feedback in the tracker located in the folder. We are working to identify the critical actions that must be addressed before Go-Live and those that can be deferred or may not require action. Additionally, please specify whether each action falls under the responsibility of the State or KPMG.

We would appreciate it if you could complete this by Thursday. I will compile the feedback, and if you believe a follow-up meeting is necessary for discussion, please let me know, and I will arrange it.

Thank you in advance,

Ellie

KIND REGARDS,

ELLIE MACLEOD

PROJECT MANAGEMENT OFFICE
PROJECT UNIFY
DEPARTMENT OF POLICE, FIRE AND EMERGENCY MANAGEMENT
S36



Garth, Rhiannon

From: McCreadie, Matthew
Sent: Tuesday, 27 May 2025 9:31 AM
To: Williams, Jeremy
Subject: RE: Security Related Issue - Project Link

Hi Jeremy,

Yes, but perhaps only after we get Eric to check and update with more specific details ?

Thoughts ?

Cheers

Matt

From: Williams, Jeremy <Jeremy.Williams@dpfem.tas.gov.au>
Sent: 27 May 2025 09:23
To: McCreadie, Matthew <Matthew.McCreadie@police.tas.gov.au>
Subject: RE: Security Related Issue - Project Link

Thanks Matt.

I think this should be shared with the CITO S35 S35

What do you think?

Regards,

Jeremy Williams

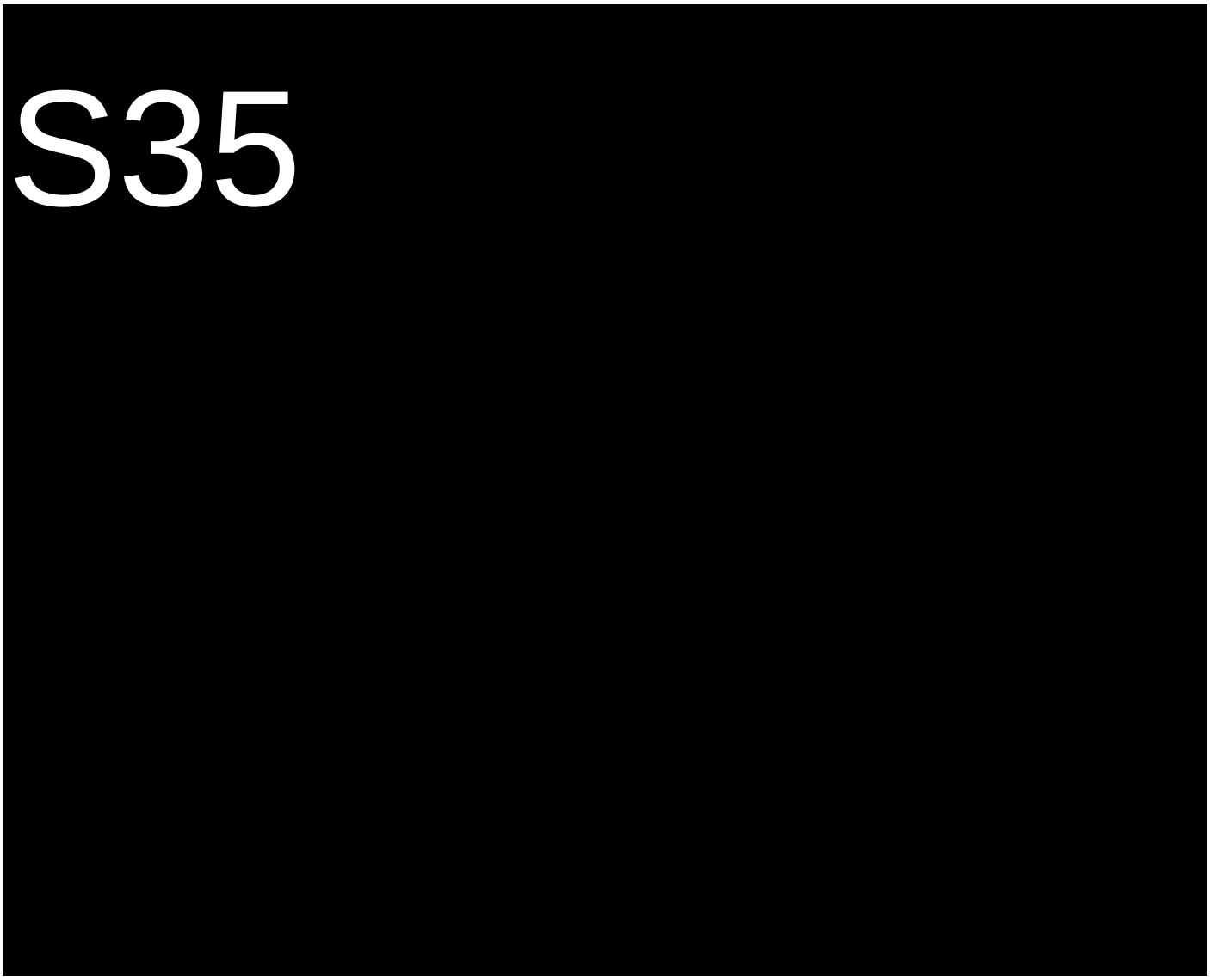
Program Director
Project Unify

Department of Police, Fire and Emergency Management
S36

From: McCreadie, Matthew S36
Sent: Tuesday, 27 May 2025 7:10 AM
To: Williams, Jeremy S36
Cc: Brumby, Eric S36 Macleod, Ellie S36
Subject: Security Related Issue - Project Link

Morning Jeremy,

S35



Eric and Ellie,

Feel free to add to, or update any of the above

Kind regards,

Matt

Matthew McCreadie
Inspector
Tasmania Police
Project Unify

S36



PROJECT UNIFY

PROJECT LINK

Garth, Rhiannon

From: Brown, Clare
Sent: Friday, 31 January 2025 12:26 PM
To: McCreadie, Matthew
Cc: Williams, Jeremy
Subject: KPMG Security Testing

Hi Matt

S35

Please refer to highlighted text below.
Thanks

CLARE BROWN

PROJECT MANAGEMENT OFFICE LEAD
PROJECT UNIFY
DEPARTMENT OF POLICE, FIRE AND EMERGENCY MANAGEMENT
S36



From: Brumby, Eric S36
Sent: Friday, January 31, 2025 11:57 AM
To: Brown, Clare S36
Subject: FW: Meeting to discuss KPMG security testing of the Project Link solution

ERIC BRUMBY
S36

From: Brumby, Eric
Sent: Thursday, 23 January 2025 2:21 PM
To: S36 Brown, Matt S36 ; Joannah Austen S36 Lee, Alex S36
Cc: Macleod, Ellie S36 S36 S36 Haynes, Michael S36
Subject: RE: Meeting to discuss KPMG security testing of the Project Link solution

Hi everyone,

Just confirming that Thomas from KPMG will be commencing their cybersecurity testing tomorrow.

(Note that this is separate to the CyberCX cybersecurity testing which will commence on 3/02.)

The testing will be according to the scope as agreed, and will initially be from a public-facing perspective until Thomas has been on-boarded and has clearance.

Please let me know if you have any concerns with this.

Cheers,
Eric.

ERIC BRUMBY
S36

From: Brumby, Eric
Sent: Thursday, 23 January 2025 11:48 AM
To: S36 S36
Cc: Macleod, Ellie S36 S36 Joannah Austen S36 Lee, Alex S36
Subject: RE: Meeting to discuss KPMG security testing of the Project Link solution

Hi S36

As discussed, this approach is ok. We will advise as soon as Thomas's onboarding is complete so that he can undertake the other aspects.

S36 is the WAF change a you thing? 😊

Cheers,
Eric.

ERIC BRUMBY
S36

From S36 S36
Sent: Thursday, 23 January 2025 11:41 AM
To: Brumby, Eric
Cc: Macleod, Ellie S36
Subject: RE: Meeting to discuss KPMG security testing of the Project Link solution

Hi Eric,

We would like to commence the preliminary pen testing tomorrow focusing on the online forms while the onboarding process is in progress. Can you please confirm if we can proceed?
To perform this activity, can you please include Thomas' IP address S36 to the WAF exclusion list?

Thank you.

Best regards,

S36

From: Brumby, Eric S36
Sent: Tuesday, 21 January 2025 6:17 PM
To: S36
Cc: Macleod, Ellie S36 Brown, Matt S36 Lee, Alex S36 Joannah Austen S36 Haynes, Michael S36
Subject: Re: Meeting to discuss KPMG security testing of the Project Link solution

Great, thanks S36

From: S36
Sent: Tuesday, January 21, 2025 5:54:06 PM
To: Brumby, Eric S36
Cc: Macleod, Ellie Brown, Matt S36 Lee, Alex S36 Joannah Austen S36 Haynes, Michael S36
Subject: RE: Meeting to discuss KPMG security testing of the Project Link solution

Hi Eric and Matt,

Thank you, that would be great if possible.
I will schedule a session with S36 and Thomas to ensure that Thomas has the necessary background information to proceed with this activity.
Thomas belongs to the same team as S36 and specialises in Cyber Security Testing. I will share his CV tomorrow.

Best regards,

S36

From: Brumby, Eric S36
Sent: Tuesday, 21 January 2025 4:48 PM
To: S36
Cc: Macleod, Ellie S36 Brown, Matt S36 Lee, Alex S36 Joannah Austen S36 Haynes, Michael S36
Subject: FW: Meeting to discuss KPMG security testing of the Project Link solution

Hi S36

Please see Matt's response below.

Can we please ensure that,

- the new tester is briefed by S36 on the agreed scope of testing
- the tester is a suitably qualified and experienced member of KPMG's security team

If so, then the approach that Matt has proposed would mean they can get started with the public-access testing while the on-boarding is completed.

Cheers,
Eric.

ERIC BRUMBY

S36

From: Brown, Matt S36
Sent: Tuesday, 21 January 2025 4:41 PM
To: Brumby, Eric S36 Lee, Alex S36
Cc: Haynes, Michael S36 Macleod, Ellie S36
Joannah Austen S36
Subject: Re: Meeting to discuss KPMG security testing of the Project Link solution

Hi Eric,

I assume the testing is still with the KPMG dedicated security team and just a change of tester.
If so we can move to the normal police check and on-boarding for the authenticated access 😊 once we have the contact details.

As we wait KPMG could start with the non-authenticated testing as per the Scope already agreed. Using the system as the public will.

Matt

From: Brumby, Eric S36
Sent: Tuesday, January 21, 2025 4:28 PM
To: Brown, Matt S36 ee, Alex S36
Cc: Haynes, Michae S36 Macleod, Ellie S36
Subject: RE: Meeting to discuss KPMG security testing of the Project Link solution

Hi Alex and Matt,

This is a status update to keep you across the cybersecurity/pen testing that KPMG is completing.

I understand that S36 is no longer available and am awaiting details of the resource that KPMG is putting forward.

I will provide the new person's CV to you as soon as I get it, and I'll ask KPMG to make sure the person is fully briefed by S36 n preparation.

On the assumption that the testing will be as previously agreed, are you happy with this approach?

Cheers,
Eric.

ERIC BRUMBY

[redacted]

From: Brumby, Eric
Sent: Monday, 20 January 2025 2:06 PM
To: Brown, Matt [redacted] Lee, Alex [redacted]
Cc: Haynes, Michael [redacted] Macleod, Ellie [redacted]
Subject: RE: Meeting to discuss KPMG security testing of the Project Link solution

Hi Matt and Alex,

Following the final change to our schedule, I just wanted to give you a heads-up that KPMG will be commencing the agreed cybersecurity testing tomorrow.

I am getting confirmation from KPMG at the moment, and will provide you with any additional information that I receive.

Cheers,

Eric.

ERIC BRUMBY

[redacted]

From: Brown, Matt [redacted]
Sent: Wednesday, 8 January 2025 12:51 PM
To: Brumby, Eric [redacted] .ee, Alex [redacted]
Cc: Haynes, Michael [redacted]
Subject: Re: Meeting to discuss KPMG security testing of the Project Link solution

Hi Eric,

I believe we are right to go and have the correct KPMG security team engaged.

I have no more info if the tools are available to the tester sorry.

It doesn't look like we need to notify anyone apart from our teams.

Microsoft Cloud Penetration Testing Rules of Engagement

Security testing recommendation for Power Platform workloads - Power Platform | Microsoft Learn

Matt Brown

Manager ICT Infrastructure

S36

From: S36
Sent: Thursday, 19 December 2024 4:34 PM
To: Brumby, Eric ; S36
Cc: S36 ; S36 ; S36 ; S36
Subject: Meeting to discuss KPMG security testing of the Project Link solution

Hi Eric,

Thank you for the discussion earlier. Based on our conversation, please find the following key points:

1. **Scope of Testing**
    - The test will focus on two components of the platform:
        - **Application:** PowerApps, Power Pages, etc.

[redacted]

4. **User account Documentation**
    - I have sent the required documentation for my police check and user account setup.

Thank you again for your time. Please let me know if you need any additional information or have further questions.

Best regards,

[redacted]

KPMG

[redacted]

kpmg.com.au

S36

****
*
©2024 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation. Liability limited by a scheme approved under Professional Standards Legislation.
****
*

CyberCX

OMCRS Web Application Penetration Test

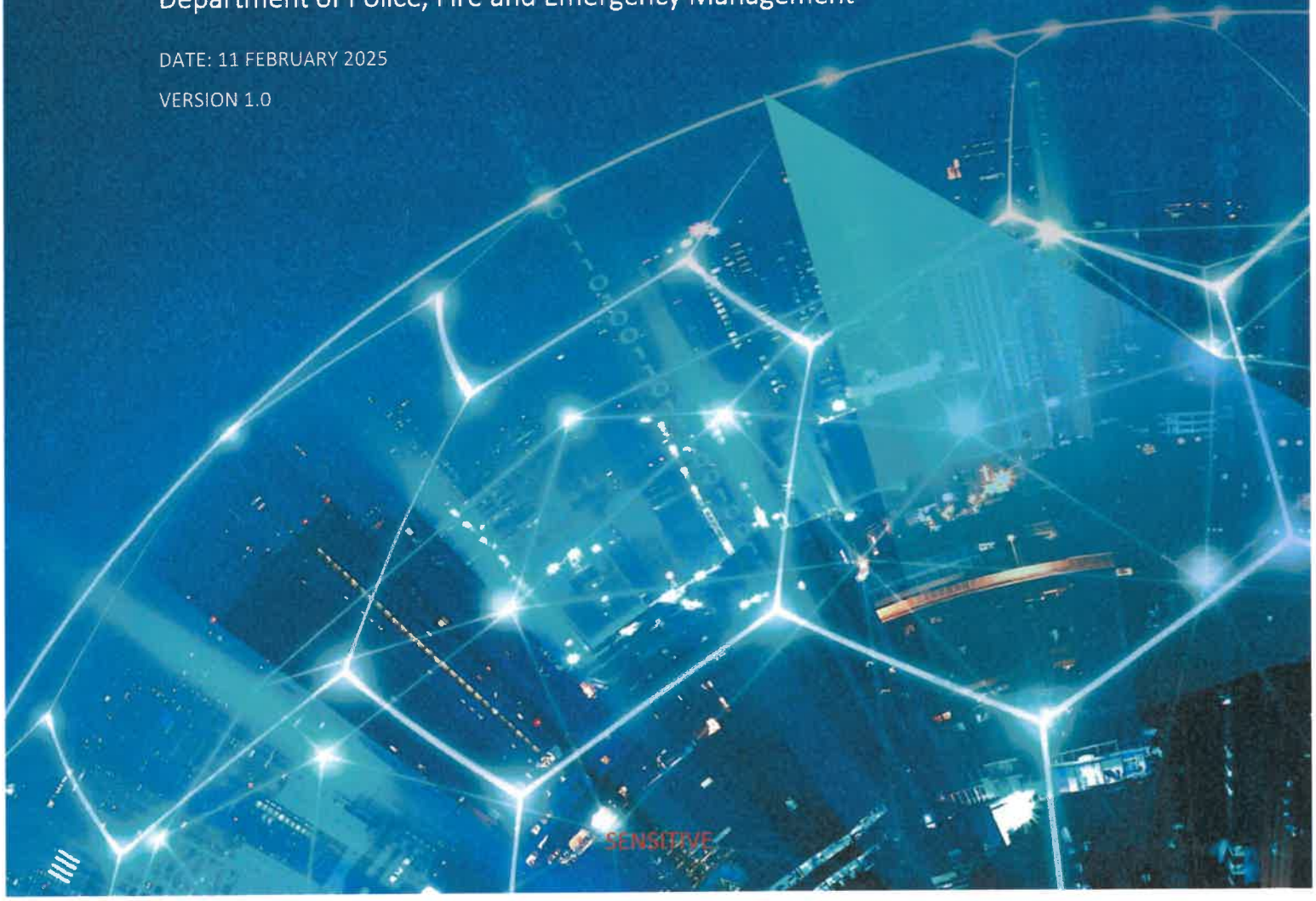
Report

Prepared by CyberCX on behalf of

Department of Police, Fire and Emergency Management

DATE: 11 FEBRUARY 2025

VERSION 1.0



SENSITIVE

REPORT

OMCRS Web Application Penetration Test

VERSION 1.0

11 February 2025

Lead Author

S36

CyberCX

SECURITY TESTING & ASSURANCE PRACTICE

SENSITIVE

This report is intended for multiple reading audiences, and as such is divided into sections to enable the reader to quickly focus on the elements that are most meaningful. For all readers, their section includes the outcome of the service as well as actionable recommendations. Consolidated research, and detailed supporting appendices are included to assist all readers in understanding the technical issues raised within the report, and importantly the associated risks. The sections include:

Executive Summary

(Page 6) The Executive Summary is aimed at board level and senior stakeholders, focusing on the business context rather than technical detail. This section provides high level context of systemic issues resulting from major findings, their impact to the business and recommended risk management strategies.

Technical Summary

(Page 7) The Technical Summary is a bridging section between the Executive Summary and Technical Findings and Recommendations section. Suitable for anyone who wants more context and detail but does not wish to read the more comprehensive and technically detailed sections that follow.

Technical Details

(Page 10) The Technical Details section provides all the information needed to understand the cause, effect, and remediation advice for each individual finding identified. For each finding, the breakdown of the risk assignment is also provided.

Appendices

(Page 20) This section includes supporting information on the ratings system, work methodologies, further details on specific findings (where required), and a summary table of all findings included within the report.

© CyberCX 2025

SENSITIVE

Contents

1 Executive Summary 6
1.1 Sector Threat Intelligence Summary 6
1.2 Assessment Summary 6
1.3 Key Recommendations 6
2 Technical Summary 7
2.1 Scope 7
2.1.1 Web Application Testing 7
2.2 Summary of Findings and Recommendations 8
2.3 Recommended Remediation Order 8
2.3.1 Short Term 8
2.3.2 Long Term 8
3 Technical Details: Web Application Penetration Test 10
3.1 Findings and Recommendations 10
3.1.1 [redacted] 10
3.1.2 13
3.1.3 15
3.1.4 18
Appendix A Testing Methodology 20
Appendix A.1 Web Application Penetration Testing 20
Appendix B Technical Risk Rating 23
Appendix C Project Limitations 25
Appendix D CyberCX Threat Intelligence Summary 26
Appendix D.1 Sector Cyber Threat Snapshot 27
Appendix E TLS / SSL Certificate and Configuration Summary 29
Appendix E.1 Certificate Details 29
Appendix E.2 [redacted] 31
Appendix E.3 31
Appendix E.4 31
Appendix E.5 32
Appendix E.5.1 32
Appendix E.5.2 32
Appendix E.5.3 32
Appendix E.5.4 33
Appendix E.5.5 33
Appendix E.5.6 33
Appendix E.5.7 34
Appendix E.6 34
Appendix E.6.1 35
Appendix E.7 35
Appendix E.8 35
Appendix F Summary of Findings 36
Appendix F.1 Web Application Penetration Test 36

© CyberCX 2025

SENSITIVE

Report Preparation

Action	Name	Title
Prepared by	S36 [redacted]	
Reviewed by		
Released by		

Revision History

Version	Revision Description	Date
1.0	Document release	11 February 2025

Distribution List

Name	Organisation	Title
Alex Lee	Department of Police, Fire and Emergency Management	Head of Cyber Security
Eric Brumby	Department of Police, Fire and Emergency Management	Project Manager
Ellie Macleod	Department of Police, Fire and Emergency Management	Project Team

LEGAL NOTICE

Unless otherwise agreed in writing, all intellectual property rights, including copyright, trade secrets, know-how, and methodologies in this document are owned by CyberCX Pty Ltd (CyberCX). CyberCX's client may use this material for its own business purposes, but may not distribute or reproduce this document, in whole or in part, or otherwise supply it for use by any third party, without the prior written consent of CyberCX. CyberCX appreciates your cooperation in protecting its intellectual property.

1 Executive Summary

Overall Rating
Low

CyberCX was engaged by Department of Police, Fire and Emergency Management (DPFEM) to perform penetration testing services against their Online Minor Crime Reporting System (OMCRS). The objective of this assessment is to identify security weaknesses, specifically unauthorised access and information disclosure of submitted cases.

1.1 Sector Threat Intelligence Summary

The Cyber Intelligence (CI) team at CyberCX determined that the most likely type of adversary to target the Australian Government sector would be nation-state actors (Refer to Appendix D), with their primary goals to perform espionage and foreign interference pre-positioning for sabotage

The complete sector snapshot summary that was leveraged during this engagement has been included in the Appendix D.

1.2 Assessment Summary

S30

The overall security posture of the application was found to be strong. It was apparent that the solution design, development frameworks and standards selected for the OMCRS were well thought out and implemented.

However, one low and several informational findings were identified during testing. CyberCX recommends that these findings are resolved to improve the overall security posture of the application and align with security best practices.

1.3 Key Recommendations

Key recommendations to address the findings in this report are outlined below.

Summary of Recommendations

-
- S30

© CyberCX 2025

SENSITIVE

2 Technical Summary

2.1 Scope

The testing was performed as described in the scope agreed between CyberCX and DPFEM per the proposal 2024071072895. Refer to Appendix A for a summary of the methodologies used.

The specific URL's, roles, platforms and similar are detailed below.

2.1.1 Web Application Testing

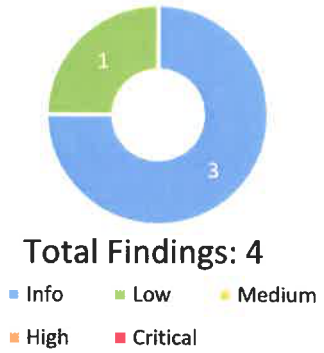
Web Application Testing	
URLs	• [redacted] S30
Roles	Unauthenticated
Source Code Provided	No
Environment	PRE-PROD
Test Period	03 February - 10 February 2025
Exclusions	• S30 [redacted]
Areas of Focus	S30 [redacted]

© CyberCX 2025

SENSITIVE

2.2 Summary of Findings and Recommendations

[redacted]



[redacted]

2.3 Recommended Remediation Order

CyberCX recommends the following remedial actions be implemented or improved to address the issues identified in this report, ordered by the suggested priority:

2.3.1 Short Term

- [redacted]

2.3.2 Long Term

- [redacted]

© CyberCX 2025

SENSITIVE

Although these issues do not pose an immediate threat to DPFEM, it is recommended that these findings be resolved to align with industry best practices.

© CyberCX 2025

SENSITIVE

3 Technical Details: Web Application Penetration Test

3.1 Findings and Recommendations

3.1.1 S30

Low

Consequence Medium Likelihood Rare

Issue Description

S30

Implication

S30



Recommendation



© CyberCX 2025

References

- [redacted]
- S30
- [redacted]

© CyberCX 2025

SENSITIVE

3.1.2 S30

Info

Consequence N/A **Likelihood** N/A

Issue Description

S30

Affected

S30

Implication

S30

Reproduction and Evidence

S30

Recommendation

S30

© CyberCX 2025

[redacted]

S30

References

[redacted]

S30

© CyberCX 2025

SENSITIVE

3.1.3 S30

Info

Consequence	N/A	Likelihood	N/A

Issue Description

S30

© CyberCX 2025

SENSITIVE

[redacted]

S30

Reproduction and Evidence

[redacted]

S30

Recommendation

[redacted]

S30

References



© CyberCX 2025

SENSITIVE

3.1.4 S30

Info

Consequence N/A **Likelihood** N/A

Issue Description

S30

Affected

Refer to Appendix E for further information regarding:

- A detailed explanation of the risk each issue poses.
- A tabular summary of protocols supported and not supported.
- A tabular summary of cipher suites supported and not supported.
- Best practice configuration settings and recommendations.

Implication

S30

Reproduction and Evidence

S30

© CyberCX 2025

SENSITIVE

Recommendation



References



© CyberCX 2025

Appendix A Testing Methodology

Appendix A.1 Web Application Penetration Testing

CyberCX utilises a staged approach for conducting a web application penetration test. Each stage of a web application penetration test is described in detail in the table below.

Stage	Description
[redacted]	[redacted]
Authorisation Testing	[redacted]
Application Design	[redacted]

© CyberCX 2025

SENSITIVE

CyberCX's web application and web service penetration testing methodology focuses on assessing the following key domains:

Component	Description
S29	

© CyberCX 2025



Note: The components contained above are in no way meant to be an exhaustive list of the tests that will be performed during an engagement. It is provided to illustrate our methodology and the testing techniques that are commonly performed during these types of reviews. The final testing performed depends entirely on components and weaknesses identified from upfront threat modelling conducted.

© CyberCX 2025

SENSITIVE

Appendix B Technical Risk Rating

Technical Risk vs Business Risk

The provided rating indicates the assessment by CyberCX as it relates to the likelihood and high-level consequences of an issue being found and exploited, from the location from which the testing was performed. Controls such as protective monitoring, personnel vetting, or restrictions on access to the location from which testing took place, are not considered. Likewise, this is not weighted for the level of threat a given organisation may be under, which may raise the likelihood in some situations. It is not possible for CyberCX to quantify financial or reputational risks for any client (within the scope of a penetration test) and so the consequences for a typical business environment are used.

As such, the vulnerability rating is not a measure of business risk, but rather is a summary of the overall importance CyberCX deems a vulnerability to have on average. It is strongly recommended that the organisation evaluate this rating considering other controls, risk tolerance, asset values, and other criteria, and determine business risk accordingly.

Consequence

Consequence is a high-level approximation of the impact if an issue was exploited to its fullest potential.

Very Low	Low	Medium	High	Critical
Little or no damage. May assist an adversary in collecting information which could be useful for other attacks. For example, internal IP address or product version disclosure.	Minor reputational damage. Loss of confidentiality of information which could be embarrassing to the system owner.	Loss of confidentiality of low-sensitivity PII. Ability to act as other non-administrative users	Administrative / privileged control over application. Loss of confidentiality of either sensitive PII for a small number of users, or less sensitive PII for large numbers of users. Possible non-fatal physical harm. Significant financial costs.	Privileged control over underlying host, and / or backend data storage. Loss of confidentiality for large amounts of sensitive PII. Very high, possibly business-altering, financial costs. Possible loss of life.

Likelihood

Likelihood is a measure combining how difficult a vulnerability is to find and to exploit. Likelihood is not intended to be interpreted as a forecast regarding the statistical chances of a future attack.

Rare	Unlikely	Possible	Likely	Very Likely
Cannot be found and exploited without significant / privileged internal access, and significant technical skills. Normally, requires either administrative or multiple credentials.	Unlikely to be found other than by an insider and / or requires technical / security skills to exploit. No pre-existing exploits exist. Normally, requires either administrative or multiple credentials.	Can only be discovered manually, and a custom exploit is required (although no advanced skills required to construct such an exploit). Normally, requires user credentials.	Either requires manual steps to discover, but has a pre-existing (or trivial) exploit, or is easy to discover but requires someone with security knowledge / skills to craft a custom exploit. Can be exploited either unauthenticated, or by a very common/large set of users.	Very easy to discover issue through automated means, and easy to exploit. Pre-existing exploit exists, or creation of an exploit is trivial. Can be exploited unauthenticated.

© CyberCX 2025

Technical Risk Rating

The Technical Risk Rating is a rating summarising CyberCX's belief in the overall importance of an issue to be resolved, based on the likelihood of it being found and exploited, the damages that may result, and the presence or absence of any mitigating controls. As discussed above, this is not an overall risk rating, and should not be used as such.

Likelihood \ Consequence	Very Low	Low	Medium	High	Critical
Very Likely	Medium	High	High	Critical	Critical
Likely	Low	Medium	High	Critical	Critical
Possible	Low	Medium	Medium	High	Critical
Unlikely	Low	Low	Medium	High	High
Rare	Low	Low	Low	Medium	High

Low	Medium	High	Critical
Where appropriate carry out local investigations.	Investigate and determine underlying causes; Consider effectiveness of controls.	Organisation needs to review the effectiveness of the current controls in place and remediate in appropriate timelines.	Immediate action must be taken to either eliminate or adequately control the risk before any activity can take place.

Informational Findings

An informational finding provides information which CyberCX believes the client should be made aware of, but which are not an exploitable issue at this time. This may be a defence-in-depth defect, or deviation from best practices. This issue probably cannot be used by an adversary at this time, however future system changes or vulnerabilities may change this.

© CyberCX 2025

SENSITIVE

Appendix C Project Limitations

As per agreement with DPFEM, the following scope exclusions were made:

- In accordance with industry best practice, all tests were performed against a test environment. Such an approach ensures that tests are performed with minimal impact to the production environment. However, in case such environments are not an exact replica of each other, there is a potential risk of vulnerabilities not being identified by this activity.
- A test of employee awareness and other human factors (social engineering) which may allow an adversary to circumvent existing security mechanisms was not performed.
- S29

© CyberCX 2025

Appendix D CyberCX Threat Intelligence Summary

CyberCX Cyber Intelligence (CI) is a dedicated team of intelligence analysts, with decades of experience across political analysis, law enforcement, security policy, cyber operations and threat intelligence. The team monitors intelligence feeds, and inputs from investigations, our clients SOC, and security testing to identify and analyse cyber threats and incidents, creating snapshots of different global regions and sectors within those regions.

If DPFEM is interested in understanding our team's methodology which was used to reach the sector snapshot conclusion, or to integrate the cyber intelligence in a more continuous manner, an executive meeting can be facilitated.

© CyberCX 2025

SENSITIVE

Appendix D.1 Sector Cyber Threat Snapshot



© CyberCX 2025

SENSITIVE



© CyberCX 2025

SENSITIVE

Appendix E TLS / SSL Certificate and Configuration Summary

For the purposes of this appendix fields are determined as follows:

		Description	Actions
Rating	Informational	Setting has no impact and is provided for informational purposes	No action is required
	Secure	Conforms to best practices and is considered fit for purpose	No action is required
	Warning	Does not conform to best practices or errors were encountered	Investigate and determine underlying causes; Consider updating
	Insecure	Poses a threat or is misconfigured or unsupported	Review the property and remediate in appropriate timelines

Appendix E.1 Certificate Details

[redacted]

S30

© CyberCX 2025



© CyberCX 2025

SENSITIVE

Appendix E.2 TLS/SSL Protocol Support

Protocol
S30

Appendix E.3 TLS/SSL Protocol Issues

Issues
S30

Appendix E.4 TLS/SSL Cipher Issues

Issues
S30

© CyberCX 2025

S30

Appendix E.5 Configuration Weaknesses

S30

Appendix E.5.2 S30

S30

S30

Appendix E.5.3 S30

S30

© CyberCX 2025

SENSITIVE

S30

Appendix E.5.4 S30

S30

Appendix E.5.5 S30

S30

Appendix E.5.6 S30

S30

© CyberCX 2025



© CyberCX 2025

SENSITIVE

S30

[redacted]

© CyberCX 2025

Appendix F Summary of Findings

Appendix F.1 Web Application Penetration Test

S30

© CyberCX 2025

SENSITIVE

CyberCX

About CyberCX

The greatest force of cyber security experts

CyberCX is a global cyber security company comprising highly-skilled consultants, capabilities, and offices in Australia, New Zealand, the United Kingdom, and the United States. With a workforce of over 1,200 professionals, we are a trusted partner to private and public sector organisations helping our customers confidently manage cyber risk, respond to incidents, and build resilience in an increasingly complex and challenging threat environment.

Through our end-to-end cyber capabilities, CyberCX empowers our customers to securely accelerate opportunities in the digital economy. Our expertise is delivered across the following services:

- Strategy and Consulting
- Governance, Risk and Compliance
- Security Testing and Assurance
- Identity and Access Management
- Network and Infrastructure Solutions
- Cloud Security and Solutions
- Managed Security Services
- Digital Forensics and Incident Response
- Cyber Capability, Education and Training

Led by industry experts and delivered by cyber security specialists committed to their craft, CyberCX represents the region's best cyber security talent, applying unmatched cyber security expertise to protect and defend both local and international organisations from cyber threats.

CyberCX Pty Ltd
Level 4, 330 Collins Street
Melbourne, VIC 3000, Australia
ABN: 90 629 363 328

T:1300 031 274
cybercx.com.au
info@cybercx.com.au

SENSITIVE

Garth, Rhiannon

From: McCreadie, Matthew
Sent: Wednesday, 8 January 2025 2:43 PM
To: S36 [redacted]
Cc: Williams, Jeremy; Brumby, Eric; projectlink.documentation; Brown, Clare; Macleod, Ellie
Subject: Signed Change Request - Project Link
Attachments: SP65125010814310.pdf

Good afternoon S36 [redacted]

Please find attached the signed copies of CR 3,4 & 7. Just a quick note, that the CR reference Atlas, when they technically should reflect Link.

Kind regards

Matt

Matthew McCreadie
Inspector
Tasmania Police
Project Unify

S36 [redacted]

-----Original Message-----
From: S36 [redacted]
Sent: 08 January 2025 15:33
To: McCreadie, Matthew S38 [redacted]
Subject: Message from P651

PROJECT UNIFY

Department *of* Police, Fire *and* Emergency Management

PROJECT UNIFY 2.0

Project Change Request

1. REQUEST DETAILS

REQUEST NUMBER:	ATLAS_CR_3	KPMG CR:3
TITLE	Enhancement: Display contact details in the code verification page	
DATE OF REQUEST	13/12/2024	
CHANGE INITIATOR NAME	S36 [redacted]	
INITIATING ORGANISATION	KPMG	
SUBMITTED TO	Jeremy Williams	

2. SUMMARY OF CHANGE REQUEST

Enhancement to online form functionality, to display the mobile number or SMS that will be used to send the verification code within the Code Verification page.

3. CHANGE REQUEST DETAIL

The following changes will be implemented:

1. A new hidden section will be added to the Contact Details Verification tab and the Contact Preference, Mobile Number and Email Address fields will be added to the hidden section. Note: This is required so that the fields are available to be retrieved by the custom Jscript below.
2. Jscript will be applied to the message displayed on the Code Verification page to dynamically display content. The message will be updated from " A code has been sent to your provided preferred method of contact." to "A code has been sent to <email/ phone number>" , where <email/ phone number> will be populated dynamically with the preferred method of contact.

Note: this change applies to all 6 online forms.

DevOps reference #: 30763

4. CHANGE IMPACT

4.1 JUSTIFICATION

Currently the reporter has to navigate to the previous page to confirm that the mobile number or email address they provided are correct, in the event that the code is not received or if there is a delay.

4.2 FINANCIAL IMPACT OF CHANGE

The fee to implement this change is: $1,352.67

4.3 CHANGE FUNDING STREAM

Please indicate how this change will be funded:

☐ Change Initiating Organisation

☒ Project Unify cost centre

☐ Technology Governance Board

☐ Nil cost

4.4 PROJECT CHANGE IMPACT

BUDGET

Minor budget impact.

SCHEDULE

Estimated build duration (excluding SIT and regression): 4 hours

4.5 SUPPORT DOCUMENTATION

N/A

4.6 MODIFICATION REQUIREMENTS

N/A

5. CHANGE INITIATOR AUTHORISATION

As the delegate/s for this Project Change Request, this request is endorsed by the below representatives to proceed to the Project Unify Joint Delivery Review Forum for approval to implement:

Name/ Position	Signature
M.J. McCREADIE, INSPECTOR BUSINESS LEAD	S36

Department *of* Police, Fire *and* Emergency Management

PROJECT UNIFY 2.0

Project Change Request

1. REQUEST DETAILS

REQUEST NUMBER:	ATLAS_CR_4	KPMG CR:4
TITLE	Enhancement: Dashboard - CMU	
DATE OF REQUEST	13/12/2024	
CHANGE INITIATOR NAME	S36	
INITIATING ORGANISATION	KPMG	
SUBMITTED TO	Jeremy Williams	

2. SUMMARY OF CHANGE REQUEST

Enhancement to the online crime reporting console, to provide better visibility to information relevant to the CMUs.

3. CHANGE REQUEST DETAIL

The following changes will be implemented:

1. A new field "Reporter Setting Description" multiline text field will be added in Reporter entity, and exposed to the Reporter form.
2. Rules will be configured to make the "Reporter Setting Description" field mandatory when the "Reporter Setting" field is populated.
3. Rules will be configured to clear the "Reporter Setting Description" field when the "Reporter Setting" is modified.
4. In the scenario where the "Reporter Setting" field is automatically populated, functionality will be implemented to automatically populate the "Reporter Setting Description" field with standard description "Automatically set to blacklisted" (description will be configurable by DPFEM).
5. A new "Reporter Review Status" global option set will be configured with the options: pending review/ reviewed.
6. A new "Reporter Review Status" option set will be added to Reporter entity using the global option set. This field will be added to the Reporter form.
    a. The following system views will be configured on Reporter entity:

S38

c. [redacted]
d. [redacted]
e. [redacted]

S38

7. A new global dashboard will be configured listing the views above.
8. A new single line of text field "ORS Reference Number" will be configured on the Online Crime Report Log entity and exposed on the Online Crime Report Log form.
9. A new "Online Crime Report" lookup field will be configured against Online Crime Report Log entity, to link the Online Crime Report with the Online Crime Report Log to enable the logic below to populate the ORS Reference Number.
10. Logic will be implemented to populate the Offence Report Number on Online Crime Report Log, from the Online Crime Report.
11. A new view "Associated Online Crime Report Logs"" view against Online Crime Report Log entity, displaying the following columns:
    a. ORS Reference Number
    b. Offence Location (Suburb)
    c. Date Submitted (Descending)
    d. Date Modified
    e. Modified By
12. A new Online Crime Report Log sub-grid will be added to the Reporter form.
13. Custom development will be applied to the newly added sub-grid, so to only return Online Crime Report Logs with a matching Reporter (based on Email or Mobile Number match)
14. All five newly created views and global dashboard will be enabled on the "Offence Reporting" model driven app.

DevOps reference #: 31065

4. CHANGE IMPACT

4.1 JUSTIFICATION

[redacted]

S38

4.2 FINANCIAL IMPACT OF CHANGE

The fee to implement this change is: $4,927.93

4.3 CHANGE FUNDING STREAM

Please indicate how this change will be funded:

☐ Change Initiating Organisation

☒ Project Unify cost centre

☐ Technology Governance Board

☐ Nil cost

4.4 PROJECT CHANGE IMPACT

BUDGET

Minor budget impact.

SCHEDULE

Estimated build duration (excluding SIT and regression): 16.5 hours

4.5 SUPPORT DOCUMENTATION

N/A

4.6 MODIFICATION REQUIREMENTS

N/A

5. CHANGE INITIATOR AUTHORISATION

As the delegate/s for this Project Change Request, this request is endorsed by the below representatives to proceed to the Project Unify Joint Delivery Review Forum for approval to implement:

Name/ Position	Signature
MJMCGRATH, INSPECTOR BUSINESS LEAD	S36

PROJECT UNIFY

Department *of* Police, Fire *and* Emergency Management

PROJECT UNIFY 2.0

Project Change Request

1. REQUEST DETAILS

REQUEST NUMBER:	ATLAS_CR_7	KPMG CR:7
TITLE	Enhancement: Property damage - Conditional display of vehicle details	
DATE OF REQUEST	13/12/2024	
CHANGE INITIATOR NAME	S36 [redacted]	
INITIATING ORGANISATION	KPMG	
SUBMITTED TO	Jeremy Williams	

2. SUMMARY OF CHANGE REQUEST

The vehicle details fields were always displayed on fuel drive off, theft and property damage forms independent if a vehicle was involved or not.

Instead, the vehicle details should only be displayed if there was a vehicle involved.

3. CHANGE REQUEST DETAIL

The following changes will be implemented:

1. A new yes/no question "Was a vehicle involved?" will be configured and added to the Property Damage form.
2. The new field will be cleared, so that the reporter has to make a selection.
3. The new field will be added to a hidden section in Incident Details property damage form and locked.
4. Code will be applied in Property Damage incident details section to only show both vehicle questions if "was a vehicle involved?" = yes
5. The manual triage flow will be adjusted to only append vehicle details field to manual triage reason field if "Was a vehicle involved?" = yes.
6. The new "Was a vehicle involved?" question will be added to a hidden section in Review Page property damage form and locked.
7. Code will be applied in Property Damage Review Page section to only show both vehicle questions if "was a vehicle involved?" = yes

Note:

The vehicle details fields are only displayed for the following offence types:

- Fuel Drive Off – always displayed (no changes required).
- Theft - only displayed if eligibility criteria question "Were items stolen from a vehicle?" = yes (no changes required)
- Property Damage – to be displayed if eligibility criteria question "was a vehicle involved? = yes (as described in this change request).

DevOps reference #: 32035

4. CHANGE IMPACT

4.1 JUSTIFICATION

The purpose of this change is to improve the end user experience and avoid confusion.

4.2 FINANCIAL IMPACT OF CHANGE

The fee to implement this change is: $3,798.67

4.3 CHANGE FUNDING STREAM

Please indicate how this change will be funded:

☐ Change Initiating Organisation

☒ Project Unify cost centre

☐ Technology Governance Board

☐ Nil cost

4.4 PROJECT CHANGE IMPACT

BUDGET

Minor budget impact.

SCHEDULE

Estimated build duration (excluding SIT and regression): 7.5 hours

4.5 SUPPORT DOCUMENTATION

N/A

4.6 MODIFICATION REQUIREMENTS

N/A

5. CHANGE INITIATOR AUTHORISATION

PROJECT
UNIFY

As the delegate/s for this Project Change Request, this request is endorsed by the below representatives to proceed to the Project Unify Joint Delivery Review Forum for approval to implement:

Name/ Position	Signature
MJ MCCREDIE, INSPECTOR BUSINESS LEAD	S36

Garth, Rhiannon

From: Williams, Jeremy
Sent: Thursday, 13 February 2025 8:20 AM
To: Lee, Alex; Rutherford, Tim
Cc: McCreadie, Matthew; Macleod, Ellie
Subject: FW: Cyber CX report
Attachments: Department of Police, Fire and Emergency Management - OMCRS Web Application Penetration Test Report v1.0 11Feb2025.pdf; Re: Change Request - Project Link Go-Live (Delay to the 11th of February 2025) - Confidential (KPMG Internal Discussion Document)

Hi Alex and Tim

Just in case you have not already seen it, here is the CyberCX report on the Link penetration with an overall risk rating of low.

In comparison we have the informal report from KPMG (attached) which sets out several additional security risks identified through their own internal testing.

I would note that we are not comparing apples with apples with regards to the scope of testing conducted by both parties.

Can you please consider both reports and I will set up a meeting for us to discuss the actions that need to be taken to satisfy the Link Go-Live criteria from a security perspective.

Jeremy

Regards,

Jeremy Williams

Program Director
Project Unify

Department of Police, Fire and Emergency Management
S36

From: Macleod, Ellie S36
Sent: Wednesday, 12 February 2025 4:19 PM
To: Williams, Jeremy S36 McCreadie, Matthew S36
Cc: Brown, Clare S36 Wojcik, Aaron S36
Subject: Cyber CX report

Afternoon,

Attached the CyberCX report.

Cheers

Ellie

KIND REGARDS,

ELLIE MACLEOD

PROJECT MANAGEMENT OFFICE
PROJECT UNIFY
DEPARTMENT OF POLICE, FIRE AND EMERGENCY MANAGEMENT
S36



Performance Testing results

This release has maintained the previously observed improvements in form submissions to ORS. The results were verified via the automated performance suite.

Automated verification of the performance results shows that there is no significant changes compared between Release 1.2.0.0. and Release 1.3.0.0 indicating that the [redacted]

The realised performance improvements between Release 10.0.29 and Release 1.2.0.0 of 3.3 seconds are sustained.

Automated verification of ORS Submission

A total of 325 submissions have been run to verify the performance results, across three forms (Property, Theft & Retail Theft) with 3 different scenarios in each form (Baseline, Multiple suspects, Multiple suspects with trigger words).

Transaction Times Overview Comparison

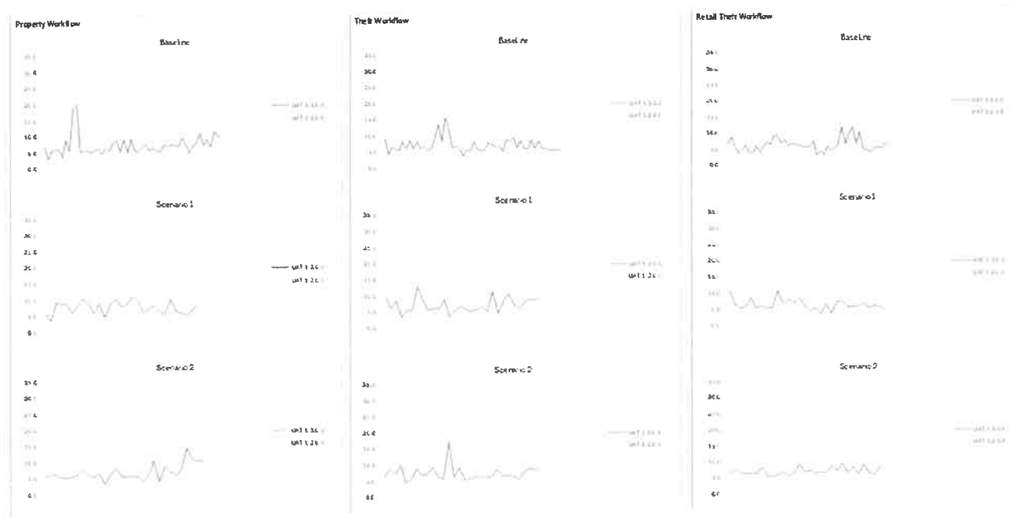
Performance Scenario's: Verification of submission step
Baseline: 0 suspects, 1 property, 0 trigger words
Scenario 1: 4 suspects, 4 property, 0 trigger words
Scenario 2: 4 suspects, 4 property, 2 trigger words

Configuration		Baseline			Scenario 1			Scenario 2		
Environment:	UAT									
Release:	UAT 1.2.0.0									
Load scenario:	10 VU Max (1 VU per second)	Property	Retailtheft	Theft	Property	Retailtheft	Theft	Property	Retailtheft	Theft
	n value	65	67	70	39	40	40	40	40	40
	Average (s)	6.5	5.7	6.4	6.4	6.7	6.2	7.2	5.9	5.7
	Highest (s)	12.3	9.7	11.9	12.0	9.1	13.2	16.0	8.2	9.2
	Lowest (s)	3.0	2.6	2.8	2.8	4.1	3.3	2.7	3.4	2.8

Total	435 Submissions
Average	6.3 Sec

Configuration		Baseline			Scenario 1			Scenario 2		
Environment:	UAT									
Release:	UAT 1.3.0.0									
Load scenario:	10 VU Max (1 VU per second)	Property	Retailtheft	Theft	Property	Retailtheft	Theft	Property	Retailtheft	Theft
	n value	30	46	50	29	30	30	30	30	30
	Average (s)	7.4	6	7	7.6	6.1	7.0	6.7	6.8	7.2
	Highest (s)	19.9	12	16	11.0	10.6	12.8	14.1	9.2	16.9
	Lowest (s)	3.1	3	3	3.4	3.2	3.2	3.0	5.3	4.2

Total	325 Submissions
Average	6.8 Sec



Automated verification Page performance

Analysis regarding the page performance of the individual steps and the transitions between pages has shown that the overall page performance is within thresholds with an average around 2.5 - 3 seconds for the key performance indicator (LCP)

[redacted]

S30

Online form step	Validation description	Condition	Validation Type	Functional Design Spec Reference	Priority
Privacy Statement Acknowledgement	Checkbox acknowledging privacy statement must be checked.	If 'I agree to the Privacy Statement' = No	Prevent submission		1
Contact Details	Make the "Email address" and "Mobile phone number" fields mandatory/optional depending on the answer to "Contact preference".	If both "Email address" and "mobile phone" are null.	Prevent submission		1
	Populate and lock the "Mobile" field if a mobile phone number was provided during the "Contact details" section.	If the mobile phone or email address doesn't match the information validated via the security code.	Prevent submission		1
	Hide the "Location of the incident" field and make "Where did it happen" mandatory if the previously provided addresses were identified as out of Tasmania, or address details were not properly provided.	If Location of the Incident street name, suburb, post code or state are null OR if State != TAS	Prevent submission		1
Incident Details	Validation checks to ensure at least one Suspect is logged if "Do you have information about, or footage of, any suspect/s?" was answered with "Yes".	If "Do you have information about, or footage of, any suspect/s?" = yes and there isn't any Suspect records associated with the Online Crime Report record	Prevent submission		5
	(For Make off without payment) Make mandatory/optional and show/hide the "Service description" field depending on the answer to "Goods/services type".	If Offence Type= Make off without payment AND Goods/ Services Type or Value is null	Prevent submission		5
	(For Property Damage, Theft, Retail Theft) Validation checks to ensure at least one Property/Good is logged.	If Offence Type= propery damage, theft or retail theft AND there isn't at least 1 property/ goods record associated with the Online Crime Report record.	Prevent submission		5
Submission	Checkbox acknowledging submission must be checked.	If 'Acknowledgement of Details Submitted' = No	Prevent submission		1

Information	Comments
S30	

Garth, Rhiannon

From: Oosterloo, Douglas
Sent: Thursday, 24 April 2025 2:05 PM
To: Joel, Craig; Wilson-Haffenden, Scott; Rutherford, Tim; S36 Parsons, Nikala
Cc: Unify; McCreadie, Matthew; Williams, Jeremy; Assistant Commissioner Capability
Subject: Change Requests for Project Link - approval out of session
Attachments: Project Unify 2.0 - Project Link - Change Request 14 Go-Live.pdf; Project Unify 2.0 - Project Link - Change Request 15 Performance 10042025.pdf

Dear P&JS (Unify) SteerCo members

As you would recall, at our meeting on 15 April 2025 the revised Go-Live date for Project Link was approved but we opted to hold off on approving the related Change Requests until we'd had a closer look at the contractual arrangements and further discussions with KPMG.

Tim Rutherford and I have now had the closer look and further discussion with KPMG (senior management). Some of those discussion are ongoing and we are confident of a positive outcome.

Our CMG including the Commissioner also had a demonstration of the new Online Crime Reporting System and has approved Go Live for this Tuesday 29 April.

I am now comfortable to approve the two attached Change Requests as they are currently worded, subject to any feedback from other members.

If you have any other views, please feel free to contact me directly before COB today, with apologies for the tight timeframe.

Doug Oosterloo
Assistant Commissioner
Capability
S36
Department of Police, Fire and Emergency Management
Accountability Integrity Respect Support

From: Unify <Unify@police.tas.gov.au>
Sent: 10 April 2025 17:36
To: Assistant Commissioner Innovation, Capability and Risk S36 Joel, Craig S36 Wilson-Haffenden, Scott S36 Rutherford, Tim S36 Whish-Wilson, Ian S36 Brumby, Eric S36 Williams, Jeremy S36 Vojcik, Aaron S36 McCreadie, Matthew S36 S36 Oosterloo, Douglas S36
Cc: Morrisby, Troy S36 Macleod, Ellie S36 Scott, Bronte S36 Brown, Clare S36
Subject: Mtg No. 46 Policing and Justice Solutions - Project Unify Steering Committee papers

Good afternoon,

Please find attached the documents for review for the upcoming meeting on the 15th of April.

The minutes from the Mtg No. 45 are currently being reviewed and will be distributed in the coming days.

Apologies for the shorter reviewal period, the meeting was brought forward due to unforeseen circumstances.

If you have any questions or concerns, please reach out.

Regards

Ellie

Kind regards,
Project Management Office
PROJECT UNIFY
DEPARTMENT OF POLICE, FIRE AND EMERGENCY MANAGEMENT
UNIFY@POLICE.TAS.GOV.AU
S36



Ref: A24/330647

BUSINESS AND EXECUTIVE SERVICES

BRIEFING NOTE

TO: **Chair, Procurement Review Committee, DPFEM**

FROM: **Jeremy Williams, Program Director, Project Unify**

SUBJECT: **Direct Sourcing - Implementation Partner Services for Project Link**

☐ APPROVED ☐ NOT APPROVED ☐ SUPPORTED ☐ NOT SUPPORTED ☐ NOTED **Assistant Commissioner G Keating** **Project Sponsor, Project Link** Dated: / /	☐ APPROVED ☐ NOT APPROVED ☐ SUPPORTED ☐ NOT SUPPORTED ☐ NOTED **Chair, Procurement Review Committee, DPFEM** Dated: / /
☐ APPROVED ☐ NOT APPROVED ☐ SUPPORTED ☐ NOT SUPPORTED ☐ NOTED Dated: / /	☐ APPROVED ☐ NOT APPROVED ☐ SUPPORTED ☐ NOT SUPPORTED ☐ NOTED **Commissioner D Adams** **Secretary, DPFEM** Dated: / /

RECOMMENDATION:

- That the Procurement Review Committee consider and approve this direct sourcing arrangement and progress this request for the approval of the Accountable Authority.
- That the Accountable Authority approve the direct sourcing of KPMG to provide implementation services for Project Link via a variation to the existing contract for implementation partner services for Project Unify.

BACKGROUND:

- In November 2020 the Tasmanian Government provided $46.1 million to the DPFEM to continue Project Unify and deliver upgrades and changes to technology.
- One of the three key outputs of Project Unify is the "development of a public facing service for the Tasmanian Community to report crime, and potentially other matters, online".
- Project Link was established as a distinct project under Project Unify to deliver a digital service for the community to report low level crime directly to Tasmania Police.
- In 2023, initial market engagement was undertaken, and which suggested the indicative external vendor costs to support the design, build and deployment of the online reporting solution was in the vicinity of $200 000.

- Soon after the market engagement the project received approval to undertake a Request for Quote (RFQ) process to procure a vendor. The Technology Governance Board approved the project budget of S38 (excluding operational and support costs).
- The Project Link RFQ was released to three suitable vendors from the Technology Services List (TSL) with two providing responses, including KPMG.
- S38 S38 to develop and implement the solution, significantly higher than the initial market estimate. As the quotes provided significantly exceeded the maximum permissible value for an RFQ (Treasurers Instruction PP-02), the RFQ was withdrawn.
- At its meeting on 17 January 2024, the Policing and Justice Solutions Steering Committee noted the failure of the RFQ process and directed Project Link to progress to a Request for Tender (RFT) process.
- The successful completion of the RFT process to procure implementation partner services for Project Unify was announced at the Policing and Justice Solutions Steering Committee meeting on 15 February 2024. Immediately after the conclusion of this meeting, there was discussion amongst members about the possibility of varying the Implementation Services Contract with KPMG (when signed) to include the Project Link scope.
- S31

CURRENT SITUATION:

- With the execution of the Project Unify Systems Implementation Partner (SIP) contract on 29th March 2024, KPMG has been engaged to provide implementation partner services to Project Unify - which includes Project Link within its auspices.
- Immediately following the execution of the SIP contract with KPMG the decision was made to pursue a contract variation to add Project Link to the scope of KPMG's services.
- To reduce the risk associated with a contract variation, and to ensure the variation will deliver Project Link outcomes, external legal services from MinterEllison have been engaged to support the OCS in the supply of transactional legal services and advice for the contract variation.
- In early May 2024, KPMG was invited to present its proposal for Project Link including a period of Q&A regarding the proposal. A series of workshops were subsequently

undertaken to allow the agency and KPMG to achieve a shared understanding of the agency's requirements, the proposed solution architecture, and the desired future state.

- During these workshops it became apparent that the use of automation within the reporting process would significantly reduce the manual handling of reports by Sworn Officers which was evident in the first proposal. To realise this benefit, the proposal was revisited with the view to increasing the level of automation in the solution.
- Following this clarification, KPMG prepared an updated proposal to reflect greater automation, provide flexibility and scalability in the solution to future proof it for new use cases and align it with the Project Unify solution architecture. The KPMG proposal also provided additional resourcing to reduce the risk of development delays should the agency have insufficient technical resources available.
- The inclusion of improved automation and robust and scalable solution architecture increased the proposal price from S37
- The scalability of the target solution architecture will position Tasmania Police to extend the scope of the solution to other online reporting, in addition to minor crime, should it choose to.
- The OCS and MinterEllison have been engaged on the updated proposal from KPMG.
- S31
- The project met with the Probity Advisor on 10 July and confirmed there are no issues with the approach being taken from a probity perspective.
- S31
- Treasurer's Instruction PP-2 provides the Accountable Authority with the discretion to directly source goods and services in certain circumstances. Clause 2.18.3 states that direct sourcing is permitted:

> "For additional goods or services (including *works*) by the original supplier (or authorised representative of the supplier) that were not included in the initial procurement, where a change of suppliers for such additional goods or services:
>
> - cannot be made for technical reasons such as requirements of interchangeability or interoperability with existing software, services or installations procured under the initial procurement, or due to conditions under original supplier warranties; and

- would cause significant inconvenience or substantial duplication of costs for the Agency;"

- The technical complexity and integrated nature of the systems and platforms transitioning during Project Unify, and specifically Offence Reporting (ORS2), are such that it would introduce both technical and project risk were another supplier to be engaged to deliver the Online Minor Crime Reporting Solution. This is further clarified as follows:



- The direct sourcing of KPMG to deliver implementation services for Link has been assessed as an efficient and effective strategy as it will leverage the existing knowledge and experience of the KPMG team to ensure the developed solution aligns and integrates with the current systems and also the future architecture of Atlas as it further develops.

- Direct sourcing represents a significant saving when compared with the cost and time required to undertake an open procurement process. Additionally, were another supplier engaged there would be significant inconvenience and duplication of costs to the Agency to on-board the supplier within the existing architectural structure.

- Treasurers Instruction PF-2 clause 2.9 provides that, as the direct sourcing is being requested in accordance with Treasurers Instruction PP-2 clause 2.18.3, a local impact assessment is not required.

FINANCIAL CONSIDERATIONS:

- The inclusion of improved automation and robust and scalable solution architecture increased the proposal price from S37

- The Project Sponsor has considered the additional amount required and confirmed that funding is available within the Project Unify Central budget.

- It is anticipated that automation within the Online Minor Crime Reporting Solution will provide value to Policing Members and the Crime Management Units by significantly reducing the manual processing requirements of minor crime reports.

WORK, HEALTH, SAFETY CONSIDERATIONS:

- Nil known.

INFORMATION DISCLOSURE CONSIDERATIONS:

- Guidance on Information Disclosure requirements are available here.

AUTHOR: **Jeremy Williams**
Program Director, Project Unify, BES

Date: 11/07/2024

CLEARED BY:

Date:

Briefing Note should be CLEARED electronically in RM8/TRIM by using the Workflow process (1) Save document in RM8/TRIM (2) Update the NOTES FIELD with CLEARED BY details and apply your USER STAMP (3) Assign document to the Addressee (4) Electronic clearing process should be continued/repeated for each/next person in the approval process, updating the notes field at each stage until final approval is received.

Ref:

BUSINESS AND EXECUTIVE SERVICES

BRIEFING NOTE

TO: **Policing & Justice Solutions Steering Committee**

FROM: **Program Director, Project Unify**

SUBJECT: **Project Link – In-principle Approval to Go-Live**

☐ APPROVED ☐ NOT APPROVED ☐ SUPPORTED ☐ NOT SUPPORTED ☐ NOTED Dated: / /	RETURN TO:

RECOMMENDATION:

That the Steering Committee notes that:

- The Online Crime Reporting System is ready to *'Go-Live'* pending completion of the outstanding activities detailed in this briefing note.
- Pending Project Sponsor approval, the Project will also brief the Commissioner on the status of the Online Crime Reporting System.
- On completion of the outstanding activities, the Project will return to the Project Sponsor seeking approval to Go-Live on the 28th April 2025.
- As part of the Project governance and following Project Sponsor approval, the Project will seek Head of Agency approval to proceed to 'Go-Live' on the 28th April 2025.

BACKGROUND:

- In October 2020, the Tasmanian Government provided the Department of Police, Fire and Emergency Management (DPFEM) with funding to develop a public facing service for the Tasmanian Community to report crime, and potentially other matters, online.
- Following the successful execution of the Project Unify contract, a supplier (KPMG) has been engaged to provide System Implementation Partner (SIP) services to Project Unify, including Project Link as a variation to the SIP contract.
- In September 2024, an acceptable contract variation was agreed with KPMG (the preferred Supplier) for the provision of the Online Crime Reporting solution (OCRS).
- The scope of this strategic action was limited to the first stage of Project Link only – the delivery of an online portal for members of the public to report crime.
- A series of workshops for in-depth analysis and consultation with stakeholder groups were conducted to define scope of offence types, monetary values, age limits, and to guide the design and functionality of the solution.

- A broad range of stakeholder groups were consulted including Intelligence Services (IS), Radio Dispatch Services (RDS), Reporting Services, Criminal Investigation Branch (CIB), and operational Divisions.
- This consultation and business analysis resulted in a comprehensive list of technical, functional and non-functional requirements to guide the development and implementation of the OCRS, and ensure the build met the agencies specifications.
- Following build completion, the Project undertook a rigorous test program including engagement with agency stakeholder groups and also externally with businesses and the public, to ensure the solution was fit for purpose.
- Public sentiment during testing was highly supportive of the OCRS, with a general consensus that the solution was simple to use.
- S35
- On 3rd April 2025 the Project submitted a request to the Technology & Innovation (T&I) Change Advisory Board (CAB) for approval to deploy the OCRS to the Production environment. On 8th April 2025 the CAB approved the Project's request.
- In consultation with Media & Communications, the Project has developed a comprehensive Communications Plan and Schedule for the launch of the OCRS
    - The Communication Plan and Schedule are currently with the Commissioner for approval.
    - The current Communication Plan and schedule are contained in CM10
        - A24/448337 - Project Link - Communications Plan v1.1
        - A24/448340 - Project Link Communications Schedule
- A Go-Live Plan and checklist has been developed for the launch of the OCRS. These documents were provided to the Steering Committee on 20th March for review.
    - A25/126795 - Project Link - Go Live Plan (LDA-014)
    - A25/126799 - Project Link - Go Live Checklist

  Note that these are living documents and small variations may occur, in alignment with governance processes.
- The Supplier will provide Hypercare for four weeks following Go-Live of the OCRS. The Hypercare Plan has been developed in consultation with key stakeholders including Technology & Innovation and BSS.
    - A25/126809 - Project Link - Hypercare Plan.

- The project has undertaken business readiness activities with key stakeholder groups, including RDS, IS, BSS and T&I to identify changes to business processes and training needs.
- Training and support have/will be provided through multiple mediums,
    - Group training has been provided to IS and T&I staff members, with recordings available to assist new staff
    - A page of support materials such as manuals and training videos will be made available on Conexus at Go-Live
    - General information about the OCRS will be made available to DPFEM staff on Conexus
    - Relevant information will be updated in the Tasmania Police Manual to reflect the introduction of the OCRS

CURRENT SITUATION

- In the approach to Go-Live there are a small number of activities to be completed prior to requesting approval to launch the OCRS:
    - S35
    - Following the deployment of the OCRS to Production, the Project will undertake Business Verification Testing to confirm the solution has deployed correctly and is fully functional.
    - The Go Live checklist and Hypercare Plan are currently undergoing final review by DPFEM to ensure alignment.
- On completion of these outstanding activities, the Project will return to the Project Sponsor seeking final approval to proceed with Go-Live on the 28th April.
- Following approval from the Project Sponsor, and in accordance with the Project governance, the project will seek approval from the Commissioner to proceed with Go-Live on the 28th April.
- Pending approval of the Project Sponsor and Commissioner, the OCRS website will be published and links added to the Tasmania Police home page.
- The Minister is currently scheduled to launch the OCRS at Eastlands on the 5th May 2025.

FINANCIAL CONSIDERATIONS

- The project has a defined budget of $1,750,000 to cover development, implementation, resources and support costs. This budget includes provisions for the initial Go-Live phase as well as Post Go-Live Support and Hypercare.
- The final negotiated fixed price with KPMG for the provision on the OCR portal for Project Link is $895,000.
- Note that the project budget does not include operational costs.

WORK, HEALTH, SAFETY CONSIDERATIONS:

- Nil

AUTHOR: **J Williams** Date: 10/04/2025
Program Director, Project Unify

Briefing Note should be CLEARED electronically in RM8/TRIM by using the Workflow process (1) Save document in RM8/TRIM (2) Update the NOTES FIELD with CLEARED BY details and apply your USER STAMP (3) Assign document to the Addressee (4) Electronic clearing process should be continued/repeated for each/next person in the approval process, updating the notes field at each stage until final approval is received.

Garth, Rhiannon

From: McCreadie, Matthew
Sent: Thursday, 24 April 2025 5:37 PM
To: Brumby, Eric; Williams, Jeremy; Macleod, Ellie
Subject: FW: OCRS Go Live Aretefacts

This is the approval from HoA to proceed to go live. So we should add this to our records please.

From: Oosterloo, Douglas S36
Sent: 24 April 2025 16:00
To: McCreadie, Matthew S36 Assistant Commissioner Innovation, Capability and Risk S36
Cc: Williams, Jeremy S36
Subject: RE: OCRS Go Live Aretefacts

Hi Matt

Please take this email as confirmation that Go Live is approved for Tuesday.

I expect the other documents will be formally approved by the COP soon, but maybe not till Monday.

Doug Oosterloo
Assistant Commissioner
Capability
S36
Department of Police, Fire and Emergency Management
Accountability Integrity Respect Support

From: McCreadie, Matthew S36
Sent: 24 April 2025 15:35
To: Oosterloo, Douglas S36 Assistant Commissioner Innovation, Capability and Risk S36
Cc: Mackenzie, Scott S36 Williams, Jeremy S36
Subject: OCRS Go Live Aretefacts

Hi AC,

Just a friendly reminder that we are still waiting on the signed Comms Plan, TPM amendment and go-live plan to be returned.

Can you also please confirm that the CoP approval at the presentation this morning is sufficient to records HoA approval to proceed to go-live or would you like one final Minute to get that ticked off and recorded ?

The above are effectively the last gateway approvals for us to start loading the communications into Conexus etc, to commence communications outwards first thing Monday.

Thanks

Matt

Matthew McCreadie
Inspector
Tasmania Police
Project Unify

S36

Accountable Authority Approval – Direct Sourcing

To: Accountable Authority
Department of Police, Fire and Emergency Management

From: A/Chair - Procurement Review Committee

Date: 10 September 2024

X APPROVED ☐ NOT APPROVED ☐ SUPPORTED ☐ NOT SUPPORTED ☐ NOTED **Accountable Authority, DPFEM** **Acting Secretary** Dated: 11 September 2024	Please return to: Secretariat, PRC

Recommendation:

As the Accountable Authority for the Department of Police, Fire and Emergency Management, you:

- approve the Direct Sourcing of implementation services for Project Link, and
- note that this will occur through a variation to KPMG's existing Systems Integration Partner contract for Project Unify.

Executive Summary:

On 20 August 2024, the Procurement Review Committee (PRC) reviewed an application from Mr Jeremy Williams, Project Director, Project Unify (A24/318047) seeking approval to directly source implementation services from KPMG for Project Link.

The PRC assessed the application and subsequently sought further clarification. PRC has reviewed the additional documentation provided and note:

- The Project has worked with and has email advice regarding this matter from Mr Simon Millington, Special Counsel of the Office of the Crown Solicitor (OCS) (A24/361105).

- Formal Probity Advice from the Project Unify independent Probity Advisor, Mr [S36] Wise Lord Ferguson has been received (A24/361112).

- A Value for Money Assessment has been conducted (A24/360222).

Contract Variation and Direct Sourcing

The DPFEM (Project Unify) awarded a contract to KPMG as the Systems Integration Partner (SIP).

A decision was subsequently made by Project Unify to seek to vary the SIP contract to include implementation services for Project Link. S31

S31

Project Unify had previously tested the market through a competitive process via a Request for Quote (RFQ), establishing the value of the initially scoped works for Project Link.

An increase in scope, additional automation features and integration alignment resulted in an additional cost applied to the original RFQ.

S31

Treasurer's Instruction PP-2 provides the Accountable Authority with the discretion to directly source goods and services in certain circumstances. Clause 2.18.3 states that direct sourcing is permitted:

> "For additional goods or services (including *works*) by the original supplier (Or authorised representatives of the supplier) that were not included in the initial procurement, where a change of suppliers for such additional goods or services:
>
> > cannot be made for technical reasons such as requirements of interchangeability or interoperability with existing software, services or installations procured under the initial procurement, or due to conditions under original supplier warranties; *and*
> >
> > would cause significant inconvenience or substantial duplication of costs for the Agency."

The PRC have considered the circumstances presented by Project Unify and assess that the reasons align to a satisfactory degree with Treasurer's Instruction PP-2 clause 2.18.3.



Details:

Procurement:	Project Link – Implementation Services
Total Value:	$895,000
PRC Outcome:	PRC has supported the direct sourcing request.
Briefing from Jeremy Williams, Project Director	A24/330647
Value for Money Assessment	A24/360222
Probity Advice	A24/361112
Consolidated advice from the OCS	A24/361105

Compliance – Treasurer's Instruction PP-2 Clause 2.18:

☑	Have the appropriate direct sourcing clauses been satisfied TI-PP-2.
☑	Has the research justified direct/limited sourcing.
☑	Has evidence of Value for Money considerations been provided.
☑	Have details of the identified supplier been provided.
☑	Has an estimated total value of the procurement been provided.
☑	Conflict of Interest Declarations have been prepared by Jeremy Williams, Eric Brumby and Glenn Keating.

MINUTE

Departmental – DPFEM

Tasmanian Government

CM references: This document - A25/152383

To: Assistant Commissioner – Capability

SUBJECT

PROJECT LINK GO-LIVE PROCESS APPROVAL (REVISED)

Critical date: 21st August 2025 (to meet the project delivery schedule)

Recommendation

That you:

- note and approve the revised Schedule for the launch of the Online Crime Reporting Solution (OCRS) (A25/288954 - DPFEM_Project_Link_Version 1.11 REMEDIATIONS_11 Aug 2025), including key governance dates as provided in this Minute.
- note the revised 'Go-Live' planning (A25/88646 - Project Link - Go Live Plan A25/88721 - Project Link - Go Live Checklist), and approve commencement of Go-Live activities by the Project.
- note that on completion of the actions noted in this Minute, the Project will return to the Steering Committee seeking endorsement to launch the OCRS.
- note the Project anticipates Head of Agency approval to launch the OCRS, and that Commissioner and Ministerial Briefing Notes will be submitted through the Steering Committee to request this approval to launch the OCRS.

Background

- In October 2020, the Tasmanian Government provided the Department of Police, Fire and Emergency Management (DPFEM) with funding to develop a public facing service for the Tasmanian Community to report crime, and potentially other matters, online.
- Following the successful execution of the Project Unify contract, a supplier (KPMG) has been engaged to provide System Implementation Partner (SIP) services to Project Unify, including Project Link as a variation to the SIP contract.
- In September, an acceptable contract variation was agreed with KPMG (the preferred Supplier) for the provision of the Online Crime Reporting Solution (OCRS) with development commencing in July 2024.
- [redacted] commissioning of a solution review by Microsoft to ensure the OCRS would be fit for purpose and meet the agencies' contractual requirements. The Supplier also undertook internal reviews to identify any additional remediations requiring attention.

- All agreed recommendations from Microsoft and Supplier reviews have been implemented and the Supplier has commenced comprehensive testing.

Current situation

- The Supplier has provided an updated Schedule which encompasses all previous delays and proposes a Go-Live date of 30th September, rather than the original date of 18th November 2024. This revised Schedule has been provided as prepared by the Supplier.
- As has previously been communicated in weekly updates, the State is conservatively recommending the addition of four weeks contingency to this timeline to accommodate any further unforeseen delays.
- On 17th April 2025, the Steering Committee provided in principle approval for the Project Go Live process and activities. The Project has updated these approved documents to reflect the revised schedule and resubmits these documents for Steering Committee review and approval (A25/88646 - Project Link - Go Live Plan A25/88721 - Project Link - Go Live Checklist). Please note these are living documents which may be subject to minor change.
- Similarly, the 'Go-Live' Communication Plan has been updated to reflect the revised schedule (A24/448337 - Project Link - Communications Plan v1.0, A24/448340 - Project Link Communications Schedule).
- Decision makers will be engaged prior to key gates to ensure they are aware of upcoming decision points and have sufficient information.
- Key governance gates for Go-Live are as follows:

When	Gate	Who
21/08	Approval to commence Go-Live activities. *(This briefing note.)*	Steering Committee
21/08	Approval of updated Communications Plan.	Steering Committee / Commissioner
2/09	Acceptance of User Acceptance Testing (UAT) report.	Business Lead
19/09	Acceptance of Cybersecurity compliance.	Manager – Information Security
19/09	Approval to deploy OCRS to Production environment.	T&I Change Advisory Board
23/09	Successful completion of BVT / acceptance of BVT report.	Business Lead
25/09	Approval to Go-Live.	Steering Committee / Project Sponsor
26/09	Final approval to launch OCRS.	Commissioner / Project Sponsor

30/09	**OCRS Go-Live *(proposed)***	

- The proposed OCRS launch date will be confirmed following consultation with the Commissioner and Office of the Minister.
- S35

Stakeholder and communications considerations

- Notification of project gate outcomes, including Go-Live, will be provided to the Project Link Steering Committee as per standard process.
- In general, public and internal stakeholder communications for the OCRS are managed within the Project Link Communication Plan.

Financial considerations

- Nil

Work, health and safety considerations

- Nil

Next steps

- The project will continue to provide weekly updates to the Policing and Justice Solutions Steering Committee as directed.
- The project will provide the Policing and Justice Solutions Steering Committee with a final briefing at its meeting scheduled on 18th September 2025, which will include an overview of the Go-Live and Communication plans, and associated documentation.
- The project will seek Policing and Justice Solutions Steering Committee approval to proceed to Go-Live at this time.

Clearance table

	NAME	POSITION	DATE
Prepared by	Eric Brumby	Project Manager (Project Link)	13/08/2025
Through	Jeremy Williams	Program Director (Project Unify)	13/08/2025
Approved			
Return to		CM tray title	

Technology Governance Committee

April 2024

To: Jeremy Williams, Project Director Unify

cc: Chief Information and Technology Officer

Please see below the out of session decision of the Technology Governance Committee - March 2024, relating to the transfer of funds from Project Recharge to Project Link (A24/19562):

The Technology Governance Committee noted that recurrent operational and support costs to maintain the new MCR online portal will be determined through the course of the RFT.

S35

But determined that Project Unify undertake the following action:

- investigate what the public commentary on this project has been.
- A submission be prepared for Budget Committee.
- Following a decision of Budget Committee the paper be updated and resubmitted to this Committee.

If you have any questions regarding this advice, please contact Louise Mills on x32352

.....

Mandy Clarke
Deputy Secretary
Chair of Technology Governance Committee

Notice of Delay – Project Link

Prepared by: S36 [redacted]

Date: 3 December 2024

Delay Details

- **LDA-010c UAT Closure Report –** UAT completion will be delayed – revised date to be confirmed (original date Wednesday 23rd October)
- **LDA-010b NFT Closure Report -** Completion of NFT will be delayed – revised date to be confirmed (original date Tuesday 15th October).

Reason for Delay

- UAT was placed on hold due to further bugs identified during the last round of UAT, exceeding the UAT exit criteria. Release version 1.0.0.30 is scheduled to be completed on the 3rd of December for SIT and regression testing on 4th of December. This release will include all outstanding UAT bug fixes, except for tickets # 32166 and 31734 which require input from Microsoft support and 32432 which requires input from the State.
- Release v1.0.0.30 will be deployed to Test (UAT) environment and available to the State for UAT on Thursday 5th of December. However, the State indicated that UAT will remain on hold until all outstanding enhancements are available, as part of release v1.1.0.0 (release timeframe to be confirmed, subject to effort estimate).
- Performance issues were identified during NFT and was resolved by applying capacity add-on licences to the environment and optimising the code based on Microsoft's recommendations. According to KPMG's performance testing results, page performance is within 3-5 seconds when navigating between pages and the submission step is executed within 10-15 seconds, with the occasional spikes of up to 30 seconds. This is due to the complexity of the final submission step, which includes the following processes:

  S30 [redacted]

- The State is not satisfied with the current performance, as it does not meet the 3 seconds acceptance criteria. An alternative solution was proposed to reduce the processing time of the confirmation page, subject to further discussion with the State to align on the next steps.

Consequence of Delay

Consequence of delay of Completion of UAT and NFT

- **Go-Live** - The delay of UAT and NFT completion will result in the postponement of the Go-Live date. The revised go-live date will be confirmed once release v1.1.0.0 timeframe is finalised (original date: 18th November 2024).
- **Hypercare -** The delay of Go-Live will result in shifting the hypercare end date. The revised hypercare end date will be confirmed once release v1.1.0.0 timeframe is finalised (original date: 16th of December 2024).
- **Warranty –** The delay of Go-Live will result in shifting the warranty end date. The revised warranty end date will be confirmed once release v1.1.0.0 timeframe is finalised (original date: 16th of February 2025).
- **Resourcing -** DPFEM and KPMG resource allocation will be extended to align with the revised Go-Live timeframe.

Notice of Delay – Project Link

Prepared by: S36

Date: 03 December 2024

Managing the Impact

The following steps will be undertaken to further minimise the delay and any subsequent impacts:

- Reduce the review cycles for UAT and NFT closure reports to 3-2-1 instead of 5-5-2
- Reduce the BVT execution to 1 day
- Review the outstanding enhancements and provide effort estimates by the 6th of December.
- Confirm solution v1.1.0.0 release date by the 6th of December.
- Revise the project schedule by the 10th of December and confirm the revised go-live date.
- Revise the go-live plan and go-live checklist to align with the revised project schedule by 11th of December.

Notice of Delay – Project Link

Prepared by S36

Date: 6 November 2024

Delay Details

- **LDA-010c UAT Closure Report –** UAT completion will be delayed by 19 days, concluding on Tuesday 19th November (original date Wednesday 23rd October)
- **LDA-010b NFT Closure Report -** Completion of NFT will be delayed by 19 days, concluding on Wednesday 13th November (original date Tuesday 15th October). Note: the revised date assumes that the performance issues are resolved by the 8th of November.

Reason for Delay

- SIT was due to commence on 24th of September and was delayed due to integration issues and due to flows not executing in the SIT environment. This has been resolved and fixes deployed, allowing SIT to officially commence on the 27th of September.
- SIT exit was postponed to the 16th of October, with the objective to allow the execution of additional test runs once all issues were resolved to confirm that the solution is stable for UAT. This resulted in a 7 days delay which impacted the commencement of UAT.
- Performance issues were identified during NFT, consisting of performance degradation, poor LCP value (11-30s instead of 2-3s) and time-outs with 20+ concurrent users accessing the online crime reporting forms. A support ticket was raised with Microsoft on 27/09 and escalated via KPMG and DPFEM channels. The issue remains under investigation to ascertain if it relates to platform, environment and/or code issues.
- UAT started on 17th of October and was placed on hold due to ongoing performance issues which prevented engaging with external stakeholders to complete UAT.

Consequence of Delay

Consequence of delay of Completion of UAT and NFT

- **Go-Live** - The delay of UAT and NFT completion will result in the postponement of the Go-Live date by 15 days, scheduled for Monday 9th of December (original date Monday 18th November). The revised Go-Live Date assumes that the performance remediation is completed by the 8th of November 2024. Delays to performance issue resolution would result in further postponement of the Go-Live Date.
- **Hypercare -** As result of the technology change freeze in effect from the 16th of December until the new year, the deployment of bug fixes/ changes during the hyper care period will be limited to 1 week post go-live. Hypercare will remain in place for 4 weeks post Go-Live, concluding on the 6th of January 2025.
- **Warranty –** The delay of Go-Live will result in shifting the warranty end date to the 9th of March 2025, instead of the 16th of February 2025.
- **Resourcing -** DPFEM and KPMG resource allocation will be extended to align with the revised Go-Live timeframe.

Notice of Delay – Project Unify

Prepared by: S36 [redacted]

Date: 1 November 2025

Managing the Impact

The following steps will be undertaken to further minimise the delay and any subsequent impacts:

- Reduce the review cycles for UAT and NFT closure reports to 3-2-1 instead of 5-5-2
- Reduce the review cycle for the Go Live Plan from 10-5-2 to 5-5-2
- Reduce the solution deployment to production from 5 days to 2 days
- Reduce the BVT execution to 1 day
- Escalate performance issues with Microsoft to ensure optimal response time
- Promptly incorporate Microsoft's recommendations

PROJECT UNIFY

Department *of* Police, Fire *and* Emergency Management

PROJECT UNIFY 2.0

Project Change Request: Project Link

1. REQUEST DETAILS

REQUEST NUMBER:	LINK_CR_15	KPMG CR:15
TITLE	Project Link – Solution Performance	
DATE OF REQUEST	10/04/2025	
CHANGE INITIATOR NAME	S36	
INITIATING ORGANISATION	KPMG	
SUBMITTED TO	Jeremy Williams	

2. SUMMARY OF CHANGE REQUEST

The current solution has not met the performance obligations stipulated in the contract. The purpose of this change request is to seek acceptance of the current solution performance.

3. CHANGE REQUEST DETAIL

The page performance upon form submission does not meet the expected performance stipulated in the contract, as per the summary below:

Criteria	Expected performance (as per contract)	Actual performance
Navigation between pages	No more than three seconds	Two to three seconds
Form submission	No more than three seconds	Five to six seconds

The supplier is seeking acceptance from the State of the actual solution performance above.

4. CHANGE IMPACT

4.1 JUSTIFICATION

The solution performance was optimised, including de-coupling processes executed on form submission to expedite the integration with ORS2 to return the Offence Report Reference Number and display on the confirmation page.

Despite the performance optimisation, the three second performance threshold could not be met.

4.2 FINANCIAL IMPACT OF CHANGE

Not applicable.

4.3 CHANGE FUNDING STREAM

Please indicate how this change will be funded:

☐ Change Initiating Organisation

☐ Project Unify cost centre

☐ Technology Governance Board

☒ Nil cost

4.4 PROJECT CHANGE IMPACT

BUDGET

No impact to the budget.

SCHEDULE

No impact to the schedule.

4.5 SUPPORT DOCUMENTATION

N/A

4.6 MODIFICATION REQUIREMENTS

N/A

5. CHANGE INITIATOR AUTHORISATION

As the delegate/s for this Project Change Request, this request is endorsed by the below representatives to proceed to the Project Unify Joint Delivery Review Forum for approval to implement:

Name/ Position	Signature

Department *of* Police, Fire *and* Emergency Management

PROJECT UNIFY 2.0

Project Change Request: Project Link

1. REQUEST DETAILS

REQUEST NUMBER:	LINK_CR_14	KPMG CR:14
TITLE	Project Link Extension	
DATE OF REQUEST	04/04/2025	
CHANGE INITIATOR NAME	S36 [redacted]	
INITIATING ORGANISATION	KPMG	
SUBMITTED TO	Jeremy Williams	

2. SUMMARY OF CHANGE REQUEST

Project extension of ~23 weeks from the original Go Live date of the 18th of November 2024.

3. CHANGE REQUEST DETAIL

The change request for project extension is due to the following reasons:

1. Performance issues arising from the final step configuration and allocation of ORS number. The performance did not meet the user experience requirements
2. Remediation of final step of ORS number allocation in the Project Link solution.
3. Through the build cycle 170 issues (112 bugs + 58 user stories) have been identified requiring resolution. Multiply defect releases requiring multiple rounds of acceptance testing (SIT, Performance, UAT) have been conducted.
4. Prioritised a list of enhancements required before go-live. Extension is necessary to implement the changes below to ensure UAT was conducted with the required solution to go-live:

CR #	DevOps Reference	Description
3	30763	Display contact details in the code verification page
4	31065	Dashboard - CMU
7	32035	Property damage - Conditional display of vehicle details

5. Penetration security testing (Internally conducted by KPMG and independent to the state conducted penetration testing by Cyber CX) has identified security issues that required remediation to meet security levels needed by the Project Link solution. This has caused a Project delay to address the below matter:

DevOps Reference #	Task	Description
35333	S30	
35335		
35334		
34914		
34914		
34917		
35336		
34915		

6. SIT and UAT will be require to be rerun after the remediations is completed.

The revised implementation timeframe is as follows:
Original project schedule:

- Go-Live Date: 18/11/2024
- Hypercare conclusion: 16/12/2024

Current revised project schedule:

- Go-Live Date: 28/04/2025
- Hypercare conclusion: 27/05/2025

4. CHANGE IMPACT

4.1 JUSTIFICATION

Due to the additional time required to implement the security enhancements, the following key areas are impacted:

- **LDA-010c UAT Closure Report –** 2nd April 2025 (previously 6th November 2024)
- **Go-Live –** 28th April 2025 (previously 18th November 2024)
- **Hypercare –** 27th May 2025 (previously 16th December 2024). Note: Hypercare will remain in place for 4 weeks post Go-Live.
- **Warranty –** 27th July 2025 (previously 16th February 2025)
- **Resourcing -** DPFEM and KPMG resource allocation will be extended to align with the revised Go-Live timeframe.
- **All details included in the attached project schedule**

4.2 FINANCIAL IMPACT OF CHANGE

Not applicable.

4.3 CHANGE FUNDING STREAM

Please indicate how this change will be funded:

☐ Change Initiating Organisation

☐ Project Unify cost centre

☐ Technology Governance Board

☒ Nil cost

4.4 PROJECT CHANGE IMPACT

BUDGET

Budget impacts are aligned with the delay to go-live, with the Supplier and State impacted as outlined in the project schedule. Both parties to bare own costs of schedule impact.

SCHEDULE

Schedule supplied in email outlining the changes to activities and go-live.

- **Go-Live** – rescheduled from 18th November 2024 to 28th April 2025.

4.5 SUPPORT DOCUMENTATION

N/A

4.6 MODIFICATION REQUIREMENTS

N/A

5. CHANGE INITIATOR AUTHORISATION

As the delegate/s for this Project Change Request, this request is endorsed by the below representatives to proceed to the Project Unify Joint Delivery Review Forum for approval to implement:

Name/ Position	Signature

PROJECT UNIFY

Department *of* Police, Fire *and* Emergency Management

PROJECT UNIFY 2.0

Project Change Request

1. REQUEST DETAILS

REQUEST NUMBER:	ATLAS_CR_3	KPMG CR:3
TITLE	Enhancement: Display contact details in the code verification page	
DATE OF REQUEST	13/12/2024	
CHANGE INITIATOR NAME	S36 [redacted]	
INITIATING ORGANISATION	KPMG	
SUBMITTED TO	Jeremy Williams	

2. SUMMARY OF CHANGE REQUEST

Enhancement to online form functionality, to display the mobile number or SMS that will be used to send the verification code within the Code Verification page.

3. CHANGE REQUEST DETAIL

The following changes will be implemented:

1. S38 [redacted]
2. Jscript will be applied to the message displayed on the Code Verification page to dynamically display content. The message will be updated from " A code has been sent to your provided preferred method of contact." to "A code has been sent to <email/ phone number>" , where <email/ phone number> will be populated dynamically with the preferred method of contact.

Note: this change applies to all 6 online forms.

DevOps reference #: 30763

4. CHANGE IMPACT

4.1 JUSTIFICATION

Currently the reporter has to navigate to the previous page to confirm that the mobile number or email address they provided are correct, in the event that the code is not received or if there is a delay.

4.2 FINANCIAL IMPACT OF CHANGE

The fee to implement this change is: $1,352.67

4.3 CHANGE FUNDING STREAM

Please indicate how this change will be funded:

☐ Change Initiating Organisation

☒ Project Unify cost centre

☐ Technology Governance Board

☐ Nil cost

4.4 PROJECT CHANGE IMPACT

BUDGET

Minor budget impact.

SCHEDULE

Estimated build duration (excluding SIT and regression): 4 hours

4.5 SUPPORT DOCUMENTATION

N/A

4.6 MODIFICATION REQUIREMENTS

N/A

5. CHANGE INITIATOR AUTHORISATION

As the delegate/s for this Project Change Request, this request is endorsed by the below representatives to proceed to the Project Unify Joint Delivery Review Forum for approval to implement:

Name/ Position	Signature
M.J. McCREADIE, INSPECTOR BUSINESS LEAD	S36

PROJECT UNIFY

Department *of* Police, Fire *and* Emergency Management

PROJECT UNIFY 2.0

Project Change Request

1. REQUEST DETAILS

REQUEST NUMBER:	ATLAS_CR_4	KPMG CR:4
TITLE	Enhancement: Dashboard - CMU	
DATE OF REQUEST	13/12/2024	
CHANGE INITIATOR NAME	S36	
INITIATING ORGANISATION	KPMG	
SUBMITTED TO	Jeremy Williams	

2. SUMMARY OF CHANGE REQUEST

Enhancement to the online crime reporting console, to provide better visibility to information relevant to the CMUs.

3. CHANGE REQUEST DETAIL

The following changes will be implemented:

1. A new field "Reporter Setting Description" multiline text field will be added in Reporter entity, and exposed to the Reporter form.
2. Rules will be configured to make the "Reporter Setting Description" field mandatory when the "Reporter Setting" field is populated.
3. Rules will be configured to clear the "Reporter Setting Description" field when the "Reporter Setting" is modified.
4. S38
5. A new "Reporter Review Status" global option set will be configured with the options: pending review/ reviewed.
6. A new "Reporter Review Status" option set will be added to Reporter entity using the global option set. This field will be added to the Reporter form.
    a. The following system views will be configured on Reporter entity:

S38

S38

7. A new global dashboard will be configured listing the views above.
8. A new single line of text field "ORS Reference Number" will be configured on the Online Crime Report Log entity and exposed on the Online Crime Report Log form.
9. A new "Online Crime Report" lookup field will be configured against Online Crime Report Log entity, to link the Online Crime Report with the Online Crime Report Log to enable the logic below to populate the ORS Reference Number.
10. Logic will be implemented to populate the Offence Report Number on Online Crime Report Log, from the Online Crime Report.
11. A new view "Associated Online Crime Report Logs"" view against Online Crime Report Log entity, displaying the following columns:
    a. ORS Reference Number
    b. Offence Location (Suburb)
    c. Date Submitted (Descending)
    d. Date Modified
    e. Modified By
12. A new Online Crime Report Log sub-grid will be added to the Reporter form.
13. Custom development will be applied to the newly added sub-grid, so to only return Online Crime Report Logs with a matching Reporter (based on Email or Mobile Number match)
14. All five newly created views and global dashboard will be enabled on the "Offence Reporting" model driven app.

DevOps reference #: 31065

4. CHANGE IMPACT

4.1 JUSTIFICATION

S38

4.2 FINANCIAL IMPACT OF CHANGE

The fee to implement this change is: $4,927.93

4.3 CHANGE FUNDING STREAM

Please indicate how this change will be funded:

☐ Change Initiating Organisation

☒ Project Unify cost centre

☐ Technology Governance Board

☐ Nil cost

4.4 PROJECT CHANGE IMPACT

BUDGET

Minor budget impact.

SCHEDULE

Estimated build duration (excluding SIT and regression): 16.5 hours

4.5 SUPPORT DOCUMENTATION

N/A

4.6 MODIFICATION REQUIREMENTS

N/A

5. CHANGE INITIATOR AUTHORISATION

As the delegate/s for this Project Change Request, this request is endorsed by the below representatives to proceed to the Project Unify Joint Delivery Review Forum for approval to implement:

Name/ Position	Signature
MJMCGUIRE, INSPECTOR BUSINESS LEAD	S36

PROJECT UNIFY

Department *of* Police, Fire *and* Emergency Management

PROJECT UNIFY 2.0

Project Change Request

1. REQUEST DETAILS

REQUEST NUMBER:	ATLAS_CR_7	KPMG CR:7
TITLE	Enhancement: Property damage - Conditional display of vehicle details	
DATE OF REQUEST	13/12/2024	
CHANGE INITIATOR NAME	S36	
INITIATING ORGANISATION	KPMG	
SUBMITTED TO	Jeremy Williams	

2. SUMMARY OF CHANGE REQUEST

The vehicle details fields were always displayed on fuel drive off, theft and property damage forms independent if a vehicle was involved or not.

Instead, the vehicle details should only be displayed if there was a vehicle involved.

3. CHANGE REQUEST DETAIL

The following changes will be implemented:

1. A new yes/no question "Was a vehicle involved?" will be configured and added to the Property Damage form.
2. The new field will be cleared, so that the reporter has to make a selection.
3. The new field will be added to a hidden section in Incident Details property damage form and locked.
4. Code will be applied in Property Damage incident details section to only show both vehicle questions if "was a vehicle involved?" = yes
5. The manual triage flow will be adjusted to only append vehicle details field to manual triage reason field if "Was a vehicle involved?" = yes.
6. The new "Was a vehicle involved?" question will be added to a hidden section in Review Page property damage form and locked.
7. Code will be applied in Property Damage Review Page section to only show both vehicle questions if "was a vehicle involved?" = yes

Note:

The vehicle details fields are only displayed for the following offence types:

- Fuel Drive Off – always displayed (no changes required).
- Theft - only displayed if eligibility criteria question "Were items stolen from a vehicle?" = yes (no changes required)
- Property Damage – to be displayed if eligibility criteria question "was a vehicle involved? = yes (as described in this change request).

DevOps reference #: 32035

4. CHANGE IMPACT

4.1 JUSTIFICATION

The purpose of this change is to improve the end user experience and avoid confusion.

4.2 FINANCIAL IMPACT OF CHANGE

The fee to implement this change is: $3,798.67

4.3 CHANGE FUNDING STREAM

Please indicate how this change will be funded:

☐ Change Initiating Organisation

☒ Project Unify cost centre

☐ Technology Governance Board

☐ Nil cost

4.4 PROJECT CHANGE IMPACT

BUDGET

Minor budget impact.

SCHEDULE

Estimated build duration (excluding SIT and regression): 7.5 hours

4.5 SUPPORT DOCUMENTATION

N/A

4.6 MODIFICATION REQUIREMENTS

N/A

5. CHANGE INITIATOR AUTHORISATION

PROJECT
UNIFY

As the delegate/s for this Project Change Request, this request is endorsed by the below representatives to proceed to the Project Unify Joint Delivery Review Forum for approval to implement:

Name/ Position	Signature
MJ McCREDIE, INSPECTOR BUSINESS LEAD	S36

PROJECT UNIFY

Department *of* Police, Fire *and* Emergency Management

PROJECT UNIFY 2.0

Project Change Request: Project Link

1. REQUEST DETAILS

REQUEST NUMBER:	LINK_CR_13.2	KPMG CR:13.2
TITLE	Project Link Extension	
DATE OF REQUEST	30/01/2025	
CHANGE INITIATOR NAME	S36 [redacted]	
INITIATING ORGANISATION	KPMG	
SUBMITTED TO	Jeremy Williams	

2. SUMMARY OF CHANGE REQUEST

Project extension from orginial Go Live of the 18th of November to the new Go Live date of the 25th of February, 2025.

3. CHANGE REQUEST DETAIL

As requested by the State, the following prioritised CRs are required before go-live:

CR #	DevOps Reference	Description
3	30763	Display contact details in the code verification page
4	31065	Dashboard - CMU
7	32035	Property damage - Conditional display of vehicle details

Project extension is required to accommodate the CRs, as per the revised project schedule below.
Original project schedule:

- Go-Live Date: 18/11/2024
- Hypercare conclusion: 16/12/2024

Current revised project schedule:

- Go-Live Date: 25/02/2025
- Hypercare conclusion: 25/03/2024

Note: In addition to the CRs, the following remaining enhancements deemed as KPMG investment will also be implemented for Go-Live:

DevOps Reference	Description	Remarks
31913	Prevent emojis in free text fields i.e. Suspect Description	The functionality currently available in the "Tell Us What Happened" field will be applied to all free text fields displayed in the online forms.
31879	Remaining error messages that are no longer relevant	The scope will be limited to triggering the total property value threshold validation whenever properties are added, deleted or modified. The message displayed upon deletion of property records will remain as per the out of the box functionality.

4. CHANGE IMPACT

4.1 JUSTIFICATION

Due to the additional time required to implement the prioritised change requests, the following key areas are impacted:

- **LDA-010c UAT Closure Report –** 5th February 2025 (original date Wednesday 23rd October).
- **LDA-010b NFT Closure Report –** 3rd February 2025 (original date Tuesday 15th October).
- **Go-Live** – 25th of February 2025 (original date Monday 18th November).
- **Hypercare –** 25th March 2025 (original date 16th of December). Note: Hypercare will remain in place for 4 weeks post Go-Live, concluding on the 25th of March 2025.
- **Warranty –** 26th May 2025 (original date 16th of February 2025).
- **Resourcing -** DPFEM and KPMG resource allocation will be extended to align with the revised Go-Live timeframe.
- **All details included in the attached project schedule**

4.2 FINANCIAL IMPACT OF CHANGE

Not applicable.

4.3 CHANGE FUNDING STREAM

Please indicate how this change will be funded:

☐ Change Initiating Organisation

☐ Project Unify cost centre

☐ Technology Governance Board

☒ Nil cost

4.4 PROJECT CHANGE IMPACT

BUDGET

Budget impacts are aligned with the delay to go-live, with the Supplier and State impacted as outlined in the project schedule. Both parties to bare own costs of schedule impact.

SCHEDULE

Schedule supplied in email outlining the changes to activities and go-live.

- **Go-Live** – rescheduled from 18th November 2024 to 25th of February 2025.

4.5 SUPPORT DOCUMENTATION

N/A

4.6 MODIFICATION REQUIREMENTS

N/A

5. CHANGE INITIATOR AUTHORISATION

As the delegate/s for this Project Change Request, this request is endorsed by the below representatives to proceed to the Project Unify Joint Delivery Review Forum for approval to implement:

Name/ Position	Signature

PROJECT UNIFY

Department *of* Police, Fire *and* Emergency Management

PROJECT UNIFY 2.0

Project Change Request: Project Link

1. REQUEST DETAILS

REQUEST NUMBER:	LINK_CR_13.3	KPMG CR:13.3
TITLE	Project Link Extension	
DATE OF REQUEST	31/01/2025	
CHANGE INITIATOR NAME	S36	
INITIATING ORGANISATION	KPMG	
SUBMITTED TO	Jeremy Williams	

2. SUMMARY OF CHANGE REQUEST

Project extension from orginial Go Live of the 18th of November to the new Go Live date of the 11th of March, 2025.

3. CHANGE REQUEST DETAIL

Delays to Go-Live have been driven by multiply factors including performance tuning of the solution, requirement for all enhancements being completed prior to UAT (orginial approach to implement CR's after go-live), bugs being addressed, and the KPMG internal pentration testing highlighting several topics to addreed by both KPMG and the State.

Project extension is required to accommodate the above items, as per the revised project schedule below.

Original project schedule:

- Go-Live Date: 18/11/2024
- Hypercare conclusion: 16/12/2024

Current revised project schedule:

- Go-Live Date: 11/03/2025
- Hypercare conclusion: 08/04/2025

4. CHANGE IMPACT

4.1 JUSTIFICATION

Due to the additional time required to implement the prioritised change requests, the following key areas are impacted:

- **LDA-010c UAT Closure Report –** 5th February 2025 (original date Wednesday 23rd October).
- **LDA-010b NFT Closure Report –** 3rd February 2025 (original date Tuesday 15th October).
- **Go-Live** – 11th of March 2025 (original date Monday 18th November).
- **Hypercare –** 8th April 2025 (original date 16th of December). Note: Hypercare will remain in place for 4 weeks post Go-Live, concluding on the 8th of April 2025.
- **Warranty –** 9th June 2025 (original date 16th of February 2025).
- **Resourcing -** DPFEM and KPMG resource allocation will be extended to align with the revised Go-Live timeframe.
- **All details included in the attached project schedule**

4.2 FINANCIAL IMPACT OF CHANGE

Not applicable.

4.3 CHANGE FUNDING STREAM

Please indicate how this change will be funded:

☐ Change Initiating Organisation

☐ Project Unify cost centre

☐ Technology Governance Board

☒ Nil cost

4.4 PROJECT CHANGE IMPACT

BUDGET

Budget impacts are aligned with the delay to go-live, with the Supplier and State impacted as outlined in the project schedule. Both parties to bare own costs of schedule impact.

SCHEDULE

Schedule supplied in email outlining the changes to activities and go-live.

- **Go-Live** – rescheduled from 18th November 2024 to 11th of March 2025.

4.5 SUPPORT DOCUMENTATION

N/A

4.6 MODIFICATION REQUIREMENTS

N/A

5. CHANGE INITIATOR AUTHORISATION

As the delegate/s for this Project Change Request, this request is endorsed by the below representatives to proceed to the Project Unify Joint Delivery Review Forum for approval to implement:

Name/ Position	Signature

First Deed of Variation

Tasmanian Technology Contract Conditions – Comprehensive Contract Details for the provision of systems integration, project and professional services to continue the implementation of the Niche Technology Records Management System

The Crown in right of Tasmania acting through the Department of Police, Fire and Emergency Management (**Customer**)

KPMG Australia Technology Solutions Pty Limited ABN 29 606 612 962 (**Contractor**)

Level 20 Collins Arch 447 Collins Street
Melbourne Vic 3000 Australia DX 204 Melbourne
T +61 3 8608 2000 F +61 3 8608 1000
minterellison.com

MinterEllison.

First Deed of Variation

Tasmanian Technology Contract Conditions – Comprehensive Contract Details for the provision of systems integration, project and professional services to continue the implementation of the Niche Technology Records Management System

Details	**3**
Parties	3
Background	3
1. Defined terms & interpretation	4
1.1 Defined terms	4
1.2 Contract defined terms	4
1.3 Interpretation	4
2. Variation of Contract	4
2.1 Variation	4
2.2 Parties bound	4
3. Acknowledgement and agreement	4
3.1 Acknowledgement and agreement by the Contractor	4
3.2 Acknowledgement and agreement by the Customer	5
4. General	5
Signing page	**6**

Details

Date

Parties

Name	**The Crown in right of Tasmania acting through the Department of Police, Fire and Emergency Management**
ABN	19 173 586 474
Short form name	**Customer**
Notice details	Level 6, 70 Collins Street, Hobart, Tasmania 7000Email: Unify@police.tas.gov.au Attention: Jeremy Williams

Name	**KPMG Australia Technology Solutions Pty Limited**
ABN	29 606 612 962
Short form name	**Contractor**
Notice details	Tower Three, International Towers Sydney, 300 Barangaroo Avenue, Sydney NSW 2000 Email S36 [redacted] Attention: S36 [redacted]

Background

A The Customer and the Contractor are parties to the 'Tasmanian Technology Contract Conditions – Comprehensive Contract Details for the provision of systems integration, project and professional services to continue the implementation of the Niche Technology Records Management System' executed 29 March 2024 (**Contract**).

B The parties have agreed to amend the Contract as set out in this deed.

1. Defined terms & interpretation

1.1 Defined terms

In this deed:

Contract is defined in Background A above.

Variation means the variations to the Contract detailed in clause 2.1 of this deed.

Variation Date means the date on which the last of the parties executes this deed.

1.2 Contract defined terms

Unless the context otherwise requires or the relevant term is defined in this deed, capitalised terms in this deed have the meaning defined in the Contract, including as varied by way of the Variation.

1.3 Interpretation

Clause 1.2 (Interpretation) of the Tasmanian Technology Contract Conditions – Comprehensive Contract – Version 2021-01 (Tas) apply to this deed except that references to clauses are references to clauses of this deed, unless specified otherwise.

2. Variation of Contract

2.1 Variation

The Contract is varied, on and from the Variation Date, as follows:

(a) in accordance with the terms and conditions of this deed; and

(b) in the manner set out in Schedule 1.

2.2 Parties bound

The Customer and the Contractor agree:

(a) to be bound by the Contract as varied by the Variation on and from the Variation Date; and

(b) that the Variation does not affect any right or obligation that arises under the Contract before the Variation Date.

3. Acknowledgement and agreement

3.1 Acknowledgement and agreement by the Contractor

The Contractor acknowledges and agrees that:

(a) it has made all reasonable enquiries, reviewed all information provided by the Customer and has taken all other due diligence action that the Contractor considers necessary or desirable to perform prior to entering into this deed;

(b) its liabilities and obligations under the Contract are not released, reduced or diminished as a result of the Variation, except as expressly provided in this deed;

(c) nothing in this deed prejudices or otherwise adversely affects any right, power or remedy of the Customer or any obligation or liability of the Contractor to the Customer, with respect to anything done or effected or otherwise arising before the date of this deed; and

(d) the Customer is relying on this deed in continuing to be a party to the Contract with the Contractor and in agreeing to the Variation.

3.2 Acknowledgement and agreement by the Customer

The Customer acknowledges and agrees that:

(a) its liabilities and obligations under the Contract are not released, reduced or diminished as a result of the Variation, except as expressly provided in this deed;

(b) nothing in this deed prejudices or otherwise adversely affects any right, power or remedy of the Contractor or any obligation or liability of the Customer to the Contractor, with respect to anything done or effected or otherwise arising before the date of this deed; and

(c) the Contractor is relying on this deed in continuing to be a party to the Contract with the Customer and in agreeing to the Variation.

4. General

(a) The parties agree to bear their own legal and other costs and expenses of, and incidental to, the preparation, execution and completion of this deed.

(b) The Contractor will pay any stamp duty or other taxes of a similar nature payable on execution of this deed.

(c) This deed may be executed in several counterparts (including electronically), all of which taken together will constitute one single deed between the parties.

(d) Each party agrees to do all things and execute all deeds, instruments, transfers or other documents as may be necessary or desirable to give full effect to the provisions of this deed.

(e) This deed is governed by the laws of Tasmania and with respect to any legal action or proceedings that may be brought with respect to this deed, the parties irrevocably and unconditionally submit to and accept the non-exclusive jurisdiction of any of the courts of Tasmania or courts of appeal from them.

(f) Any provision of this deed that is prohibited or unenforceable in any jurisdiction is ineffective as to that jurisdiction to the extent of the prohibition or unenforceability. That does not invalidate the remaining provisions of this deed nor affect the validity or enforceability of that provision in any other jurisdiction.

(g) The Contract is amended by this deed only to the extent expressly provided for in this deed. In the event of any inconsistency between the provisions of the Contract and this deed, the provisions of this deed will prevail to the extent of the inconsistency.

(h) Despite any confidentiality or intellectual property right subsisting in this deed, a party may publish all or any part of this deed without reference to another party.

(i) Nothing in clause 4(h) derogates from a party's obligations under the *Personal Information Protection Act 2004* (Tas) or the *Privacy Act 1988* (Cth).

Signing page

EXECUTED as a deed.

EXECUTION BY CUSTOMER:

Executed as a deed on behalf of the Crown in right of Tasmania by the person named below in the presence of the witness named below:

Signature: → S36

Being a person who has authority to sign this Deed on behalf of the Customer

*Print name and position: Ross Hinkley Acting Secretary

Witness' signature: → S36

*Witness print name and position: MANON DENBY DIRECTOR

*Use BLOCK LETTERS

*Witness print address: LIVERPOOL ST HOBART

Date: 13/9/24

EXECUTION BY CONTRACTOR:

Executed as a deed by KPMG Australia Technology Solutions Pty Limited ABN 29 606 612 962 in accordance with section 127(1) of the *Corporations Act 2001* (Cwlth):

Signature: → S36

*Print name and office held: S36

Date: 13/09/2024

Signature: → S36

*Print name and office held: S36

Date 13/9/2024

*Use BLOCK LETTERS

Note: In the case of a company that has only one director and one secretary, show the office held as 'SOLE DIRECTOR AND SOLE COMPANY SECRETARY'

Schedule 1 – Amendments to the Contract

1. The Details are replaced with the version in Attachment A to this schedule.
2. Module Order Form 2 as set out in Attachment B to this schedule is added to the Contract.
3. Module Order Form 4 – Link as set out in Attachment C to this schedule is added to the Contract.
4. Appendix 13 (Business, Functional, Non-Functional and Technical Requirements) to Module Order Form 4 – Link as set out in Attachment D to this schedule is added to the Contract.
5. Appendix 14 (Customer Furnished Items and Dependencies) to Module Order Form 4 – Link as set out in Attachment E to this schedule is added to the Contract.
6. Appendix 15 (Deliverables) to Module Order Form 4 – Link as set out in Attachment F to this schedule is added to the Contract.
7. Appendix 16 (Key Resource List) to Module Order Form 4 – Link as set out in Attachment G to this schedule is added to the Contract.
8. Module Order Form 4 – Unify is replaced with the version in Attachment H to this schedule.
9. Schedule 1 (Price and Payment Terms) to the Contract is replaced with the version in Attachment I to this schedule.
10. Schedule 9 (Acceptance Testing) to the Contract replaced with the version in Attachment J to this schedule.

Attachment A – Details

Tasmanian Technology Contract Conditions – Comprehensive Contract Details

Provision of software development, systems integration, project and professional services to continue the implementation of the Niche Technology Records Management System (NicheRMS) PU-01-23

The Crown in right of Tasmania acting through the Department of Police, Fire and Emergency Management

KPMG Australia Technology Solutions Pty Limited ABN 29 606 612 962

This document is a derivative of Comprehensive Contract Details – ICT Products and Services (publications.qld.gov.au) created in 2017 by the Department of Science, Information Technology and Innovation, Queensland Government and is used under Creative Commons licence CC BY 4.0

Table of Contents

1. Customer 4
2. Customer contact details 4
3. Supplier 6
4. Supplier Contact Details 6
5. Modules and documents that form part of the Contract (Clause 1.3) 7
6. Additional Provisions (Clause 1.4) 9
7. Term (Clause 3) 33
8. Authorisations (Clause 4.2) 33
9. Tasmanian Industry Participation Plan (Clause 4.5) 33
10. Documentation (Clause 5) 33
11. Policies, codes of conduct, rules, standards and procedures (Clause 6.1) 34
12. Customer Inputs (Clause 6.4) 34
13. Customer Assistance (Clause 6.5) 35
14. Management committee (Clause 7.1) 35
15. Performance reviews (Clause 7.2) 36
16. Site Specification (Clause 7.3) 37
17. Project Implementation and Payment Plan (Clause 7.4) 37
18. Staged Implementation (Clause 7.5) 37
19. Liquidated Damages (Clause 7.7) 37
20. Training (Clause 7.10) 38

21. Subcontractor(s) (Clause 8) 39
22. Subcontractor(s) statutory declaration (Clause 8.1(d)) 39
23. Background checks (Clause 8.2) 39
24. Confidentiality, Privacy and Conflict of Interest Deed (Clause 8.2(f)) 39
25. Key Personnel (Clause 8.4) 40
26. Customer's Personnel (Clause 8.5) 41
27. Acceptance Testing (Clause 9) 41
28. Price and payment (Clause 10) 41
29. Intellectual Property Rights in Pre-Existing Material (Clause 12.1) 42
30. Intellectual Property Rights in New Material (Clauses 12.2 to 12.4) 42
31. Escrow (Clause 12.6) 43
32. Customer Data (Clause 13(f)) 44
33. Confidential Provisions (Clause 14.2) 44
34. Cap on liability (Clause 17.3 and 17.7) 45
35. Insurance (Clause 19) 45
36. Security (Clause 20) 46
37. Conflict of Interest (Clause 21.2) 46
38. Reports (Clause 22.1) 46
39. Termination for convenience (Clause 24.3) 46
40. Business Hours (Clause 27.1) 47
41. Designated Environment (Clause 27.1) 47

General information

The Tasmanian Technology Contract Conditions – Comprehensive Conditions www.purchasing.tas.gov.au/contracts apply to these Details.

The definitions and rules of interpretation applicable to these Details are set out in the Tasmanian Technology Contract Conditions – Comprehensive Conditions.

1. Customer

Name

The Crown in right of Tasmania acting through the Department of Police, Fire and Emergency Management

ABN or ACN

ABN 19 173 586 474

2. Customer contact details

Authorised Representative

The Honourable Felix Ellis MP

Position title / role

Minister for Police, Fire and Emergency Management

Phone number

Not applicable – the Supplier is to direct all enquiries relating to the Contract to another Authorised Representative of the Customer.

Street address

Not applicable – the Supplier is to direct all enquiries relating to the Contract, and send all notices under the Contract, to another Authorised Representative of the Customer.

Postal address

Not applicable – the Supplier is to direct all enquiries relating to the Contract, and send all notices under the Contract, to another Authorised Representative of the Customer.

Email

Not applicable – the Supplier is to direct all enquiries relating to the Contract, and send all notices under the Contract, to another Authorised Representative of the Customer.

Authorised Representative

Glenn Keating

Position title / role

Assistant Commissioner, Innovation, Risk and Capability

Phone number

Not applicable – the Supplier is to direct all enquiries relating to the Contract, and send all notices under the Contract, to another Authorised Representative of the Customer.

Street address

Not applicable – the Supplier is to direct all enquiries relating to the Contract, and send all notices under the Contract, to another Authorised Representative of the Customer.

Postal address

Not applicable – the Supplier is to direct all enquiries relating to the Contract, and send all notices under the Contract, to another Authorised Representative of the Customer.

Email

Not applicable – the Supplier is to direct all enquiries relating to the Contract, and send all notices under the Contract, to another Authorised Representative of the Customer.

Authorised Representative

Tim Rutherford

Position title / role

Chief Information and Technology Officer

Phone number

Not applicable – the Supplier is to direct all enquiries relating to the Contract, and send all notices under the Contract, to another Authorised Representative of the Customer.

Street address

Not applicable – the Supplier is to direct all enquiries relating to the Contract, and send all notices under the Contract, to another Authorised Representative of the Customer.

Postal address

Not applicable – the Supplier is to direct all enquiries relating to the Contract, and send all notices under the Contract, to another Authorised Representative of the Customer.

Email

Not applicable – the Supplier is to direct all enquiries relating to the Contract, and send all notices under the Contract, to another Authorised Representative of the Customer.

Authorised Representative

Jeremy Williams

Position title / role

Program Director, Project Unify

Phone number

S36

Street address

Level 6, 70 Collins Street, Hobart, Tasmania 7000

Postal address

GPO Box 308, Hobart, Tasmania 7001

Email

Unify@police.tas.gov.au

3. Supplier

Name

KPMG Australia Technology Solutions Pty Limited

ABN or ACN or ABRN

ABN 29 606 612 962

4. Supplier Contact Details

Authorised Representative

S36

Position title / role

Partner

Phone number

S36

Street address

Tower Three
International Towers Sydney
300 Barangaroo Avenue
Sydney NSW 2000

Postal address

As above

Email

S36

Authorised Representative

S36

Position title / role

Partner

Phone number

S36

Street address

Level 3, 100 Melville Street
Hobart TAS 7000

Postal address

As above

Email

S36

5. Modules and documents that form part of the Contract (Clause 1.3)

Modules

- ☐ Module 1 – Hardware
- ☒ Module 2 – Software
- ☐ Module 3 – As a Service
- ☒ Module 4 – Systems Integration
- ☐ Module 5 – Telecommunications Services
- ☐ Module 6 – Managed Services
- ☐ Module 7 – ICT Professional Services

Documents

In accordance with clause 1.3(h) of the Comprehensive Contract Conditions, the following documents are incorporated into the Contract by reference:

(a) Business functions overview (including the appended business functions and business process model diagram), as annexed to the RFT as Annexure C.

(b) Atlas architecture overview (including the appended systems architecture diagrams and systems impact summary), as annexed to the RFT as Annexure D.

(c) Database background and overview, as annexed to the RFT as Annexure E.

(d) Data dictionaries which list fields (and associated details) in relevant in-scope databases provided through the BAFO process via the Electronic Data Room, including:

(i) DOSE Data Dictionary extracted from Project Unify wiki, Nov 9 2023;

(ii) DVIR Data Dictionary extracted from Project Unify wiki, Nov 9 2023;

(iii) FVMS Data Dictionary extracted from Project Unify wiki, Nov 7 2023; and

(iv) ORS Data Dictionary extracted from Project Unify wiki, Nov 7 2023.

(e) Detail regarding the scope and requirements for the infrastructure move to S30 S30 for Distribution), provided through the BAFO process via the Electronic Data Room.

(f) Detail regarding the context for organisational change management challenges, themes of user perceptions and practical implications, in the document PAT Survey Data Summary and Practical OCM Implications. provided through the BAFO process via the Electronic Data Room.

(g) Detail regarding training systems in the document Training Systems and Lessons Learned, provided through the BAFO process via the Electronic Data Room.

(h) Appendix 01 (to Module Order Form 4 - Unify) – High Level Project Plan

(i) Appendix 02 (to Module Order Form 4 - Unify) – KPMG Project GANTT Chart

(j) Appendix 03 (to Module Order Form 4 - Unify) – Establishment Services

(k) Appendix 04 (to Module Order Form 4 - Unify) – Design Services

(l) Appendix 05 (to Module Order Form 4 - Unify) – Implementation Services

(m) Appendix 06 (to Module Order Form 4 - Unify) – Data Analysis, Migration and Management

(n) Appendix 07 (to Module Order Form 4 - Unify) – Hypercare

(o) Appendix 08 (to Module Order Form 4 - Unify) – Key Resource List

(p) Appendix 09 (to Module Order Form 4 - Unify) – Resource Requirements, Customer Furnished Items and Risks

(q) Appendix 10 (to Module Order Form 4 - Unify) – NicheRMS Relationship

(r) Appendix 11 (to Module Order Form 4 - Unify) – Business Design Workshop Examples

(s) Appendix 12 (to Module Order Form 4 - Unify) – FVMS External Access

(t) Project Unify Resource Schedule

(u) Tasmanian Industry Participation Plan completed and endorsed by the Supplier on 22 February 2024

(v) Appendix 13 (to Module Order Form 4 - Link) – Business Functional, Non-Functional and Technical Requirements

(w) Appendix 14 (to Module Order Form 4 - Link) – Customer Furnished Items and Dependencies

(x) Appendix 15 (to Module Order Form 4 - Link) – Deliverables

(y) Appendix 16 (to Module Order Form 4 – Link) – Project Link – Key Resource List

each of which documents in paragraphs (h) to (t) was attached to these Details or Module Order Form 4 - Unify for the purposes of the parties' Authorised Representative signing the appropriate section of these Details, and each of which documents in paragraphs (v), (w), (x) and (y) was attached to the Link Deed of Variation.

In the event and to the extent of any inconsistency between the terms of the above documents, the order of hierarchy in descending order will prevail.

6. Additional Provisions (Clause 1.4)

Additional provisions A3, A5, A6, A8 and A9 only apply to the parties' rights and obligations associated with the activities undertaken pursuant to Module Order Form 4 - Unify and any further Module Order Form 4 for a Unify Stage that is agreed between the parties as contemplated by Additional Provision A8.

All other additional provisions apply to the parties' rights and obligations associated with all activities undertaken pursuant to the Contract.

A1. Additional definitions

In the Contract, the following definitions apply in addition to those in clause 27 of the Tasmanian Technology Contract Conditions – Comprehensive Conditions and the applicable Modules.

Atlas Architecture Overview means the document referred to in paragraph (b) of section 5 of these Details.

Azure Move Overview means the document referred to in paragraph (e) of section 5 of these Details.

Business Functions Overview means the document referred to in paragraph (a) of section 5 of these Details.

Data Dictionaries means the documents referred to in paragraph (d) of section 5 of these Details.

Database Background and Overview means the document referred to in paragraph (c) of section 5 of these Details.

Detailed Project Plan means the detailed project plan for a Unify Stage developed as a Deliverable and accepted under Module 4 – Systems Integration.

Developed Software has the meaning given to it in Module 2 – Software.

Drop means a software release within a Stage of the Integration Services conducted under Module Order Form 4 - Unify that is the subject of design, implementation and testing as well as involving configuration (or, if required, customisation) activities by Niche, as described in the applicable Detailed Project Plan.

Electronic Data Room means the electronic repository for documents and other information that were made available by the Customer in the course of the procurement process conducted pursuant to the RFT.

Exit Criteria means the Acceptance Criteria and/or other criteria that are required to be satisfied in order for a Milestone to be achieved, as set out in the Pricing Schedule and Item 4 of Section 2 of Annexure 1 to Module Order Form 4 - Unify.

Go Live means the achievement of the 'Go Live' Milestone.

Grace Period Contingency Requirement has the meaning given to it in Additional Provision A5(b)(iii).

Integration Services has the meaning given to it in Module 4 – Systems Integration.

Link Deed of Variation means the first deed of variation of the Contract entered into by the Customer and the Supplier in or around September 2024.

Link Stage means the Stage referred to in paragraph (b) of the definition of 'Stage' (as amended by way of Additional Provision A10(qq)).

Link Variation Date means the date on which the variations to the Contract by way of the Link Deed of Variation came into effect.

Milestone means a milestone that is required to be achieved in order for the Supplier to be entitled to invoice the Customer for, and be paid, part of the Price, as described in the Pricing Schedule.

Module Order Form 4 - Link means the Module Order Form setting out the agreed details for the supply of additional Services under Module 4 – Systems Integration that became one of the documents comprising the Contract by way of the Link Deed of Variation.

Module Order Form 4 - Unify means the Module Order Form setting out the agreed details for the supply of Services under Module 4 – Systems Integration as at the start date of the Contract.

Niche means Niche Technology Inc.

Niche Contingency Requirement has the meaning given to it in Additional Provision A5(b)(i).

Niche Delays has the meaning given to it in Additional Provision A5(b)(i).

NicheRMS means the Niche Records Management System software that is licensed by Niche to the Customer, which comprises part of the Designated Environment.

Project Team means:

(a) the Development Team; and

(b) the Customer's Personnel who are deployed by the Customer from time to time to assist the Supplier in performing its obligations under Module 4 – Systems Integration and associated obligations under the remainder of the Contract.

Rate Card means the rate card for the Supplier's personnel that forms part of the Contract, as set out in the Pricing Schedule.

Resource Schedule means the document referred to in paragraph (t) of section 5 of these Details, except that:

(a) the parties acknowledge that the document was prepared on the assumption that the Integration Services would commence on 1 March 2024, and the parties subsequently agreed that the Integration Services are to be provided commencing on 8 April 2024; and

(b) for the purposes of the Contract, the document will (unless and until it is varied by agreement to reflect the timing referred to in paragraph (a)) be read as being adjusted to reflect the updated timing specified in the Contract as at the start date of the Contract.

RFT means the request for tender issued under the Technology Services List with unique reference ID PU-01-23.

System has the meaning given to it in Module 4 – Systems Integration.

Tasmania Police means the Tasmania Police Service established under the *Police Service Act 2003* (Tas).

Unify Stage means a Stage referred to in paragraph (a) of the definition of 'Stage' (as amended by way of Additional Provision A10(qq)).

Workaround means a fix or alternative procedure to temporarily address a Defect.

A2. Third party benefits

(a) The Supplier agrees that the Deliverables are to be provided for the benefit of Tasmania Police as well as the Customer, and the Customer acknowledges that any Deliverables provided to Tasmania Police in accordance with the Contract are deemed to have been provided to the Customer for the purposes of the Contract.

(b) The Supplier agrees that the Customer may enforce the Contract on behalf of itself and Tasmania Police.

(c) For the purposes of the Contract, the Supplier agrees that all loss, damage, costs or expenses of any kind incurred or sustained by Tasmania Police are deemed to be incurred or sustained by the Customer and any remedy available in respect of those matters may be claimed or exercised by the Customer on behalf of Tasmania Police to the extent that such loss, damage, costs or expenses would have been recoverable by the Customer from the Supplier under the Contract had they been suffered by the Customer itself.

(d) The Supplier agrees that, except to the extent otherwise expressly advised in writing by the Supplier, Tasmania Police does not have any right or authority to give any directions under, provide any approvals under, agree any variations to, enforce any rights under or otherwise act for or to bind the Customer in relation to, the Contract.

A3. Cooperation with Niche

Without limiting clause 4.4 of the Comprehensive Contract Conditions, any of the Deliverables or clause A5 in these Additional Provisions, the Supplier must:

(a) cooperate with Niche as reasonably necessary for the Supplier to provide the Deliverables in accordance with the Contract;

(b) in dealing with Niche, use reasonable efforts to:

(i) act in the best interests of the Customer; and

(ii) facilitate Niche complying with its own obligations to the Customer;

(c) in the event that:

(i) any disagreement or dispute arises between the Supplier and Niche;

(ii) the Supplier considers that there is any uncertainty as to the Supplier's and Niche's respective allocation of responsibilities in relation to the System or the Deliverables; or

(iii) the Supplier considers that the provision of the Deliverables may adversely impact on, or be inconsistent with, the performance by Niche of its responsibilities to the Customer, or vice versa,

promptly notify the Customer of that matter and cooperate with the Customer to resolve it;

(d) establish and maintain a good working relationship with Niche through which, to the extent reasonably required in order to provide the Deliverables, it:

(i) works together with Niche;

(ii) co-ordinates its activities with those of Niche;

(iii) integrates the Deliverables with deliverables provided by Niche to the Customer, and facilitates Niche doing the same;

(iv) establishes integrated processes that preserve the Supplier's and Niche's prime responsibility for their respective obligations to the Customer; and

(v) agrees with Niche (with input from the Customer as reasonably required) the scope of obligations and interactions needed between themselves to minimise the need for the Customer to be involved in resolving service problems or managing their relationship; and

(e) without limiting any of its other obligations under this Additional Provision A3 or Additional Provision A5, work with Niche in accordance with, and otherwise employ the management approach set out in, Appendix 10 to Module Order Form 4 - Unify.

A4. Additional permitted disclosures of Confidential Information

(a) In addition to the disclosures of Confidential Information of the Supplier permitted under clause 14.1(c) of the Comprehensive Contract Conditions, the Customer may disclose Confidential Information of the Supplier to:

(i) Tasmania Police for the purposes of its functions and activities, including those that relate to or rely on any of the Deliverables; and

(ii) Niche for the purposes of it carrying out any of its activities as contemplated by the Contract and otherwise supplying the Customer with (including

maintaining and supporting) NicheRMS. Nothing in the Contract (including this Additional Provision A4) permits the Customer or Tasmania Police to disclose the Supplier's pricing to Niche.

(b) In addition to the disclosures of Confidential Information of the Customer permitted under clause 14.1(c) of the Comprehensive Contract Conditions, the Supplier may disclose Confidential Information of the Customer to Tasmania Police or Niche to the extent required for the purposes of the Supplier performing the Supplier's obligations and exercising the Supplier's rights under the Contract.

A5. Flexibility requirements

Without limiting clause 7.4 of the Comprehensive Contract Conditions or any of the Deliverables, the Supplier:

(a) must work with the Customer as reasonably required to seek to ensure that:

(i) appropriate times are scheduled with Niche for its configuration (and, if required, customisation) activities contemplated by the Contract, including:

(A) a delivery drop; and

(B) a remediation drop, on the assumption that this will be required to resolve defects in or omissions from the outputs delivered as part of the delivery drop, and should be scheduled in advance of the associated delivery drop having been undertaken and its outputs having been tested;

(ii) the scope of configuration (and, if required, customisation) activities to be conducted by Niche as part of each delivery drop (and associated remediation drop) referred to in paragraph (i) is agreed with Niche as appropriate and so as to facilitate the efficient and effective performance of the Customer's Project Unify program;

(iii) timing is agreed with Niche for the reporting of defects arising from Niche's configuration (and, if required, customisation) activities, so as to facilitate those defects being resolved as part of the appropriate remediation drop or an emergency patch, or within another appropriate timeframe; and

(iv) defects are promptly reported to Niche as identified, as contemplated by paragraph (iii);

(b) must take a flexible approach to the delivery of the Integration Services and the order and timing of the Integration Services, in order to accommodate:

(i) any delays:

(A) in the activities referred to in Additional Provision A5(a); and

(B) arising out of any omissions from, or other defects in, the outputs delivered by or on behalf of Niche as part of the activities referred to in Additional Provision A5(a),

(**Niche Delays**) of up to 10 Business Days in aggregate across each Stage without affecting the Supplier's ability to do everything required in order for

each of Niche's delivery drops (and associated remediation drops) to be able to be conducted at the applicable times referred to in Additional Provision A5(a)(i) (**Niche Contingency Requirement**);

(ii) further Niche Delays beyond the 10 Business Days allowed as part of the Niche Contingency Requirement, to the extent it is reasonably feasible do so; and

(iii) (without limiting the Supplier's right to seek and obtain an extension of time in the event of a Delay Event under clause 7.6) any delays that cause the LD Grace Period to elapse after each relevant LD Due Date without affecting the Supplier's ability to do everything required in order for each of Niche's delivery drops (and associated remediation drops) to be able to be conducted at the applicable times referred to in Additional Provision A5(a)(i) (**Grace Period Contingency Requirement**);

(c) warrants to the Customer that, as at the date on which its Authorised Representative signs the appropriate section of these Details, any document setting out the schedule for delivery of the Integration Services (including the high level plan that forms part of the Contract, as referred to in Item 5(h) of these Details) satisfies the Niche Contingency Requirement and the Grace Period Contingency Requirement;

(d) must ensure that, subject to Additional Provision A5(e), each:

(i) updated schedule for delivery of the Integration Services (including the Detailed Project Plan); and

(ii) schedule for delivery of the Integration Services for each subsequent Stage (including the applicable Detailed Project Plan),

that is prepared subsequent to the date referred to in Additional Provision A5(c) satisfies the Niche Contingency Requirement and the Grace Period Contingency Requirement; and

(e) must ensure that, in the event of any Change, the schedule for delivery of the Integration Services continues to satisfy the Niche Contingency Requirement and the Grace Period Contingency Requirement except to the extent that:

(i) the Customer explicitly agrees otherwise in accepting the relevant Change Request;

(ii) the available contingency required to satisfy the Niche Contingency Requirement has been reduced or exhausted as a result of Niche Delays; or

(iii) the available contingency required to satisfy the Grace Period Contingency Requirement in relation to any LD Due Date has been reduced or exhausted by any delays entitling the Supplier to benefit from the LD Grace Period.

A6. Impact of Niche issues

(a) Without limiting clause 9 of the Comprehensive Contract Conditions, clause 3.12 of Module 4 – Systems Integration or Schedule 9, each Drop of the System under the Contract will be tested against the Acceptance Criteria as a whole, including those

elements that have been configured (or, if required, customised) by Niche rather than by the Supplier, including by way of the conduct of Acceptance Tests designed to ensure that the relevant Drop of the System is in accordance with the Requirements.

(b) Despite clause 3.15(c)(iii) of Module 4 – Systems Integration, the parties acknowledge and agree that the Supplier's obligation to remedy Defects in the System under clause 3.15 of Module 4 – Systems Integration:

(i) does not apply to failures of the outputs of any configuration or customisation work undertaken by Niche to meet the Requirements (which failures are to be remedied by Niche, not by the Supplier); but

(ii) applies if other components or element of the System delivered or required to be delivered by the Supplier fail to meet the Requirements as a result of a failure referred to in paragraph (i), on the basis that the Supplier is responsible for the compliance of the System as a whole with the Requirements other than those components or elements that are the responsibility of Niche.

(c) The Supplier must:

(i) comply with its obligations under Additional Provisions A3 and A5(a)(iv) so as to ensure or seek to ensure (as applicable) that any failure referred to in Additional Provision A6(b)(i) is promptly identified and notified to Niche and Niche is given an opportunity to remedy it; and

(ii) as part of remedying a Defect of the kind referred to in Additional Provision A6(b)(ii), employ any reasonable workarounds so as to ensure that the System as a whole complies with the Requirements to the extent possible despite the Niche failure referred to in Additional Provision A6(b)(i).

A7. Defects in Deliverables other than System

(a) The Supplier agrees under this Additional Provision A7 to provide a warranty in respect of the training materials that are delivered in relation to the System or any of the Developed Software, for the same period as applies to the System.

(b) Subject to Additional Provision A7(c), the Supplier must, at no cost to the Customer, during the period set out in paragraph (a):

(i) remedy any Defects in the Deliverables referred to in Additional Provision A7(a); and

(ii) take all reasonable measures (including providing a Workaround) to enable the Customer to continue to productively use those Deliverables while remedying Defects.

(c) The Supplier is not required under Additional Provision A7(b) to remedy any Defects in the Deliverables to the extent that the Defect arises as a result of:

(i) any failure of the Customer to comply with its obligations under the Contract;

(ii) any failure of a Customer Input (if applicable) to comply with the requirements specified in the Details;

(iii) any Harmful Code that adversely affects the Deliverable (as applicable), except to the extent that the Harmful Code was introduced by, or arose due to an act or omission of, the Supplier or its Personnel;

(iv) an Unexpected Event; or

(v) any changes made to the Deliverables made by anyone other than the Supplier after the date when the Deliverables were provided.

(d) Where the Supplier, acting reasonably, determines that the Defect arises as a result of circumstances set out in Additional Provision A7(c) and notifies the Customer of that determination, then if the Customer requests the Supplier to remedy the Defect subsequent to that notification, the Supplier is entitled to charge the Customer for the costs and expenses (calculated using the rates set out in the applicable Pricing Schedule, or if none are stated, at the Supplier's then current commercial rates subject to clause 10.4 of the Comprehensive Contract Conditions (if applicable)) that arise out of or in connection with identifying and attempting to remedy that Defect, subject to the Supplier having:

(i) provided the Customer with an estimate of those costs and expenses for approval prior to incurring them; and

(ii) received written approval for the incurring of those costs and expenses.

A8. Process for completing Stages and proceeding to further Stages

(a) Without limiting the Supplier's other obligations under the Contract, if, in order to achieve the exit criteria to successfully complete the Services under Module 4 – Systems Integration in respect of a Drop or in a Stage, the Supplier agrees with the Customer a plan to remedy any outstanding Defects in the System, the Supplier must implement and comply with that plan.

(b) The parties:

(i) acknowledge that, as part of the performance of the Services under Module 4 – Systems Integration in a Stage (and in order to achieve the exit criteria for completion of those Services), the Supplier is obliged to prepare as Deliverables:

(A) a high-level plan for, and pricing and other details of, the Services to be performed in the following Stage; and

(B) a draft Module Order Form for the Services to be performed in the following Stage; and

(ii) agree that:

(A) the Customer's notice to proceed to each subsequent Stage will be given by way of the Customer agreeing the details for that Stage and executing the Module Order Form contemplated by paragraph (i); and

(B) accordingly no particular notice period is required for the purposes of clause 7.5(c) of the Comprehensive Contract Conditions.

(c) Without limiting clause 7.5(e) of the Comprehensive Contract Conditions or any other basis on which the Customer may decide not to proceed with any further Stage, the Supplier acknowledges that the Customer does not intend to proceed with any further Stage if:

(i) any of the exit criteria for completion of the Services in the preceding Stage have not been satisfied; or

(ii) the Price for that Stage proposed by the Supplier (as contemplated by Additional Provision A8(b)(i)) exceeds the price for that Stage specified in Schedule 1 of the Contract (as at the date on which the Supplier's Authorised Representative signs the appropriate section of these Details) by more than 10%, except to the extent that such an increase in the Price is caused by a change in the Requirements for that Stage (including the performance of additional Services or any other increase in the scope of the Services) requested by the Customer.

(d) Once the pricing for a further Stage has been agreed in writing between the parties as contemplated by Additional Provision A8(b)(ii)(A), it will form part of Schedule 1 and supersede any inconsistent pre-existing content in Schedule 1 to the extent of the inconsistency.

(e) Once the Module Order Form for a further Stage has been agreed in writing between the parties as contemplated by Additional Provision A8(b)(ii)(A), it will form part of the Contract consistent with clause 1.3 of the Comprehensive Contract Conditions.

A9. Detailed Project Plan

The parties must perform their obligations at the times and in the manner specified in the applicable Detailed Project Plan.

A10. Other amendments to Comprehensive Contract Conditions

For the purposes of the Contract, the Comprehensive Contract Conditions will be treated as having been amended as follows (with additions to the Comprehensive Contract Conditions shown in underlining, and deletions from the Comprehensive Contract Conditions shown in strike-out):

(a) clause 4.1(d) will be amended as follows:

(d) ensure that all Deliverables are of a high quality, professional standard and fit for ~~their usual purpose~~ the purposes specified in or reasonably apparent from the Contract and, during the Warranty Period, meet the Requirements in all material respects;

(b) clause 4.2(b) will be amended as follows:

(b) ~~ensure that the Deliverables comply with all Laws~~[not used];

(c) the opening wording of clause 4.3 will be amended as follows:

Without limiting clauses 4.2, 6.1 or 6.2, the Supplier must, to the extent applicable to the performance of its obligations under the Contract:

(d) clause 5.3(b)(ii) will be amended as follows:

(ii) promptly advise the Supplier if it approves or rejects the draft Bespoke Documentation. The Customer may reject draft Bespoke Documentation if it does not materially meet the Requirements, and must specify why the Requirements have not been met.

(e) clause 6.3 will be amended as follows:

6.3 Access to Customer's IT System

(a) Where access to the Customer's IT System is required to provide the Deliverables or is otherwise granted to the Supplier by the Customer (including in connection with any audit conducted by the Supplier in accordance with a Module), the Supplier must:

(~~a~~i) only access and use that part of the Customer's IT System for which the Supplier is authorised, and only for the purpose of performing the Contract and to the extent necessary to perform the Contract;

(~~b~~ii) not tamper with, hinder the operation of (except as expressly permitted by the Contract) or make unauthorised modifications to the Customer's IT System or maliciously or negligently introduce any Harmful Code to the Customer's IT System; and

(~~c~~iii) not permit any Supplier's Personnel who do not have an appropriate level of security clearance, or who are not otherwise authorised, from gaining access to the Customer's IT System.

(b) Either party must notify the other party promptly and without undue delay if it becomes aware of any breach by the Supplier of clause 6.3(a), or of any material breach of clause 6.1(a) in relation to any Customer policies, codes of conduct, rules, standards and procedures that apply to the Customer's IT System. The Supplier must:

(i) promptly take all reasonable steps to investigate, mitigate and remediate any such breach;

(ii) within five Business Days after becoming aware of the breach, provide a summary report detailing the findings of its investigation and the steps it is taking to mitigate and remediate the breach (the substance and form of which must be reasonably acceptable to the Customer), including such details as are available at the time having regard to the nature and seriousness of the breach; and

(iii) provide the Customer with reasonable updates as soon as reasonably possible after they become available.

(f) clause 7.5(a) will be amended as follows:

(a) The parties agree to perform the Contract in accordance with the Stages ~~(if any) described in the PIPP~~.

(g) clause 7.6(a) will be amended as follows:

(a) If the Supplier is or will be delayed in achieving a Delivery Date directly as a result of:

(i) any failure of the Customer or its Personnel to perform its obligations in accordance with the Contract (within the time required or at all), including any failure of the Customer to provide any approval or consent that it is required to provide (and not entitled in the circumstances to withhold) under the Contract (including within any timeframe required under the Contract) and any failure of the Customer to provide any Customer Inputs in accordance with the requirements specified in the Details (including any failure to provide any Customer Inputs that are to be procured from Niche), to the extent that the failure, or the delay to achievement of a Delivery Date caused by it, ought not reasonably have been prevented or mitigated against by the Supplier complying with its obligations under the Contract (including under Additional Provisions A3 and A5);

(ii) any inability of the Supplier to access the Customer's Site at any time specified in the Contract, or at which access is otherwise reasonably required in order for the Supplier to perform its obligations in accordance with the Contract (including any denial or suspension of access under clause 6.2(c)), unless the inability is due to an adverse finding arising out of an investigation into the conduct of the Supplier or its Personnel or the Supplier's breach of the Contract; ~~or~~

(iii) the amendment to, or introduction of a new, policy, code of conduct, rule, standard or procedure relevant to the Supplier's obligations under the Contract; or~~,~~

(iv) any Niche Delay which exceeds the 10 Business Days required to be allowed for as part of the Niche Contingency Requirement to the extent that the failure, or the delay to achievement of a Delivery Date caused by the Niche Delay, ought not reasonably have been prevented or mitigated against by the Supplier complying with its obligations under the Contract (including under Additional Provisions A3 and A5),

(**Delay Event**), the Supplier must:

(iv) within ~~10~~ two Business Days of becoming aware of the Delay Event, provide to the Customer a notice setting out detailed particulars of the Delay Event, including the reasons for and consequences of the Delay Event;

(vi) within ~~10~~ two Business Days of providing notice to the Customer under clause 7.6(a)(iv) (or such other period agreed by the Customer in writing, which agreement will not be unreasonably withheld by the Customer, taking into account the nature of the Delay Event and the complexity of the arrangements to address the impact of the Delay Event), provide to the Customer:

(A) a plan developed in consultation with the Customer setting out in detail the steps the Supplier proposes to take to minimise the impact of the Delay Event; and

(B) a Change Request under clause 7.8(d) for:

(1) an extension of the Delivery Date affected by the Delay Event; and

(2) a reasonable adjustment to the Price to account for the additional effort expended by the Supplier as a result of the Delay Event, calculated in accordance with the rates set out in the Rate Card (provided that, if there is no rate in the Rate Card applicable to a particular individual, the rate in the Rate Card applicable to another role that is most commensurate with that individual's relevant role and responsibilities will be used), and any other reasonable and documented expenses incurred by the Supplier as a direct result of the Delay Event.

(h) the opening wording of clause 7.6(b) will be amended as follows:

(b) The Customer must not unreasonably refuse or delay the acceptance of a Change Request submitted by the Supplier under clause 7.6(a) provided that the Supplier:

(i) clause 7.7(a) will be amended as follows:

(a) If specified in the Details, where the Supplier has not completed a LD Obligation by the expiry of the LD Grace Period ~~Due Date~~, the Supplier must pay the Customer the Liquidated Damages unless the late completion of the LD Obligation is:

(i) a delay or failure for which the Supplier is not liable ~~caused by an Unexpected Event~~ under clause 22.8;

(ii) caused by the Customer or its Personnel or by Niche, including any failure of the Customer to provide any Customer Inputs in accordance with the requirements specified in the Details and including any suspension of the Contract by the Customer under clause 24.4, to the extent that:

(A) the act or omission, or the delay caused by it, ought not reasonably have been prevented or mitigated against by the Supplier complying with its obligations under the Contract (including under Additional Provisions A3 and A5); and

(B) the Supplier has notified the Customer promptly after becoming aware of the act or omission and the delay caused (or likely to be caused) by it, whether under clause 7.6(a)(iv) (if applicable) or not; or

(iii) permitted because an extension of time to the relevant LD Due Date has been granted by the Customer under clause 7.6.

(j) clause 7.7(d) will be amended as follows:

(d) The Supplier must pay any Liquidated Damages that are due from the expiry of the LD Grace Period ~~Due Date~~ until the date on which the Supplier successfully completes the relevant LD Obligation, provided that the Supplier's liability under this clause 7.7 will not exceed any applicable LD Cap specified in the Details.

(k) clause 7.7(e)(i) will be amended as follows:

(i) are the Customer's sole and exclusive financial remedy for the Customer's loss, damage and expense that the Customer suffers during the period in which Liquidated Damages are payable under clause 7.7(d) (and during any LD Grace Period, notwithstanding that no Liquidated Damages are payable under clause 7.7(d) in respect of an LD Grace Period) as a result of the Supplier not completing the LD Obligation by the LD Due Date; but

(l) clause 7.7 will be amended by inserting new paragraphs at the end as follows:

(g) For the purposes of clause 7.7(a), where there has been more than one cause of delay in completing an LD Obligation by the expiry of the LD Grace Period and at least one cause is not an event of the kind referred to in clauses 7.7(a)(i), (ii) and (iii), the Supplier remains liable to pay the Customer Liquidated Damages to the extent that the period of delay not caused by such an event exceeds the period of delay caused by such an event.

(h) If the Supplier reasonably disputes the extent to which a failure to complete an LD Obligation by the expiry of the LD Grace Period was or was not caused by an event of the kind referred to in clause 7.7(a) (including on the basis of whether or not the conditions set out in clauses 7.7(a)(ii)(A) and (B) were satisfied), the parties will (acting reasonably and in good faith) undertake a root cause analysis to determine the cause of failure as soon as possible (and in any event no more than 10 Business Days) after the Supplier notifies the Customer of the dispute. If the parties do not agree the cause of the failure following such analysis, either one of them may escalate the matter to senior management representatives under clause 23.3 as if it were a dispute not resolved under clause 23.2. For the purposes of clause 23.6, the dispute will be deemed to be a Technical Dispute and (for the purposes of clause 23.6(b) only) the date of expiry of the LD Grace Period will be deemed to be the dispute notice date.

(i) Clause 7.7 will not apply to the work performed and Deliverables supplied under the Link Stage.

(m) clause 7.8(c) will be amended as follows:

(c) If the Customer requests a Change, the Customer must provide to the Supplier details of the requested Change and the Supplier must prepare and submit to the Customer a Change Request within 5 Business Days of such request or as otherwise agreed, unless the Supplier instead notifies the Customer that it will not implement the requested Change on the basis that the proposed Change or its implementation:

(i) would place the Supplier in breach of Laws;

(ii) is technically infeasible; or

(iii) requires expertise or resources that the Supplier does not have available.

(n) clause 7.9(b) will be amended as follows:

(b) The Supplier must submit its proposal to the Customer promptly (and within a time agreed) after receipt of the Customer's request, in the form of a completed Statement of Work Form, unless the Supplier instead notifies the Customer that it will not supply the additional Products or Services on the basis that such supply:

(i) would place the Supplier in breach of Laws;

(ii) is technically infeasible; or

(iii) requires expertise or resources that the Supplier does not have available.

(o) clause 8.3 will be amended as follows:

8.3 Removal of Supplier Personnel

If:

(a) a Conflict of Interest arises or is disclosed with respect to any of the Supplier's Personnel which cannot be appropriately managed to the Customer's satisfaction;

(b) the Customer is not satisfied with the results of any of the Supplier's Personnel criminal background check or any other checks required by the Customer under clause 8.2(b) or notification provided by the Supplier under clause 8.2(c); or

(c) the Customer ~~requires, at its discretion and without having to give reasons~~ otherwise requires on reasonable grounds that any of the Supplier's Personnel cease being involved in the performance of the Contract, including on the ground that:

(i) the relevant member of the Supplier's Personnel has caused the Supplier to breach any of its obligations under the Contract;

(ii) the relevant member of the Supplier's Personnel has engaged in conduct that constitutes a material safety or security risk, or

serious misconduct (including fraudulent or dishonest conduct); or

(iii) the State reasonably believes that the relevant member of the Supplier's Personnel is failing or has failed to comply with the behavioural standards required under clause 8.7,

the Supplier must:

(d) promptly remove from the Customer's premises and/or the performance of the Contract, ~~any individual who is a~~ the relevant member of the Supplier's Personnel ~~(including Key Personnel), used in performance of the Contract~~; and

(e) in consultation with the Customer, replace them with another individual who is a member of the Supplier's Personnel ~~acceptable to the Customer (acting reasonably)~~, who has at least equivalent relevant skills, qualifications and experience and in relation to whom the requirement in clause 8.2(b) has been satisfied, at no additional cost to the Customer.

(p) clause 9.2(b)(v) will be amended as follows:

(v) accept the Deliverable subject to a reasonable reduction in the Price as ~~reasonably determined by the Customer~~ agreed by the parties (acting reasonably and in good faith) to reflect the Testing Defects~~, provided that if the Supplier does not agree with the determination it may dispute the determination in accordance with clause 23~~;

(q) a new clause 9.2(c) will be inserted as follows:

(c) The Supplier will have no liability in connection with the live production use of a Deliverable that has been rejected in accordance with clause 9.2(b)(vi) (including under any warranty or indemnity or otherwise).

(r) clause 10.7(c) will be amended as follows:

(c) ~~The Supplier~~ Both parties must continue to perform ~~its~~ their obligations under the Contract despite any dispute about an invoice, while that dispute is being resolved.

(s) clause 12.1 will be amended as follows:

12.1 Pre-Existing Material

(a) All Intellectual Property Rights in:

(i) any Pre-Existing Material remain vested in the party that owns the Intellectual Property Rights (**Owner**);

(ii) any adaptation, translation or derivative of that Pre-Existing Material vests in, or is transferred or assigned to, the Owner immediately on creation.

(aa) During the Term, the Customer grants the Supplier and its Personnel an irrevocable, unconditional (subject to this clause), royalty-free,

non-exclusive, worldwide and non-transferable licence to exercise all such Intellectual Property Rights in any:

(i) Customer Inputs; and

(ii) Pre-Existing Material of the Customer,

which are provided to the Supplier, strictly for the purposes of fulfilling its obligations under the Contract, and subject to any restrictions, limitations or conditions that are reasonably notified by the Customer to the Supplier (including for the purpose of the Customer being able to give the warranty under clause 16.2(c)), which licence includes the right to grant sublicences to any Subcontractor for the purposes of that Subcontractor fulfilling the obligations under the Contract that have been subcontracted to it.

(ab) During the Term, the Supplier grants to the Customer a revocable, royalty-free, non-exclusive, worldwide and transferable licence to exercise all such Intellectual Property Rights in any Pre-Existing Material of the Supplier which is not incorporated into a Deliverable strictly for the purposes of obtaining the full benefit of the Services.

(b) The Supplier grants the Customer an irrevocable, unconditional (subject to this clause), perpetual, royalty-free, non-exclusive, worldwide and transferable licence to exercise all such Intellectual Property Rights in any Pre-Existing Material of the Supplier which is incorporated into a Deliverable for the purposes of using, supporting and/or modifying that Deliverable, in the course of the Customer's functions or activities, and for such other purposes specified in the Details.

(c) The licences to Pre-Existing Material in clauses 12.1(ab) and 12.1(b):

(i) does not permit the Customer to manufacture, sell or otherwise commercially exploit any Pre-Existing Material of the Supplier (or allow any third party to do so) unless otherwise specified in the Details; and

(ii) permits the Customer to sublicense any of the rights in clause 12.1(ab) or clause 12.1(b) to any:

(A) Agency;

(B) contractor that is providing services to the Customer that includes the use of the Pre-Existing Material, provided that such sublicence contains the same restriction set out in clause 12.1(c)(i), is strictly for the purpose of providing services to the Customer, and automatically terminates at the end of the period of the service arrangement between the Customer and contractor;

(C) other entity specified in the Details; and

at no additional cost, unless the additional cost is specified in the Details.

(t) clause 12.2(b)(ii) will be amended as follows:

(ii) the Customer grants the Supplier and its Personnel an irrevocable, unconditional (subject to this clause), perpetual, royalty-free, non-exclusive, worldwide, sublicensable, non- transferable licence to exercise all such Intellectual Property Rights in the relevant New Material, for:

(A) the purpose of fulfilling its obligations under the Contract; and

(B) any other purpose of the Supplier,

subject to the Supplier removing any of the Customer's Confidential Information and Personal Information incorporated or otherwise contained in the New Material prior to exercising its rights under this clause 12.2(b)(ii), and the Supplier will confirm to the Customer when this has been done.

(u) clause 14.1(c) will be amended as follows:

(c) not disclose the Confidential Information except:

(i) to its Personnel on a need to know basis for the purpose of performing its obligations under the Contract;

(ii) with the Discloser's consent;

(iii) to the extent required by Law or applicable professional standards or regulations;

(iv) to its professional advisors;

(v) in the case of the Customer:

(A) to a Minister, their advisors or Parliament; or

(B) as required under the Right to Information Act or the PIP Act; ~~or~~

(vi) in the case of the Customer, it may disclose the terms of the Contract to any Agency; or

(vii) in the case of the Supplier, where expressly required for the purpose of providing the Services.

(v) clause 14.2(d)(ii) will be amended as follows:

(ii) a Law, professional standard or regulation requires a party to disclose the Confidential Provision;

(w) clause 14.4 will be amended by inserting a new paragraph at the end as follows:

(d) Notwithstanding anything else in the Contract, the Supplier may retain its Work Papers, which may contain the Customer's Confidential Information and Personal Information, for quality assurance and risk management purposes. The Supplier will retain the Work Papers in accordance with its confidentiality obligations under the Contract.

(x) clause 15.1(c) will be amended as follows:

(c) The Supplier must:

(i) ensure that Personal Information collected or accessed in connection with the Contract and transferred to or stored in the Supplier's or its Personnel's IT systems is protected against loss and against unauthorised access, use, modification, disclosure or other misuse;

(iA) without limiting any of its other obligations under the Contract, comply with the security policies, procedures and directions of the Customer that apply to the Supplier's and its Personnel's access to and use of the Customer's and Tasmania Police's IT systems, including the protection of Personal Information and other data accessible to or stored in those systems;

(ii) not use Personal Information collected or accessed in connection with the Contract other than for the purpose of performing its obligations under the Contract;

(iii) not disclose Personal Information collected or accessed in connection with the Contract without the prior written consent of the Customer, unless required or authorised by Law;

(iv) not transfer any Personal Information collected or accessed in connection with the Contract, outside of Australia, except:

(A) with the prior written consent of the Customer; or

(B) where the Personal Information is about the Customer's ordering officer or other personnel which is provided in connection with account management purposes or service delivery management under the Contract;

(v) ensure that access to Personal Information for the purposes of the Contract is restricted to those of its Personnel who require access in order to perform their duties under this Contract;

(vi) ensure that its Personnel are aware of the Supplier's obligations under this clause 15 and comply with the same obligations imposed on the Supplier under this clause;

(vii) fully cooperate with the Customer to enable the Customer to respond to applications for access to, or amendment of, a document containing a person's Personal Information and to privacy complaints where the application or complaint relates to Personal Information collected or accessed in connection with the Contract; and

(viii) comply with such other privacy measures as the Customer reasonably advises the Supplier in writing from time to time.

(y) clause 16.2(c) is amended as follows:

(c) it has the right to grant the licence under clause 12.1(aa) and ~~to the best of its knowledge and belief having made all reasonable enquiries,~~ the use by

the Supplier of the Customer Inputs or any other Pre-Existing Material of the Customer provided to the Supplier under the Contract, each ~~by the Supplier~~ as permitted by the Contract, will not infringe the Intellectual Property Rights or Moral Rights of any person.

(z) clause 17.3 will be amended as follows:

17.3 Limitation of liability

Subject to clause 17.4:

(a) to the extent permitted by Law and subject to clause 17.3(aa), the maximum aggregate liability of the Supplier to the Customer, whether in contract, tort (including negligence) or otherwise in connection with each Stage under the Contract (including under an indemnity or by way of Liquidated Damages), except for liability for loss of Customer Data under Module 3 – As a Service (as applicable), is limited to the amount specified in the Details;

(aa) in relation to any liability of the Supplier to the Customer in connection with any breach by the Supplier of any obligation under clause 14 or clause 15 or under the indemnity in clause 18.1(a)(iv), in the course of performing any of the Stages (other than the Link Stage), the Supplier's maximum aggregate liability (across all of those Stages) will be increased by $5 million (**Unify Enhanced Cap**). The parties agree that any amounts recovered by the Customer in connection with such liability will first contribute to the exhaustion of the Unify Enhanced Cap, and will only contribute to the exhaustion of a cap under clause 17.3(a) if the amount of the Unify Enhanced Cap has been exhausted. For clarity, the Unify Enhanced Cap is fixed, applies across all Stages (other than the Link Stage) and does not refresh or reset based on the commencement or completion of any stage;

(bb) in relation to any liability of the Supplier to the Customer in connection with any breach by the Supplier of any obligation under clause 14 or clause 15 or under the indemnity in clause 18.1(a)(iv), in the course of performing the Link Stage, the Supplier's maximum aggregate liability (in respect of the Link Stage) will be increased by $750,000 (**Link Enhanced Cap**). The parties agree that any amounts recovered by the Customer in connection with such liability will first contribute to the exhaustion of the Link Enhanced Cap, and will only contribute to the exhaustion of a cap under clause 17.3(a) if the amount of the Link Enhanced Cap has been exhausted; and

(b) to the extent permitted by Law, the maximum aggregate liability of the Customer to the Supplier, whether in contract, tort (including negligence) or otherwise in connection with each Stage under the Contract, is limited to the amount specified in the Details,

and for the purposes of this clause 17.3, any liability in connection with any period prior to the start date of the Contract will be taken to relate to the first Stage and any liability in connection with any period after the termination or expiry of the Contract will be taken to relate to the final Stage that was proceeded with prior to that termination or expiry.

(aa) clause 17.4 will be amended as follows:

17.4 No limitation

The exclusions and limitations of liability in clauses 17.2 and 17.3 do not apply to liability in relation to:

(a) personal injury, including sickness and death;

(b) loss of, or damage to, tangible property;

(c) any IP Claim ~~infringement of Intellectual Property Rights or Moral Rights~~; or

(d) any fraudulent act or omission of the Supplier or its Personnel; or

(e) ~~any breach by the Supplier or its Personnel of any obligation under clause 14 or 15~~[not used].

(bb) clause 17.5 will be amended as follows:

17.5 Mitigation

(a) A party who suffers loss or damage (including under any indemnity) must take reasonable steps to mitigate its loss.

(b) The other party will not be responsible for any loss, damage or expenses (including under any indemnity) to the extent that the injured party could have avoided or reduced the amount of the loss, damage or expense, by taking reasonable steps to mitigate its loss.

(cc) clause 18.1(a)(ii) will be amended as follows:

(ii) Wilful Misconduct or fraudulent ~~or wilfully wrong~~ act or omission of the Supplier or its Personnel; and

(dd) clause 18.1(a)(v) will be amended as follows:

(v) ~~Claim by a third party arising out of any negligent act or omission of the Supplier or its Personnel in the performance of the Supplier's obligations under the Contract~~[not used].

(ee) clause 21.2 will be amended as follows:

21.2 Conflict of Interest

(a) The Supplier warrants that it and its Personnel:

(i) do not hold any office or possess any property;

(ii) are not engaged in any business or activity; or

(iii) do not have any obligations,

where a Conflict of Interest is created, or might reasonably appear to be created, in conflict with the Supplier's obligations under the Contract, except as disclosed in the Details or in accordance with clause 21.2(b)(i).

(~~a~~b) If, during the Term, a Conflict of Interest arises, or reasonably appears likely to arise, the Supplier must:

(i) notify the Customer promptly; and

(ii) take such steps (if any) to resolve or otherwise deal with the Conflict of Interest to the reasonable satisfaction of the Customer.

(ff) clause 21.3 will be amended as follows:

21.3 Warranties are ongoing

(a) The warranties in this clause 21 are provided as at the date of the Contract and on an ongoing basis.

(b) The Supplier warrants that it will ~~immediately~~ promptly notify the Customer if it becomes aware that any warranty made in this clause 21 was inaccurate, incomplete, out of date or misleading in any way at any time when the warranty was made~~, or becomes inaccurate, incomplete, out of date or misleading in any way~~.

(gg) clause 22.4 will be amended as follows:

The Supplier must, on reasonable prior written notice from the Customer, give the Customer reasonable access during Business Hours to the client floors of the Supplier's premises where the Deliverables (excluding Services supplied under Module 3 – As a Service) are being performed or produced, and to the Supplier's documentation, records and Personnel, to enable the Customer to verify that the Supplier is complying with its obligations under the Contract, and will promptly address any non-compliance identified by the Customer and notified to the Supplier. Nothing in this clause 22.4 requires the Supplier to provide the Customer with access to any documents or records of or in respect of a third party or to any Supplier systems (on the basis that, to avoid doubt, the Supplier will generate records, reports and other documents from its systems as reasonably required for the purposes of verification under this clause 22.4).

(hh) clause 22.8(d)(i) will be amended as follows:

(i) the Supplier will be entitled to payment for all Deliverables which have been supplied (whether or not they have completed Acceptance Testing, ~~(~~where applicable) in accordance with the Contract up to the date of termination; and

(ii) clause 24.1(a)(i) will be amended as follows:

(i) the Supplier materially breaches the Contract and the breach cannot be remedied, or the breach can be remedied but the Supplier has not remedied

the breach within 30 days (or such longer period stated in the notice in writing) of the Customer issuing a notice of the breach to the Supplier;

(jj) clause 24.1(a)(v) will be amended as follows:

(v) the Customer believes the Supplier has breached any warranty in clause 21.1 or 21.3 (other than by way of having failed to notify the Customer under clause 21.3(b) in relation to a Conflict of Interest that is anticipated or perceived rather than actual), after having issued a notice of the breach that is believed to have occurred and given the Supplier the period specified in the notice (which must be no less than five Business Days) to demonstrate that such a breach has not occurred or how any breach is being managed; or

(kk) clause 24.1(b) will be amended as follows:

(b) Without limiting any other rights or remedies the Customer may have, if the Customer terminates the Contract under clause 24.1(a), the Customer may obtain from any other source a reasonably similar alternative to the Deliverables ~~in which case the Supplier is liable to the Customer for any reasonable losses, damages or expenses incurred (including any price difference between the Deliverable and the similar alternative) or suffered by the Customer~~.

(ll) clause 24.3(b) will be amended as follows:

(b) If the Customer terminates the Contract under clause 24.3(a), the Customer will pay:

(i) the Supplier for the work performed and Deliverables supplied in accordance with the Contract but not yet invoiced, substantiated to the reasonable satisfaction of the Customer; ~~and~~

(ia) the rates (calculated in accordance with the Rate Card, provided that, if there is no rate in the Rate Card applicable to a particular individual, the rate in the Rate Card applicable to another role that is most commensurate with that individual's relevant role and responsibilities will be used) associated with the relevant employees and contractors to the extent that those individuals would (in the absence of the early termination) have been involved in the performance of the Services and those rates would otherwise have been payable by the Customer under the Contract, for a period ending:

(A) four weeks from the date of termination; or

(B) at any earlier time at which the individual is redeployed, or would have been redeployed had the Supplier made good faith efforts to redeploy the individual; and

(ii) either:

(A) the Supplier's reasonable and documented expenses incurred directly relating to the termination; or

(B) any amount specified in the Details.

(mm) clause 26.6(a) will be amended as follows:

(a) Clauses 1.2, 1.3, 7.7, 8.6, 12 (excluding clauses 12.1(aa) and 12.1(ab)), 13, 14, 15, 16, 17, 18, 19(c), 20, 22.2, 22.8(d), 23, 24.5, 25.4 and 26; and

(nn) the definition of 'Change' in clause 27.1 will be amended as follows:

Change means a change (including addition or deletion) to the scope of the Deliverables or ~~PIPP (if applicable)~~ Detailed Project Plan, including any change to the type of Deliverables to be supplied under the Contract, or the Requirements applying to such Deliverables. For clarity, a request for or purchase of additional Products or Services under clause 7.9 is not a Change.

(oo) paragraph (b) of the definition of 'Consequential Loss' in clause 27.1 will be amended as follows:

(b) any loss of profits, loss of revenue, loss of any contract value, loss of anticipated profit, loss of or damage to business, goodwill or reputation, or damages for business interruption (to the extent that they are of the nature contemplated by paragraph (a) of this definition) or lost opportunity; or

(pp) clause 27.1 will be amended by inserting new definitions as follows:

LD Grace Period means the period of 10 Business Days after an LD Due Date.

Wilful Misconduct means any wrongful act or omission which is committed or omitted to be done with reckless disregard as to the adverse consequences of that act or omission or as to whether the act or omission constitutes a breach of the Contract.

Work Papers means the Supplier's internal working documents created in delivery of the Deliverables.

(qq) the definition of 'Stage' in clause 27.1 will be amended as follows:

Stage means each of:

(a) one or more milestones that are identified as a stage in ~~the PIPP~~ Item 7 of the Module Order Form 4 - Unify, and the Business Functions Overview; and

(b) the milestones identified in Module Order Form 2 and Module Order Form 4 - Link (which, to avoid doubt, comprise a Stage separate from each Stage referred to in paragraph (a)).

(rr) the definition of 'Unexpected Event' in clause 27.1 will be amended as follows:

Unexpected Event means any ~~of the following events provided~~ that is ~~they are~~ outside the reasonable control of the affected party and could not have been prevented or avoided by that party by reasonable diligence or reasonable precautions, including:

(a) an act of God, lightning strike, meteor strike, earthquake, storm, flood, landslide, tsunami, explosion or fire;

(b) strikes or other industrial action~~, other than strikes or other industrial action of some or all of the Supplier's Personnel~~; and

(c) war, terrorism, sabotage, blockade, revolution, riot, insurrection, civil commotion or epidemic,

but excludes:

(d) any act or omission of a Subcontractor (except where that act or omission was caused by ~~a~~ an Unexpected Event);

(e) strikes or other industrial action of some or all of the Supplier's or a Subcontractor's Personnel; and

(f) Delay Events and other acts and omissions of the Customer, its Personnel and Niche (any applicable consequences of which are to be separately addressed in clauses 7.6 and 7.7 rather than such events being Unexpected Events).

A11. Amendments to Module 4 – Systems Integration

For the purposes of the Contract, clause 3.3(a) of Module 4 – Systems Integration will be treated as having been amended as follows (with additions to Module 4 shown in underlining, and deletions from Module 4 shown in strike-out):

(a) ensuring that (on and from the date it is accepted) the Detailed Project Plan (to the extent applicable) ~~PIPP (if any)~~ is followed and that delays are dealt with in accordance with clause 7.6 of the Comprehensive Contract Conditions;

To avoid doubt, if any further Module Order Form 4 is agreed between the parties (including as contemplated by Additional Provision A8), the same amendment set out in this Additional Provision A11 will apply for the purposes of the Services described in that further Module Order Form.

A12. Link Stage

(a) The signing of the Link Deed of Variation is deemed to be sufficient notification to proceed with the work in the Link Stage.

(b) To the extent that the parties commenced any activities pursuant to Module Order Form 2 or Module Order Form 4 - Link prior to the Link Variation Date, the parties agree that those activities will be taken to have been performed under the Contract, including as varied by way of the Link Deed of Variation.

(c) To avoid doubt, the commencement and completion of the Link Stage does not impact on the commencement and completion of the Unify Stages under clause 7.5 of the Comprehensive Contract Conditions and Additional Provision A8.

7. Term (Clause 3)

Start date

The date on which the Contract is formed in accordance with clause 1.1(a) of the Comprehensive Contract Conditions.

End date

The first date on which:

(a) the Warranty Period in respect of the System has ended and all of the Integration Services (to the extent that they form part of the first Stage or a further Stage with which the Supplier has been required to proceed under clause 7.5 of the Comprehensive Contract Conditions) have otherwise been fully performance in accordance with the Contract; and

(c) if the Customer has not required the Supplier to proceed with work in all of the Stages under clause 7.5 of the Comprehensive Contract Conditions, the notice period within which it is required to give the Supplier notice of such a requirement has expired.

Extension options

Not applicable.

Notice period for extension

Not applicable.

8. Authorisations (Clause 4.2)

Not applicable.

9. Tasmanian Industry Participation Plan (Clause 4.5)

The Tasmanian Industry Participation Plan completed and endorsed by the Supplier on 22 February 2024, which forms part of the Contract.

10. Documentation (Clause 5)

User Documentation

As set out in Appendix 13 (Business, Functional, Non-Functional And Technical Requirements).

User Documentation must be provided:

☒ electronically

☐ in hard copy

Bespoke Documentation

As set out in the applicable Module Order Form, any applicable Detailed Project Plan and any Statement of Work.

Bespoke Documentation must be provided:

☒ electronically

☐ in hard copy

The Customer's review and approval of the Bespoke Documentation will be undertaken in accordance with clause 5.3 of the Comprehensive Contract Conditions, and any applicable requirements set out in the applicable Module Order Form, any applicable Detailed Project Plan and any Statement of Work.

11. Policies, codes of conduct, rules, standards and procedures (Clause 6.1)

Site Policies

Not applicable – as specified in clause 6.1(a)(i) of the Comprehensive Contract Conditions.

Policies, codes of conduct, rules, standards and procedures

Without limiting clause 6.1(a)(i) of the Comprehensive Contract Conditions, the Supplier must comply with the behavioural standards set out in the Customer's Diversity and Inclusion Policy and Framework.

Without limiting clause 6.1(a)(i) of the Comprehensive Contract Conditions, the Supplier must comply with all security and confidentiality policies with respect to all Customer premises, information holdings, data and any other matters of a confidential nature which may be encountered by the Supplier or any of its Personnel in connection with the performance of the Services, at the applicable security or confidentiality level (as determined by the Customer).

12. Customer Inputs (Clause 6.4)

Details of Customer Inputs to be provided

In respect of Customer Inputs relevant to the performance of the activities undertaken pursuant to Module Order Form 4 - Unify, as set out as 'Customer Requirements' in Appendix 09 to Module Order Form 4 - Unify – Resource Requirements, Customer Furnished Items and Risks and the Resource Schedule, each of which forms part of the Contract.

In respect of Customer Inputs relevant to the performance of the activities undertaken pursuant to Module Order Form 2 or Module Order Form 4 - Link, as set out as 'Customer Requirements' in Appendix 14 to Module Order Form 4 – Link – Customer Furnished Items and Dependencies, which forms part of the Contract.

Times when each Customer Input is to be provided

In respect of Customer Inputs relevant to the performance of the activities undertaken pursuant to Module Order Form 4 - Unify, as set out in the applicable Detailed Project Plan and any Statement

of Work or (to the extent not set out in either of those documents) in Appendix 09 to Module Order Form 4 - Unify or the Resource Schedule.

In respect of Customer Inputs relevant to the performance of the activities undertaken pursuant to Module Order Form 2 or Module Order Form 4 - Link, as set out in the applicable Detailed Project Plan (to the extent not set out in Appendix 14 to Module Order Form 4 – Link – Customer Furnished Items and Dependencies).

Requirements or specifications for the Customer Inputs (if any)

In respect of Customer Inputs relevant to the performance of the activities undertaken pursuant to Module Order Form 4 - Unify, as set out in the applicable Detailed Project Plan and any Statement of Work or (to the extent not set out in either of those documents) in Appendix 09 to Module Order Form 4 - Unify or the Resource Schedule.

In respect of Customer Inputs relevant to the performance of the activities undertaken pursuant to Module Order Form 2 or Module Order Form 4 - Link, as set out in the applicable Detailed Project Plan (to the extent not set out in Appendix 14 to Module Order Form 4 – Link – Customer Furnished Items and Dependencies).

Amount payable by the Supplier for the Customer Inputs (if any)

None.

Additional requirements that apply to the use of any Customer Inputs (if any)

To avoid doubt, all Customer Inputs comprising or containing Confidential Information of the Customer (which, for clarity, includes information that is designated by the Customer as being, or that the Supplier should reasonably realise is, confidential to a third party to whom the Customer would owe confidentiality obligations in relation to that information) must be used, disclosed and otherwise handled in accordance with the relevant provisions of the Contract, including clause 14.

13. Customer Assistance (Clause 6.5)

Instructions, information, data, documents, specifications, plans, drawings and other materials that must be provided by the Customer to the Supplier

Not applicable – all instructions, information, data, documents, specifications, plans, drawings and other materials to be provided by the Customer are specified as Customer Inputs.

14. Management committee (Clause 7.1)

Specify whether a management committee is to be established

☒ Yes

☐ No

Members of management committee

As representatives of the Customer, the Customer's project director, project manager and commercial manager for the project from time to time.

As representatives of the Supplier, the Supplier's engagement partner, technical partner and project manager from time to time.

Date the management committee is required to be established

30 April 2024.

Any additional functions of the management committee

(a) Discussion of any complaints or concerns raised under the Contract from time to time.

(b) Negotiation and use of reasonable endeavours to resolve any dispute that is the subject of a dispute notice, as the parties' initial representatives appointed under clause 23.2(b) (provided that, consistently with clause 7.1(e), any in principle resolution agreed by the management committee will not bind the parties unless and until it is confirmed in writing by the parties' Authorised Representatives).

(c) Discussion and in principle agreement on any Change to be requested by a party or Change Requests submitted by the Supplier, to inform the Customer's decision as to the acceptance, negotiation or rejection of the Change Request.

Meeting frequency

Monthly, or more frequently if reasonably required by the Customer.

Meeting time

As agreed between the parties from time to time, or as reasonably directed by the Customer from time to time (including, for example, if the Customer considers that there is an urgent need for a management committee meeting or if it has been unable to secure the Supplier's agreement to a meeting time).

Meeting location

As agreed between the parties from time to time, or as reasonably directed by the Customer from time to time (including, for example, if the Customer considers that there is an urgent need for a management committee meeting or if it has been unable to secure the Supplier's agreement to a meeting location).

15. Performance reviews (Clause 7.2)

Specify whether performance reviews are required under the Contract

☒ Yes

☐ No

Specify intervals for service and performance reviews

On request by the Customer if and when the Customer considers that a service and performance review may be required in addition to other management processes under the Contract.

16. Site Specification (Clause 7.3)

Specify whether the Supplier is required to provide a Site Specification under the Contract

☐ Yes

☒ No

17. Project Implementation and Payment Plan (Clause 7.4)

Specify whether a Project Implementation and Payment Plan is required under the Contract

☐ Yes

☒ No

If yes, complete Schedule 2 – Project Implementation and Payment Plan.

18. Staged Implementation (Clause 7.5)

Specify whether staged implementation applies to the Contract

☒ Yes

☐ No

Specify the notice period which the Customer must give written notice to move to the next Stage

No applicable notice period – see Additional Provision A8.

19. Liquidated Damages (Clause 7.7)

Specify whether Liquidated Damages apply to the Contract

☒ Yes

☐ No

Specify the Supplier's obligations which are LD Obligations

See table below.

Specify the LD Due Date for completion of each LD Obligation

LD Obligation	LD Due Date
Occurrence of the Actual Acceptance Date for the business design for Drop 1	25 October 2024
Occurrence of the Actual Acceptance Date for the System and Services delivered as part of	18 April 2025

LD Obligation	LD Due Date
Drop 1 by way of user acceptance testing being successfully completed and the applicable exit criteria being satisfied for Drop 1	
Occurrence of the Actual Acceptance Date for the business design for Drop 2	7 March 2025
Occurrence of the Actual Acceptance Date for the System and Services delivered as part of Drop 2 by way of user acceptance testing being successfully completed and the applicable exit criteria being satisfied for Drop 2	1 August 2025
Occurrence of the Actual Acceptance Date for the business design for Drop 3	20 June 2025
Occurrence of the Actual Acceptance Date for the System and Services delivered as part of Drop 3 by way of user acceptance testing being successfully completed and the applicable exit criteria being satisfied for Drop 3 and final acceptance of System under clause 3.12(b) of Module 4 in respect of the System required to be provided as part of each Stage)	20 October 2025

Specify the calculation and amount of liquidated damages for each LD Obligation

$32,000 per day.

Specify any cap on the Liquidated Damages

$3 million

20. Training (Clause 7.10)

Details of any training requirement

As set out in the applicable Module Order Form, any applicable Detailed Project Plan and any Statement of Work.

Rates for additional training

Not applicable. The Price is inclusive of the provision of the training referred to in this section 20.

21. Subcontractor(s) (Clause 8)

Name (and legal entity)

Bdna Group Pty Ltd (ABN 53 629 959 360)

Street address

Level 10, 231 North Quay, Brisbane, QLD 4000

Postal address

GPO Box 78, Hobart, Tasmania 7001

Obligations

Those parts of the Services comprising business analysis (NicheRMS), systems configuration (NicheRMS) and data migration

22. Subcontractor(s) statutory declaration (Clause 8.1(d))

Specify if the Subcontractor(s) are required to provide a statutory declaration substantially in the form of Schedule 3 – Statutory Declaration by Subcontractor, or other agreed form.

☐ Yes

☒ No

23. Background checks (Clause 8.2)

Without limiting the Customer's right to make any request under clause 8.2 from time to time, the Supplier must conduct, and provide to the Customer an original or certified copy of the results of, a criminal background check for each of its Personnel involved in the supply of any Deliverables under the Contract:

(a) prior to such involvement commencing (for which purpose any criminal background check conducted and provided to the Customer pursuant to the RFT and prior to the Contract being formed will be accepted); and

(b) within two years after the conduct of the criminal background check most recently conducted for that Personnel, if they continue to be involved in the supply of any Deliverables under the Contract,

each in accordance with clause 8.2(b)(i).

24. Confidentiality, Privacy and Conflict of Interest Deed (Clause 8.2(f))

All Personnel (including Subcontractors and their officers, directors, employees and agents) involved in the supply of any Deliverables under the Contract are required to sign a confidentiality, privacy and conflict of interest deed substantially in the form of Schedule 4 – Confidentiality, Privacy and Conflict of Interest Deed or such other form reasonably acceptable to the Customer.

25. Key Personnel (Clause 8.4)

Name and Position

As set out in the document forming part of the Contract entitled 'Appendix 08 – Key Resource List'.

In addition, in respect of the activities to be undertaken pursuant to Module Order Form 2 or Module Order Form 4 - Link, the following persons:

- 

Contact details

As set out in the document forming part of the Contract entitled 'Appendix 08 – Key Resource List' or, in respect of the individuals named above, as set out in the document forming part of the Contract entitled 'Appendix 16 – Project Link – Key Resource List'.

Role / Key obligations

As set out in the document forming part of the Contract entitled 'Appendix 08 – Key Resource List' or, in respect of the individuals named above, as set out in as set out in the document forming part of the Contract entitled 'Appendix 16 – Project Link – Key Resource List'.

Committed level

As set out in the document forming part of the Contract entitled 'Appendix 08 – Key Resource List' or, in respect of the individuals named above, as set out in as set out in the document forming part of the Contract entitled 'Appendix 16 – Project Link – Key Resource List'.

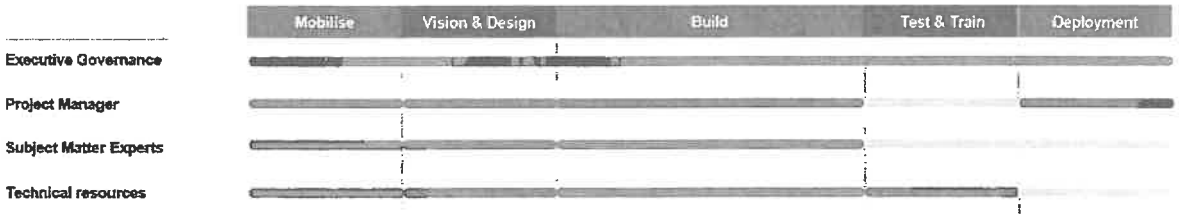
Summary of Key Personnel's skills, qualifications and experience

As set out in the document forming part of the Contract entitled 'Appendix 08 – Key Resource List' or, in respect of the individuals named above, as set out in as set out in the document forming part of the Contract entitled 'Appendix 16 – Project Link – Key Resource List'.

26. Customer's Personnel (Clause 8.5)

In respect of the activities to be undertaken pursuant to Module Order Form 4 - Unify, as set out in Appendix 09 to Module Order Form 4 - Unify – Resource Requirements, Customer Furnished Items and Risks.

In respect of the activities to be undertaken pursuant to Module Order Form 2 or Module Order Form 4 - Link, as set out below:



The increased/high levels of technical resource allocation (as indicated above) is largely due to the expected input across the technical integration stream.

- DPFEM's PM will need to be more involved during the first phase of the project – working with KPMG to coordinate project mobilisation and workshops and support the team during the validation workshops. After the build phase of the project, the PM will also be involved in the preparation and planification of UAT sessions, and work with KPMG to coordinate the train-the-trainer session.
- SME's and Technical resources will be heavily involved during the "vision and validate" phase of the project: they will actively participate in the workshops and action the checklist provided by KPMG. After the construct phase, SMEs will be executing all User Acceptance Tests. Technical Resources will also actively participate in the mobilisation phase by setting up the environment and licences required.

	Duration (in days per week)
Low	
Medium	
High	

27. Acceptance Testing (Clause 9)

Will Acceptance Testing of Deliverables be required?

☒ Yes

☐ No

If yes, complete Schedule 9 – Acceptance Testing.

28. Price and payment (Clause 10)

The applicable Pricing Schedule which sets out the Price and payment terms is:

☒ Schedule 1 – Price and Payment Terms

☐ Schedule 2 – Project Implementation and Payment Plan

Total Price

$14,367,678 (exclusive of GST), unless and until the Customer gives a notice to proceed with a further Unify Stage after the first Unify Stage in accordance with the Contract, in which event the

total Price will be increased by the price agreed for that further Unify Stage under Additional Provision A8.

29. Intellectual Property Rights in Pre-Existing Material (Clause 12.1)

Pre-Existing Material

Pre-Existing Material of the Customer includes:

(a) the documents forming part of the Contract that are described in section 5 of these Details;

(b) the Material supplied in or with the Request for Tender or otherwise supplied by or on behalf of the Customer as part of the procurement process commenced by way of the issue of the Request for Tender (including addenda and information released as part of any best and final offer process);

(c) any Material comprised in or containing processes and workflows in relation to the Designated Environment;

(d) any Material describing any of the business functions referred to in Business Functions Overview; and

(e) any Material made available by the Customer for incorporation into, or otherwise for the development of, a data schema.

Customer's use of Pre-Existing Material

The licence of Pre-Existing Material of the Supplier under clause 12.1(b) of the Comprehensive Contract Conditions is also granted for the purposes of:

(a) Tasmania Police; and

(b) any other Agency that may in the future undertake any of the relevant functions or activities of the Customer or Tasmania Police,

using, supporting and/or modifying the Deliverables in the course of its functions and activities.

Sublicensees and cost

Not applicable.

30. Intellectual Property Rights in New Material (Clauses 12.2 to 12.4)

New Material

In relation to the activities undertaken pursuant to Module Order Form 4 - Unify, no particular Material is specified as being New Material, but the definition in the Comprehensive Contract Conditions applies.

In relation to the activities undertaken pursuant to Module Order Form 2 and Module Order Form 4 - Link, New Material includes (without limiting the definition in the Comprehensive Contract

Conditions) all of the Materials comprised in or relating to the online crime reporting solution including:

- crime reporting online form solution
- crime reporting triage solution
- integration between solution and ORS2
- integration between solution and Axon Community Portal
- all associated documentation developed as Deliverables (including as set out in Appendix 15 to Module Order Form 4 - Link – Deliverables)

Ownership of New Material

Will Intellectual Property Rights in the New Material be owned by the Customer or Supplier?

☒ Customer (clause 12.2 of the Comprehensive Contract Conditions applies) – in respect of all New Material other than Work Papers

☒ Supplier (clause 12.3 of the Comprehensive Contract Conditions applies) – in respect of Work Papers only

Supplier owned – Customer's use of New Material

Not applicable – Work Papers cannot include any materials incorporated into a Deliverable and, accordingly, there is no licence granted of Work Papers under clause 12.3(b).

Supplier owned – Sublicensees and costs

Not applicable – Work Papers cannot include any materials incorporated into a Deliverable and, accordingly, there is no licence granted of Work Papers under clause 12.3(b).

Will any Deliverables incorporate any Third Party Material?

☐ Yes

☒ No

The licence of Third Party Material under clause 12.4 of the Comprehensive Contract Conditions is also granted for the purposes of:

(a) Tasmania Police; and

(b) any other Agency that may in the future undertake any of the relevant functions or activities of the Customer or Tasmania Police,

using, supporting and/or modifying the Deliverables in the course of its functions and activities.

31. Escrow (Clause 12.6)

Specify if an escrow arrangement is required

☐ Yes – in the form of Schedule 5 – Escrow Agreement

☐ Yes – in a form reasonably acceptable to the Customer

☒ No

Specify the third party escrow agent

Not applicable.

Specify the minimum duration of the Escrow Agreement

Not applicable.

32. Customer Data (Clause 13(f))

None.

33. Confidential Provisions (Clause 14.2)

The following clauses, schedules, attachments, annexures, appendices or other material, are to remain confidential to the parties and are designated as Confidential Provisions under clauses 14.2(c) and 14.2(d) of the Comprehensive Contract Conditions until the content in that clause, schedule, attachment, annexure, appendix or other material enters the public domain:

(a) Additional Provision A5(b)(iii) in these Details;

(b) the words 'and the Grace Period Contingency Requirement' in Additional Provision A5(c), (d) and (e) in these Details;

(c) Additional Provision A5(e)(iii) in these Details;

(d) Additional Provisions A10(g) to A10(l) in these Details;

(e) Additional Provisions A10(z) to A10(dd) in these Details;

(f) the definition of 'LD Grace Period' set out in Additional Provision A10(pp) in these Details;

(g) paragraph (f) of the definition of 'Unexpected Event' set out in Additional Provision A10(rr) in these Details;

(h) Item 19 (Liquidated Damages) of these Details;

(i) Item 28 (Price and payment) of these Details;

(j) Item 34 (Cap on liability) of these Details;

(k) the documents referred to in Items 5(a) to (g) and 5(s) in these Details;

(l) Appendices 01 through 12 to Module Order Form 4 - Unify as referred to in Items 5(h) to (s) in these Details;

(m) Annexures J, K and L to the Supplier's response to the RFT;

(n) Attachments 4, 5, 6 and 7 to the Supplier's response to the RFT;

(o) the Resource Schedule as referred to in Item 5(t) in these Details; and

(p) Appendices 13 through 15 to Module Order Form 4 - Link as referred to in Items 5(v) to (x) in these Details.

34. Cap on liability (Clause 17.3 and 17.7)

Supplier's liability cap

An amount equal to the Price paid or payable by the Customer for the relevant Stage, multiplied by 1.25.

Customer's liability cap

An amount equal to the Price paid or payable by the Customer for the relevant Stage.

Supplier's liability cap where a scheme applies to the Supplier

Not applicable.

35. Insurance (Clause 19)

Workers compensation insurance as required by law.

Public liability and products liability insurance minimum amount

$20 million in the aggregate per annum

Professional indemnity insurance minimum amount

$20 million in the aggregate per annum

Other insurances

Not applicable

Minimum period of insurance (for insurance on a "claims made" basis)

Not applicable; the period specified in clause 19(c) of the Comprehensive Contract Conditions applies.

Other evidence of insurance

Not applicable; the evidence of the required insurances is as specified in clause 19(d)(i) of the Comprehensive Contract Conditions.

Exclusions and deductibles for insurance policies

Is the Supplier required to notify the Customer in writing of any exclusions and deductibles relevant to the insurance policies that the Supplier is required to have in place?

☐ Yes

☒ No

36. Security (Clause 20)

Nil.

37. Conflict of Interest (Clause 21.2)

A member of the Supplier's Key Personnel is married to the Executive Director People and Business Services for the Department of Police, Fire & Emergency Management. The parties acknowledge that for the purposes of clauses 21.2(a) and (b), this perceived Conflict of Interest was disclosed by the Supplier prior to the release of the RFT, and the parties took steps to deal with the matter prior to the release of the RFT which have remained in place since that time and will remain in place for as long as the Conflict of Interest subsists, or until the end of the Term.

38. Reports (Clause 22.1)

Specify the reports to be provided by the Supplier

(a) Written fortnightly reports that set out the Supplier's performance under the Contract, including:

(i) details of the Supplier's progress in providing each Deliverable;

(ii) details of any actual or potential risks identified by the Supplier as impacting or potentially impacting on such performance (including any foreseeable or actual delay in the Supplier performing its obligations under the Contract), and how such risks are being managed; and

(iii) any other details reasonably requested by the Customer from time to time,

which reports must be submitted in accordance with the timing requested by the Customer from time to time so as to facilitate its program and project governance.

(b) Reporting on status of the supply of the Deliverables, and any other information reasonably requested by the Customer from time to time, to the steering committee established by the Customer for its Project Unify program.

(c) Any other reports specified in any Detailed Project Plan or otherwise in the Contract as being required to be provided by the Supplier.

39. Termination for convenience (Clause 24.3)

In the event that the Contract is terminated for convenience and that termination takes effect once a Stage has been completed and prior to the Customer having given notice to the Supplier to commence the following Stage, the amount specified in this section applies and is nil.

In the event that the Contract is terminated for convenience in any other circumstances, the amount specified in clause 24.3(b)(ii)(A) applies.

40. Business Hours (Clause 27.1)

Not applicable – the Business Hours are the hours between 9.00am and 5.00pm on Business Days.

41. Designated Environment (Clause 27.1)

(a) The Atlas software environment, comprising NicheRMS and the existing and future configurations and integrations of NicheRMS, as described in the Atlas Architecture Overview.

(b) The other existing software applications with which NicheRMS is to be integrated as part of the Services, being those that carry out the business functions described in the Business Functions Overview and/or store data described in the Database Background and Overview or the Data Dictionaries.

(c) The infrastructure environment associated with the software described in paragraphs (a) and (b), as described in the Atlas Architecture Overview and the Azure Move Overview.

(d) The Power Platform (including Power Apps and Power Pages).

Acknowledgments and Certifications

The Supplier:

(a) agrees to provide the Products, Services and other Deliverables to the Customer on the terms described in the Contract.

(b) certifies that it has read, understands, and complies with all the requirements of the Contract.

(c) represents that all the information provided by it and referenced in the Contract is complete, accurate, up to date and not misleading in any way.

(d) acknowledges that the Customer is relying on the information provided by the Supplier and referenced in the Contract in entering into the Contract.

(e) acknowledges that the Customer may suffer damage if any of that information is incomplete, inaccurate, out of date or misleading in any way.

1.1 Forming the Contract

1.1.1 Agreement by Supplier

The Supplier will sign in this section. By signing, the Supplier is offering to enter the Contract on the terms set out in this document. If the Supplier does not execute this document itself, it must (if the Customer requests) provide adequate evidence that the signatory is properly authorised to execute this agreement.

If the parties agree any changes to this document after the date of the Supplier's signature (but before the Customer accepts the Supplier's offer as described below), the Supplier and Customer will prepare a new version of the document incorporating the agreed changes, which will replace this document. The Supplier will sign the new document, offering to enter the Contract on the amended terms.

Date ..... EXECUTED as an agreement by **KPMG Australia Technology Solutions Pty Limited ABN 29 606 612 962** in accordance with section 127(1) of the *Corporations Act 2001* (Cwlth):			
Signature:		Signature:	
* Print name and office held:		* Print name and office held:	
*Use BLOCK LETTERS Note: In the case of a company that has only one director and one secretary, show the office held as 'SOLE DIRECTOR AND SOLE COMPANY SECRETARY'			

1.1.2 Agreement by Customer

Date .....

EXECUTED for and on behalf of **The Crown in right of Tasmania acting through the Department of Police, Fire and Emergency Management** by its Authorised Representative, in the presence of:	)	..... Signature of Authorised Representative By executing this agreement the signatory warrants that the signatory is duly authorised to execute this agreement on behalf of the Customer
..... Signature of witness	)	..... Name of Authorised Representative (block letters)
..... Name of witness (block letters)	)	..... Position of Authorised Representative

Attachment B - Module Order Form 2

Module Order Form 2 – Software - Link

This document is a derivative of Module Order Form 2 - Software (publications.qld.gov.au) created in 2017 by the Department of Science, Information Technology and Innovation, Queensland Government and is used under Creative Commons licence CC BY 4.0

Module Order Form 2A – Licensed Software

The following Module Order Form 2A to be completed if the Customer is procuring Licensed Software (refer to clause 3 of Module 2). Note: Licensed Software will include Developed Software where the Supplier (not the Customer) will own the Intellectual Property Rights in that Developed Software.

1. Licensed Software

Clause 3.1 of Module 2

Name of Licensed Software (including version number and all applicable modules/components)

Not applicable.

2. Requirements

Specifications for Licensed Software (or annex specifications to the Module Order Form)

Not applicable.

3. Use of Licensed Software

Clause 3.1 of Module 2

Not applicable.

4. Class of Licence

Clause 3.1 of Module 2

Not applicable.

5. Copies of Licensed Software to be provided by Supplier

Clause 3.1 of Module 2

Not applicable.

6. Licence Period

Clause 3.2 of Module 2

Not applicable.

Is the Licence Period perpetual?

☐ Yes

☐ No

Not applicable.

Start of Licence Period

Not applicable.

End of Licence Period

Not applicable.

Extension options

Not applicable.

Notice period for extension

Not applicable.

7. Supply through a Reseller

Clause 3.3 of Module 2

Not applicable.

Specify whether the Licensed Software is being supplied by the Supplier in the capacity as a Reseller

☐ Yes

If yes, insert name of the Third Party Provider:

☐ No

Not applicable.

If yes, specify which of the following applies:

☐ Reseller to supply the Licensed Software from the Third Party Provider to the Customer in accordance with the Contract (except in relation to the Licensed Software warranty provisions set out in Module 2) in accordance with clause 3.3(b) of Module 2.

☐ Reseller to facilitate the supply of the Licensed Software from the Third Party Provider to the Customer in accordance with clause 3.3(c) of Module 2.

Specify the assistance to be provided by the Supplier in coordinating warranty claims:

Not applicable.

8. Sublicensing

Clause 3.4 of Module 2

Not applicable.

9. Additional licence conditions and restrictions

Clause 3.5 of Module 2

Not applicable.

10. Third Party Software

Clause 3.6 of Module 2

Not applicable.

Does the Licensed Software include any components of Third Party Software?

☐ Yes

☐ No

If yes, specify the details of any Third Party Software (if any) associated with the Licensed Software:

If yes, specify the terms and conditions which apply to the Third Party Software (where the Third Party Software is not licensed as part of the Licensed Software:

11. Open Source Licence

Clause 3.7 of Module 2

Not applicable.

Does the Licensed Software include any components of open source software?

☐ Yes

☐ No

If yes, specify the Open Source Licence that governs the use of the open source software:

12. Delivery and installation requirements

Clause 3.9 of Module 2

Site

Not applicable.

Delivery Date

Is the Supplier required to install the Licensed Software?

☐ Yes

☐ No

If the Supplier is required to install the Licensed Software, specify the requirements for the installation of the Licensed Software:

13. Back-ups

Clause 3.11of Module 2

Not applicable.

Specify if the Customer or the Supplier is to maintain back-ups:

☐ Customer

☐ Supplier

If Supplier, insert details of the backups to be performed (including frequency and format of back-ups):

14. Updates and New Releases

Clause 3.12 of Module 2

Not applicable.

Specify if the Customer is entitled to Updates and/or New Releases for the Licensed Software (as part of the Licence as opposed to part of separate Software Support Services)

☐ Yes

☐ No

If yes, insert any installation obligations of the Supplier:

15. Ancillary services

Clause 3.13 of Module 2

Not applicable.

16. Warranty Period

Clause 3.15 of Module 2

Not applicable.

17. Records of Licensed Software

Clause 3.17 of Module 2

Not applicable.

Module Order Form 2B – Software Support Services

The following Module Order Form to be completed if the Customer is procuring Software Support Services (refer to clause 4 of Module 2).

1. Support Period

Clause 4.1 of Module 2

Start of Support Period

Not applicable.

End of Support Period

Not applicable.

Extension options

Not applicable.

Notice period for extension

Not applicable.

2. Requirements

Clause 4.1 of Module 2

Specifications for Software Support Services (or annex specifications to the Module Order Form)

Not applicable.

3. Supported Software

Clause 4.2 of Module 2

Name of Supported Software (including version number and all applicable modules/components)

Not applicable.

4. Remote access

Clause 4.2(c) of Module 2

Not applicable.

The Supplier is to be provided remote access to provide the Software Support Services:

☐ Yes

☐ No

If yes, specify any additional terms which apply to the Supplier's remote access to the Supported Software (if any):

5. Supply through a Reseller

Clause 4.3 of Module 2

Not applicable.

Specify whether the Software Support Services are being supplied by the Supplier in the capacity as a Reseller

☐ Yes

If yes, insert name of the Third Party Provider:

☐ No

If yes, specify which of the following applies:

☐ Reseller to supply the Software Support Services from the Third Party Provider to the Customer in accordance with the Contract (except in relation to the warranty provisions set out in clause 4.7 of Module 2) in accordance with clause 4.3(b) of Module 2.

☐ Reseller to facilitate the supply of the Software Support Services from the Third Party Provider to the Customer in accordance with clause 4.3(c) of Module 2.

Specify the assistance to be provided by the Supplier in coordinating warranty claims:

6. General Support

Clause 4.4 of Module 2

Not applicable.

7. Updates and New Releases

Clause 4.6 of Module 2

Not applicable.

Updates and New Releases to be provided?

☐ Yes

☐ No

If yes, is training to be provided by the Supplier in respect of the Updates and New Releases?

☐ Yes

If yes, specify the training (if any) to be provided by the Supplier in respect of the Updates and New Releases (e.g. training to enable the Customer to operate the Update or New Release:

☐ No

If yes, specify any additional terms which apply to the supply of the Update and New Release:

Period of support for each New Release

8. Service Levels

Clause 4.9 of Module 2

Not applicable.

The Service Levels are set out in:

☐ Schedule 8 – Service Levels

☐

9. Service Credits

Clause 4.9 of Module 2

Not applicable.

The Service Credits are set out in:

☐ Schedule 8 – Service Levels

☐

Module Order Form 2C – Developed Software

The following Module Order Form to be completed if the Customer is procuring Developed Software (refer to clause 5 of Module 2).

1. Developed Software and Design Specification

Clause 5.1 and 5.3 of Module 2

Description of Developed Software

The Developed Software will:

- Enable members of the public to report minor crimes via an interactive and intuitive online form;
- Enable nominated internal staff to view recently submitted minor crime reports and triage accordingly by selecting the appropriate outcome from a pre-defined list; and
- Develop a core functionality that covers the specific requirements for the Crime Reporting Process, and that can be easily adapted future processes.

Requirements

As set out in Appendix 13 to Module Order Form 4 - Link – Business Functional, Non-functional and Technical Requirements.

Is Supplier required to prepare a Design Specification?

☒ Yes

☐ No

2. Delivery Dates

Clause 5.1 and 5.3 of Module 2

Design Specification

In respect of the requirements backlog described in Appendix 15 to Module Order Form 4 - Link – Deliverables: by two weeks after the Link Variation Date.

In respect of the remainder of the Design Specification (including the Functional Solution Design Specification and the Integration Design Specification described in Appendix 15 to Module Order Form 4 - Link – Deliverables): by four weeks after the Link Variation Date.

Developed Software

1 October 2024.

3. Delivery and installation requirements

Clause 5.1 and 5.3 of Module 2

Site

Level 6, 70 Collins Street, Hobart 7000

Is Supplier required to install the Developed Software?

☒ Yes

☐ No

If the Supplier is required to install the Developed Software, specify the requirements for the installation of the Developed Software:

The Supplier will install the Developed Software in the development and test environments of the Designated Environment.

The Supplier will lead, and provide appropriate guidance and co-ordination, for the Customer's Technology & Innovation staff to install the Developed Software in the production environment of the Designated Environment.

4. Ancillary services

Clause 5.6 of Module 2

- The Supplier must establish the Power Platform environments including Power Apps and Power Pages (including development, testing and production), in order that it can commence development of the Developed Software within those environments, in accordance with the applicable timing set out in Appendix 15 to Module Order Form 4 - Link – Deliverables and in accordance with any applicable requirements set out in Appendix 13 to Module Order Form 4 - Link – Business, Functional, Technical and Non-Technical Requirements.
- The Supplier must:
    - conduct an environment threat risk assessment; and
    - provide the outcomes of that assessment to the Customer,

  in accordance with the applicable timing set out in Appendix 15 to Module Order Form 4 - Link – Deliverables and any applicable requirements set out in Appendix 13 to Module Order Form 4 - Link – Business, Functional, Technical and Non-Technical Requirements.
- The Supplier must:
    - create a configuration, release and environment strategy for validation and approval by the Customer in accordance with the applicable timing set out in Appendix 15 to Module Order Form 4 - Link – Deliverables, which strategy must satisfy any applicable requirements set out in Appendix 13 to Module Order Form 4 - Link – Business, Functional, Technical and Non-Technical Requirements and the criteria set out in Appendix 15 to Module Order Form 4 - Link – Deliverables; and
    - undertake the activities pursuant to this Module Order Form 2 and Module Order Form 4 - Link in accordance with the approved configuration, release and environment strategy.
- The Supplier must develop a test strategy for validation and approval by the Customer in accordance with the applicable timing set out in Appendix 15 to Module Order Form 4 - Link – Deliverables, which strategy must satisfy any applicable requirements set out in Appendix 13 to Module Order Form 4 - Link – Business, Functional, Technical and Non-Technical

Requirements and the criteria set out in Appendix 15 to Module Order Form 4 - Link – Deliverables, and must provide for the conduct of:

- unit testing of individual units/components of the configuration of the Developed Software and the System implemented under Module Order Form 4 - Unify, by the Supplier's configuration teams during the build phase;
- non-functional testing, focusing on the performance, stability and usability of the Developed Software, by the Supplier by 15 weeks after the Link Variation Date; and
- Acceptance Tests in order to confirm that the process, procedures and workflow are understood by the Customer and meet the Customer's documented business needs, using test cases based on the scenarios used during the design phases and further extended by the Customer to create a representative reflection of the usage of the Developed Software.

- The Supplier must:
  - develop a deployment plan for validation and approval by the Customer in accordance with the applicable timing set out in Appendix 15 to Module Order Form 4 - Link – Deliverables, which plan must satisfy any applicable requirements set out in Appendix 13 to Module Order Form 4 - Link – Business, Functional, Technical and Non-Technical Requirements and the criteria set out in Appendix 15 to Module Order Form 4 - Link – Deliverables; and
  - undertake deployment activities pursuant to this Module Order Form 2 and Module Order Form 4 - Link in accordance with the approved deployment plan.
- As part of the development of the Developed Software, the Supplier must conduct, and ensure appropriate Personnel of the Supplier attend:
  - sprint planning meetings at the start of each weekly build sprint (which are intended to be each of the fifth to tenth weeks after the Link Variation Date), to confirm the requirements to be implemented in the upcoming sprint;
  - daily stand-ups, with a view to removing any blockers to the development work; and
  - sprint reviews at the end of each sprint, including for project team members and key stakeholders to provide feedback on the functionality implemented during the sprint.
- The Supplier must design and set up the S30 [redacted] y 13 weeks after the Link Variation Date in accordance with any applicable requirements set out in Appendix 13 to Module Order Form 4 - Link – Business, Functional, Technical and Non-Technical Requirements.
- The Supplier must prepare and deliver the materials (including a training guide) for delivery of train the trainer training and administrator training, for validation and approval by the Customer in accordance with the applicable timing set out in Appendix 15 to Module Order Form 4 - Link – Deliverables, which materials must satisfy any applicable requirements set out in Appendix 13 to Module Order Form 4 - Link – Business, Functional, Technical and Non-Technical Requirements and the criteria set out in Appendix 15 to Module Order Form 4 - Link – Deliverables.

- The Supplier must deliver:
    - two train the trainer sessions, for up to four hours each and a maximum of 20 attendees each; and
    - one administrator training session, for up to four hours and a maximum of six attendees,

  by 15 weeks after the Link Variation Deed, in accordance with any applicable requirements set out in Appendix 13 to Module Order Form 4 - Link – Business, Functional, Technical and Non-Technical Requirements.
- The Supplier must conduct the testing that is its responsibility under the test strategy developed pursuant to this Module Order Form 2.
- The Supplier must create and provide to the Customer a test closure report at the end of each phase of the testing (including the Acceptance Tests), in accordance with the applicable timing set out in Appendix 15 to Module Order Form 4 - Link – Deliverables, each of which reports must satisfy any applicable requirements set out in Appendix 13 to Module Order Form 4 - Link – Business, Functional, Technical and Non-Technical Requirements and the criteria set out in Appendix 15 to Module Order Form 4 - Link – Deliverables.
- The Supplier must:
    - develop a go live plan for validation and approval by the Customer in accordance with the applicable timing set out in Appendix 15 to Module Order Form 4 - Link – Deliverables, which plan must satisfy any applicable requirements set out in Appendix 13 to Module Order Form 4 - Link – Business, Functional, Technical and Non-Technical Requirements and the criteria set out in Appendix 15 to Module Order Form 4 - Link – Deliverables; and
    - undertake go live activities pursuant to this Module Order Form 2 and Module Order Form 4 - Link in accordance with the approved go live plan.
- The Supplier must:
    - develop a hypercare plan for validation and approval by the Customer by 19 weeks after the Link Variation Date, which plan must satisfy any applicable requirements set out in Appendix 13 to Module Order Form 4 - Link – Business, Functional, Technical and Non-Technical Requirements and must specify the exit criteria for the hypercare services and the Warranty Period; and
    - undertake support activities pursuant to this Module Order Form 2 and Module Order Form 4 - Link in accordance with the approved hypercare plan.
- The Supplier must provide a project closure report plan for validation and approval by the Customer in accordance with the applicable timing set out in Appendix 15 to Module Order Form 4 - Link – Deliverables, which report must satisfy any applicable requirements set out in Appendix 13 to Module Order Form 4 - Link – Business, Functional, Technical and Non-Technical Requirements and the criteria set out in Appendix 15 to Module Order Form 4 - Link – Deliverables.

5. Warranty Period

Clause 5.7 of Module 2

The Warranty Period for the Developed Software is the period of at least 90 days commencing on successful achievement of go live in accordance with the go live plan that is a Deliverable under this Module Order Form 2, and will run concurrently with the provision of hypercare services (as described in the hypercare plan that is a Deliverable under this Module Order Form 2).

Where Defects are identified by the Customer during the Warranty Period (including through the provision of hypercare services), other than Defects that the Supplier is not obliged to remedy under clause 5.8 of Module 2, the Customer will assign the Defect a Priority Level in accordance with the classification set out in Attachment A to Schedule 9 (Acceptance Testing).

The Supplier must successfully achieve the exit criteria for exit from hypercare and the Warranty Period (as set out in the hypercare plan that is a Deliverable under this Module Order Form 2) in order to exit the Warranty Period. If the exit criteria are not satisfied at the end of the 90 day period, the Warranty Period (and performance of hypercare services) will be extended until those exit criteria are achieved. To avoid doubt, any extension of the Warranty Period and the performance of the hypercare services does not increase the Price payable to the Supplier.

Attachment C - Module Order Form 4 – Link

Module Order Form 4 – Systems Integration - Link

This document is a derivative of Mo dule Order Form 4 – Systems Integration (publications.qld.gov.au) created in 2017 by the Department of Science, Information Technology and Innovation, Queensland Government and is used under Creative Commons licence CC BY 4.0

Module Order Form 4 – Systems Integration

The following Module Order Form to be completed if the Customer is procuring Systems Integration (refer to clause 3 of Module 4).

1. Commencement of Integration Services

Clause 3.1 of Module 4

1 October 2024.

2. Integration Services

Clause 3.2 of Module 4

The Supplier will undertake integration services so as to provide the following:

- Functionality for the Developed Software to create new offence records within the DPFEM Offence Reporting System (ORS2), and
- Functionality for the Developed Software to send a request for digital evidence via the Axon (evidence.com) Community Portal API,

as further described in Appendix 13 – Business, Functional, Non-Functional and Technical Requirements.

3. System

As described in the Detailed Specifications.

4. Requirements

Specifications for Integration Services (or annex specifications to the Module Order Form)

As described in Appendix 13 – Business, Functional, Non-Functional and Technical Requirements.

5. Implementation planning

Clause 3.4 of Module 4

The Supplier will undertake implementation planning for the Integration Services , including by way of conducting and participating in integration design workshops with relevant Customer personnel. In addition to the items specified in clause 3.4 of Module 4 – Systems Integration, the Supplier must conduct implementation planning to:

- assess and define the Customer's needs and pain points; and
- refine the project scope in collaboration and with the approval of the Customer.

6. Detailed Specifications

Clause 3.5 of Module 4

Documents comprising the Detailed Specifications

The integration solution design specification described in Appendix 15 – Deliverables, and any other Deliverables described in Appendix 15 – Deliverables to the extent that they contain specifications for the Integration Services.

7. Interfaces

Clause 3.6 of Module 4

Supplier Interfaces

The Supplier will provide:

- Integration from the S30 and
- Integration to the S30

as further described in Appendix 13 – Business, Functional, Non-functional and Technical Requirements and the Detailed Interface Specifications.

Customer Interfaces

S30

8. Delivery Dates

Clauses 3.4, 3.5, 3.7, 3.8 and 3.9 of Module 4

Implementation planning (Design Services)

20 August 2024.

Detailed Specifications

20 August 2024.

Data Migration Plan

Not applicable.

Installation and configuration

30 October 2024.

Integration

1 October 2024.

9. Site

Clause 3.7 of Module 4

The Supplier will perform the Services at the Customer's Site with resources attending on-site as required.

The Supplier will otherwise install and configure all components of the System on the Designated Environment, in accordance with its obligations under the Contract, including Module 4.

The capability for secure remote working will also be enabled.

10. Data Migration Services and Data Cleansing Services

Clauses 3.9 - 3.10 of Module 4

Data Migration Services

Are Data Migration Services required?

☐ Yes

☒ No

Extraction of Customer Data

Not applicable.

Data Cleansing Services

Not applicable.

Are Data Cleansing Services required?

☐ Yes

☒ No

Date for completion of Data Cleansing Services

Not applicable.

11. Data Tools

Clauses 3.11 of Module 4

Not applicable.

12. Ancillary services

Clause 3.13 of Module 4

To the extent that any of the ancillary services described in Module Order Form 2 are applicable to the Integration Services under this Module Order Form rather than the development of the Developed Software under Module 2, those ancillary services will be treated as being services to be performed under this Module Order Form.

13. Warranty Period

Clause 3.14 of Module 4

The Warranty Period for the System is the period of at least 90 days commencing on successful achievement of go live in accordance with the go live plan that is a Deliverable under Module Order Form 2 and/or this Module Order Form, and will run concurrently with the provision of Hypercare Services (as described in the hypercare plan that is a Deliverable under Module Order Form 2 and/or this Module Order Form).

Where Defects are identified by the Customer during the Warranty Period (including through the provision of hypercare services), other than Defects that the Supplier is not obliged to remedy under clause 3.15(c) of Module 4, the Customer will assign the Defect a Priority Level in accordance with the classification set out in Attachment A to Schedule 9 (Acceptance Testing).

The Supplier must successfully achieve the Exit Criteria for Exit from Hypercare/Warranty (as set out in the hypercare plan that is a Deliverable under Module Order Form 2 and/or this Module Order Form) in order to exit the Warranty Period. If the exit criteria are not satisfied at the end of the 90 day period, the Warranty Period (and performance of hypercare services) will be extended until those exit criteria are achieved. To avoid doubt, any extension of the Warranty Period and the performance of the hypercare services does not increase the Price payable to the Supplier.

Attachment D - Appendix 13 (Business, Functional, Non-Functional and Technical Requirements) to Module Order Form 4 – Link

Department *of* Police, Fire *and* Emergency Management

PROJECT LINK

MODULE 4 - APPENDIX 13

BUSINESS, FUNCTIONAL, NON-FUNCTIONAL AND TECHNICAL REQUIREMENTS

Version No: 2.0 17/07/2024

Copy: Uncontrolled

EDRMS: A24/xxxxxx

Document Acceptance and Release Notice

This document is Version 2.0 17/07/2024 of the Project Link – Online Minor Crime Reporting Requirements.

The Project Link – Online Minor Crime Reporting Requirements document is a managed document. For identification of amendments, each page contains a release number and a page number. Changes will only be issued as a complete replacement. Recipients should remove superseded versions from circulation. This document is authorised for release once all signatures have been obtained.

PREPARED:	S36	Date:	18/07/2023
(for acceptance)	**Eric Brumby** Project Manager		
ACCEPTED:		Date:	
(for acceptance)	**Ian Whish-Wilson** Business Owner		
APPROVED:		Date:	
(for release)	**Jeremy Williams** Program Director		

Document Development History

Build Status

Version	Date	Author	Reason	Description
0.1	30/03/2023	E. Brumby M. Mackenzie		Initial draft
0.2	20/07/2023	E. Brumby		Review and update to include working group feedback.
0.3	21/07/2023	M. Mackenzie	Updates	Adding in prioritisation of requirements
1.0	29/09/2023	E. Brumby	Updates	Review and update to include working group feedback.
2.0	17/07/2024	J. Alcock	Update	Minor updates and combine business and technical requirements.

Amendments in this Release

Section N°	Section Title	Amendment Summary
		This is the first release of this document, for internal review

Distribution

Copy No	Version	Issue Date	Issued To
Electronic	0.3	21/07/2023	Working Group for review
Electronic	0.4	27/09/2023	Working group for endorsement

Table of Contents

1. Overview 5

1.1 Document Purpose 5

1.2 Glossary 5

1.3 Scope 5

1.4 Optional Requirements 5

1.5 Overview/Context 6

1.5.1 Business Areas 6

1.6 Systems 6

1.6.1 Overview Diagram 6

1.6.2 Processes 7

1.6.3 Other Systems 7

2 **Functional Requirements** 9

2.1 Online Portal (Public Reporting) 9

2.2 Internal Portal (Offence Verification) 10

2.3 Process Automation 11

3 **Non-functional Requirements** 13

3.1 Usability 13

3.2 Security 14

3.3 Automation 15

3.4 Performance 15

3.5 Maintainability 15

4 [redacted] 17

S30 17

17

5 **Technical Requirements** 19

5.1 Integrated System 19

5.2 System Access and Security 19

5.3 User Access Control and Permissions 21

5.4 Operational Support 21

5.4.1 System Maintenance 21

5.4.2 *System Monitoring* 22
5.4.3 *Tenderer Support* 23
5.5 Operational Support 23
5.5.1 *System Maintenance* 23
5.5.2 *Online Help* 24
5.6 Implementation Services 25
5.6.1 *Documentation* 25
5.6.2 *Training Services* 25
5.6.3 *Software Testing* 26
5.7 Systems Configuration 26
5.7.1 *General Configuration* 26
5.7.2 *Maintain and Use Reference Code Data* 27
5.8 Performance and Capacity 29
5.9 Availability and Recovery 29
5.10 Data Storage, Archiving and Access 30
5.11 Technology Platform 31

1. Overview

1.1 Document Purpose

The purpose of this document is to define the business and technical requirements for the DPFEM (Department of Police, Fire & Emergency Management) Online Minor Crime Reporting Portal and associated automated data transfer mechanisms. The requirements are to be used to identify and assess potential solutions to provision a supporting secure public online service.

1.2 Glossary

Term	Description
Atlas	The Tasmania Police operational policing system
Axon Community	A third-party portal used to collect image and video evidence from the community.
DPFEM	Department of Police, Fire & Emergency Management
ORS2	Offence Reporting System 2
Portal	The Online Minor Crime Reporting presence for Tasmania Police

1.3 Scope

The scope of this document is limited to the business, technical, functional and non-functional requirements to identify potential solutions to implement an online portal for the reporting of minor crime, basic validation by DPFEM staff, and automated data transfer into the Offence Reporting system (ORS2).

The scope of this document does not include:

- Current and Future State Minor Crime Reporting processes (refer *Annexure B – Minor Crime Current and Future State Process Description*)

1.4 Optional Requirements

Note that this document contains section/requirements which are optional for the purposes of the OMCRS RFQ, and are for informational purposes only, (see 3.9 Support Services in Annexure F – OMCR Overview and Implementation Plan Response).

These requirements have been marked as Optional in the Notes column.

1.5 Overview/Context

1.5.1 Business Areas

The requirements are specific to the primary business areas that investigate minor criminal offences, identify commonalities and trends in offending, and provide detailed reporting on crime statistics.

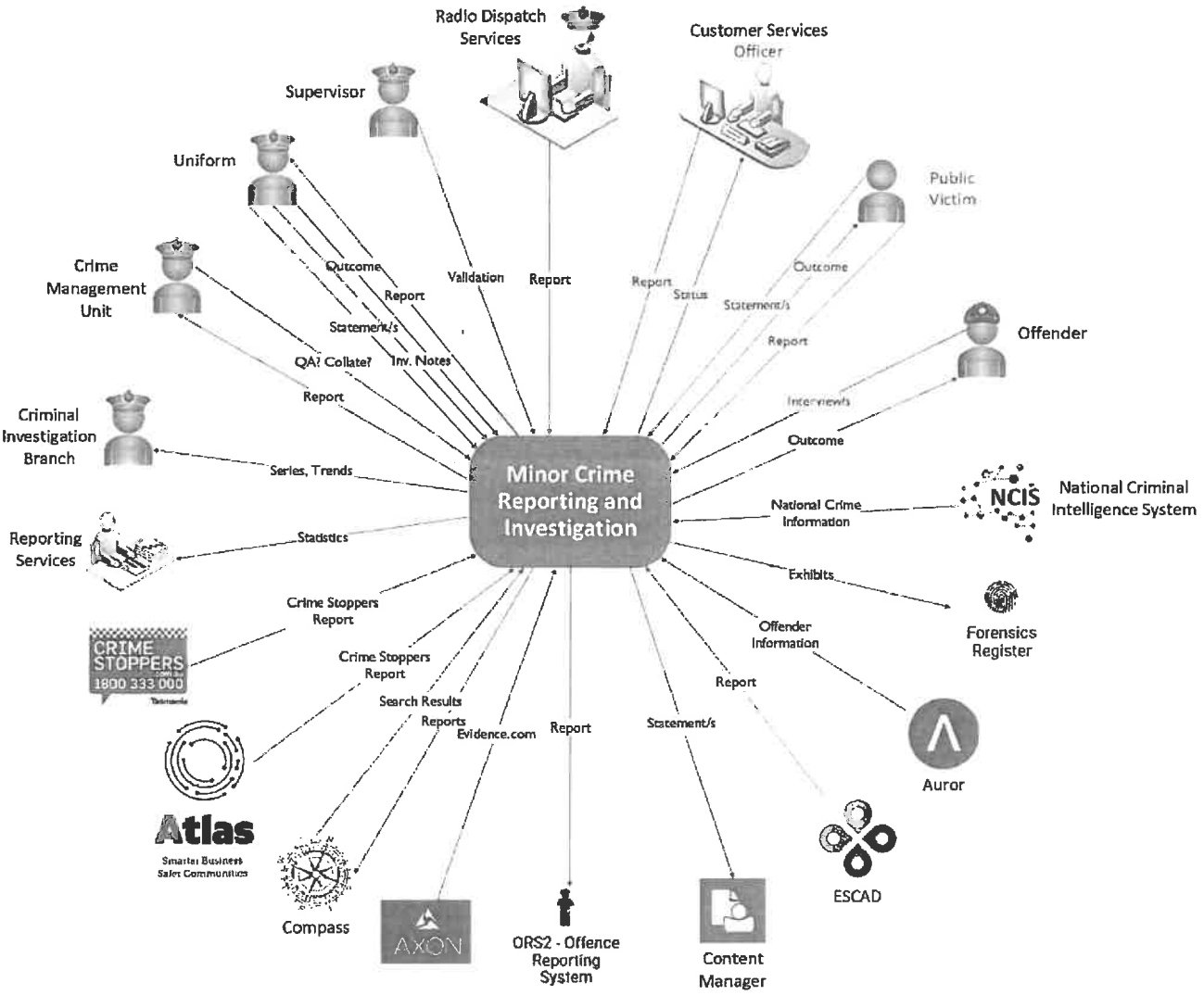
The main business areas that use minor crime reports include:

- Criminal Investigation Branch (all Districts)
- Crime Management Units (all Districts)
- Radio Dispatch Service
- Reporting Services
- Information Services
- Operational police members

1.6 Systems

1.6.1 Overview Diagram

The following diagram provides context of the current minor crime reporting process, and its interactions with internal and external systems.



1.6.2 Processes

Refer *Project Link – Minor Crime Current and Future State Process Description* document.

1.6.3 Other Systems

The following systems will have key interactions (interface, integration) with the Online Minor Crime Reporting Portal:

- Offence Reporting System 2 (ORS2). Central repository of all Offence Reports. Target system for automated data transfer from the online portal submitted data.
- Axon (Evidence.com) – Digital evidence management system utilised to store, manage and share digital evidence securely. Functionality exists for members of the public to upload footage, upon receiving a unique link from Axon.

2 Functional Requirements

Requirements should be read in context of the table heading together with the actual requirement, for example: "The system will *Use a decision tree (Yes/No questions) to triage incoming requests so only valid Minor Crime Reports are lodged into ORS2.*".

Requirements have been prioritised using the MoSCoW prioritisation model:

Priority	Definition
Must	An essential requirement that is non-negotiable. The requirement must be delivered for the solution to be accepted.
Should	A requirement with considerable significance but no pressing need to be delivered.
Could	A nice to have requirement in the event there is available time and budget.
Won't	An out-of-scope requirement.

2.1 Online Portal (Public Reporting)

Provision of a public facing portal which guides the public through a triage process prior to verifying the lodger and lodging the minor crime report.

No.	Priority	Requirement: "The solution will provide facilities to ..."	Notes
FR-01	Must	Provide an intuitive, user-friendly and dynamic form that adapts based on user input and captures essential information about the crime, including the type of crime, location, date and time, description, and any supporting details or evidence.	
MCR-FR-02	Must	Use a decision tree (Yes/No questions) to triage incoming requests so only valid Minor Crime Reports are lodged.	Decision tree is fully configurable and maintainable by authorised DPFEM users.
MCR-FR-03	Must	Provide correct guidance to the report initiator where Minor Crime Reporting is identified as the wrong path, such as providing a phone number or redirecting to a URL.	Guidance prompts are fully configurable and maintainable by authorised DPFEM users.
MCR-FR-04	Must	Perform verification check on report initiator using their nominated preferred contact method of email address or SMS, to prevent fraudulent reports or spamming.	

No.	Priority	Requirement: "The solution will provide facilities to ..."	Notes
MCR-FR-05	Must	Verify entered data against standard DPFEM data sets and standards (such as valid addresses, correct formatted email/phone number, etc.), allowing the initiator to correct identified errors.	
MCR-FR-06	Must	Format and store successfully submitted data in a secure location/system for consumption by verification and automation processes.	
MCR-FR-07	Must	Provide failure notification (including relevant detail) to nominated recipient/s on failure to store data.	
MCR-FR-08	Must	Facilitate entry and validation of addresses via features such as auto-address completion, drop a pin, and verification against a DPFEM address source, e.g. GNAF.	
MCR-FR-09	Must	Apply consistent verification rules with the back-end system to avoid rejection of applications after being lodged.	
MCR-FR-10	Should	Provide functionality to manage submission forms, such as editing, archiving, or deleting forms.	Fully configurable and maintainable by authorised DPFEM users.
MCR-FR-11	Must	S30	Fully configurable and maintainable by authorised DPFEM users.
MCR-FR-12	Must	Integrate with the branding and 'look and feel' of the Tasmania Police web site.	
MCR-FR-13	Should	Use DPFEM data tables (or copy of) to populate relevant list of Location (Class of Premises) and Property Types for selection	Fully configurable and maintainable by authorised DPFEM users as per TR71.
MCR-FR-14	Should	Provide functionality for tooltips/help icons to populate contextual help messages and guidance throughout the online reporting process for relevant fields and entry.	

2.2 Internal Portal (Offence Verification)

Provision of a secure portal and data repository for authenticated Tasmania Police staff to modify, verify and allocate incoming minor crime reports prior to transfer of data to a new Online Charging System 2 (ORS2) report (or rejection).

No.	Priority	Requirement: "The solution will provide facilities to ..."	Notes
MCR-FR-15	Must	Allow a reviewer to modify reported data as required based on access roles/restrictions.	
MCR-FR-16	Must	Allow a reviewer to mark a submitted report as rejected.	
MCR-FR-17	Must	Allow a reviewer to approve a submitted report as a valid report.	
MCR-FR-18	Must	Allow a reviewer to select the designated offence type from a configurable list of approved offences.	Fully configurable and maintainable by authorised DPFEM users.
MCR-FR-19	Must	Allow a reviewer to assign the report to business area using a configurable list of Tasmania Police Districts.	Fully configurable and maintainable by authorised DPFEM users.
MCR-FR-20	Must	Restrict update access to the verification portal to Tasmania Police staff with defined workgroup membership.	
MCR-FR-21	Must	Provide view access to a defined group of Tasmania Police staff.	

2.3 Process Automation

Provision of an automated process to transfer data from the source system and create a new Online Charging System 2 (ORS2) report.

No.	Priority	Requirement: "The solution will provide facilities to ..."	Notes
MCR-FR-22	Must	Establish a secure connection to the source database and the destination database.	
MCR-FR-23	Must	Establish a secure and scalable database infrastructure to store submitted reports and related information. Regularly backup the data to prevent loss or corruption.	
MCR-FR-24	Must	Extract data from the source database using appropriate query mechanisms.	
MCR-FR-25	Must	Identify the relevant data to be transferred based on specific criteria.	
MCR-FR-26	Must	Transform data, if necessary, to ensure compatibility with the destination database.	

No.	Priority	Requirement: "The solution will provide facilities to ..."	Notes
MCR-FR-27	Must	Load data into the destination database using appropriate insert/update mechanisms.	
MCR-FR-28	Must	Send a closure email or text message to the reporting person where a report is rejected.	
MCR-FR-29	Must	Once confirmed as valid, send a confirmation email or text message to the reporting person with the created Offence Report number, including a link to provide further information.	
MCR-FR-30	Must	Support an efficient message facility including email and SMS notifications.	
MCR-FR-31	Must	S30	
MCR-FR-32	Must	S30	
MCR-FR-33	Must	Integrate with Axon to allow members of the public to upload digital evidence related to their report.	
MCR-FR-34	Must	Analyse, route and process reports based on pre-defined and configurable automation rules.	
MCR-FR-35	Must	Implement scheduled jobs to transfer/delete data from relevant database based on specific criteria	

3 Non-functional Requirements

Requirements should be read in context of the table heading together with the actual requirement, for example: "The solution will support "*Consistent workflow, user interface and user interaction for conceptually similar tasks.*".

The following non-functional requirements should be read in conjunction with the Annexure C – Online Minor Crime Reporting Technical Requirements.

Requirements have been prioritised using the MoSCoW prioritisation model:

Priority	Definition
Must	An essential requirement that is non-negotiable. The requirement must be delivered for the solution to be accepted.
Should	A requirement with considerable significance but no pressing need to be delivered.
Could	A nice to have requirement in the event there is available time and budget.
Won't	An out-of-scope requirement.

3.1 Usability

No.	Priority	Requirement: "The solution will deliver..."	Notes
MCR-NFR-01	Must	An intuitive and user-friendly look and feel, providing consistent workflows, interfaces and user interaction for conceptually similar tasks.	
MCR-NFR-02	Must	Meaningful and helpful error messages and system prompts being displayed on screen.	Meaningful end user messages when an exception or error occurs to the underlying system or environment that contains no sensitive information.
MCR-NFR-03	Must	The capability to handle errors and exceptions gracefully, providing appropriate notifications and recovery mechanisms.	*Ability to review report (ie review each page) before submission?
MCR-NFR-04	Should	An intuitive experience, allowing users to successfully accomplish basic tasks the first time they use the system.	
MCR-NFR-05	Should	Be easy to use and maintain, requiring minimal technical expertise.	

No.	Priority	Requirement: "The solution will deliver..."	Notes
MCR-NFR-06	Must	An 'appropriate use' / 'terms and conditions' warning banner prior to a user accessing the portal.	Appearance of banner and banner message contents will be configurable by authorised DPFEM users.

3.2 Security

No.	Priority	Requirement: "The solution will support..."	Notes
MCR-NFR-07	Must	S30	
MCR-NFR-08	Must		
MCR-NFR-09	Must		
MCR-NFR-10	Must		
MCR-NFR-11	Must		
MCR-NFR-12	Must		
MCR-NFR-13	Must		
MCR-NFR-14	Must		
MCR-NFR-15	Must		
MCR-NFR-16	Must		
MCR-NFR-17	Must		

3.3 Automation

No.	Priority	Requirement: "The solution will support..."	Notes
MCR-NFR-18	Must	Automation of the data transfer process to eliminate the need for manual intervention.	
MCR-NFR-19	Must	Reliable and accurate transfer of data, ensuring that data is not lost or corrupted during the transfer process.	
MCR-NFR-20	Should	Scalability to accommodate future data growth and changes in data structure.	

3.4 Performance

No.	Priority	Requirement: "The solution will support..."	Notes
MCR-NFR-21	Must	Each application transaction performed being completed in no more than three seconds.	
MCR-NFR-22	Must	At least five concurrent reports being able to be submitted by the system at the same time.	
MCR-NFR-23	Must	The solution having no single point of failure and being designed to be fault tolerant.	

3.5 Maintainability

No.	Priority	Requirement: "The solution will support..."	Notes
MCR-NFR-24	Must	The solution providing a data archiving mechanism for storage of historical data.	
MCR-NFR-25	Must	Full, comprehensive backups for all solution components being performed on a definable schedule.	
MCR-NFR-26	Must	Incremental backups for all solution components being performed on a definable schedule.	
MCR-NFR-27	Must	All backups associated with the solution being performed in a secure manner.	
MCR-NFR-28	Must	Solution components remaining available during any backup activity.	

No.	Priority	Requirement: "The solution will support..."	Notes
MCR-NFR-29	Must	[redacted]	
MCR-NFR-30	Must		
MCR-NFR-31	Should		
MCR-NFR-32	Must	Fine grain monitoring of the solution being undertaken.	
MCR-NFR-33	Must	[redacted]	
MCR-NFR-34	Should		
MCR-NFR-35	Must		
MCR-NFR-36	Must	Upgrades and/or patches to the solution being applied while maintaining availability.	
MCR-NFR-37	Must	A mechanism to allow for roll-back of any changes applied.	
MCR-NFR-38	Must	Testing of solution modifications independent to the production environment of the solution.	

4

4.1

S30

S30

4.2 Network/Firewall Architecture

S30

An independent threat and risk assessment of the solution to the existing DPFEM environment will be undertaken with identified controls to be included into the solution architecture.

5 Technical Requirements

Requirements should be read in context of the heading together with the actual requirement, for example: "The Tenderer to Provide an overall diagram that shows all software components of the Offered Solution".

5.1 Integrated System

No.	Requirement: "The Tenderer to ..."	Notes
TR1.	Provide an overall diagram that shows all software components of the Offered Solution.	
TR2.	Detail all software modules of the Offered Solution and for each software module involved, describe and provide: • Module name • Description • Current version number • Anticipated version number being offered to DPFEM • Client component name • Server component name • Database component name.	
TR3.	Warrant that the offered System is an integrated solution that does not require duplicate data entry for any of the data. Detail and explain any deviations of the offered System from this requirement.	

5.2 System Access and Security

No.	Requirement: "The Tenderer to ..."	Notes
TR4.	Be certified to provide secure information systems to clients, preferably to a defined level of one or more of the following: • ISO 27001/2 Information Security Management • ASD Certified Cloud Service Provider • Certified under ISO Standard for Risk Management (ISO 31000:2009 Risk Management). In your response, for each information security certification that is held by your organisation, provide: • The level of certification that is held; documentary evidence must also be included with the response • The scope of services that the certification covers	

- Whether the certification will apply to the solution delivered to DPFEM. Tenderers will ensure that the prices in the pricing schedule match the level of security that is offered here.

If no comparable certification is held or not relevant, detail how you will provide a comparable level of information security to DPFEM, given that your personnel will obtain access to DPFEM production system data.

TR5. Ensure that all Authorised Users, System and Security Administrators can be held accountable for their actions within the system.

TR6. Store security audit records for a period of time, which will be able to be configured by DPFEM, of all security relevant events such that Unauthorised Agents, Authorised Users, System and Security Administrators actions can be detected and potentially held accountable for their actions.

TR7. Provide the capability to selectively view security audit information. Viewing of security audit information must also be auditable, logged and based on Role-based Access Control (RBAC).

TR8. Ensure that only authorised users gain access to the system and to the resources that it controls. Please outline.

TR9. Securely manage all remote user access to the system.

TR10. Ensure that all transfers of information within the system and between the system and DPFEM client computers are protected from unauthorised actions including disclosure, modification, deletion and replay. This protection is to apply to transfers of both live data and backup data.

TR11. Ensure data 'in transit' is encrypted in line with the ACSC Information Security Manual standards.

Encryption of data 'at rest' is desirable.

TR12. Provide procedures and/or mechanisms to assure that, after a system failure or other outage, recovery is achieved without compromising system integrity.

TR13. Confirm the cloud-based application with a web based front-end is OWASP compliant, perform a Threat Risk Assessment with a suitable security provider and remediate all reported concerns prior to publishing to the internet.

TR14. Confirm whether Multi-Factor Authentication (MFA) is available for the operational access portal.

TR15. Specify which web standard(s) will be supported, for example HTML5.

5.3 User Access Control and Permissions

No.	Requirement: "The Tenderer to ..."	Notes
TR16.	Allow for DPFEM administrators to assign one or more functional roles (RBAC), which will be selected from a list of values defined by DPFEM, e.g. Editor, View-only. The system will enforce access privileges determined by DPFEM based on an individual's functional role, for example: view only role, access to view all information except as restricted by other rules such as security classification.	
TR17.	Apply permissions cumulatively if a user has multiple functional roles: • Step 1: determine the complete set of features the user is not permitted to access, by collating the restrictions of each their functional roles; • Step 2: add back features they are permitted to access, based on the access granted by each of their functional roles	
TR18.	Allow business units (organisational units) to obtain reports of team member's roles for auditing purposes (i.e. Permissions Audit).	
TR19.	Record and maintain the list of members of each workgroup.	
TR20.	Record a hierarchy of workgroups, so that access to records can be allocated at multiple levels.	
TR21.	S30	

5.4 Operational Support

5.4.1 System Maintenance

No.	Requirement: "The Tenderer will provide details of ..."	Notes
TR22.	The offered system's regular maintenance requirements, for example type of maintenance activity (e.g. data archival), anticipated DPFEM effort (FTEs) and if they require downtime.	
TR23.	The Tenderer's proposal for the supply of maintenance services as to whether the services will be supplied remotely, through onsite support or by a combination of both.	Optional

No.	Requirement: "The Tenderer will provide details of ..."	Notes
TR24.	Specify whether the system supports user activities continuously for more than, for example, one year between interventions by administrators or technicians, i.e. no intervention is required to archive data, perform backups, empty log files etc.	
TR25.	Any issues the Tenderer may wish to raise with regard to DPFEM requirements for the manner in which maintenance services are to be supplied and the Tenderer's proposal for dealing with any such issues.	
TR26.	The process of distributing maintenance releases with respect to the offered system. Include details such as whether software patches can be optionally applied, whether the product is a full new release or just patched components.	
TR27.	How changes to software and software configuration are implemented (e.g. whether outage is required, impact to users, process to progress through environments).	
TR28.	Any application management functionality included in the offered system. Include details concerning the ability to start and stop processes, monitor completion of tasks, detect software problems. Detail any special management tools that are required to manage your system.	

5.4.2 *System Monitoring*

No.	Requirement: "The system will provide facilities to ..."	Notes
TR29.	S30 [redacted]	
TR30.	Provide reports that show, for a user-selected period, counts and types of errors and warnings encountered and generated by the system.	

No.	Requirement: "The Tenderer will provide details of ..."	Notes
TR31.	How to configure the monitoring solution for the offered system.	
TR32.	Any application monitoring functionality included in the offered system or third-party products required for this purpose, and how the application logs events, such as errors.	

5.4.3 *Tenderer Support*

No.	Requirement: "The Tenderer will provide details of ..."	Notes
TR33.	Methods of contact supported by the Tenderer.	Optional
TR34.	The method for registering requests and problems with the offered system with the Tenderer.	Optional
TR35.	How current clients report requests and problems to the Tenderer.	Optional
TR36.	Any local support office available in Australia.	Optional
TR37.	Categories or severity levels in place to prioritise reported requests and problems, with corresponding response times for each category, or severity level. (e.g. Initial Response time, Resolution time, Implementation).	Optional
TR38.	The terms of the Service Level Agreement that are being offered.	Optional
TR39.	Any knowledge base of known issues and resolutions provided by the Tenderer for client access.	Optional

5.5 Operational Support

5.5.1 *System Maintenance*

No.	Requirement: "The System will ..."	Notes
TR40.	Provide a user interface with a: • common look and feel throughout • consistent interaction style and window construction • consistent use of terminology across the entire solution • straightforward navigation between fields within a screen and from screen to screen.	
TR41.	Adhere to appropriate user interface standards based on published industry standards, e.g. the Microsoft Windows GUI Guidelines, where relevant.	
TR42.	Provide facilities to allow experienced users to perform rapid navigation and data entry. This will include features such as: • keyboard shortcut access to all features • sequential navigation through forms.	Using commonly accepted standards where possible.

No.	Requirement: "The System will ..."	Notes
TR43.	Provide the ability in all lists of records to: • filter the list, e.g. to hide non-current values • sort the list ascending or descending by any of the columns • print the contents of the list including all columns • display or hide data columns in the list.	
TR44.	Incorporate a generic data entry mechanism for code and description fields, providing users with the ability to: • select a code or description from a scrolling dropdown list • start typing in the code or description field, and the system dynamically filters the available list to display only values matching the filter criteria entered.	
TR45.	Web-based components of the solution complying with the W3C Web Content Accessibility Guidelines (WCAG) 2.1 Level AA at a minimum (refer to http://www.w3.org/TR/WCAG/).	

5.5.2 *Online Help*

No.	Requirement: "The System will ..."	Notes
TR46.	Provide context sensitive help, with contexts including the role of the user, the task or function being performed, and the data field being used.	Configurable by DPFEM
TR47.	Provide tool tips as the cursor hovers over data fields and toolbar items.	For both the public and DPFEM portals
TR48.	Provide modifications to the Help system to include linkages, including hyperlinks, to existing DPFEM documentation and to external information locations (e.g. Workplace Health and Safety, Hazardous Goods, etc).	Links configurable by DPFEM
TR49.	Incorporate online user manuals / help screens that are context-sensitive and that support business rules and workflows.	
TR50.	Provide the facility for DPFEM administrators to update the online user manuals and online help.	

5.6 Implementation Services

5.6.1 Documentation

No.	Requirement: "The Tenderer to ..."	Notes
TR51.	Provide documentation: • tailored to the DPFEM operating environment that accurately describes the system and software, and how it is to be used in a manner clear and useful to DPFEM. • that is reviewed and approved by appropriately authorised officers of the Tenderer prior to publication.	
TR52.	Provide documentation in the form of both indexed online and offline document libraries.	
TR53.	Provide documentation that will include at least as a minimum: • Installation Guide. • Upgrade Guide (detailed instructions for system implementation teams to be able to implement any subsequent patches). • System Administration and Configuration Guide. • Product Information Guide. • Product Technical Guide. • Support and Maintenance Guide. • System Operations Guide. • System Troubleshooting Guide. • User documentation, including screen-flow diagrams (preferably with User Hints and Tips, Shortcuts, Frequently Asked Questions (FAQs). • Train the Trainer material.	

5.6.2 Training Services

No.	Requirement: "The Tenderer to ..."	Notes
TR54.	Include an approach to incorporate DPFEM staff onto the Tenderer project team (as a part of the knowledge transfer process).	
TR55.	Detail any forms of training to be made available to DPFEM, e.g. electronic form of training.	
TR56.	Detail the facilities available for the provision of training environments.	

5.6.3 *Software Testing*

No.	Requirement: "The Tenderer to ..."	Notes
TR57.	A set of generic configuration reference data such that the system can be readily build verification tested.	
TR58.	A set of tenderer manufactured test data such that the system can be readily build verification tested.	
TR59.	Evidence of and certification of the appropriate levels of Unit and System testing.	
TR60.	A tested reversion process so that the application software can be successfully withdrawn from an environment without impacting other services.	
TR61.	Test Plans for conducting the identified build verification tests.	
TR62.	Qualified Tenderer resources to assist with the necessary build verification tests, migration tests, system tests and validation tests.	
TR63.	Release notes describing the release contents and instructions on how to verify software releases are installed correctly and completely.	
TR64.	Automated testing tools or scripts for functional, load, performance, volume and stress testing that are provided as part of the offered system.	
TR65.	Any automated testing tools that are known to be compatible with the offered system.	
TR66.	a Penetration Test Assessment performed by a suitable security provider with remediation of all reported concerns following publishing to the internet but prior to launch.	

5.7 Systems Configuration

5.7.1 *General Configuration*

No.	Requirement: "The system will provide facilities to ..."	Notes
TR67.	Allow DPFEM system administrators to manage reference data (codes, values) in the live system. Refer Maintain and Use Reference Code Data section below for detailed requirements.	

5.7.2 *Maintain and Use Reference Code Data*

No.	Requirement: "The system will provide facilities to ..."	Notes
TR68.	Display reference data lists to assist the user wherever a coded value is required to be entered. The system will: • display help against each reference data list • display help against each reference data value • restrict the values list to those reference data values, which are active at the "reference date" of the record being entered. For example, when entering the offence code for an incident that occurred on 1/1/2001, only offence codes which were effective at that date should be presented • allow users to view other alternative names for any reference data value.	
TR69.	Create and maintain the list of values within each reference data list. The system will record the following for each entry within the list: • the code of the entry (e.g. G2) • display text for the entry (i.e. the user-friendly version e.g. Genuine Reason 2"). • help text that describes the meaning and usage of the entry, to help users determine when to use it • start and end dates of the entry; the system will ensure that entries are only used within their effective date ranges • whether date effectivity is to be applied based on the current date or based on the occurred date for an incident/information report. • display sort position (if appropriate for the list).	
TR70.	Create and maintain list information about reference data lists. The system will record: • the reference data list name • help text describes the usage of the reference data • sorting method, e.g. ascending, DPFEM-defined sequence, or a combination of the two.	
TR71.	Allow a DPFEM administrator to configure the contents of lookup/dropdown lists in the live system. The system will provide facilities for a DPFEM administrator to maintain the entries in reference data lists including: • Add new entries to reference data lists and specify all values for them. • Maintain the display text, help text and alternative names for existing entries. Where the system has defined validation or actions for entries, it will still allow DPFEM to change the text that is displayed and printed for these list entries without affecting the system functionality. • Maintain the effective dates for existing entries, i.e. the date at which the entry becomes active and/or the date at which the entry becomes inactive.	

No.	Requirement: "The system will provide facilities to ..."	Notes
	In your response, articulate any variation from this configurability, and advise whether the configuration could be done by DPFEM personnel or must be performed by your maintenance staff.	
TR72.	Record reference data lists that form hierarchies with multiple levels where appropriate.	
TR73.	Retain history of changes to reference data items, including changes to values and to validity, with the date when each change took effect.	

5.8 Performance and Capacity

No.	Requirement: "The Tenderer will ..."	Notes
TR74.	Define the minimum DPFEM network architecture for the offered system to operate in an optimised manner. Include as a minimum the following and specify the minimum recommended speeds/items: • Telecommunications type • Bandwidth (total or per user/device) • Redundancy • Latency • Optimisation • Mobile data access.	
TR75.	Provide an indication of anticipated production storage requirements for an organisation the size of DPFEM (i.e. given the initial load of DPFEM data and subsequent growth).	
TR76.	Provide response times of less than 2 seconds under normal load – i.e. when used by the 'Expected' number of concurrent users for all normal query, record creation and record update activities. It is noted that latency is also depended on the network carrier, service capacity and the capability of devices used.	
TR77.	Support remote working over low bandwidth connections. The system shall provide response times of less than 4 seconds for all normal usage of functions when used over a limited speed WAN connection, i.e. 256 kbit/s.	

5.9 Availability and Recovery

No.	Requirement: "The Tenderer will ..."	Notes
TR78.	Detail the percentage availability they are able to provide, and pricing for all availability options. e.g. system available 99.99% of the time (DPFEM preferred), all outages for maintenance less than 1 hour in duration.	Optional
TR79.	Provide comprehensive details of any platform, hardware or software dependencies external to the offered system that are required to ensure high availability.	
TR80.	Outline any system-related constraints that may impact DPFEM's availability requirements.	
TR81.	Outline the maintenance window (planned outage) anticipated for the offered system, including: • Types, frequency and duration of regular maintenance activities	Optional

- Frequency of system upgrades (minor and major)
- Expected length of outage for each type of upgrade.

TR82. Outline how the offered system will operate in a clustered, or high availability environment, specifically addressing how the application manages client session state.

No.	Requirement: "The system will provide facilities to ..."	Notes
TR83.	Integrate with DPFEM's backup/restore solution to ensure backup of all DPFEM data on a regular basis, with full access to past data for restoration where required.	
TR84.	Backup DPFEM data in a way that does not disrupt use of the environment by users, e.g. perform backups whilst the environment is live or backup the data at a time that is pre-agreed with DPFEM and does not disrupt operations.	

5.10 Data Storage, Archiving and Access

No.	Requirement: "The Tenderer will ..."	Notes
TR85.	Include all historical data within the scope of generated reports, regardless of where that data is stored, but subject to user access and permissions. All data shall be available for retrieval and reporting purposes, whether the data has been archived or not.	
TR86.	Allow for application data from the offered system to be able to be replicated to another data store for analytical and statistical reporting. If yes, provide details of any potential issues relating to data replication in near real time, or in overnight batch processes, with respect to having a detrimental effect on the performance of the offered system.	
TR87.	Confirm that all data is managed uniquely within the bounds of the systems, for example not using a file share with content accessible by users that the system has no control over.	
TR88.	Manage all data within Australia (Data Sovereignty).	

No.	Requirement: "The Tenderer will provide details of ..."	Notes
TR89.	Any additional requirements of the offered system with respect to a data backup and recovery regime, over and above standard industry practice.	
TR90.	Any specific data archiving capability within the offered system.	

TR91.	How the offered system ensures that its data conforms to a very high level of accuracy and integrity. Include details on how the offered system is structured to provide data validation to ensure data quality and integrity.

5.11 Technology Platform

No.	Requirement: "The system will ..."	Notes
TR92.	Be developed using the Microsoft Power Platform, (Power Pages, Power Apps, Logic Apps and Dataverse) in Australia East.	
TR93.	S30	
TR94.	Be usable on mobile devices, for example mobile phones, with a Responsive page design. Describe the minimum screen resolution required to support the offered system.	
TR95.	Be deployed using Infrastructure as Code and maintained using the DPFEM DevOps repository.	

No.	Requirement: "The Tenderer will provide details of ..."	Notes
TR96.	Any minimum hardware requirements for mobile and desktop devices to effectively operate the offered system. Include any details of minimum CPU speed, quantity of memory and maximum disk space, also any Operating System limitations.	
TR97.	Any dependencies on third party software required for your application to operate correctly, for example Internet Explorer, Java Virtual Machine, ActiveX Controls, Bootstrap, Angular/React or other applications). If so: • provide specific details of those components that are required and their supported version numbers • does your offer include the costs and licence terms and conditions for the software? If not, please explain why • if they are open source, are they actively developed with established backing?	
TR98.	Supported hardware/virtualisation platforms and server architecture.	
TR99.	Estimated production server hardware specification required to support the application usage within DPFEM.	
TR100.	Whether multiple instances, or environments, of the offered system can coexist on common host system hardware. If so, describe any additional hardware and software services that are required for this logical partitioning to operate effectively.	

No.	Requirement: "The Tenderer will provide details of ..."	Notes
TR101.	Whether the offered system requires access to disk or the file system, other than what is required by the offered system's nominated database or audit system.	
TR102.	Support for any of the common electronic mail technologies, such as Simple Mail Transport Protocol (SMTP) and Exchange Web Services (EWS). If none of these common technologies are supported, describe any alternative electronic mail technologies that your application may support.	
TR103.	The minimum network architecture, across all system tiers, required by the offered system to ensure acceptable performance from a client perspective. Include details of factors such as bandwidth and latency.	
TR104.	The architecture of the offered system. Specifically, provide: • a comprehensive description of all the application components (application and information architecture) • the technology architecture of each of the solution tiers • details on how the solution is structured to support a service-oriented architecture.	
TR105.	External systems integration architecture. Specifically, describe in detail, the ability of the offered system to: • participate in an environment where events related to business entities may be published to other systems • participate in an environment where business entities may need to be affected by subscribing to events in another system • access business objects, data or services from external systems • expose business objects, data or services to external systems • expose interfaces such that external systems may leverage or reuse the solution's functionality.	
TR106.	The ability to publish and consume web services, based on SOAP or REST. If not, provide details of any future strategy to support web services.	

Attachment E - Appendix 14 (Customer Furnished Items and Dependencies) to Module Order Form 4 – Link

Appendix 14 – Customer Furnished Items and Dependencies

Contents

Summary Assumptions, Dependencies and Customer Requirements 2
Summary of all assumptions from all appendixes 2
Summary of all dependencies from all appendixes 2
Summary Customer Requirements (including those previously marked as assumptions) 3

Summary Assumptions, Dependencies and Customer Requirements

Summary of all assumptions from all appendixes

For completeness the uniquely numbered assumptions are repeated in the below table. In the unlikely case that there is a difference in wording between the two documents the Appendix 14 is considered to be the master.

#	Assumption
	N/A

Summary of all dependencies from all appendixes

For completeness the uniquely numbered dependencies are repeated in the below table. In the unlikely case that there is a difference in wording between the two documents this document is considered to be the master.

#	Dependency	Required in week no.
D1	Contract executed	Week 0
D2	Supplier team members confirmed and onboarded	Week 0
D3	Power Apps and Power Pages subscriptions available	Week 0
D4	Customer project team members and SMEs identified and onboarded	Week 1
D5	Project plan approved	Week 1
D6	Stakeholders identified and confirmed for all workshops	Week 1
D7	Customer signed the Functional Solution Design Specification	Week 4
D8	Customer signed the Integration Design Specification	Week 4
D9	User acceptance criteria defined on requirements	Week 4
D10	Customer signed the Test Strategy	Week 4
D11	Power Platform environments available (at a minimum dev, test and production, with Power Apps and Power Pages)	Week 4

D12	DevOps is available and set with the appropriate project template	Week 4
D13	ORS2 Integration APIs are available	Week 7
D14	Availability of the code developed for the Project Unify integration platform dev environment	Week 7
D15	Build completed Note: the focus on the 1st week of SIT will be the integration between the online form and the triage app. The end to end process, including ORS2 integration, will be tested in the 2nd week of SIT.	Week 14
D16	UAT completed	Week 17
D17	Go live approval	Week 17

Summary Customer Requirements (including those previously marked as assumptions)

For completeness the uniquely numbered customer requirements are repeated in the below table. In the unlikely case that there is a difference in wording between the two documents this document is considered to be the master.
Please note that at the bottom of this list (C105 to C120) the Customer Requirements were originally Assumptions. During one of the consultation session these have been moved to be Customer Requirements. For tracking purposes, we have kept the initial identification (starting with an A, however we have added a C identification for consistency.

#	Customer requirements	First required in week no.
C1	Customer to create user accounts, laptops, appropriate tools and licences installed for Project Link Team Members and allocate the appropriate licences: • **Project Manager (x1)** • [redacted]	Week 4

	S30	
C2	Customer to create a single generic system administrator user account and a security principal for each Power Platform environment. Note: all Power Automate Flows configured during the build will be allocated to the generic system administrator account and Connection References will be allocated to the appropriate service principal account.	Week 4
C3	S30	Week 4
C4	Customer to provide access to the documentation site (SharePoint / S30	Week 4
C5	Customer to grant access to the Power Platform tenant and enable the Supplier to progress with the environment setup activities.	Week 4
C6	Validate and approve the Project Plan	Week 1
C7	Validate and approve the Configuration, Release & Environment Strategy	Week 4
C8	Provision SMS gateway	Week 5
C9	Setup mailboxes in Exchange	Week 5
C10	Provide future state processes	Week 1
C11	Client to provide website branding (Logos, colour schemes, banners, and branding material)	Week 2
C12	Review and prioritise the Requirements Backlog	Week 1
C13	Validate & approve the Functional Solution Design Specification	Week 4
C14	Validate & approve the Integration Solution Design	Week 4
C15	Validate & approve the Test Strategy	Week 4
C16	Apply the necessary controls to mitigate risks identified in the Environment Threat Risk Assessment.	Week 4
C18	Build ORS2 APIs to enable integration with Dataverse	Week 10
C19	Availability of the stakeholders to review/approve test results	Week 14
C20	Availability of test data for UAT and training	Week 16
C21	Write User Acceptance Test Plan and Test Cases for all new configurations and functionalities	Week 16
C22	Conduct UAT within the timeframe stipulated in the project timeline, record defects, and produce the UAT Report	Week 16
C23	Provide input and approval on Test Closure Reports	Depending on phase
C24	Conduct BVT within the timeframe stipulated in the project timeline, record defects, and produce the BVT Report	Week 19

C25	Plan and execute change management activities and communications	Throughout the project
C26	Plan and deliver end-user training	Week 18
C27	Perform the necessary security and cyber compliance validation and testing. This includes External Penetration Testing, Cyber assessments, and other similar security compliance activities.	Week 15
C28	Approve Deployment Plan	Week 6
C29	Approve Go Live Plan	Week 17
C30	Approve the system for go-live	Week 17
C31	Deploy to the Production environment with the supplier providing support. This will facilitate a proper knowledge transfer and ensure supportability after the end of the project.	Week 18
C32	Prepare hyper care plan	Week 19
C33	Assign or establish the BAU team that will manage the solution following go-live.	Week 19
C34	Execute go-live communications	Week 19

Attachment F - Appendix 15 (Deliverables) to Module Order Form 4 – Link

Appendix 15 – Deliverables

Contents

Deliverables 2

Deliverables

ID	Deliverable name	Deliverable description	Delivery Date (weeks after Link Variation Date)	Acceptance Criteria	Reviewer/Approver
LDA-001	Detailed Project Plan	Plan outlining the project timeline, including tasks, CFIs, resources, milestones and deliverables.	Week 1	• Critical path is agreed to by the Customer and Supplier • Any divergences from the high-level plan entitled *'Project Link – Implementation Services'* provided by the Supplier to the Customer prior to the Link Variation Date (**High-level Plan**) and this Module Order Form (including Appendix 13 (Business, Functional, Non-Functional And Technical Requirements) are explained and are acceptable to the Customer • Is in accordance with the stated Deliverable description • Is otherwise in accordance with the Customer's Requirements	• Program governance stakeholders
LDA-002	Configuration, Release & Environment Strategy	Plan outlining the release process for Power Apps, Power Automate flows and other component.	Week 4	• Clearly articulates the purpose of each environment and the release strategy including approach to solution packaging and version control. • Is in accordance with the stated Deliverable description • Is otherwise in accordance with the Customer's Requirements	• Customer Architecture Team • Customer Infrastructure Team • Program governance stakeholders
LDA-003	Requirements Backlog	Outlines the list of features and functionalities planned for the Crime Reporting solution	Week 2	• Clearly articulates the requirement and corresponding acceptance criteria	• Program governance stakeholders

ID	Deliverable name	Deliverable description	Delivery Date (weeks after Link Variation Date)	Acceptance Criteria	Reviewer/Approver
				• Is in accordance with the stated Deliverable description • Is otherwise in accordance with the Customer's Requirements	
LDA-004	Functional Solution Design Specification	Blueprint outlining how the system will work to meet the identified requirements.	Week 4	• Includes the following detail: - ERD diagram - System architecture – a high-level overview of the system's components and how they interact - Business rules - User interface considerations • Is in accordance with the stated Deliverable description • Is otherwise in accordance with the Customer's Requirements	• Program governance stakeholders and architecture team members
LDA-005	Integration Solution Design Specification	Blueprint for connecting Dataverse and ORS2 to achieve the project objectives. It translates the need to exchange data and functionalities between various software components into a technical roadmap, inc. Axon.	Week 4	• Includes the following detail: - Integration technical architecture diagram - High-level data flow - Data mapping - Data transformations • Is in accordance with the stated Deliverable description • Is otherwise in accordance with the Customer's Requirements	• Program governance stakeholders, architecture and infrastructure team members

ID	Deliverable name	Deliverable description	Delivery Date (weeks after Link Variation Date)	Acceptance Criteria	Reviewer/Approver
LDA-006	Test strategy	Outlines the overall testing approach and risk criteria that will be applied in the program regarding all planned testing activities. Includes timelines and resource estimates for completion of the agreed testing activities	Week 4	• Provides a clear and succinct description of the overall approach to ensuring thorough and appropriate levels of testing • Entry criteria are defined • Exit criteria are defined • Contains description of Supplier and Customer responsibilities • Is in accordance with the stated Deliverable description • Is otherwise in accordance with the Customer's Requirements	• Program governance stakeholders
LDA-007	Draft crime reporting online form solution	Draft Crime Reporting Online Form solution built leveraging Power Pages, subject to SIT and UAT	Week 10	• Is per the design specification • Is in accordance with the stated Deliverable description • Is otherwise in accordance with the Customer's Requirements	• Program governance stakeholders
LDA-008	Draft crime reporting triage solution	Draft Crime Reporting Triage solution built leveraging Power Pages, subject to SIT and UAT	Week 10	• Is per the design specification • Is in accordance with the stated Deliverable description • Is otherwise in accordance with the Customer's Requirements	• Program governance stakeholders
LDA-009	Draft integration between Dataverse and ORS2	Draft integration between Dataverse and ORS2 leveraging the Load Balancer Server	Week 14	• Is per the design specification • Is in accordance with the stated Deliverable description • Is otherwise in accordance with the Customer's Requirements	• Customer Integration Team • Program governance stakeholders

ID	Deliverable name	Deliverable description	Delivery Date (weeks after Link Variation Date)	Acceptance Criteria	Reviewer/Approver
LDA-010a	SIT Test Closure Report	A test closure report will be created, including the following information: - Executed test cases - Explanation for test cases that were not executed (if any) - Actual results (Passed/failed/No Result, as applicable) Defect report and status, including a plan for the resolution of outstanding Defects	Week 17	• Summarises test execution outcomes • Demonstrates the exit criteria for the relevant test phase have been achieved • Is in accordance with the stated Deliverable description • Is otherwise in accordance with the Customer's Requirements	• Program governance stakeholders
LDA-010b	NFT Test Closure Report	A test closure report will be created, including the following information: - Executed test cases - Explanation for test cases that were not executed (if any) - Actual results (Passed/failed/No Result, as applicable) Defect report and status, including a plan for the resolution of outstanding Defects	Week 19	• Summarises test execution outcomes • Demonstrates the exit criteria for the relevant test phase have been achieved • Is in accordance with the stated Deliverable description • Is otherwise in accordance with the Customer's Requirements	• Program governance stakeholders
LDA-010c	UAT Test Closure Report	A test closure report will be created, including the following information: - Executed test cases - Explanation for test cases that were not executed (if any)	Week 19	• Summarises test execution outcomes • Demonstrates the exit criteria for the relevant test phase have been achieved • Is in accordance with the stated Deliverable description	• Program governance stakeholders

ID	Deliverable name	Deliverable description	Delivery Date (weeks after Link Variation Date)	Acceptance Criteria	Reviewer/Approver
		- Actual results (Passed/failed/No Result, as applicable) Defect report and status, including a plan for the resolution of outstanding Defects		• Is otherwise in accordance with the Customer's Requirements	
LDA-010d	BVT Test Closure Report	A test closure report will be created, including the following information: - Executed test cases - Explanation for test cases that were not executed (if any) - Actual results (Passed/failed/No Result, as applicable) Defect report and status, including a plan for the resolution of outstanding Defects	Week 20	• Summarises test execution outcomes • Demonstrates the exit criteria for the relevant test phase have been achieved • Is in accordance with the stated Deliverable description • Is otherwise in accordance with the Customer's Requirements	• Program governance stakeholders
LDA-011	UAT Acceptance Certificate	Customer acceptance of the end-to-end Crime reporting solution	Week 19	• The solution meets the agreed requirements, within the agreed UAT exit criteria. • Is in accordance with the stated Deliverable description • Is otherwise in accordance with the Customer's Requirements	• Program governance stakeholders
LDA-012	Training Guide	The supplier will deliver materials to support face-to-face or virtual in instructor-led training to support the train-trainer and administrator training sessions. Any multimedia training materials required are out of scope.	Week 14	• Is in accordance with the stated Deliverable description • Is otherwise in accordance with the Customer's Requirements	• Program governance stakeholders • Training Lead/Change management team

ID	Deliverable name	Deliverable description	Delivery Date (weeks after Link Variation Date)	Acceptance Criteria	Reviewer/Approver
LDA-013	Deployment Plan	A plan that contains the step-by-step activities for the business, the Project team and the Supplier to deploy the solution.	Week 6	• Is in accordance with the stated Deliverable description • Is otherwise in accordance with the Customer's Requirements • Includes the following: - Deployment scope definition - Resource allocation (personnel tools, and infrastructure required for the deployment process) -Deployment approach -Task schedule (timeline for each deployment activity)	• Customer Architecture Team • Customer Infrastructure Team • Program governance stakeholders
LDA-014	Go Live Plan	Outlines Go Live Plan for all components of the solution	Week 19	• Clearly articulates each step for Go-Live, including timeframe, pre-requisites and roles • Checklists articulate tasks, requisite resources and TACI for each workstream (business, technical, Project team, change management/training) pre/during/post Go Live to confirm its success • Is in accordance with the stated Deliverable description • Is otherwise in accordance with the Customer's Requirements	• Customer Architecture Team • Customer Security Team • Customer Executive Stakeholders • Program governance stakeholders
LDA-015	Project Closure Report	Outlines the official completion of the project	Week 23	• Includes lessons learned and handover of ongoing maintenance responsibilities to the designated team. • Is in accordance with the stated Deliverable description	• Customer Executive Stakeholders • Program governance stakeholders

ID	Deliverable name	Deliverable description	Delivery Date (weeks after Link Variation Date)	Acceptance Criteria	Reviewer/Approver
				• Is otherwise in accordance with the Customer's Requirements	

Attachment G - Appendix 16 (Key Resource List) to Module Order Form 4 – Link

Appendix 16 – Key Resource List

Key Resource List

The key resource list identifies individuals, their role on the project, their FTE percentage allocation to the project, their home office location, as well as their anticipated onsite attendance. Our expectation is that resources will be predominantly on-site in most instances as required by the Customer in line with Customer preferred ways of working a degree of remote working where appropriate as indicated below.

#	Name	Role	FTE	Home Office	Onsite Attendance %
[redacted]	S36	[redacted]	20%	TAS	100%
			50%	Non-TAS	10%
			20%	Non-TAS	30%
			40%	Non-TAS	20%
			75%	Non-TAS	10%
			80%	Non-TAS	10%
			50%	Non-TAS	50%
			50%	TAS	100%
			25%	Non-TAS	10%
			20%	Non-TAS	15%
			50%	TAS	50%

©2023 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.
Document Classification: KPMG Confidential
Liability limited by a scheme approved under Professional Standards Legislation.

Contact

S36

S36

KPMG.com.au

This proposal is made by KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee, and is in all respects subject to the satisfactory completion of KPMG's internal risk management processes and the negotiation, agreement, and signing of a specific engagement letter or contract. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm.

©2023 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.
The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.

Liability limited by a scheme approved under Professional Standards Legislation.

Document Classification: KPMG Confidential

Attachment H - Module Order Form 4 – Unify

Module Order Form 4 – Systems Integration - Unify

This document is a derivative of Mo dule Order Form 4 – Systems Integration (publications.qld.gov.au) created in 2017 by the Department of Science, Information Technology and Innovation, Queensland Government and is used under Creative Commons licence CC BY 4.0

Module Order Form 4 – Systems Integration

The following Module Order Form to be completed if the Customer is procuring Systems Integration (refer to clause 3 of Module 4).

1. Commencement of Integration Services

Clause 3.1 of Module 4

8 April 2024

2. Integration Services

Clause 3.2 of Module 4

For the purposes of this Module Order Form, Integration Services will be referred to as Implementation Services.

The Supplier will perform the Implementation Services as set out in Item 2, Section 1 of Annexure 1 to this Module Order Form.

In addition, as part of the Implementation Services, the Supplier must comply with any plan agreed for the resolution of outstanding Defects, as set out in Item 4 of Section 2 of Annexure 1 to this Module Order Form.

3. System

As described in the Detailed Specifications (as described in Item 6 below).

4. Requirements

Specifications for Integration Services (or annex specifications to the Module Order Form)

As described in the documents referred to in Item 5(a) to (g) of the Details.

5. Implementation planning

Clause 3.4 of Module 4

For the purposes of this Module Order Form, Implementation planning will be referred to as Design Services.

The Supplier will perform the Design Services as described in Item 1, Section 1 of Annexure 1 to this Module Order Form.

6. Detailed Specifications

Clause 3.5 of Module 4

Documents comprising the Detailed Specifications

All of the Deliverables set out in Appendix 04 to this Module Order Form – KPMG Design Services that include technical documentation, architectural documentation and traceability matrix.

7. Interfaces

Clause 3.6 of Module 4

Supplier Interfaces

Following interfaces will be delivered by the Supplier as part of Project Unify Phase 2.1.

In addition, this Item sets out the scope of the second and third Stages (Stages 2.2 and 2.3) that are to be covered by the Integration Requirements Specification and the Integration Solution Outline that are to be provided as Deliverables under this Module Order Form.

S30

S30

S30

Stage 2.1 – Updates to current integrations / configuration

Original Source System	New Source System	Target	Notes

S30

Stage 2.2 – Integration Catalogue

Source	Target	Entity	Operation(s)	Approach	T-Shirt Size

S30

Source	Target	Entity	Operation(s)	Approach	T-Shirt Size
[redacted]					

S30

Stage 2.2 – Updates to current integrations / configuration

Original Source System	New Source System	Target	Notes

S30

Stage 2.3 – Integration Catalogue

Source	Target	Entity	Operation(s)	Approach	T-Shirt Size

S30

Customer Interfaces

Customer will provide network connectivity between Cloud Hosted ATLAS system and downstream systems for the purpose of system and data integration. This includes ancillary services including but not limited to secure network connectivity, DNS resolution of hostnames, implementation of Firewall rules (Inbound and Outbound), and authentication.

8. Delivery Dates

Clauses 3.4, 3.5, 3.7, 3.8 and 3.9 of Module 4

Implementation planning (Design Services)

As set out in the Detailed Project Plan.

Detailed Specifications

As set out in the Detailed Project Plan.

Data Migration Plan

As set out in the Detailed Project Plan.

Installation and configuration

As set out in the Detailed Project Plan.

Integration

As set out in the Detailed Project Plan.

9. Site

Clause 3.7 of Module 4

The Supplier will perform the Services at the Customer's Site in accordance with Item 2 of Section 1 of Annexure 1 to this Module Order Form, with resources attending on-site in accordance with the Resource Schedule.

The Supplier will otherwise install and configure all components of the System on the Designated Environment, in accordance with its obligations under the Contract, including Module 4.

The capability for secure remote working will also be enabled.

10. Data Migration Services and Data Cleansing Services

Clauses 3.9 - 3.10 of Module 4

Data Migration Services

Are Data Migration Services required?

☒ Yes

☐ No

Extraction of Customer Data

Customer must extract and provide the Customer Data to the Supplier for data migration and conversion into the production environment by the date specified in the applicable Data Migration Plan (each of which plans is a Deliverable under Module 4).

Data Cleansing Services

Customer will be responsible for Data Cleansing. Supplier will provide feedback for Data Cleansing activities where data cannot be successfully migrated. Data Cleansing should be performed in the source system to maximise data quality and reliability.

Data extraction, provision and cleansing responsibilities are detailed in Appendix 06.

Are Data Cleansing Services required?

☒ Yes

☐ No

Date for completion of Data Cleansing Services

N/A

11. Data Tools

Clauses 3.11 of Module 4

Customer to provide Data Tools required for Data Migration activities as outlined in Appendix 09 – KPMG Resource Requirements, Customer Furnished Items and Risks.

12. Ancillary services

Clause 3.13 of Module 4

Not applicable.

13. Warranty Period

Clause 3.14 of Module 4

The Warranty Period for the System is the period of at least 90 days commencing on successful achievement of Go Live, and will run concurrently with the provision of Hypercare Services (as described in Appendix 07 – Hypercare).

Where Defects are identified by the Customer during the Warranty Period (including through the provision of Hypercare Services), other than Defects that the Supplier is not obliged to remedy under clause 3.15(c) of Module 4 (including taking into account Additional Provision A6), the Customer will assign the Defect a Priority Level in accordance with the classification set out in Attachment A to Schedule 9 (Acceptance Testing).

The Supplier must successfully achieve the Exit Criteria for Exit from Hypercare/Warranty (as set out in Item 4, Section 2 of Annexure 1 to this Module Order Form) in order to exit the Warranty Period. If the Exit Criteria are not satisfied at the end of the 90 day period, the Warranty Period (and performance of Hypercare Services) will be extended until those Exit Criteria are achieved. To avoid doubt, any extension of the Warranty Period and the performance of the Hypercare Services does not increase the Price payable to the Supplier.

Annexure 1

1. Scope of Services

Item 1 Design Services

The scope of the Design Services to be performed is as detailed in the following Appendices to this Module Order Form:

- Appendix 03 - Establishment Services
- Appendix 04 – Design Services
- Appendix 11 – Business Design Workshop Examples

In addition, the Supplier must employ the mitigations described in Appendix 09 to this Module Form – Resource Requirements, Customer Furnished Items and Risks as relevant to the performance of the services referred to in this Item 1.

Item 2 Implementation Services

The scope of the Implementation Services to be performed is as detailed in the following Appendices to this Module Order Form:

- Appendix 03 - Establishment Services
- Appendix 05 – Implementation Services
- Appendix 06 – Data Analysis, Migration and Management
- Appendix 07 - Hypercare

In addition, the Supplier must employ the mitigations described in Appendix 09 to this Module Form – Resource Requirements, Customer Furnished Items and Risks as relevant to the performance of the services referred to in this Item 2.

2. Deliverables

Item 1 Deliverables details

The Supplier will deliver the Deliverables as detailed in the following Appendices to this Module Order Form:

- Appendix 03 – Establishment Services
- Appendix 04 – Design Services
- Appendix 05 – Implementation Services
- Appendix 06 – Data Analysis, Migration and Management

Item 2 Acceptance Test Period

The Acceptance Test Period is as specified in the Customer's test strategy.

Item 3 Acceptance Criteria

The Acceptance Criteria for the Deliverables are as set out in Appendices 3 – 6 to this Module Order Form.

Where a Deliverable is a document, the following Acceptance Criteria will apply in addition to the Acceptance Criteria set out in the applicable Appendix to this Module Order Form:

- the document is compliant (that is, it captures the stated objectives and describes how they will be achieved);
- the document is complete (that is, it covers the scope detailed in the description and what would be reasonably expected in a document of stated nature);
- the document is coherent; and
- the document is consistent within itself and with the requirements set out in this Module Order Form.

Item 4 Acceptance Tests

The Acceptance Test for Deliverables that are documents is an assessment of that Deliverable against the applicable Acceptance Criteria, as specified in Item 3 of this Section 2.

The Acceptance Test(s) for all other Deliverables are as set out in the Customer's test strategy.

Exit Criteria

The following Exit Criteria shall apply to the following Milestones for Integration Services (where the Priority Levels are as defined in Attachment A to Schedule 9 (Acceptance Testing):

Milestone	Priority 1	Priority 2	Priority 3	Priority 4
Exit from SIT (per Drop)	0	0	20	40
Exit from UAT (per Drop and final)	0	0	15	30
Go live	0	0	10	20
Exit from Hypercare/Warranty	0	0	0	15

In addition to the above, the parties must have an agreed plan for resolution of any outstanding Defects in order to achieve the relevant Exit Criteria.

Attachment I - Schedule 1 (Price and Payment Terms) to the Contract

Schedule 1 –
Price and Payment Terms

Provision of software development, systems integration, project and professional services to continue the implementation of the Niche Technology Records Management System (NicheRMS) PU-01-23

The Crown in right of Tasmania acting through the Department of Police, Fire and Emergency Management

KPMG Australia Technology Solutions Pty Limited ABN 29 606 612 962

This document is a derivative of Schedule 1 – Price and Payment Terms (included in the Comprehensive Contract Details) (publications.qld.gov.au) created in 2017 by the Department of Science, Information Technology and Innovation, Queensland Government and is used under Creative Commons licence CC BY 4.0

1. Price

The fixed Price for Stage 2.1 is: $13,072,678.00

The fixed Price for the Link Stage is: $895,000

The fixed Price estimate for Stage 2.2 is: $8,536,394.00

The fixed Price estimate for Stage 2.3 is $5,072,410.00

The above fixed Prices and Price estimates are exclusive of all expenses set out in section 1.1 below.

Consistent with Additional Provision A8, the parties will agree the Prices for Stages 2.2 and 2.3 as and when the parties agree to enter into further Module Order Forms for those Stages, and this schedule will be varied in writing to incorporate such agreed details at that time.

1.1 Expenses

The Customer will reimburse the Supplier for travel, accommodation and related expenses incurred by the Supplier where Key Personnel who are specified (in Appendix 08 to Module Order Form 4 - Unify – Key Resource List), and Personnel required as part of the delivery team, being based outside Tasmania, travelling between Hobart and a place outside Tasmania (but within Australia) for the purposes performing the Services pursuant to Module Order Form 4 - Unify and any further Module Order Form 4 for a Unify Stage that is agreed between the parties as contemplated by Additional Provision A8, subject to:

(a) such travel, accommodation and related expenses being incurred:

  (i) for the purposes of Key Personnel who are specified (in Appendix 08 to Module Order Form 4 - Unify – Key Resource List), and Personnel required as part of the delivery team, being based outside Tasmania travelling between Hobart and a place outside Tasmania (but within Australia) for the purposes of performing the Services; and

  (ii) the supplier has estimated 930 nights of accommodation for Personnel being based outside Tasmania travelling between Hobart and a place outside Tasmania (but within Australia) for the purposes of performing the Services.

(b) satisfaction of the requirements in clauses 10.2(b) and 10.2(c)(ii) of the Comprehensive Contract Conditions; and

(c) the prior written approval of the Customer being required in order for the Supplier to be entitled to reimbursement of any expenses in excess of the applicable estimate set out below.

The estimated travel expenses for Stage 2.1 is: $400,000.00

The estimated travel expenses for Stage 2.2 is: $240,000.00

The estimated travel expenses for Stage 2.3 is $160,000.00

1.2 Price reviews (including during any extension period(s))

Not applicable.

1.3 Payment plan/milestones

Stage 2.1:

The Supplier may invoice the Customer after successful achievement of the milestones as follows (that is, when Acceptance and/or Exit Criteria have been achieved as notified by the Customer to the Supplier):

Milestone	% Price	$ Price (excl. GST)	Acceptance Criteria/Exit Criteria
Contract Signing	10	$1,307,267.80	Contract executed
Project mobilized	5	$653,633.90	Sign-off of Project mobilization and delivery of Detailed Project Plan by way of acceptance of all of the following Deliverables: • Risk Register & Decision Log • Project Reporting • Detailed Project Plan • Project Delivery Structure (with Escalations)
Overall design completed	5	$653,633.90	Acceptance of high-level solution design by way of acceptance of all of the following Deliverables: • Program Design Authority Document • End-to-End High Level Solution Architecture document • End-to-End High Level Solution Architecture presentation

Milestone	% Price	$ Price (excl. GST)	Acceptance Criteria/Exit Criteria
Drop 1 business design	10	$1,307,267.80	Acceptance of Drop 1 business design by Customer by way of acceptance of all of the following Deliverables: • Configuration Strategy and Methodology • NicheRMS System Requirements, Drop 1 • Future State Processes Drop 1 (final update) • Future State Business Scenarios Drop 1 (final update) • Business Requirement Specification Drop 1 (final update) • Gap Analysis Drop 1 (final update)
Drop 1 - UAT Complete	5	$653,633.90	Exit Criteria for UAT (as specified in Item 4 of Section 2 of Annexure 1 to Module Order Form 4 - Unify) successfully achieved
Drop 2 business design	10	$1,307,267.80	Acceptance of Drop 2 business design by Customer by way of acceptance of all of the following Deliverables: • NicheRMS System Requirements, Drop 2 • Future State Processes Drop 2 (final update) • Future State Business Scenarios Drop 2 (final update) • Business Requirement Specification Drop 2 (final update) • Gap Analysis Drop 2 (final update)
Drop 2 – UAT Complete	5	$653,633.90	Exit Criteria for UAT (as specified in Item 4 of Section 2 of Annexure 1 to Module Order Form 4 - Unify) successfully achieved

Milestone	% Price	$ Price (excl. GST)	Acceptance Criteria/Exit Criteria
Drop 3 business design	10	$1,307,267.80	Acceptance of Drop 3 business design by Customer by way of acceptance of all of the following Deliverables: • NicheRMS System Requirements, Drop 3 • Future State Processes Drop 3 (final update) • Future State Business Scenarios Drop 3 (final update) • Business Requirement Specification Drop 3 (final update) • Gap Analysis Drop 3 (final update)
Drop 3 - UAT Complete	5	$653,633.90	Exit Criteria for UAT (as specified in Item 4 of Section 2 of Annexure 1 to Module Order Form 4 - Unify) successfully achieved
Testing complete	5	$653,633.90	Exit Criteria for final end-to-end Nonfunctional testing (UAT) (excluding regression testing) (as specified in Item 4 of Section 2 of Annexure 1 to Module Order Form 4 - Unify) successfully achieved
Go Live	15	$1,960,901.70	Stage 2.1 cut over and Go Live completed in accordance with Cutover Strategy and Plan and Go Live Plan
Hand over to BAU	10	$1,307,267.80	Stage 2.1 transition from Go Live to BAU requires the system to be operational in business as usual usage for 5 Business Days from Go Live.
Exit Hypercare/Warranty	5	$653,633.90	Exit Criteria for Exit Hypercare/Warranty Period (as specified in Item 4 of Section 2 of Annexure 1 to Module Order Form 4 - Unify) successfully achieved
TOTAL	100	$13,072,678.00	

Link Stage:

The Supplier may invoice the Customer after successful achievement of the milestones as follows (that is, when Acceptance and/or Exit Criteria have been achieved as notified by the Customer to the Supplier):

Milestone	% Price	$ Price (excl. GST)	Acceptance Criteria/Exit Criteria
Project kick-off	20	$179,000.00	Acceptance of the configuration, release & environment strategy that is a Deliverable under Module Order Form 2
Vision and design completion	10	$89,500.00	Acceptance of all the following Deliverables under Module Order Form 2 and Module Order Form 4 - Link: • Design Specification • Test strategy
Build completion	40	$358,000.00	Completion of all elements of the build described in Module Order Form 2 and Module Order Form 4 - Link in readiness for testing, including completion of Deliverables LDA-007, LDA-008, and LDA-009, and satisfaction of the test entry criteria specified in the testing strategy that is a deliverable under Module Order Form 4 – Link.
UAT completion	20	$179,000.00	Exit criteria for the UAT element of the Acceptance Tests UAT (as specified in the test strategy that is a Deliverable under Module Order Form 2 and Module Order Form 4 - Link) successfully achieved

Milestone	% Price	$ Price (excl. GST)	Acceptance Criteria/Exit Criteria
Go live and warranty completion	10	$89,500.00	• Go live completed in accordance with the go live plan that is a Deliverable under Module Order Form 2 and Module Order Form 4 - Link • Exit criteria for exiting of hypercare/Warranty Period (as specified in the hypercare plan that is a Deliverable under Module Order Form 2 and Module Order Form 4 - Link) successfully achieved
TOTAL	100	$895,000.00	

The timing for payment of invoices is as set out in clause 10 of the Comprehensive Contract Conditions.

The parties will agree the milestones, payment percentages and relevant Acceptance and/or Exit Criteria for Stages 2.2 and 2.3 as and when the parties agree to enter into further Module Order Forms for those Stages, and this schedule will be varied in writing to incorporate such agreed details at that time.

1.4 Retention of money

Not applicable.

1.5 Rates for additional Products and Services (if applicable)

The rates for any additional Products and Services which may be procured by the Customer under the Contract (e.g. additional Products and Services to be provided under a Statement of Work, additional Products and Services to be provided as a result of a Change or additional services under a Module where the Supplier is not otherwise responsible for rectifying a Defect) are as follows:

Rate Card for Services for Stage 1		
Role	**Unit Price (AUD ex GST)**	**Unit Type** (Per Day - 7.5 Hours)
Partner Leadership	S37	
Project Manager		
Project Coordinator		

Rate Card for Services for Stage 1	
Senior Business Analyst / Design Lead	S37
Senior Business Analyst	
Business Analyst	
Lead Solution Architect	
Configuration Lead	
Niche Report Developer	
System Integration and Platform Lead	
Senior Integration Developer	
Integration Developer	
Azure Platform Specialist	
Test, Release and Deployment Lead	
Test Analyst	
Information Security Specialist	
Data Migration Lead	
Senior Data Analyst	
Data Analyst	
Business Transformation Lead	
Organisational Change and Training Design and Delivery	

1.6 Payment methods

Customer can make payment through EFT to the Supplier's bank account details as outlined on the rendered tax invoice.

1.7 Discounts or rebates

Not applicable.

1.8 Address details for invoice

Invoices are to be emailed to: Unify@police.tas.gov.au

Referencing: Level 6, 70 Collins Street, Hobart 7000

1.9 Other pricing information

Pricing variation will be governed by the terms of the Contract covering scope variation, and delivery delays caused by the Customer.

Attachment J - Schedule 9 (Acceptance Testing) to the Contract

Schedule 9 – Acceptance Testing

Provision of software development, systems integration, project and professional services to continue the implementation of the Niche Technology Records Management System (NicheRMS) PU-01-23

The Crown in right of Tasmania acting through the Department of Police, Fire and Emergency Management

KPMG Australia Technology Solutions Pty Limited ABN 29 606 612 962

This document is a derivative of Schedule 9 – Acceptance Testing (publications.qld.gov.au) created in 2017 by the Department of Science, Information Technology and Innovation, Queensland Government and is used under Creative Commons licence CC BY 4.0

Acceptance Testing

1. Specify the Deliverables that are to undergo Acceptance Testing.

Acceptance Testing applies to:

- ☐ Hardware supplied under Module 1
- ☐ Licensed Software supplied under Module 2
- ☒ Developed Software supplied under Module 2
- ☐ As a Service supplied under Module 3
- ☒ Systems Integration supplied under Module 4
- ☐ Telecommunications Services supplied under Module 5
- ☐ Managed Services supplied under Module 6
- ☐ ICT Professional Services supplied under Module 7
- ☒ Documents which are Deliverables
- ☐ Other Deliverables:

2. Specify the allocation of each party's responsibilities in relation to testing (including the party responsible for conducting the Acceptance Tests)

Party responsible for conducting Acceptance Tests

- ☒ Customer
- ☐ Supplier

Customer responsibilities

The Customer will perform Acceptance Testing in accordance with:

(a) in respect of testing conducted as part of the activities undertaken pursuant to Module Order Form 4 - Unify, the Customer's testing strategy; or

(b) in respect of testing conducted as part of the activities undertaken pursuant to Module Order Form 2 or Module Order Form 4 - Link, the testing strategy that is a Deliverable under Module Order Form 2 or Module Order Form 4 - Link.

Supplier responsibilities

The Supplier will support the Customer's Acceptance Testing in accordance with the Test Strategy and Test Phase Plans which are Deliverables under Module Order Form 4 - Unify, Module Order Form 2 - Link or Module Order Form 4 - Link, as applicable.

3. Specify which party is to provide the test environment, including hardware, software, power, consumables and other resources and when the environment and resources must be ready for use

Party responsible for providing test environment

Customer

Requirements for test environment

As outlined in Appendix 09 to Module Order Form 4 – Unify – KPMG Resource Requirements, Customer Furnished Items and Risks, or Appendix 14 to Module Order Form 4 – Link – Customer Furnished Items and Dependencies (as applicable).

When environment should be ready for use

In respect of the environment for the purposes of the testing pursuant to Module Order Form 4 - Unify – as outlined in the Detailed Project Plan or (to the extent that dates are not outlined in the Detailed Project Plan) in line with dates as outlined in Appendix 09 to Module Order Form 4 – Unify – KPMG Resource Requirements, Customer Furnished Items and Risks.

In respect of the environment for the purposes of the testing of Deliverables pursuant to Module Order Form 2 or Module Order Form 4 - Link – as outlined in Appendix 14 to Module Order Form 4 – Link – Customer Furnished Items and Dependencies.

4. Specify the methodology and process for conducting Acceptance Tests

The Acceptance Test for Deliverables that are documents is an assessment of that Deliverable against the applicable Acceptance Criteria, as set out in Appendices 3-6 to Module Order Form 4 - Unify, or Appendix 15 to Module Order Form 4 – Link – Deliverables (as applicable).

The Acceptance Test(s) for all other Deliverables are as set out in:

(a) in respect of testing conducted as part of the activities undertaken pursuant to Module Order Form 4 - Unify – the Customer's test strategy; or

(b) in respect of testing conducted as part of the activities undertaken pursuant to Module Order Form 2 or Module Order Form 4 - Link – the testing strategy that is a Deliverable under Module Order Form 2 or Module Order Form 4 - Link.

Where Defects are identified by the Customer during Acceptance Testing Period (other than Defects that the Supplier is not obliged to remedy under clause 3.15(c) of Module 4, including taking into account Additional Provision A6), the Customer will assign the Defect a Priority Level in accordance with the classifications set out in Attachment A to this Schedule 9, and the Supplier will promptly rectify such Defect to ensure Acceptance Testing can be successfully completed by the end of the Acceptance Test Period.

Subject to the Supplier's obligations regarding the rectification of Defects in the Niche software, where Defects are identified by the Customer during the Warranty Period (including through the provision of Hypercare Services), the Customer will assign the Defect a Priority Level in accordance with the classification set out in Attachment A to this Schedule 9, and the Supplier will promptly rectify such Defect to ensure the Supplier achieves the Exit Criteria for Exit from Hypercare/Warranty.

5. Specify the scheduling of Acceptance Tests including the Acceptance Test Period and the Acceptance Test Notification Period

As set out in the Customer's test strategy (where applicable) and/or the Test Strategy and Test Phase Plans which are Deliverables under Module Order Form 4 – Unify, Module Order Form 2 or Module Order Form 4 – Link, as applicable.

Acceptance Test Period

As set out in:

(a) in respect of testing conducted as part of the activities undertaken pursuant to Module Order Form 4 - Unify – the Customer's test strategy; or

(b) in respect of testing conducted as part of the activities undertaken pursuant to Module Order Form 2 or Module Order Form 4 - Link – the testing strategy that is a Deliverable under Module Order Form 2 or Module Order Form 4 - Link.

Acceptance Test Notification Period

The Customer will use reasonable endeavours to notify the Supplier of the results of the Acceptance Tests within 5 Business Days after the end of the Acceptance Test Period.

6. Specify the Acceptance Criteria used to test whether the Deliverable meets the Requirements

As set out in the Customer's test strategy or the testing strategy that is a Deliverable under Module Order Form 2 or Module Order Form 4 - Link, as applicable, and Module Order Form 4 - Unify, Module Order Form 2 or Module Order Form 4 - Link, as applicable.

7. Specify the Acceptance Test Data required and when it is required.

Acceptance Test Data

As outlined in Appendix 09 to Module Order Form 4 – Unify – KPMG Resource Requirements, Customer Furnished Items and Risks, or Appendix 14 to Module Order Form 4 – Link – Customer Furnished Items and Dependencies, as applicable.

Date Acceptance Test Data required

As outlined in:

(a) in respect of testing conducted as part of the activities undertaken pursuant to Module Order Form 4 - Unify – the respective Detailed Project Plan or in line with dates provided in Appendix 09 to Module Order Form 4 – Unify – KPMG Resource Requirements, Customer Furnished Items and Risks; or

(b) in respect of testing conducted as part of the activities undertaken pursuant to Module Order Form 2 or Module Order Form 4 - Link – Appendix 14 to Module Order Form 4 – Link – Customer Furnished Items and Dependencies.

Attachment A – Testing and Defect Priority Levels

Where a Defect meets the description of a Priority Level below but an acceptable Workaround is available such that it would allow such Defect to be reclassified by the Customer as a lower Priority Level, then that lower Priority Level will apply.

Description
Priority 1 - Critical
This may include a Defect that: • prevents the Customer from performing a critical core function which impacts Acceptance Testing, service delivery or business operations requirements; or • renders the System or Developed Software completely unavailable or substantially inoperable; or • prevents or substantially delays multiple users from performing time critical tasks.
Priority 2 - Major
A Defect that • severely diminishes, delays or disrupts the Customer's ability to use the System or Developed Software for its intended purpose or to continue testing of the System or a substantial part of it; or • causes a failure of a System or Developed Software function or group of functions; or • causes performance degradation to the point of significant user experience impact.
Priority 3 - Moderate
A Defect that: • diminishes, delays or disrupts the Customer's ability to use the System or Developed Software for its intended purpose or to continue testing of the System or Developed Software in a manner that is not severe in its impact and can be overcome albeit with greater effort or a non-business impacting delay; or • causes a failure of a System or Developed Software function or group of functions without impacting time critical tasks; or • allows all core areas of functionality to operate without material impact to business operations and processes but the System or Developed Software is not operating in accordance with the Detailed Specifications and/or there is performance degradation that materially impacts the user experience.
Priority 4 - Residual
Business/operational inconvenience not of a material nature such that the System and Developed Software continues to be fully usable and data integrity is unaffected directly