Document 3

RISK ASSESSMENT

Item	Risk/s	Likelihood	Consequence/s	Risk Rating	Mitigation/s	Residual Risk Rating
1	ACIC loses access to Palantir maintenance due to the procurement not being finalised before the current contract expiry.				s 47(1)(b), s 47E(d) [redacted] Unlikely + Minor impact.	Low
2	Unplanned or extended Palantir outages (>3 days) due to technical or other issues beyond ACIC control	Unlikely	Major	Medium	s 37(2)(b), s 47E(d) [redacted] The RFQ contains the requirement for bi-annual Contract Management meetings. Rare + Moderate impact. A risk reduction strategy has been implemented by inclusion of Service Levels proposed in the ACIC RFQ, as well as an issue escalation process and quarterly review process. A shift to quarterly payments in arrears (in lieu of the previous annual payments) will also mitigate this risk.	Low
3	Quality of support services decline under the new contrac s 37(2)(b), s 47E(d) [redacted]	Possible	Moderate	Moderate	Risk reduction strategy implemented by: • required six monthly contract management meetings to address issues/concerns • adoption of "Service Levels proposed by ACIC" • quarterly payments in arrears. The evaluation took particular account of recent performance in the supply of maintenance, support services and the stability of the existing installation of Palantir in the ACIC. The majority of BAU incidents and problems have been successfully managed by the ACIC Intelligence and Corproate Technical Support team with .	
4	Palantir does not remain fit for purpose for ACIC requirements during life of the new contract	Rare	Major	Low	The Evaluation Committee will conduct an assessment of the Palantir services offered against ACIC business and techcnal requirements. Regular upgrades of the Palantir capability means it is likely to remain fit for purpose.	
5	Cost of Palantir maintenance and support significantly increases	Rare	Moderate	Low	Cost has been fixed for the 3-year life of the contract (1 year and options to extend for further 2 additional years at fixed cost). Prices quoted address the key ACIC RFQ requirements below and support is unlikely to require significant additional resourcing: • "Support Services (error correction and technical support) for the term, and • An Update Service that will bring the software up to current version 3.16.X (latest patch at the time)"	
6	Current services lapse before a new process/arrangement is able to be finalised.	Unlikely	Minor	Low	Risk avoidance strategy includes seeking periods of grace allowing time for evaluation and review, s 47(1)(b) [redacted] Committee has also agreed to commence an early tender review process (prior to expiry of the first year) to review the market and ensure finalisation within required timeframes.	
7	Maintenance costs will increase significantly, causing a material impact on the ICT budget.				s 47(1)(b), s 47E(d) [redacted]	Low
8						
9						
10						
11						
12						
13						
14						
15						

Released under the Freedom of Information Act 1982 (Cth)

EXAMPLES OF POTENTIAL RISKS

Identifying the need
Inappropriate method of procurement
Over or understating the requirement
Insufficient funding
Impractical target dates
Insufficient time provided to complete the procurement process
Probity failure
Misinterpretation of user needs
Political environment
Likely media interest

Developing the specification
Narrow definition or commercial specification (e.g. brand name)
Definition of inappropriate product or service
Biased specification
Inadequate specification or statement of requirement (for services)
Software or Intellectual Property licensing not adequately addressed

Selecting the procurement method
Commonwealth Procurement Rules not followed/applied correctly
Failure to identify potential sources
Selecting inappropriate method
Supplier collusion
Strength of domestic and international market

Contract documents
Terms and conditions unacceptable to service providers
Providing inadequate information

Clarification
Failure to address enquiries adequately
Actual or perceived favouritism in providing information
Actual or perceived breach of confidentiality

Evaluating offers
Failure to follow effective evaluation procedures
Breaches of security
Offers fail to meet needs
Failure to identify a clear winner. Decision made on subjective grounds
Selecting a preferred supplier before all issues (technical, business, financial) are resolve and competitive tension reduced
Insufficient number of responses
No response from known quality service providers
Market unresponsive

Selecting the preferred service provider
Selecting an inappropriate service provider
Selecting inappropriate goods/services
Potential, perceived, actual conflict of interest

Closing offers
Not matching the expectations of buyer and service provider
Deadlock on details of agreement
Failure to secure mandatory conditions
Unfair or onerous requirements on the service provider in the contract conditions
Failure to reflect the terms offered and agreed in the actual contract
Inadvertently creating a contract without the delegate's prior approval
Negotiations commence too late in the process after competitive tension removed

Financial
Liability Cap
Indemnity

Contract management
Project commencement is delayed after selection
Variations in price and foreign exchange
Unwillingness of the service provider to accept the contract
Failure of either party to fulfil the conditions of the contract
Inadequately administering the contract
Commencement of work by the service provider before contract is exchanged or letter of acceptance issued
Unauthorised increase in scope of work
Loss of intellectual property
Failure to meet liabilities of third parties (e.g. royalties or third party property insurance)
Supplier delivers but goods/services provided do not meet the requirement
Supplier completes, but not on time
Supplier claims the Commonwealth is in breach of contract
Loss of or damage to goods in transit
Key personnel not available
Supplier goes out of business
No Insurance
Fraud

WHS/Environmental
Inappropriate training provided
Environment unsafe to install and operate goods
Malfunction of goods resulting in injury or harm to people or damage to property
Exposure to hazardous substances that could cause injury or harm to people
Supplier injures or kills people in the course of performing the contract
Detrimental environmental impacts

Released under the Freedom of Information Act 1982 (Cth)

Document 4

Category	Sub-category	Key	Health check question	Things to think about when answering	Health assessment	Health rating	EA Assessment
Sustainable		Yes	[redacted]	s 47(1)(b), s 47E(d)	[redacted]	[redacted]	[redacted]
Sustainable		Yes	s 47(1)(b), s 47E(d)	[redacted]	[redacted]	[redacted]	[redacted]
Sustainable		Yes	s 47(1)(b), s 47E(d)	[redacted]	[redacted]	[redacted]	[redacted]
Sustainable		Yes	Do you maintain the knowledge and capability to decommission the system?	Do you understand all the interactions between the system and other systems?	Limited.	2: Limited decommission capability, interaction knowledge gap of integrations.	Decommissioning requires further understanding
Sustainable		Yes	s 47(1)(b) [redacted]	[redacted]	s 47(1)(b) [redacted]	2: Outdated version, blocks other upgrades	Getting to a supported version will be difficult.
Sustainable		Yes	[redacted]	s 47E(d) [redacted]	s 47(1)(b) [redacted]	s 47E(d) [redacted]	Getting to a supported version will be difficult.
Sustainable		Yes	Is there a commitment by vendor/support team that the solution will not be subject to unsolicited change that adversely affects suitability of the product (e.g., licensing changes, platforms no longer supported)?	Consider the impact that change of ownership may have.	No!	1: No commitment, high risk of impact	Vendor roadmap requires unplanned change.
Sustainable		Yes	What is the commitment to long term solution support and enhancement (e.g., existence of product roadmaps and a workforce dedicated to implementing these)?	Is there a feature request backlog that has no staff dedicated to implementing? Is the solution only receiving security updates and not functional upd tes?	s 47(1)(b) [redacted]	1: No commitment, no enhancements	Vendor roadmap requires unplanned change.
Sustainable		Yes	Is the solution compatible with preferred ACIC technologies?	Is the use of the solution blocking changes to other systems? Is th sol tion blocking the adoption of modern application architectures?	Yes, at the moment.	[redacted]	
Sustainable		Yes	Does the solution have support resources that are cleared, available, have access, and are trained?	Do you have vacant positions that you are struggling to fill?	Two people can backfill. Dependent on Palantir for some support	4: Mostly available, minor training gaps	
Sustainable		Yes	s 47(1)(b), s 47E(d) [redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Sustainable			Are a maintenance plan and operating procedures in place?	If a new person was given responsibility for mainten nce and support, how would they know what to do?	Support contract.	5: Comprehensive plan, clear procedures	
Sustainable		Yes	Are there components of the solution that have a limited life?	Consider deprecation of features, end of ife announcements, useful lifetime of hardware, end of contract, Machine y of Government changes, impact of disruptive technology. Was the solution inten ed to have a limited lifespan when it was implemented?	s 47(1)(b) [redacted]	1: Most components have limited lifespan	Vendor roadmap requires unplanned change.
Sustainable			Does the solution have a documented governance model? Does the model include data governance?		No.	1: No governance model, no data governance	Documentation and data governance is limited.
Sustainable			Is there a simple mechanism through which the solution receives vendor upgrades?	How difficult is it to stay up-to-date? Does the ACIC have limitations that make upgrading mo e difficult, such as not being able to use a vendor-managed upgrade service? Are updates able to be done using a standard tooling?	Not the current required upgrade.	2: Difficult upgrades, tooling issues	Getting to a supported version will be difficult.
Sustainable			s 47(1)(b), s 47E(d) [redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Sustainable			Does the system provide real-time logs, metrics, and traces for comprehensive state observability?	Evaluate the system's ability to provide a complete and accurate picture of its current state through these observability tools. Does the solution provide actionable alerts, and not ones that can be ignored?	s 47E(d) [redacted]	4: Mostly real-time, minor gaps	
Sustainable			Are you able to query the system, component and interface versions, as well as the upgrade history, pa ticularly for APIs?	How are APIs/interfaces versioned? Does the application support multiple versions of an API to allow graceful migration of clients? What is the deprecation lifetime for these?	Unknown APIs. Workspace client provide Java version and Palantir version. Every plugin named and versioned.	3: Basic query ability, standard versioning	
Data Mature		Yes	Is data stored and accessed using standard, non-proprietary formats?	Is there vendor lock-in?	No	2: Many non-standard formats, notable lock-in	There is significant vendor lock-in.
Data Mature		Yes	Can data be accessed in bulk for analytical and reporting purposes?	Does it have APIs, built-in reporting, or a known database structure?	Not sure at this stage	0: Unknown data access capability	
Data Mature		Yes	Is there regular monitoring and reporting of data quality?	What measures do you have to indicate the quality of the data?	No	2: Infrequent reporting, some quality issues	Documentation and data governance is limited.
Data Mature		Yes	Can data can be a cessed directly through standard APIs?	If not, could APIs be added?	No. No.	1: No direct access, APIs not feasible	Documentation and data governance is limited.
Data Mature		Yes	Are we optimising data eferencing by using in-situ methods where poss ble to minimise unnecessary duplication with multiple copies?	Are copies of the whole database or a significant portion used for production purposes?	e.g. person entity created, turned out to be a duplicate person entity.	3: Some in-situ methods, occasional copies	
Data Mature		Yes	f co ies of data are being created, are they maintained for ac uracy, completeness, and timeliness.	Is there a process to automatically refresh?	needs to be addressed	2: Limited maintenance, infrequent refresh	Documentation and data governance is limited.

Released under the Freedom of Information Act 1982 (Cth)

Data Mature		Is data treated as an asset? Is it considered separately from the solution itself? It may have a different classification and generally a different governance model.	Are you able to describe the ownership and responsibility for the data, its classification and access controls, the governance policies guiding its use, and the security measures in place to protect it?	Yes	4: Data mostly treated as asset, good controls	
Data Mature		Is there consistent naming and semantics across all data, including adoption of common standards?	If I looked at another system that also uses the same element, would it have the same name, quality, and attributes?	No	2: Inconsistent naming, few standards	Documentation and data governance is limited.
Data Mature		Does the business metadata help humans understand the data? Does the technical metadata support automated management? Does the operational metadata support lifecycle management?		Yes	5: Accurate, easily consumed metadata	
Data Mature		Does the solution attach generalised metadata, such as source information and conditions of use, to ensure data can be utilised in other systems with minimal risk?	Would I be able to look at the metadata and understand the restrictions in use and who controls those restrictions?	Yes	5: Comprehensive metadata attached	
Data Mature		Does the solution implement the appropriate data standards, such as universal time versus local time?	Are there any issues caused by inconsistent data standards?	Yes	5: Adheres to all standards	
Efficient	Yes	Is the solution cost-effective in terms of both delivery and sustainment, and does it align with the agency's cost appetite?	Consider vendor costs such as support and licensing. What is the cost of adding features? How many staff are required to support the system?	Being questioned.	2: Somewhat cost-ineffective	Additional budget may be required.
Efficient	Yes	Is the system sensibly decomposed to maximise internal reuse and maintainability?	Does the system's architecture promote modularity and reuse of components? Consider the ease of maintaining the system and whether its design allows for efficient updates and scalability.	Only modules we see are plugins	1: Poor decomposition, not reusable	tolerate
Efficient	Yes	Is the system designed to be simple, avoiding unnecessary complexity?	Does complexity get in the way of doing changes?	Backend is pretty complex	3: Moderate complexity	
Efficient	Yes	Does the system adhere to established software patterns, such as the façade pattern and reusable interfaces, to ensure standardisation and quality?	Are you able to describe what patterns the system aligns with, or is it unique?		0: Adherence to patterns unknown	
Efficient	Yes	s 47E(d), s 47(1)(b) [redacted]	[redacted]	[redacted]	3: Moderate reuse of existing tech	
Performant	Yes	Does the system have acceptable performance from the perspective of non-functional aspects?	Do the times make it difficult to resolve incidents within target times? Does the system cause excessive resource utilisation? Is replication able to occur in a timely manner? Are backups able to fit within the backup window?	OK	4: Meets most performance targets	
Performant		Can the computation intensity be justified for what needs to be done?	Is the most efficient method being used? E.g., if a rules-based approach provides the correct result, then the use of AI would not be justified.	Yes.	5: Computation fully justified	
Performant		Is performance across all layers in the tech stack acceptable (compute, storage, database, network)?	Consider bottlenecking, which may not be visible to the user.	s 47(1)(b), s 47E(d) [redacted]	3: Adequate performance, some issues	
Scalable	Yes	Is the system able to scale to meet predicted growth?	Consider the projected increase in users or system integrations and whether the system's design and infrastructure can accommodate this growth without performance issues.	With licensing.	5: Scales well, meets growth needs	
Scalable		Is the cost of scaling understood and budgeted for?	Capacity often doesn't grow linearly as a purchase often has a minimum increment size.	Understood, not budgeted.	3: Adequately understood, some budgeting	
Available	Yes	[redacted]	s 47E(d) [redacted]	OK	4: Mostly met, minor adjustments needed	
Available	Yes	s 47E(d) [redacted]	[redacted]	[redacted]	[redacted]	
Available	Yes	[redacted]	s 47E(d) [redacted]	[redacted]	[redacted]	
Available	Yes	Is the system allocated the correct System Class, and does the solution meet the architecture and service levels associated with the System Class?	Consider the impact of the whole technical stack. Is the answer the same for every user in every location?	Yes	5: Correct class, meets all levels	
Available	Yes	Is the system capable of handling invalid inputs without causing unnecessary loss of function?	Consider whether the system has adequate validation checks and failsafes.	Yes	5: Handles all invalid inputs well	
Available	Yes	s 47E(d) [redacted]	[redacted]	[redacted]	[redacted]	
Available	Yes	[redacted]	s 47E(d) [redacted]	[redacted]	3: Adequate resilience, some delays	
Available	Yes	Do the configured backups align with the backup requirements?	Do you need backups that are aware of the application state? Are there things that should be run before a backup? Is the frequency and retention of the backups right?	Yes	5: Backups fully align with requirements	
Available	Yes	s 47E(d) [redacted]	[redacted]	[redacted]	[redacted]	
Available	Yes	s 47E(d) [redacted]	[redacted]	[redacted]	[redacted]	
Available	Yes	s 47(1)(b), s 47E(d) [redacted]	[redacted]	[redacted]	[redacted]	[redacted] data requires vendor engagement.

Released under the Freedom of Information Act 1982 (Cth)

Available			Does the system maintain the integrity of its state throughout the recovery process?	Evaluate the mechanisms in place to ensure data consistency and system state accuracy during and after recovery.	Yes	5: Full data integrity ensured	
Available			Does your system effectively manage the accumulation of information to maintain optimal performance?	Consider the efficiency of data archiving and purging processes.	Logs are good. Unused investigations are retained.	3: Average data handling	
Available			[redacted]	s 47E(d) [redacted]		0: Security status unknown	
Secure		Yes	Is the solution capable of receiving an Approval to Operate (ATO) and can it maintain ongoing operation in compliance with the Protective Security Policy Framework (PSPF) and the Information Security Manual (ISM)?		Probably.	4: Mostly c mpliant with standards	
Secure		Yes	Is the solution appropriately classifying data and handling sensitivities in accordance with organisational and regulatory standards?	Are there adequate protections for sensitive information? What would happen if the data is leaked outside the organisation? Over-classification is common, so confirm the maximum level.	Access control is tight.	5: Fully compliant, secure handling	
Secure		Yes	Does the solution integrate and comply with the agency's authentication and access control solutions?	Is the solution using an appropriate identity management authority?	s 47E(d) [redacted]	5: Fully integrated authentication, authorisation and accounting (AAA)	
Secure		Yes	Does the solution log query requests and responses, and are these logs analysed and managed in accordance with compliance requirements?	Don't just assume backups will look after it.	Probably retained within the system for a month	3: Adequate log management	
Secure		Yes	s 47(1)(b), s 47E(d) [redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Secure		Yes	s 47E(d) [redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Secure		Yes	s 47E(d), s 47(1)(b) [redacted]	[redacted]	[redacted]	[redacted]	
Secure		Yes	s 47(1)(b) [redacted]		Probably not	0: Integration status unknown	
Secure		Yes	s 47(1)(b), s 47E(d) [redacted]	Privileged access should not occur from an operating system that has web or email access.	Yes	s 47(1)(b), s 47E(d)	
Secure			Is the solution meeting auditor requirements, and are the frequency and subjects of audits in line with organisational and regulatory expectations?	Are there any auditor items in a backlog?	No issues	5: Fully meets audit requirements	
Secure			Is any external access secure?	Is the solution restricted in where it may be accessed from? Is a thorisation, authentication, and access control adequate?	s 47E(d) [redacted]	3: Adequate access control	
Secure			Does the solution use standard access control mechanisms, such as Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC)?	Are the access control mechanisms robust, flexib , and calable enough to manage user permissions effectively?	Yes	5: Robust, scalable RBAC/ABAC	
~~Secure~~			~~Is it possible to recreate a historical system state?~~	~~Backups can have dependencies for a sys em to be able to be recovered to a particular point in time. Applications tend t be better at being able to manage state.~~	~~Not sure~~	~~0: State recreation unknown~~	
Useable			Is the solution's interface intuitive and easy to learn or remember for all users?	How much time is spent providing individual guidance on use of the system?	Requires training	3: Moderate guidance needed	
Useable			Is the system efficient and effective to use, with low error rates and minimal repetition?	Are there validation hecks to prevent errors? Is it easy to correct mistakes? Do people need o enter the same information into two different systems or more than once into t e same system? Have there been complaints about usability?	Yes	5: Efficient, low error rate	
Useable			Does the system have adequate system and user documentation?	Is it up-to-date?	s 47(1)(b) [redacted]	1: Poorly documented system	Documentation and data governance is limited.
Useable			Is there consistency in the user experience and functionality between this solution and other existing solutions?	Does n outdated user interface make people think the system is no longer fit for purpose? Are the same conventions followed as other solutions in the ecosystem?	OK	5: Consistent user experience	
Useable			Is the solution accessible to users with limited capacities, constraints, or special needs, and does it comply with the Web Content Accessibility Guidelines (WCAG)?	Does the solution accommodate users with a variety of needs and abilities?		0: Accessibility status unknown	
Useable			Is the solution readily accessible through all ne essary access channels and in all required contexts?	Consider all platforms and devices that are a part of the solution.	Is used desktop and that is appropriate.	3: Adequately accessible	
Useable			Is the solution accessible to all user group facets, including those with different languages and cultu al sensitivities?	Is it sensitive to cultural nuances and practices? Does it respect and address the diversity of the user base?	Satisfactory	3: Adequately addresses diversity	
Useable			Does the solution offer in-line guida ce to assist users during their interaction with the system?	Consider tooltips, contextual help, interactive tutorials.	Limited.	3: Basic guidance	
Useable		Yes	Are the system me sages, including error messages, easily understood by all use types such as end-users, admin users, and technical support?	Are the messages able to be understood by people presented with the messages? Do they provide meaningful guidance that aids in problem resolution?	Yes	5: Clear for all user types	
Adaptable	Interoperable		Does the solution expose its data and methods through standard AP s as required?	Also consider the documentation and support available for the APIs.	We don't know how to use the APIs, and not certain what they are.	1: No standard APIs, no docs	Documentation and data governance is limited.
Adaptable	Interoperable		Does the solution adhere to the required data exchange protocols and formats (standards)?	Do they enable seamless integration and communication with other systems? Does the system support internationalisation (and what if clients do not support it?)	Yes, not in bulk.	3: Mostly adheres, some issues	

Released under the Freedom of Information Act 1982 (Cth)

Adaptable	Interoperable	Is the system obstructing modifications to other systems?	Is it compatible with the most recent versions of the hardware and software it is integrated with?	No	5: Non-obstructive, fully compatible	
Adaptable	Interoperable	Does the solution ensure loose coupling between its components?	Can the system accommodate changes or replacements of individual components with minimal impact on the overall functionality?	Plug-ins can be updated separately, but platform is tightly coupled.	2: Coupled, noticeable impact	tolerate
Adaptable	Extensible / Flexible / Reusable	Can the solution accommodate additional future modules within its framework?		Plugin architecture	5: Fully adaptable framework	
Adaptable	Extensible / Flexible / Reusable	Does the solution have a minimal schema?	Does the schema cause issues with performance, maintenance, or integration with new components or systems?		0: Unknown	
Adaptable	Extensible / Flexible / Reusable	Does the solution accommodate limited business requirements and adapt to changing business focus as required?	Does the system have the scalability and modularity that can facilitate easy adaptation?	Yes	5: Adapts ea ly	
Adaptable	Extensible / Flexible / Reusable	Does the solution's licensing model align with the business requirements and allow for the necessary flexibility?	Can licensing be scaled up and down or varied as requirements change?	s 47(1)(b) [redacted]	3: Aligned, ome flexibility	
Adaptable	Extensible / Flexible / Reusable	s 47E(d) [redacted]	[redacted]	[redacted]	2: imited alignment, few practices supported	Vendor roadmap requires unplanned change.
Adaptable	Configurable	What is the complexity involved in making configuration changes?	Does configuration require advanced skills?	Infrequent changes. Tool is easy, but configuration files are complex, some mes requiring support.	2: Complex, advanced skills	Changes can require vendor support.
Adaptable	Configurable	How robust are the testing and assurance processes for configuration changes?	Do the testing and assurance processes reliably catch potential issues before deployment?	Robust	4: Mostly robust, minor oversights	
Adaptable	Automatable	Are repetitive, time-consuming, or error-prone activities such as deployment, patching, and testing automated?		The version we are on no	1: Not automated, error-prone	Deployment, patching, and testing are not automated.
Compliant		Does the solution align with legal, regulatory and policy compliance requirements, such as ACIC policies?	Have the compliance requirements been assessed? Has compliance with the requirements been assessed?	Yes	5: Fully compliant, assessed	
Compliant		Does the solution ensure the privacy of user data?	If the system was compromised, what information could be leaked?	Yes	5: Fully ensures privacy	
Compliant		Does the solution adhere to the relevant standards e.g., ISO standards?		Y s	5: Fully adheres to standards	
Compliant		Does the solution have a process in place for responding to Freedom of Information subpoenas effectively?	Are FoI requests able to be completed in a timely and accurate manner?	Yes	5: Efficient process, timely response	
Compliant		Is the archiving process in alignment with the relevant National Archives of Australia (NAA) records authorities?	How do you ensure no data is lost and the archive remains accessi e? How do you make sure archives are destroyed when they are supposed to be destr yed?		0: Unknown	
Compliant		Can you explain how results are derived by your solution and validate their accuracy?	Especially when making consequential decisions, it can be ne essary to justify a decision.		0: Unknown	

Released under the Freedom of Information Act 1982 (Cth)

Document 8

AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION

Contract Risk Assessment

Date last updated: 5/03/2024

Procurement No: P22/361

Last edited by: s 22(1)(a)(ii)

Consider additional potential risks once the contract is signed. Risks can emerge from the vendor's capacityto deliver and variations of contract conditions.

Risk Details				Current Risks		Risk Assessment *(with current controls)*					Monitor and Review		
Risk #	Source of Risk	Risk Owner (e.g. contract manager, Delegate, Vendor etc)	Risk *That may result in loses to the achievement of objectives*	Causes / Threats	How are risks mitigated?	Likelihood Rating	Safety	Governance & Security	Delivery	Overall Risk Rating	Review Frequency	Next Review Date	Notes
1	***Roles & Responsibilities***	*Delegate/ Contract Manager*	*Due to unclear and/or misunderstood roles and responsibilities for aspects of contract management, critical contract management activities are not performed.*	*Lack of contract management experience or contract awareness*	*Communciation with the vendor to clarify the roles and rresponsibilities of each side of the contract.*	Unlikely	Minor	Insignificant	Minor	Low	Annually		
2	***Contract Management Capability***	*Contract Manager*	*Due to a lack of expertise in management of contracts, may encounter unintended fraud and/or unethical conduct*	*Lack of contract management expertise*	*The contract manager is experienced in contract management. Ensure that the mandatory training (Misconduct, Fraud and Corruption) for the contract manager and other roles is up-to-date.*	Possible	Mino	Minor	Minor	Low	Annually		
3	***Supplier performance***	*Contract Manager/ Delegate*	*Failure of the supplier to provide contract deliverables on time, to the agreed quality standards, leading to ACIC having to seek further work and loosing value for money (VfM) on the contract.*	Too optimistic time frames proposed by the supplier Poor supplier performance	Create a detailed project schedule with the ACIC time frames Establish regular performance management meetings to address any performance issues	Possible	Minor	Moderate	Moderate	Medium	Quarterly		
4	***Changes in circumstances or requirements***	Contract Manager/ Delegate	*Informal conversations (verbal, email, text messages) leading to contract variations, impacting the VfM of the contract.*	Changes to provisional service arangement	Agree with the vendor on a formal way to make changes to the requirements, so that any changes conv yed through phone	Possible	Minor	Insignificant	Minor	Low	Annually		
5	***Stakeholder relationships***	Contract Manager/ Delegate	*Failure to manage relationships with the supplier, leading to the inability to mance contract performance and delivery.*	Lack of clear guidance or communication resulting in poor service function or delivery	Establish regular eetings and consultation with the supplier to promote positive wor ing relationships and open dialouge Monitor and man ge service expectations and delivery capability	Unlikely	Minor	Minor	Minor	Low	Annually		
6	***Contract materials information and records***	Contract Manager/ Delegate	*Failure of the supplier to return or destroy all materials, information and records in the agreed timeframe leading to a security information breach.*	Loss of sensitive personal information	P lantir data is classified as Protected and Palantir staff is prohibited from viewing it. In addition, any sensitive information	Unlikely	Minor	Minor	Minor	Low	Annually		
7	***Payment***	contract manager	*Failure to pay correctly rendered invoices from the supplier in a timely manner causing a breach in contractual obligations for ACIC.*	Lack of money in the current budget to pay for the Titanium upgrade.	The proposed project schedule starts in July 2024 when the agency expects to have money to pay for the upgrade.	Likely	Minor	Moderate	Moderate	High	Monthly		
8	***Transition Arrangements***	Delegate/ Contract Manager	*Not addressing performance problems with an outgoing supplier, only for ACIC to then re-procure services/goods from the same supplier.*	Palantir upgrade completion and 3rd level support continuity	Palantir is an established multinational company that have	Unlikely	Minor	Insignificant	Minor	Low	Annually		
9	***ICT risks***	vendor/ delegate	*Failure to have appropriate securi y controls and measures in place to protect ACIC data and asse ts.*	Inf rmation breach	Palantir data is classified as Protected and Palantir staff is prohibited from viewing it. In addition, any sensitive information	Rare	Minor	Minor	Minor	Low	Annually		
10						[Please Select]	[Please Select]	[Please Select]	[Please Select]	[Please Select]	[Please Select]		

Released under the Freedom of Information Act 1982 (Cth)

RISK MANAGEMENT PLAN

The purpose of this Risk Management Plan is to identify the risk to the Limited Tender procurement for the renewal by the Australian Criminal Intelligence Commission (ACIC) of Palantir Maintenance services.

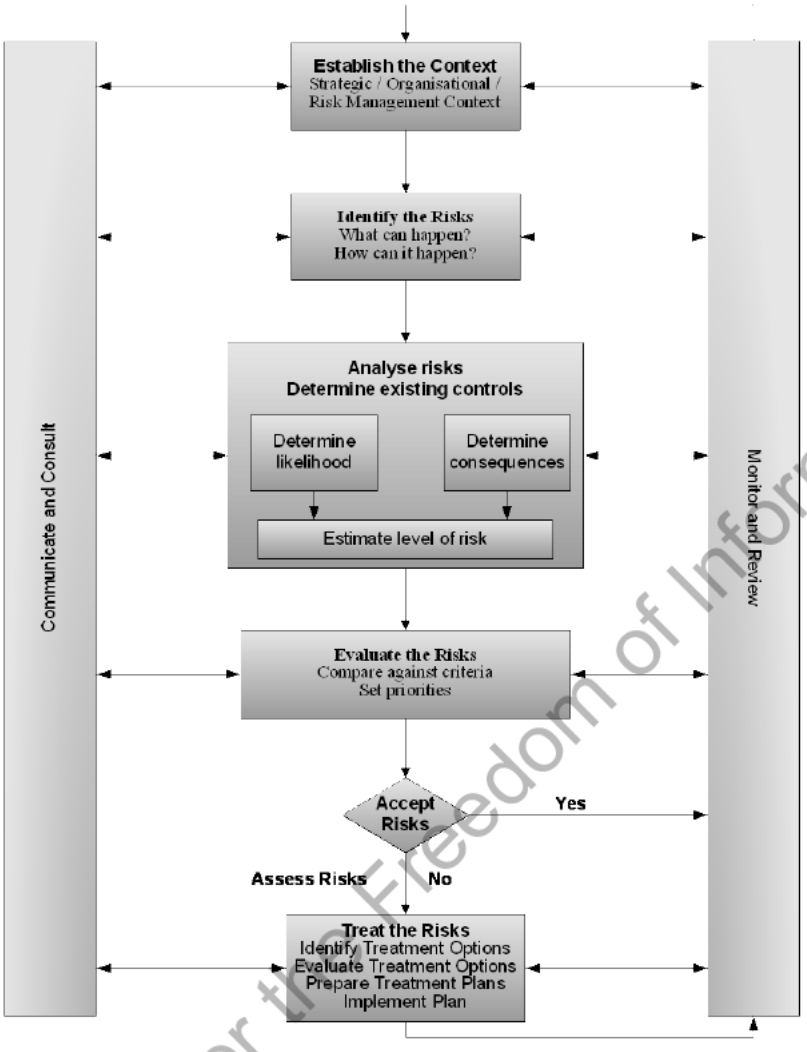
RISK PLAN: P18/223 Palantir Maintenance
1. Procurement Policy
The procurement shall be undertaken in accordance with the Commonwealth Procurement Rules (CPRs) March 2017. Applicable ACIC Accountable Authority Instructions (AAI) will inform and guide the process, in addition to the Department of Finance published guidance. The procurement risk plan conforms with the ACIC Enterprise Risk Management Framework trim:[17/145855]
2. Risk Management Plan
Through this Risk Management Plan (RMP) ACIC is establishing processes for the identification, analysis, allocation and treatment of risk when conducting the procurement to renew Palantir Maintenance services.
3. Objectives
The RMP Objectives are to: • Establish the risk management and risk control context • Define the strategies for risk • Identification • Analysis • Assessment, Evaluation • Treatment • Monitoring and review, and • Communication and consultation. Define the risk administration processes.
4. Broad Risk Management Strategy
Risk management is focussed on managing uncertainty in order to meet ACIC stakeholders' objectives and expectations. As a consequence, the risk management strategies adopted shall focus on identifying the key uncertainties and associated risks, developing appropriate responses and implementing a monitoring and review process. This strategy will ensure that the identified risks are effectively controlled and the likelihood of the process being successful is maximised. Risk reporting will occur in accordance with the reporting regime defined in the contract, or following on from meetings with ACIC stakeholders, and as part of the regular status reports and by exception if required. This mechanism helps to ensure that key stakeholders are aware of: • Known risks • The intended control strategies • Current risk status, and • Risk related issues.
5. Risk Management Process Review

Released under the Freedom of Information Act 1982 (Cth)

RISK PLAN: P18/223 Palantir Maintenance

The risk management process that shall be applied throughout the procurement is based on industry best practice, and is consistent with Risk Management Standard AS/NZS 4360:2004. This process is built on a defined risk context and the iterative application of risk management steps, supported by an ongoing communication and review process, as illustrated in below.

Risk Management Process Overview



6. Risk Identification

Risk Identification aims to identify the risks to be managed. Comprehensive identification includes using a well-structured, systematic process.

Risk identification shall be conducted via:

- Direct stakeholder consultation and liaison,
- Review of past projects,
- The application of professional knowledge in resource management, and Consultation with ACIC stakeholders as needed.

7. Risk Analysis

Released under the Freedom of Information Act 1982 (Cth)

RISK PLAN: P18/223 Palantir Maintenance

Risk Analysis is focussed on determining risk likelihood and consequence in order to evaluate and prioritise risks and their specific control measures. Risk Analysis shall be conducted for all identified risks.
In the first instance, qualitative analysis techniques shall be used when assessing risks. Qualitative risk analysis shall be based on an assessment of available information, historical precedence (where applicable), and professional knowledge / experience.
It is not envisaged that quantitative analysis will be required in this case.

Risk Likelihood

Analysis of *Risk Likelihood* shall result in one of the following determinations as demonstrated below.

Likelihood	Definition of the Purposes of this RMP
Rare	Event may occur in exceptional circumstances
Unlikely	Event could occur
Possible	Event may occur at some time
Likely	Event will probably occur
Almost Certain	Event is expected to occur

Risk Consequence

Analysis of Risk Consequence shall result in one of the following determinations as demonstrated below.

Consequence	Definition for the Purposes of this RMP
Insignificant	Event would be of trivial consequence
Minor	Event would be of limited, but acceptable, consequence
Moderate	Event would be of significant, but manageable, consequence
Major	Event would have extensive and unacceptable consequence
Catastrophic	Event would be project fatal

Level of Risk

The following Risk Matrix shall be applied: These tables will be utilised to define the *level of risk* based on the assessed likelihood and consequence (note: this risk-matrix logic has been automated in the Risk Register – refer to Risk Administration below).

Extreme	Immediate action required, Senior Executive will be involved
High	Senior management attention needed, action plans and management responsibilities specified
Medium	Manage by specific monitoring or response procedures, with management responsibility specified
Low	Manage by routine procedures, unlikely to need specific application of resources

8. Risk Evaluation

A Risk Evaluation Panel will be appointed by the Approving Delegate. The Evaluation Panel's role is to:

- rate the Submission received against the approved Evaluation Criteria in accordance with an agreed methodology
- identify any issues requiring resolution, further discussion and/or clarification with the Supplier
- establish a clear, defensible, accountable and properly documented basis for the selection or rejection of the Supplier

Released under the Freedom of Information Act 1982 (Cth)

RISK PLAN: P18/223 Palantir Maintenance

- provide a clear recommendation to the Approving Delegate as to the successful Supplier, if any, and course of action.

The Evaluation Panel will conduct an initial technical review and score the Submission having regard to the Evaluation Criteria set out below and as per the scoring system described in the RFQ document. If the Submission receives a combined technical score of 3 or above it will pass this initial Stage. If the Submission does not, the Evaluation Panel will provide the Supplier with an opportunity to submit another response (considering that this procurement is a Limited Tender to one supplier).

The Evaluation Panel will make recommendations, via an Evaluation Report to the Approving Delegate on whether it is recommended to proceed with the Supplier, conduct negotiations (if required), or other course of action.

9. Risk Treatment

Risk treatment involves the identification of treatment options based on the Risk Evaluation, and the preparation and implementation of a risk treatment plan. Risks should be addressed in accordance with their priority identified during risk evaluation, regardless of the risk level.

Risk treatment shall be effected in one of the five following ways.

Risk Avoidance

Risk Avoidance shall be applied where possible. This strategy involves the adoption of alternate approaches that effectively side-step the identified risk.

Risk Reduction

Risk Reduction will be used when the risk cannot be avoided but may be reduced to an acceptable level. This is the most common form of risk treatment and involves the identification and implementation of strategies that effectively reduce the risk. The options here are numerous.

Risk Transfer

This treatment strategy shall be used when the risk cannot be avoided nor effectively minimised but may be transferred. This is often the strategy of last resort and unlikely in this procurement context. If implemented, risk transfer does not diminish the RFT Project Manager's ongoing responsibility or accountability for risk management.

Risk Referral

In circumstances where, within resources available, all treatment options have failed to reduce the risk to an acceptable level in accordance with the risk criteria, the risk may be referred to a higher authority (via the RFT Project Manager) for acceptance. The authority must be made aware of all related considerations.

Risk Acceptance

This treatment strategy can be adopted for risks that fall within the bounds specified in the risk criteria. It may also be used as a last resort should resources not be available to treat the risk.
Once a risk treatment strategy is determined, the strategy shall be converted into meaningful activities / tasks. These activities shall be managed via (for example) tasking requests.

10. Monitor & Review

Risk monitoring and review processes shall occur on an ongoing basis and will include:

- Changes in assessed existing risk status and level
- New and emerging risks
- Effectiveness of risk treatment strategies
- Options for increasing the effectiveness of risk treatment strategies

Released under the Freedom of Information Act 1982 (Cth)

RISK PLAN: P18/223 Palantir Maintenance

- Currency and appropriateness of risk assessments, and
- Possible sources of evolving risk.

Risk Administration

11. Risk Management / Monitoring

The Palantir Contract Manager will ensure:

- Identified risks are documented throughout all procurement documentation in TRIM
- Specified risk treatments are implemented and risk in general is routinely monitored
- Risk assessments are updated after Palantir Contract Management Meetings.

12. Risk Reporting

'On Occurrence' risk reporting will occur as follows:

- Upon request;
- When an unacceptable risk has been identified and it is envisaged that identified treatments will not reduce it to an acceptable level; and
- When resources required to treat a risk have not been forecast or available.

Released under the Freedom of Information Act 1982 (Cth)