Instructions for completing the risk tables and risk register

- 1 Complete the risk impact and risk likelihood tables to define the ratings in the context of your project. It can be useful to provide example risks to help people categorise new risks identified.
- 2 Capture your risks in the Risks tab. Use the drop down values to capture the impact and likelihood for each risk before and after mitigation.
- 3 Revisit your mitigation for any risks with a risk rating of high or extreme.
- 4 Identify the person or role responsible to manage each risk.

Disclaimer

Risk Impact

Impost description	Dating	Define or describe	Example of a rick at this imp	
Impact description	Rating	Commercial	Example of a risk at this imp	
Insignificant	1	Under \$50k	Near Miss	
Minor	2	\$50k to \$250k	First Aid Incident	
Moderate	3	250k to \$1M	Minor Safety Incident	
Major	4	\$1M - \$5M	Major Safety Incident	
Catastrophic	7	\$5M +	Fatality	

Risk Likelihood

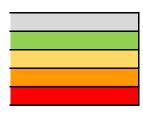
description	Rating	Define or describe this likelihood rating	Example of a risk at this likelil
Unlikely	1		
Possible	2		
Likely	3		
Very Likely	4		
Almost Certain	5		

Risk Rating (Likelihood x Impact)

From	То	Risk	Criteria for risk mitigation strategies
0	3	Low	Acceptable with adequate controls. No action required unless level increases.
4	7	Medium	May be acceptable with adequate controls. Should be monitored regularly.
8	14	High	Unacceptable and must be addressed.
15	35	Extreme	Unacceptable and must be addressed.

act rating								

hood rating	



DPC2142 RISK REGISTER

Note: Clear (white) cells are for free text; cells shaded in light grey feature drop-down selections; blue cells autocomplete.

Ref	Risk Description	Risk Impact or Consequence		Rating before mitigation		Mitigation	Rating after mitigation			Risk Owner
			Impact	Likelihood	Rating	Controls to manage the risk	Impact	Likelihood	Rating	
0	Describe the risk	Who/what would it impact, how, and to what extent?	Moderate	Very Likely	High	What actions will you take to reduce the likelihood or impact of the risk?	Moderate	Unlikely	Low	Who is responsible to manage this risk?
	Technical Risks									
1	Integration failure with ServiceWA or Digital Trust Platform (DTP)	Project delays, cost overruns, stakeholder dissatisfaction	Major	Possible	High	Conduct early Proof-of-Operation testing, use pre-production staging environments, and engage WA Government dev partners closely.	Moderate	Unlikely	Low	Project Manager
2	SDK incompatibility across iOS and Android	Limited user adoption, degraded experience	Minor	Possible	Medium	Include cross-platform testing in PoO, follow ISO/IEC 18013 and 23220 standards, and ensure APIs are standards-based.	Minor	Unlikely	Low	Project Manager
3	Scalability and performance bottlenecks	Slow response times, degraded UX, system outages under load	Moderate	Possible	Medium	Perform load testing, monitor dashboards during pilot, and plan for horizontal scaling before full deployment.	Minor	Possible	Medium	
4	Third-party system dependencies (e.g., DoT integration, WA Identity Exchange)	Delays, integration failures	Moderate	Possible	Medium	Establish API contracts early, engage external stakeholders, and create fallback pathways.	Minor	Possible	Medium	
5										
	Security & Privacy Risks									
6	Data breach or unauthorised access	Breach of citizen privacy, reputational damage, regulatory non-compliance	Minor	Possible	Medium	Encrypt data at rest and in transit, enforce MFA, maintain strict access controls, and comply with ISO/IEC 27001 & ACSC Essential Eight.	Minor	Possible	Medium	
7	Credential forgery or compromise	Invalid credentials used for identity verification	Minor	Possible	Medium	Use cryptographic proofs, secure key binding, and offline verification capabilities.	Insignifica nt	Unlikely	Low	

8	Security vulnerabilities in SDK or backend	Exploitation of unpatched code or dependencies	Moderate	Possible	Medium	Regular vulnerability scanning, penetration testing, and third-party audits before production release.	Minor	Unlikely	Low	
9	Delayed breach notification	Non-compliance with WA Gov policies, reputational harm	Minor	Unlikely	Low	Follow immediate notification protocols (report within 24 hrs), maintain incident response plans, and prepare post-incident reports.	Insignifica nt	Unlikely	Low	
10										
	Compliance & Standards Risks									
11	Failure to comply with ISO/eIDAS standards	Incompatibility with WA Gov frameworks, project rejection	Moderate	Unlikely	Low	Maintain ISO 27001 certification, run regular compliance audits, and integrate automated conformance testing suites.	Insignifica nt	Unlikely	Low	
	Changing legislative or regulatory requirements	Rework, delays, or cost increases	Minor	Possible	Medium	Monitor evolving eIDAS, ISO, and privacy laws; design modular solutions adaptable to regulatory changes.	Minor	Possible	Medium	
12	Privacy non-compliance (e.g., GDPR-equivalent)	Legal penalties, loss of trust	Minor	Unlikely	Low	Conduct Privacy Impact Assessments (PIAs), segregate data, and implement strict access controls.	Insignifica nt	Unlikely	Low	
13										
	Project Delivery & Operational Risks									
14	Delayed Proof-of-Operation or Pilot milestones	Missed contractual deadlines, reduced stakeholder confidence	Moderate	Possible	Medium	Create detailed project schedules, monitor weekly, and establish clear escalation pathways.	Minor	Possible	Medium	Project Manager
15	Insufficient resourcing or skills	Inability to deliver technical scope	Minor	Possible	Medium	Allocate skilled personnel early, provide upskilling through training, and maintain backup personnel plans.	Minor	Possible	Medium	Project Manager
16	Poor training uptake by Department staff	Reduced operational readiness post- pilot	Minor	Possible	Medium	Deliver comprehensive training at least 4 weeks pre-pilot, measure training effectiveness, and refresh as required	Minor	Possible	Medium	Integration Lead
17	Stakeholder misalignment	Conflicting priorities delay progress	Minor	Possible	Medium	Maintain structured governance meetings and regular reporting to ensure stakeholder alignment.	Insignifica nt	Possible	Low	
18	Uncontrolled scope creep	Increased costs and missed deadlines	Moderate	Possible	Medium	Enforce strict Statement of Work (SOW) variation processes, secure Department approval before changes.	Minor	Possible	Medium	
19										

	User Adoption & Experience Risks								
20		Low citizen uptake, negative feedback	Minor	Possible	Conduct usability testing during PoO, collect structured participant feedback, and iterate rapidly.	Minor	Possible	Medium	
21	Accessibility non-compliance	Excludes key user groups, legal risks	Insignifica nt	Possible	Test against WCAG 2.1 AA standards, ensure UI/UX aligns with ServiceWA guidelines, and incorporate user onboarding flows.	Insignifica nt	Unlikely	Low	
22	Low trust in digital credentials	Citizens reject wallet adoption	Moderate	Possible	Engage in transparent communication, publish privacy assurances, and highlight WA Gov endorsement.	Minor	Possible	Medium	
23									
24									
25									
26									
27									
28									
29									
30									
31									
32									

					п
33					
34					
35					
36					
37					
38					
30					
39					
40					
41					
71					
42					
43					
44					
44					
45					

П 40	T				
46					
47					
48					
40					
49					
50					
51					
52					
52					
53					
54					