

Task Name

- 1.1.5 Monitor pilot and close project
- 1.3.2 Research Canadian Regulation
- 1.3.3 Identify target users & Strategy
- 1.3.6 Reserve audit requirement
- 1.5.3 Run penetration test & attack simulations
 - 1.2.1 Select blockchain infrastructure
 - 1.2.2 Set up Cloud Dev
 - 1.2.3 Implement Consensus mechanism
- 1.4.2 Draft and publish white paper
- 1.4.3 Produce marketing campaign media
- 1.6.4 Provide beta user Credits & Monitor metrics
 - 1.1.4 Launch CADC on main net
- 1.2.5 Allocate budget & 10% Contingency
 - 1.3.1 Analyze Blockchain Ecosystems
 - 1.3.4 Assess competing sublecoins
 - 1.3.5 Define CADC peg Mechanism
- 1.5.1 Conduct internal code audits
 - 1.5.2 Implement multi-sig
- 1.6.1 Design trading interface
- 1.6.3 Launch governance token
- 1.1.3 Approve Project Objectives
- 1.2.4 Configure Developer Environment
 - 1.4.1 Polish brand identity
- 1.4.4 Plan community-building events
 - 1.1.2 Identify Stakeholders
- 1.6.2 Test Contracts and Dex on testnet
 - 1.1.1 Draft Project Charter
- 1.5.4 Engage independent security audit

Sum

Ts(Week/Day)	Optimistic Activity Time(week)
3(21)	20
3(21)	19
2(14)	13
2(14)	13
3(21)	19
2(14)	12
2(14)	13
3(21)	19
3(21)	19
3(21)	20
3(21)	19
2(14)	11
2(14)	12
3(21)	18
2(14)	11
3(21)	18
3(21)	18
2(14)	11
3(21)	18
2(14)	11
2(14)	11
2(14)	10
2(14)	10
2(14)	10
2(14)	9
3(21)	16
2(14)	7
3(21)	13
	400

Pessimistic Activity Time (week)Most Likely Activity Time(week)

21	23
20	22
14	15
14	17
20	26
14	17
15	16
21	25
21	23
22	27
21	27
14	15
15	20
21	23
14	16
21	24
21	23
14	17
21	23
14	19
15	16
14	19
14	22
14	17
14	20
21	25
14	25
22	29
486	591

Weighted Average Activity(week)	Variance
21.17	0.0278
20.17	0.0278
15.3	0.0278
14.3	0.0278
20.83	0.0278
14.17	0.1111
14.83	0.1111
21.33	0.1111
21	0.1111
22.5	0.1111
21.67	0.1111
13.67	0.25
15.3	0.25
20.83	0.25
13.83	0.25
21	0.25
20.83	0.25
14	0.25
20.83	0.25
14.33	0.25
19.5	0.4444
14.17	0.4444
14.67	0.4444
18.5	0.4444
14.17	0.6944
20.83	0.6944
14.67	1.3611
21.67	2.25

2.25

Task Name	Ts(Week/Day)
1.1.1 Draft Project Charter	2(14)
1.1.2 Identify Stakeholders	2(14)
1.1.3 Approve Project Objectives	2(14)
1.1.4 Launch CADC on main net	2(14)
1.1.5 Monitor pilot and close project	3(21)
1.2.1 Select blockchain infrastructure	2(14)
1.2.2 Set up Cloud Dev	2(14)
1.2.3 Implement Consensus mechanism	3(21)
1.5.1 Conduct internal code audits	3(21)
1.5.2 Implement multi-sig	2(14)
1.5.3 Run penetration test & attack simulation	3(21)
1.5.4 Engage independent security audit	3(21)
1.6.3 Launch governance token	2(14)
Provide beta user Credits & Monitor m	3(21)
Sum in Days	238
Sum in Week	34

Optimistic Activity Time(Week/Day) Pessimistic Activity Time (Week/Day)

7	14
9	14
11	15
11	14
20	21
12	14
13	15
19	21
18	21
11	14
19	20
13	22
11	14
19	21
193	240

27.5714285714286

34.2857142857143

Most Likely Activity TimeWeek/Day)	Weighted Average ActivityWeek/Day)
25	14.67
20	14.17
16	19.5
15	13.67
23	21.17
17	14.17
16	14.83
25	21.33
23	20.83
17	14
26	20.83
29	21.67
19	14.33
27	21.67
298	246.84
42.5714285714286	35.2628571428571

Variance

Task ID
1.1.1
1.1.2
1.1.3
1.1.4
1.1.5
1.2.1
1.2.2
1.2.3
1.2.4
1.2.5
1.3.1
1.3.2
1.3.3
1.3.4
1.3.5
1.3.6
1.4.1
1.4.2
1.4.3
1.4.4
1.5.1
1.5.2
1.5.3
1.5.4
1.6.1
1.6.2
1.6.3
1.6.4

Risk ID
1.1.1
1.1.2
1.4.4

	Description
	Delay in formalizing the project charter may lead to scope ambiguity, authori
	Insufficient stakeholder identification may result in requirement volatili
	Delays in objective approval may hinder baseline establishment
	Late deployment to the main net may lead to contractual non-compliance
	Insufficient monitoring of project closure activities may cause outstanding
	Misalignment between selected architecture and regulatory or performance requi
	Improper cloud configuration may result in security exposure, resource m
	Consensus design flaws may introduce downstream functional inc
	Environment misconfiguration may delay developer onboarding and impe
	Ineffective resource allocation may reduce financial resilie
	Incorrect ecosystem assessment may impair competitive pos
	Incomplete regulatory analysis may cause future complia
	Misinterpretation of target user groups may undermine ad
	Poor assessment of competitors may impair pricing log
	Peg mechanism deficiencies may introduce volatility exp
	Delays or inaccuracies in reserve audit planning may lead to re
	Brand misalignment may reduce user trust and impair communio
	Incomplete or delayed publication may affect regulatory ac
	Ineffective campaign assets may fail to meet requirement trac
	Event preparation delays may reduce outreach effectiveness and
	Insufficient audit coverage may expose security vulnerabi
	Incorrect multi-sig integration may introduce key-management r
	Limited penetration-testing scope may fail to ide
	Third-party audit delays or findings may require remediation that jec
	Misaligned UI/UX requirements may cause functional i
	Smart-contract or DEX failures during testnet validation may
	Governance token deployment delays may impact utility
	Insufficient monitoring of early-stage metrics may reduce reliability of

Strategy

Avoid

Avoid

Avoid

Avoid

Imapct	Likelyhood	
5	5	25
5	4	20
5	3	15
5	3	15
5	2	10
5	2	10
5	2	10
5	2	10
5	4	20
5	3	15
4	3	12
4	1	4
4	1	4
4	3	12
4	3	12
4	1	4
5	3	15
5	2	10
5	2	10
5	4	20
5	3	15
5	3	15
5	1	5
5	5	25
4	3	12
4	4	16
5	3	15
5	2	10

Risk ID	Strategy	Strategy Description
1.1.1	Avoid	Avoid by scheduling an early charter drafting workshop with key stakeholders
1.1.2	Avoid	Avoid by standardizing the developer environment through validated configurations
1.4.4	Avoid	Avoid by preparing community-engagement events on fixed lead times with clear agendas
1.5.4	Avoid	Avoid by engaging the independent security auditor early, agreeing on as-is state of the code

ders and requiring formal approval at a fixed milestone to lock scope and authorization before configuration templates and automated setup scripts to eliminate misconfiguration risk during early pre-approved logistics, content plans, and contingency arrangements to reduce the likelihood of assessment scope and timing contractually, and allocating a dedicated remediation team to address

subsequent work packages begin.

ly development stages.

od of delay or cancellation.

ess findings rapidly and prevent schedule slippage.

Risk ID	Strategy
1.1.1	Avoid
1.1.2	Avoid
1.4.4	Avoid
1.5.4	Avoid

S	
Avoid by scheduling an early charter drafting workshop with key stakeholders	subsequ
Avoid by standardizing the developer environment through validated configurations	c
Avoid by preparing community-engagement events on fixed lead times with	of
Avoid by engaging the independent security auditor early, agreeing on assessment findings rapid	