**CSG 2344 – PROJECT METHODS AND PROFESSIONALISM - ASSIGNMENT 2**

**SECURE E-VOTING SYSTEM PROJECT PROPOSAL**

**TEAM GAMMA**

|  |  |  |
| --- | --- | --- |
| **Student Name** | **Student number** | **Student Email** |
| Visahl Samson David Selvam | 10498743 | [vdavidse@our.ecu.edu.au](mailto:vdavidse@our.ecu.edu.au) |
| Phone Toe Kyaw | 10502161 | [tphone@our.ecu.edu.au](mailto:tphone@our.ecu.edu.au) |
| Hyejoon Nam | 10512830 | [hnam@our.ecu.edu.au](mailto:hnam@our.ecu.edu.au) |

Contents

[Executive Summary 3](#_Toc25953866)

[Project Background 3](#_Toc25953867)

[Literature review 3](#_Toc25953868)

[E-Voting system merits and demerits 4](#_Toc25953869)

[Proposal 5](#_Toc25953870)

[Process flow 5](#_Toc25953871)

[Process breakdown 5](#_Toc25953872)

[Scope 9](#_Toc25953873)

[In-scope 9](#_Toc25953874)

[WBS creation 9](#_Toc25953875)

[Out of Scope 10](#_Toc25953876)

[Scope control 10](#_Toc25953877)

[Incorporating with existing system 10](#_Toc25953878)

[Gantt Chart 11](#_Toc25953879)

[Time Management 15](#_Toc25953880)

[Cost Management 16](#_Toc25953881)

[Human Resource Management 17](#_Toc25953882)

[Project Methodologies integration 18](#_Toc25953883)

[Risks 19](#_Toc25953884)

[Risk Matrix 19](#_Toc25953885)

[Weigh Factor Analysis 20](#_Toc25953886)

[Risk register priorities (TOP 10) 20](#_Toc25953887)

[Recommendations 25](#_Toc25953888)

[References 26](#_Toc25953889)

**SECURE E-VOTING SYSTEM USING BLOCKCHAIN**

# Executive Summary

The following is a proposal for building a Secure E-Voting system using Blockchain technology. Our goal is to utilize blockchain technology to build a system that can be used for e-voting process. This project involves both business, and technology processes and activities. Business part includes collecting data from banks, maintaining good business relations between banks and Government. Whereas technology part includes utilization of blockchain for the e-voting system which includes development and testing of the system. This report starts with our proposal then moves to scope statement then continues to our solution then moves to integration of traditional and agile project methodologies and then continues to risk assessment and finally ends with recommendations and conclusion.

# Project Background

To improve the online technology for people to vote using E-voting system so that every voter can cast their vote from their home using online technology. The previous E-voting system in Australia is inappropriate due to interference, computer malfunction and fraud. 85% of people in Australia is currently using online mobile banking and looks to use existing online banking technology and capable of meeting the privacy and secrecy requirements for each Australia citizen. The Australia Government want to create the e-voting system with both cost-effective and secure (authentication process) system. Federal Australian election will link and partner with Australia 4 biggest banks which are ANZ, N.A.B, Westpac and Commonwealth Bank). Also, in this project we have to consider CIA (Confidentiality, Integrity and Availability) of data, preventing fraudulent/multiple voting, and increasing voting percentage.

# Literature review

In order to come design our proposed solution we have gone through several researches. E-voting systems merits and demerits (Election Canada, n.d.) helped us to understand general things about e-voting which encouraged us to design our project to suit for the scenario. Also, Mosco (Ami Rojkes Dombe, 2019) (Aqeel, K., Kuldip, S., & Sandeep, S, 2010) (Sharon, C., & Gari, S, 2018) helped us to understand appropriate measures to ensure CIA which is vital for the given scenario. Apart from that (Mekebeb, T, 2019) enabled us to find an easy way to get data from bank without any hassles.

Apart from technical part for the business-related processes importance of integrating different project methodologies (Yatin, P, 2017) have been learned and applied. Apart from that importance of risk analysis in IT project has been learned (Lavanya, N. & Malarvizhi, T, 2008) (Spacey, J,2017), (Sharon, C., & Gari, S ,2018.

# E-Voting system merits and demerits

E-voting is fundamentally using electronic medium to vote. In this precise project we are implementing internet-based voting.  Canada, Estonia, France and Switzerland are some of the examples countries that are using internet-based voting (Election Canada, n.d.). Same as any other systems E-voting also has its own advantages and disadvantages.

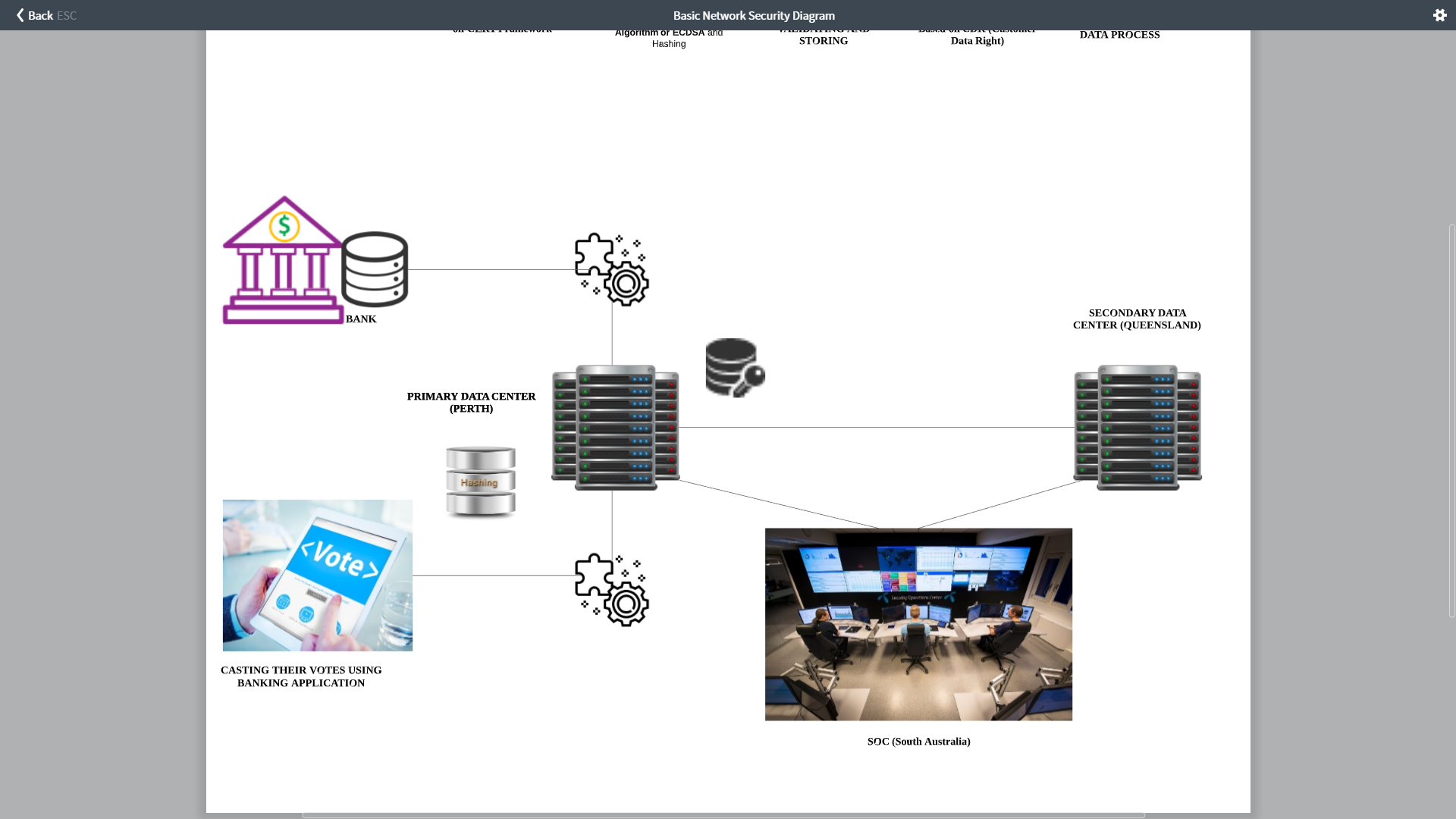
Advantages includes (Election Canada, n.d.) convenience and accessibility for the voters. Because in e-voting the user need only a device, and internet connectivity to cast their votes. Also, it will be beneficial to certain group of voters such as persons with disabilities, people working abroad, people who travel for various purposes, etc... E-voting also provides flexible voting time for the voters. Because in this need of method waiting in pooling station can be eliminated and voters can cast their vote at any time they want. Also, it provides more accurate election efficiency.

At the same time e-voting also includes few drawbacks (Election Canada, n.d.) such as limited access to internet which will affect the pooling percentage. Also, security is second major thing to consider because inadequate security measures will lead to data leakage that will affect the voter’s privacy. Moreover, security can affect the availability of system which cause severe impact in election pooling. Thirdly, ensuring votes are casted by rightful voters because it is possible that lack of e-voting knowledge cause misuse of votes.

# Proposal

Our proposal here is using Blockchain technology in-order to develop a secure e-voting system that focuses on voter’s privacy and convenient, CIA of data, increasing pooling ratio. Our design consists two parts first one is front-end, and second one is back-end. Since, the voters going to cast their votes through their existing mobile banking application, in front-end we will add an option in mobile banking application that will allow the users to cast their votes. To make sure the users are eligible to vote we are going to collect user details from all the 4 banks, and we will store in dedicated data centres and the data centres will be monitored by a dedicated SOC.

## Process flow



Screenshot Process flow

Given screenshot 1 shows how the process flows from the beginning.

## Process breakdown

**Data collection**

The primary function of our projects starts from collecting data from 4 major banks. In order to avoid any risks that may affect the process we are going to utilize Customer Data Right (CDR) legislation passed by the Australian parliament in August 2019 (Mekebeb, 2019) . CDR framework will allow consumers in the country to direct banks to share their data with fintech organizations (Financial Technology) and other third-party providers (TPPs). So, while collecting data from bank this framework can used which will eliminate most of the risks related with user’s data.

**Framework**

To overcome security issues and preserver CIA, we are intended to follow the CERT framework developed by Australian Cyber Security Centre (ACSC) which is from Australian Government. This framework provides a cyber security framework that organisations can apply, using their risk management framework, to protect their information and systems from cyber threats. Also, since this project is fully based on Australia usage this framework would be appropriate,

This framework guides each and everything from how we design the infrastructure to till how we should we maintain the information security.

**Infrastructure configuration**

As mentioned, previously in the report in this project we must ensure the CIA. So apart from following CERT framework, our design consists following technology enhancements to ensure maximum security and reliability. Moreover, we are going to use private blockchain where only the Australian Electoral Commission can access the pooling data.

Also, we analysed few incidents happened in previous blockchain based voting system implementations. Specifically, the Mosco incident that took place in August 2019 (Ami Rojkes Dombe, 2019) . After analysed the incident we have decided to harden the security. The detailed methodology break-down can be found below.

**To Ensure Confidentiality**

Confidentiality deals with data storage. To maintain the confidentiality of information our design equipped with RSA algorithm. The reason to use RSA here is due it’s complexity. Also, in the Masco incident the system was broken due to weak security algorithm. So, comparing with other algorithms RSA would be greater choice. The confidentiality part applies to the data collected from bank, and the data of votes casted by citizens.

**To ensure Integrity**

Integrity part comes while data in transit. In order to ensure this integrity hash function will be placed. Also, to make sure the votes are casted by its rightful owners the hash algorithm implemented here would be Elliptic Curve Digital Signature Algorithm or ECDSA (Aqeel, Kuldip & Sandeep, 2010) which is basically used by Bitcoin to make sure the funds can only spend by its rightful possessor.

By implementing this algorithm, we can prevent multiple voting and as well as fraudulent voting.

**To Ensure Availability**

Availability meant to make sure the system is accessible whenever the user wants to access. Availability can be affected due to several factors includes forces of nature, physical destruction, DDOS attacks, and advances persistent attack vectors. So, to make sure the system’s availability we are using 2 data centres and 1 SOC. So, if one data centre faces any issue the other data centre can continue its process without any issues. Also, the 24/7 dedicated SOC monitor both the data centres for any unusual activities and they can take care of all the security measures like SIEM, IPS, and IDS. To ensure the blockchain servers can handle multiple data at same time we are going to add Hyperledger fabric over blockchain (Sharon & Gari, 2018) , The main advantages of Hyperledger over blockchain is it will increase the scalability and performance so our blockchain design can have enough throughput to handle larger number of data simultaneously

Since, all the 3 infrastructures located in different the possibility of technical problems can be eliminated.

**Increasing pooling percentage**

One more task to consider here is ways to increase the pooling percentage. As mentioned in pre-requisites the current pooling percentage is 85%. To increase the pooling percentage, we have come up with following plans.

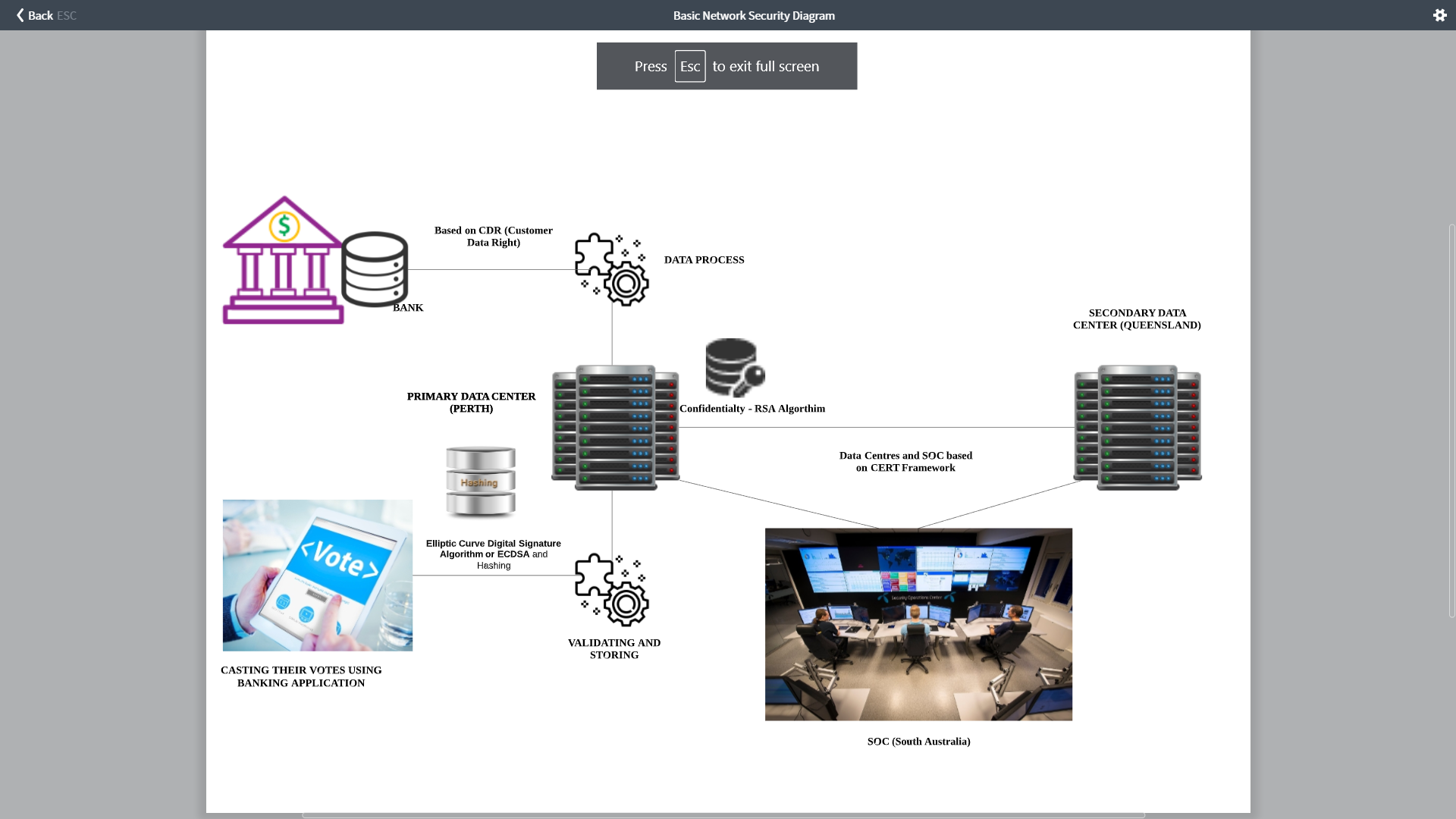
**Before election**

Using online and offline campaigns about the voting system. This activity will include a demonstration of how to use this e-voting system to cast their votes. So, users can gain knowledge on the e-voting's process. Also, this will increase awareness of e-voting system.

**During Election**

As mentioned earlier option to add family members in front-end will be useful. By using this option elder people in home who don’t have enough resources can cast their votes in single device.

Using on-pool vehicle during the election period and using public places like library, and people centres. In this method a vehicle equipped with voting system will travelling all over the regions and will be placed in common places like Universities, community centres, etc... And people who don’t have accessibility or bank account can use one of their identity documents to cast their vote.



Screenshot Process flow full technology

Screenshot 2 shows how the process works with detailed technology configuration.

# Scope

## In-scope

The scope of this project is to design a system that let Australian citizens to cast their vote using their existing banking mobile application. For the implication we are going to use Blockchain as a backend system to connect all the 4 banks together for the period and to store the votes as well as to prevent multiple voting. Also, this project aims to increase the voting percentage. Also, in order to increase the security and reliability we are going to build 3 physical infrastructures, out of these 3 infrastructures 2 will be Block chain data centres where primary one will be at Perth and Secondary (Backup) data centre will be located at Queensland. Also, the 3rd infrastructure would be a dedicated SOC (security operations centre) that will be located at South Australia. For front-end we’re going to add family control feature that allow user to add their family members who are eligible to vote so that the family can use singe device to cast their vote. This process also includes business activities such as creation of policies between banks and risk governance. The Project methodology we’re going to use here is “Agile”. The activities specified in WBS will be carry-on to complete the project. Also, everything should be completed within the given cost, and time frame.

## WBS creation

1. **Pre implementation phase**
   1. Designing POC for Blockchain
   2. Preparing contract documents for banks and Governments
   3. Getting Approval for POC
2. **Implementation**

2.1 **Technical**

2.1.1 Making Data Centres ready according to ISO standards

2.1.2 Implementing Backend design

2.1.3 Testing Backend system with duplicate data

2.1.4 Implementing Frontend design

2.1.5 Testing Frontend System with duplicate data

2.2 **Business**

2.2.1 Reporting to client once in a week

2.2.2 Doing awareness campaigns (offline) every weekend

2.2.3 Doing online campaigns

1. **Post implantation**

**3.1 Testing**

3.1.1. Performing Blackbox testing on both Front-end and Back-end

3.1.2 Patching if any vulnerabilities found

3.1.3 Rebuild if it’s necessary

3.1.4 Taking system live in testing phase to get user experience

3.1.5 Rebuild if it’s necessary

3.1.6 Showing completed system demo to clients

3.2 **Handing over**

3.2.1 Reviewing all the financial activities

3.2.2 Auditing the financial statements

3.2.3 Preparing documents for handing over

3.3 **Maintenance**

3.3.1 Performing routine on data stored in data centres

3.3.2 Actively monitoring the data

## Out of Scope

* ISP Problems during the election period.
* Forgotten Login credentials to the existing mobile banking application.

## Scope control

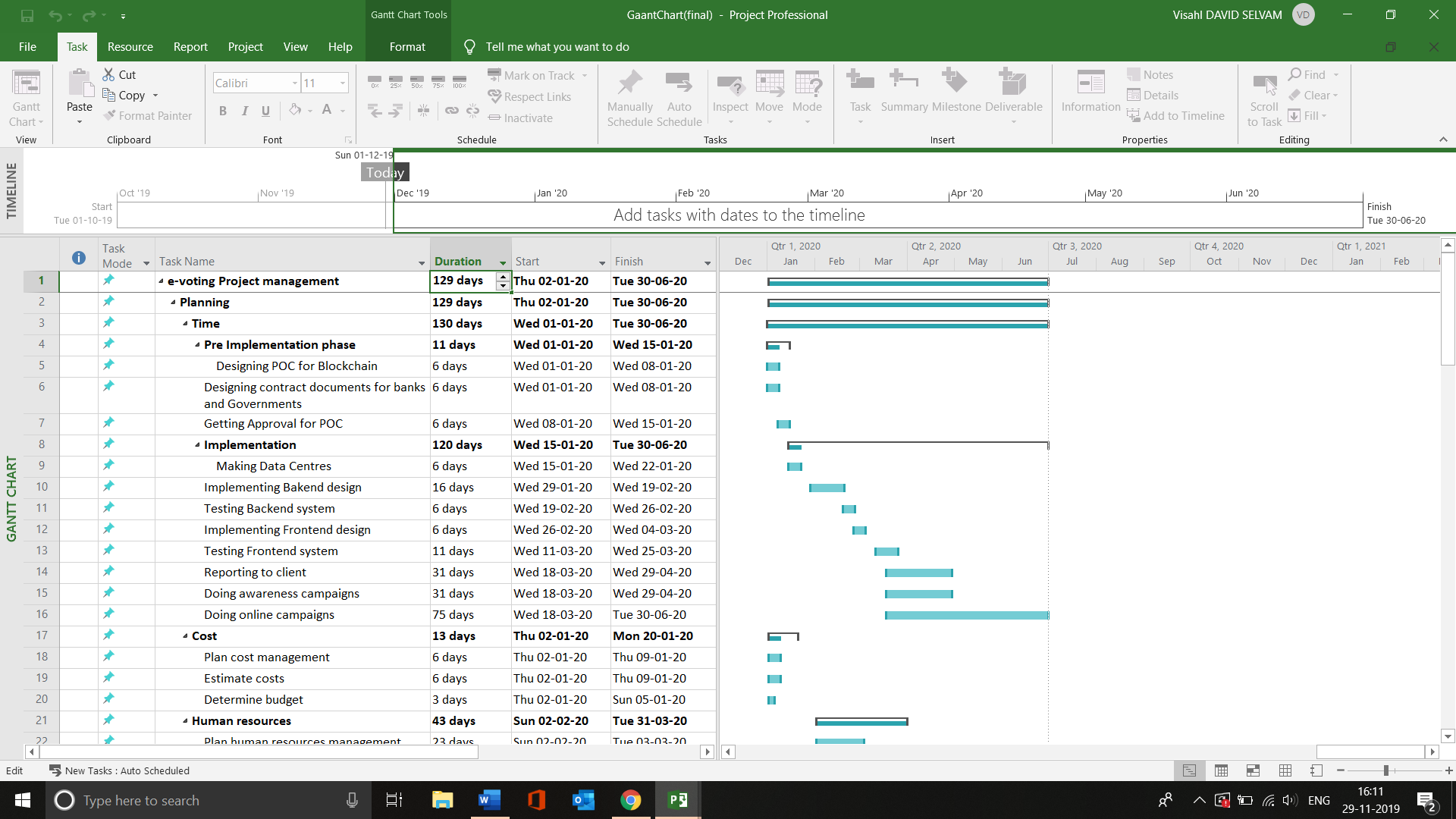
If stake holder likes to add few activities that are not present in WBS then the stake holder must fill a request form. Also, the requests will be analyzed and taken in account only if they are valid/purposeful.

# Incorporating with existing system

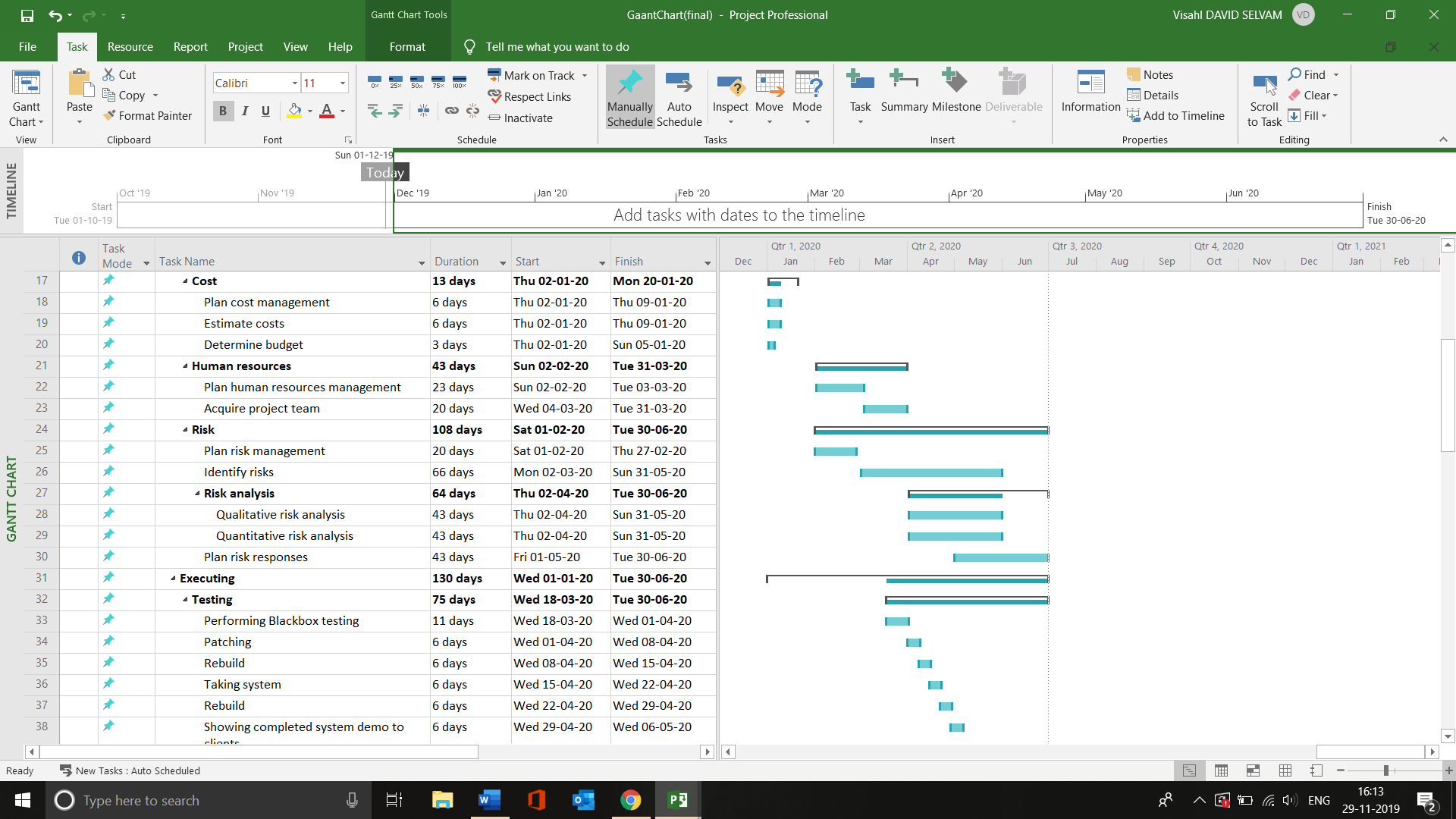
As mentioned previously in our proposal part we are utilizing Customer Data Right (CDR) legislation passed by the Australian parliament in August 2019 (Mekebeb, 2019). With this bill the bank can share their existing user data to us.

# Gantt Chart

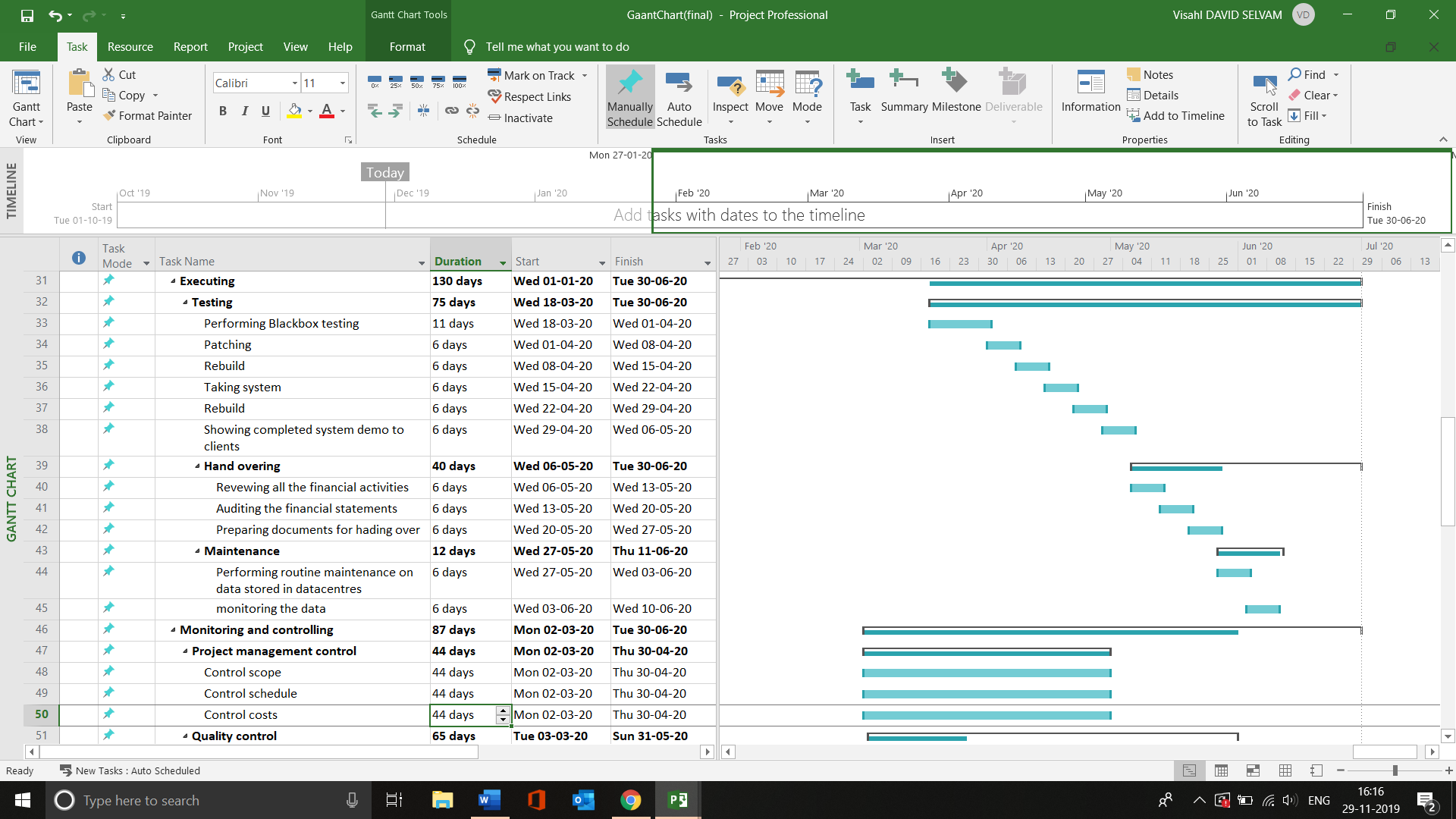
|  |  |  |  |
| --- | --- | --- | --- |
| Task Name | Duration | Start Date | End Date |
| **1.0. e-voting Project** | **129 days** | **Jan 02** | **Jun 30** |
| **2.0. Planning** | **129 days** | **Jan 02** | **Jun 30** |
| **2.1. Time** | **130 days** | **Jan 01** | **Jun 30** |
| **2.1.1. Pre- Implementation phase** | **11 days** | **Jan 01** | **Jan 15** |
| 2.1.1.1. Designing POC for Blockchain | 6 days | Jan 01 | Jan 08 |
| 2.1.1.2. Designing contract documents  for banks and Governments | 6 days | Jan 01 | Jan 08 |
| 2.1.1.3. Getting Approval for POC | 6 days | Jan 08 | Jan 15 |
| **2.1.2 Implementation** | **120 days** | **Jan 15** | **Jun 30** |
| 2.1.2.1. Making Data Centres | 6 days | Jan 15 | Jan 22 |
| 2.1.2.2. Implementing Backend design | 16 days | Jan 29 | Feb 19 |
| 2.1.2.3. Testing Backend system | 6 days | Feb 19 | Feb 26 |
| 2.1.2.4. Implementing Frontend design | 6 days | Feb 26 | Mar 04 |
| 2.1.2.5. Testing Frontend system | 11 days | Mar 11 | Mar 25 |
| 2.1.2.6. Reporting to client | 31 days | Mar 18 | Apr 29 |
| 2.1.2.7. Doing awareness campaigns | 31 days | Mar 18 | Apr 29 |
| 2.1.2.8. Doing online campaigns | 75 days | Mar 18 | Jun 30 |
| **2.2. Cost** | **13 days** | **Jan 02** | **Jan 20** |
| 2.2.1. Plan cost management | 6 days | Jan 02 | Jan 09 |
| 2.2.2. Estimate costs | 6 days | Jan 02 | Jan 09 |
| 2.2.3. Determine budget | 3 days | Jan 02 | Jan 05 |
| **2.3. Human resources** | **43 days** | **Feb 02** | **Mar 31** |
| 2.3.1. Plan human resources management | 23 days | Feb 02 | Mar 03 |
| 2.3.2. Acquire project team | 20 days | Mar 04 | Mar 31 |
| **2.4. Risk** | **108 days** | **Feb 01** | **Jun 30** |
| 2.4.1. Plan risk management | 20 days | Feb 01 | Feb 27 |
| 2.4.2. Identify risks | 66 days | Mar 02 | May 31 |
| **2.5. Risk analysis** | **64 days** | **Apr 02** | **Jun 30** |
| 2.5.1. Qualitative risk analysis | 43 days | Apr 02 | May 31 |
| 2.5.2. Quantitative risk analysis | 43 days | Apr 02 | May 31 |
| 2.5.3. Plan risk responses | 43 days | May 01 | Jun 30 |
| **3.0. Executing** | **130 days** | **Jan 01** | **Jun 30** |
| **3.1. Testing** | **75 days** | **Mar 18** | **Jun 30** |
| 3.1.1. Performing Blackbox testing | 11 days | Mar 18 | Apr 01 |
| 3.1.2. Patching | 6 days | Apr 01 | Apr 08 |
| 3.1.3. Rebuild | 6 days | Apr 08 | Apr 15 |
| 3.1.4. Taking system | 6 days | Apr 15 | Apr 22 |
| 3.1.5. Rebuild | 6 days | Apr 22 | Apr 29 |
| 3.1.6. Showing completed system demo  to clients | 6 days | Apr 29 | May 06 |
| **3.2. Hand overring** | **40 days** | **May 06** | **Jun 30** |
| 3.2.1. Reviewing all the financial activities | 6 days | May 06 | May 13 |
| 3.2.2. Auditing the financial statements | 6 days | May 13 | May 20 |
| 3.2.3. Preparing documents  for handing over | 6 days | May 20 | May 27 |
| **3.3. Maintenance** | **12 days** | **May 27** | **Jun 11** |
| 3.3.1. Performing routine maintenance  on data stored in datacentres | 6 days | May 27 | Jun 03 |
| 3.3.2. monitoring the data | 6 days | Jun 03 | Jun 10 |
| **4.0. Monitoring and controlling** | **87 days** | **Mar 02** | **Jun 30** |
| **4.1. Project management control** | **44 days** | **Mar 02** | **Apr 30** |
| 4.1.1. Control scope | 44 days | Mar 02 | Apr 30 |
| 4.1.2. Control schedule | 44 days | Mar 02 | Apr 30 |
| 4.1.3. Control costs | 44 days | Mar 02 | Apr 30 |
| **4.2. Quality control** | **65days** | **Mar 03** | **May 31** |
| 4.2.1. Control quality | 18 days | Mar 03 | Mar 26 |
| 4.2.2. Control risk | 43 days | Mar 03 | Mar 26 |
| 4.2.3. Control procurements | 44 days | Apr 01 | May 31 |
| **5.0. Closing** | **43 days** | **May 01** | **Jun 30** |
| 5.0.1. Deliver products | 15 days | May 01 | May 21 |
| 5.0.2. Close procurements | 28 days | May 23 | Jun 30 |
| 5.0.3. Update process assets | 22 days | Jun 01 | Jun 30 |
|  |  |  |  |
|  |  |  |  |
| **E-voting group Project** | **39 days** | **Oct 08** | **Nov 29** |
| **Stage 1** | **36 days** | **Oct 08** | **Nov 26** |
| Form project team | 1 day | Oct 08 | Oct 08 |
| Select project manager | 1 day | Oct 11 | Oct 11 |
| Create team contract | 1 day | Nov 04 | Nov 04 |
| In/Out of scope table | 6 days | Nov 04 | Nov 10 |
| Create WBS / WBS dictionary | 21 days | Oct 11 | Nov 08 |
| Team meeting | 1 day | Oct 11 | Oct 11 |
| Stage 1 progress report | 5 days | Nov 04 | Nov 08 |
| **Stage 2** | **31 days** | **Oct 16** | **Nov 27** |
| Define scope | 6 days | Nov 01 | Nov 08 |
| Develop project charter | 18 days | Oct 16 | Nov 08 |
| HR requirements table | 2 days | Nov 16 | Nov 18 |
| Team meeting | 1 day | Oct 18 | Oct 18 |
| Stage 2 progress report | 6 days | Nov 11 | Nov 18 |
| **Stage 3** | **26 days** | **Oct 25** | **Nov 29** |
| Scope Control | 8 days | Oct 25 | Nov 05 |
| Validate scope | 8 days | Oct 25 | Nov 05 |
| Risk assessment table | 5 days | Nov 21 | Nov 27 |
| Team meeting | 1 day | Oct 25 | Oct 25 |
| Stage 3 progress report | 6 days | Nov 16 | Nov 22 |
| **Stage 4** | **21 days** | **Nov 01** | **Nov 29** |
| Project costs breakdown table | 15 days | Nov 05 | Nov 24 |
| Gantt chart w/ milestones & deliverables | 16 days | Nov 04 | Nov 23 |
| Team meeting | 1 day | Nov 01 | Nov 01 |
| Stage 4 progress report | 6 days | Nov 23 | Nov 29 |
| **Final proposal** | **8 days** | **Nov 20** | **Nov 29** |
| Presentation | 1 day | Nov 20 | Nov 20 |
| Submit final proposal | 1 day | Nov 29 | Nov 29 |



Screenshot 3 Gantt chart



Screenshot 4 Gantt chart (cont...)



Screenshot 5 Gantt chart (cont...)

Given screenshots 3,4,5 shows Gannt chart view in the form of graph.

# Time Management

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Time Management for e-voting system (1st January to 30th June 2020) | | | | | |
| No | | | Activity | Plan Start (week) | Plan Duration(week) |
| 1 |  |  | **Pre implementation phase** |  |  |
|  | 1.1 |  | Designing POC for Blockchain | 1 | 1 |
|  | 1.2 |  | Designing contract documents for banks and Governments | 1 | 1 |
|  | 1.3 |  | Getting Approval for POC | 2 | 1 |
| 2 |  |  | **Implementation** |  |  |
|  | 2.1 |  | Technical |  |  |
|  |  | 2.1.1 | Making Data Centres ready according to ISO standards | 3 | 1 |
|  |  | 2.1.2 | Implementing Backend design | 5 | 3 |
|  |  | 2.1.3 | Testing Backend system with duplicate data | 8 | 1 |
|  |  | 2.1.4 | Implementing Frontend design | 9 | 2 |
|  |  | 2.1.5 | Testing Frontend System with duplicate data | 11 | 1 |
|  | 2.2 |  | Business |  |  |
|  |  | 2.2.1 | Reporting to client once in a week | 12 | 6 |
|  |  | 2.2.2 | Doing awareness campaigns (offline) every weekend | 12 | 11 |
| 3 |  |  | **Post implantation** |  |  |
|  | 3.1 |  | Testing |  |  |
|  |  | 3.1.1 | Performing Blackbox testing on both Front-end and Back-end | 12 | 2 |
|  |  | 3.1.2 | Patching if any vulnerabilities found | 14 | 1 |
|  |  | 3.1.3 | Rebuild if it’s necessary | 15 | 1 |
|  |  | 3.1.4 | Taking system live in testing phase to get user experience | 16 | 1 |
|  |  | 3.1.5 | Rebuild if it’s necessary | 17 | 1 |
|  |  | 3.1.6 | Showing completed system demo to clients | 18 | 1 |
|  | 3.2 |  | Hand Over |  |  |
|  |  | 3.2.1 | Reviewing all the financial activities | 19 | 1 |
|  |  | 3.2.2 | Auditing the financial statements | 20 | 1 |
|  |  | 3.2.3 | Preparing documents for handing over | 21 | 1 |
|  |  |  | **Maintenance** |  |  |
|  |  | 3.2.4 | Performing routine maintenance on data stored in data centres | 22 | 1 |
|  |  | 3.2.5 | Actively monitoring the data | 23 | 1 |

# Cost Management

|  |  |
| --- | --- |
| **Cost Management ($400 of Overall Budget)** | |
| Activity | Cost |
| **1.0. Voter who eligible to vote** | 17 million(persons) x $10 = 170 million |
| 1.1. Currently Total budget | $400 - $170 = $230 million |
| **2.0. Human Resource** |  |
| 2.1. Developers (20persons) | Each person = $15000  => $15000 x 20 x 6months = 1.8 million |
| 2.2. Testing & SOC  (Security of Centre) | Testing: (each) $10000 x 10 (persons) x 6 (months)  = $600000  SOC: $5000 (each) x 10 (persons) x 6 (months)  = $300000  => Testing + SOC = 0.9 million |
| 2.3. Business Managers  (10 persons) | $10000 (each) x 10 (persons) x 6 (months) = $600000 |
| **3.0. Plan Activity** |  |
| 3.1. Hiring Office | $3 million |
| 3.2. Data Centres &  Physical Infrastructure | $140million |
| 3.3. Implementing Backend  & Frontend Design | $30million |
| 3.4. Blackbox Testing Backend  & Frontend Design | $5million |
| 3.5. Offline and Online Advertise Campaigns | $ 10 million |
| 3.6. Maintenance | $ 20 million |
| **4.0. Cost Estimate** |  |
| 4.1. Total for the project | $208.3 million |
| 4.2. Emergency for the Project | $21.7 million |

# Human Resource Management

**Improve employees hiring process**

We build the project with well-experienced professionals’ employees and willing to stay to end of the project. Make each other friendly so that each employee will be motivated therefore will be more productive. Invest some time in pre-employment, check their communication skills, inaccuracy report information or criminal histories.

**Train the employees**

To make the employees work happy and satisfy, provide them the opportunities with their personal and professional developments. Since they improved their skills, they can support for the project efficiently. Make employee appraisals to each other to improve the skills for the employees.

**Make clear about the expectations**

Make a set of straightforward rules that should be respected by every employee. If one of them have trouble with the expectations, make him/her feel free to tell the consequences of the behaviour, firm and determine about it.

**Work on reward programs**

For some, punishment is the way to motivate people. At here, reward programs are much better way to motivate the employees. Reward them for the good job so that we can expect more quality and productivity in the project.

# Project Methodologies integration

For this project management, we integrated traditional and agile methodologies.

|  |  |
| --- | --- |
| **Activity** | **Methodology (project management)** |
| Pre-Implementation Phase | Traditional |
| Implementation | Agile |
| Post Implantation | Both |

**Traditional Project Management**

Usually it follows a fixed sequence, so once one stage is completed, only next one should start. This method is more suitable for only a few changes from begin to end. If there are some unexpected obstacles, individuals should deliver the problems to their managers. However, it could be caused delays and exceed the estimated time limit, because it is hard to approach manager every time.

**Agile Project Management**

This project is for software development, and the teams focus on the increasing efficiency instead of planning the whole project in advance. The benefits of Agile are that engage stakeholder, delivery is earlier and predictable and cost and schedule as well. Also, it allows for change and focuses on business value and users so that make quality improvement. The team of agile must decide by themselves. They solve all of issues to avoid wasting time.

# Risks

## Risk Matrix

Risk Matrix or likelihood against the consequence’s severity. It may assist the management decision making and increase the visibility of risks.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Probability** |  | **Consequences** | | | | | |
|  |  |  | **Insignificant** | **Minor** | **Moderate** | **Major** | **Severe** |
| **80-100**% | **Likelihood** | Very high probability | Low | Medium | High | Extreme | Extreme |
| **61-80%** | High Probability | Low | Medium | High | High | Extreme |
| **41-60%** | Equal Probability | Low | Medium | Medium | High | High |
| **21-40%** | Low Probability | Low | Low | Medium | Medium | High |
| **1-20%** | Too low  probability | Low | Low | Medium | Medium | High |

## Weigh Factor Analysis

|  |  |  |  |
| --- | --- | --- | --- |
| **Weigh factor** | **Risk Level** | **Consequence** | **Action** |
| 70% - 100% | High/ Extreme | Imminent danger or serious | -Combat of the risk perform the immediate measurement.  -Reduce risk to a reasonable low level by identifying and imposing controls. |
| 40% - 70% | Medium | Moderate danger | The risk should be implemented as fast as you can, but immediate action is not necessary |
| 10% - 40% | Low | less danger/ Negligible danger | Do preventative steps and mitigate the risk. |

## Risk register priorities (TOP 10)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk** | **Likelihood** | **Consequence (impact)** | **Countermeasure** | **Weigh Factor** |
| Corrupted Data from bank  -Technical issues while transferring the data | Medium | High | Conducting Integrity check | 90% |
| Project Scope Risks  -Scope is not well structured | Medium | High | All employees discuss together and understand the nature of the project | 85% |
| Project Management Risks  -Poor decision making of project manager | Low | High | Finding Skilful or experienced project manager. | 80% |
| Planning Risks  - Poor scheduling the plans | Medium | High | Organize and prioritize the tasks | 80% |
| Technical Risks  - Technology hardware used in data centre are not stable  - Unexperienced developers | Medium | High | -Make a good infrastructure of the system and experienced workers.  - train the employees | 80% |
| Security Risks  -Vulnerabilities to hack | Low | High | -Testing and fix each of the tasks | 75% |
| Budget Risks  -Hardware/ employees cost too high | Medium | High | -Train the Human resources | 70% |
| Government Risks  -Making contracts between government and banks | Low | High | -understand the law, legal & policies in the contracts between governments and | 70% |
| Threat Risks  - Copyright or privacy infringement | Low | High | - understand the law, legal & policies. | 70% |
| Business Risks  - wrong targets/ poor advertising online. | Medium | Medium | Set the right targets using SEO system. | 60% |

|  |  |
| --- | --- |
| **Risk No** | **Risk** |
| **R11** | The requirements are given very complex |
| **R12** | Requirements may change during the project from the government |
| **R13** | Some of the scope’s tasks may not identify all the deliverables |
| **R14** | Scope is not well structured |
| **R15** | Project methodologies integration would be complex |
| **R16** | Management systems may be inadequate to implement the project |
| **R17** | Poor decision making of project manager |
| **R18** | Some significant tasks may miss from project schedule |
| **R19** | Project dependencies risks (Finish to Start, Finish to Finish, …) |
| **R20** | Project strategy risks |
| **R21** | Reputational risks |
| **R22** | Quality risks |
| **R23** | Senior level of developers may hard to find |
| **R24** | Expected level of Business Managers may hard to find |
| **R25** | Experienced SOC analysts may hard to find |
| **R26** | No resource planning |
| **R27** | Poor communication in team |
| **R28** | Each of the employee fail to take responsibilities |
| **R29** | Some of the employees are corrupt |
| **R30** | Employees turnover |
| **R31** | Developers may misunderstand the user’s requirement |
| **R32** | Costs are not well identified |
| **R33** | Budgets estimations different too much |
| **R34** | Poor scheduling the plans |
| **R35** | Poor planning of risk management |
| **R36** | Data Centre place hiring delay |
| **R37** | Internal Infrastructure risk |
| **R38** | Unexpected equipment failure |
| **R39** | Specifications are unclear to the developers |
| **R40** | Unexperienced developers |
| **R41** | Backend design errors |
| **R42** | Frontend design |
| **R43** | Server down |
| **R44** | the design incomplete or infeasible |
| **R45** | Blackbox testing aren’t well-tested |
| **R46** | The vulnerabilities aren’t well-patched |
| **R47** | Devices that are linked to the system is not secure |
| **R48** | Result is not meet with expected performance |
| **R49** | GUI is not friendly to the users |
| **R50** | Compromise the user’s information |
| **R51** | Some users may not like the technology used in system |
| **R52** | compromising the design of the system |
| **R53** | Vulnerabilities to hack |
| **R54** | Susceptibility to fraud |
| **R55** | Malicious software programming |
| **R56** | Physical securities of machines |
| **R57** | Accuracy in capturing voter’s intent |
| **R58** | Secure storage of cast votes |
| **R59** | Hardware components cost are high |
| **R60** | Data centre rental fees too high |
| **R61** | Doing offline and online advertisements cost over limit |
| **R62** | Exchange rate going too high during the project |
| **R63** | No follow up the schedule |
| **R64** | Poor use from historical records for estimates |
| **R65** | Missing tasks and tasks dependencies |
| **R66** | Insufficient of monitoring the whole process |
| **R67** | Over optimistic in tasks and time scheduling |
| **R68** | Poor data collecting the process |
| **R69** | Formal time reporting |
| **R70** | Integration of technology |
| **R71** | Integration of processes |
| **R72** | Integration of information |
| **R73** | Integration of organizations or departments |
| **R74** | Slow budget approval may delay process |
| **R75** | Software Technicians leave before the project finish |
| **R76** | Hiring process taking so long |
| **R77** | Technicians unfamiliar with current technology |
| **R78** | The places are hard to find for doing offline campaign |
| **R79** | Poor advertising in offline campaign |
| **R80** | Wrong targets/ poor advertising online |
| **R81** | Facilities for customers are not enough |
| **R82** | Reputational risk |
| **R83** | Market risk |
| **R84** | Health & safety of employees doing offline campaigns |
| **R85** | Making contracts within government and banks |
| **R86** | Government may ask for changes after implementation |
| **R87** | The approval for POC is delay |
| **R88** | Regulatory or Legal is changed |
| **R89** | Political factors may influence to project |
| **R90** | Electricity goes off |
| **R91** | Copyright or privacy infringement |
| **R92** | Deviation of quality (WAN, ISP, Power Outage) |
| **R93** | Forces of nature (Flood, Fire, Earthquake) |
| **R94** | Unauthorize data collection or access |
| **R95** | Human error (employee accidents) |
| **R96** | Information extortion from external |
| **R97** | Destruction of information or system |
| **R98** | Technical hardware errors |
| **R99** | Technical software errors |
| **R100** | Theft of information |
| **R101** | Voters may not have their own device |
| **R102** | Voters may not have internet access |
| **R103** | Voters may compromise their identity when malware have |
| **R104** | Server cannot control to all the voters |
| **R105** | Users forget their login information |
| **R106** | Users may not receive One Time Password (OTP) |
| **R107** | Old people don’t know how to use |
| **R108** | Terrorist attack on data centres |

# Recommendations

* Apart from all the 4 big banks requesting other small banks to promote the e-vote concept would be recommended.
* Encouraging voters share their point of view to us is recommended so that, we can try to understand end-users need and activities can be modified based on them.
* The reason for not choosing any other methods like cloud, or traditional database it due to their security issues than comparing with blockchain method.

# References

al., e. (2012). 11.2 Risk Management Process. Retrieved 29 November 2019, from <https://pm4id.org/chapter/11-2-risk-management-process/>

Ami Rojkes Dombe. (2019). Moscow Blockchain Voting System Hacked in 20 Minutes | Israel Defense. Retrieved 29 November 2019, from <https://www.israeldefense.co.il/en/node/39852>

Aqeel, K., Kuldip, S., & Sandeep, S. (2010). Implementation of Elliptic Curve Digital Signature Algorithm. *International Journal Of Computer Applications (0975 – 8887)*, *Volume 2 – No.2*.

Crisitine, F. (2018). How to Improve a Human Resources Department. Retrieved 29 November 2019, from <https://www.trainingzone.co.uk/community/blogs/cristinefelt/how-to-improve-a-human-resources-department>

Election Canada. A Comparative Assessment of Electronic Voting - Elections Canada. Retrieved 29 November 2019, from <https://www.elections.ca/content.aspx?section=res&dir=rec/tech/ivote/comp&document=benefit&lang=e>

Mekebeb, T. (2019). New customer data legislation paves way for open banking in Australia. Retrieved 29 November 2019, from <https://www.businessinsider.com/australia-kick-starts-open-banking-2019-8?IR=T>

Sharon, C., & Gari, S. (2018). Top 6 technical advantages of Hyperledger Fabric for blockchain networks. Retrieved 29 November 2019, from <https://developer.ibm.com/articles/top-technical-advantages-of-hyperledger-fabric-for-blockchain-networks>

Spacey, J. (2017). 20 Types of Business Risk. Retrieved 29 November 2019, from <https://simplicable.com/new/business-risk>

Yatin, P. (2017). What is the difference between Traditional and Agile Project Management | UpRaise. Retrieved 29 November 2019, from <https://upraise.io/blog/traditional-vs-agile-project-management-3/>

Lavanya, N. & Malarvizhi, T. (2008). Risk analysis and management: a vital key to effective project management. Paper presented at PMI® Global Congress 2008—Asia Pacific, Sydney, New South Wales, Australia. Newtown Square, PA: Project Management Institute