Security application development for Equifax

**Table of Contents**

[1. Executive summary 3](#_Toc532038197)

[1.1 Background 3](#_Toc532038198)

[1.2 Problem 3](#_Toc532038199)

[1.3 Objectives 3](#_Toc532038200)

[1.4 Overall goal of the project including duration and budget 3](#_Toc532038201)

[1.5 Critical assumption 4](#_Toc532038202)

[2. Scope management 4](#_Toc532038203)

[2.1 Project scope statement 4](#_Toc532038204)

[2.2 Project deliverables 5](#_Toc532038205)

[2.3 Work breakdown structure 6](#_Toc532038206)

[2.4 WBS Dictionary 8](#_Toc532038207)

[3. Stakeholder management 9](#_Toc532038208)

[4. Time management 11](#_Toc532038209)

[4.2 Project schedule analysis 16](#_Toc532038210)

[5. Cost management 20](#_Toc532038211)

[Work element costing 20](#_Toc532038212)

[Constraints in project cost management 22](#_Toc532038213)

[5.2 Project cost budgeting and control 23](#_Toc532038214)

[6. Human resource management 24](#_Toc532038215)

[6.1 Project human resource planning 24](#_Toc532038216)

[6.2 Human resource estimation 25](#_Toc532038217)

[7. Quality management 27](#_Toc532038218)

[7.1 Project quality planning 27](#_Toc532038219)

[7.2 Project quality assurance 28](#_Toc532038220)

[8. Communication plan 29](#_Toc532038221)

[8.1 Project communication planning 29](#_Toc532038222)

[8.2 Stakeholder communication and requirement analysis 29](#_Toc532038223)

[9. Risk management 30](#_Toc532038224)

[9.1 Project risk management planning 30](#_Toc532038225)

[9.2 Risk identification 31](#_Toc532038226)

[9.3 Qualitative and quantitative risk analysis 31](#_Toc532038227)

[9.4 Risk prioritization 32](#_Toc532038228)

[9.5 Risk response plan 33](#_Toc532038229)

[Bibliography 34](#_Toc532038230)

# 1. Executive summary

## 1.1 Background

The organization “Equifax” which is one of the consumer reporting agencies that generally involves in combining analytics, robust data as well as advanced technology in order to provide proper actionable insights to businesses. It is found that the organization faces number of security challenges in managing their data and information and therefore they want to develop proper security application.

## 1.2 Problem

The organization “Equifax” faces number of security challenges in managing its organisational operations and the issues mainly include cybersecurity breaches, hacking of data and more. In order to resolve this issue, it is very much necessary to develop security application within the organization.

## 1.3 Objectives

The objectives of the project are listed below:

* To develop security application development
* To manage security challenges

## 1.4 Overall goal of the project including duration and budget

The main goal of the project is to develop proper security application within the organization so that security related challenges can be resolved. It is found that in order to finish the project successfully it is quite necessary to finish the project within 111 days by utilizing budget of around $91,760.

## 1.5 Critical assumption

The critical assumption is mainly elaborated below:

* The entire project will be completed successfully within 111 days
* The project will be finished within the budget that is around $91,760
* The project will follow the scope of the project.

# 2. Scope management

## 2.1 Project scope statement

The paper mainly reflects on the organization “Equifax” which is one of the consumer reporting agencies that mainly faces number of security related challenges due to the unavailability of proper application security. In order to resolve this issue, the organization wants to develop security application for the organization in order to protect the organization from external threats. It is found that by getting a loan, by developing the system as well as by testing it for making the necessary changes it is found that security application system can be developed successfully. It is found that with the help of the application security, the organization will be able to maintain the confidentiality of the information

**Project characteristics and requirements**

The project characteristics as well as requirements which are mainly associated with the project are generally elaborated properly:

* The security application system is mainly needed within the organization in order to detect the complex vulnerabilities which are mainly not visible without the help of the source code.
* The system is mainly used in order to maintain the confidentiality of the information as well as data that is mainly stored within the organization.
* It is found that security application system generally assists in managing the sound market reputation by avoiding cybersecurity related issues and challenges.

**Project success criteria**

The success criteria of the project are generally elaborated below:

**Achieving project objectives:** It is found that if the objectives of the project are me successfully then it can be identified that the project which was undertaken is successful.

**Meeting deadlines and budget:** If the entire project is successfully completed within he expected budget and time then the project can be considered to be successful.

**Maintaining project quality:** If the proper quality of the project is maintained and the project quality id not compromised in achieving the deadline reveals that the project will be successful.

**Specific constraints in project scope statement**

The constraints in project scope statement are generally elaborated below:

**Time:** If the scope of the project is not followed then it would be quite difficult to finish the entire project on time which further increases the budget on the project.

**Budget:** It is quite necessary to complete the project within the approved budget so that the project manager does not face any type of financial challenges and issues.

# 2.2 Project deliverables

**Project management related deliverables**

The project management related deliverables of the project are generally listed below:

* Stakeholder analysis
* Scope statement
* Work breakdown structure
* Project scheduling
* Project quality checklist
* Risk management plan
* Risk register
* Progress report
* Schedule
* Presentation of project

**Product related deliverables**

The product related deliverables are listed below:

* Proper security
* Multiple security layers
* Privilege separation

## 2.3 Work breakdown structure

**Summary of the stages and their main tasks**

|  |  |
| --- | --- |
| **WBS** | **Task Name** |
| **0** | **Development of security application** |
| **1** | **Initiation phase** |
| 1.1 | Analyzing the needs of the business |
| 1.2 | Project plan |
| 1.3 | Feasibility analysis |
| 1.4 | Milestone 1: Completion of initiation phase |
| **2** | **Requirement analysis stage** |
| 2.1 | Employing use and misuse cases |
| 2.2 | Conducting security testing |
| 2.3 | Application of risk profile |
| 2.4 | Milestone 2: Completion of requirement analysis phase |
| **3** | **Design stage** |
| 3.1 | Least privilege |
| 3.2 | Privilege separation |
| 3.3 | Complete meditation |
| 3.4 | Multiple Security layers |
| 3.5 | Secure failure |
| 3.6 | User-friendly failure |
| **4** | **Development phase** |
| 4.1 | Secure development defend software |
| 4.2 | Secure coding practices |
| 4.3 | Development of security application |
| 4.4 | Milestone 3: Completion of development phase |
| **4.5** | **Code review** |
| 4.5.1 | Fixing vulnerabilities |
| 4.5.2 | Provide guidance about the vulnerabilities |
| **5** | **Testing phase** |
| 5.1 | Penetration testing |
| 5.2 | Testing of the software |
| 5.3 | Milestone 4: Completion of testing phase |
| **6** | **Production stages** |
| 6.1 | Creating incidence response plan |
| 6.2 | Security review |
| 6.3 | Achieving final product |
| 6.4 | Executing incidence response plan |
| 6.5 | Milestone 5: Completion of production phase |
| **7** | **Closure phase** |
| 7.1 | Project review |
| 7.2 | Stakeholder sign off |
| 7.3 | Documentation |
| 7.4 | Milestone 6: Completion of closure phase |

**Development of WBS**

## 2.4 WBS Dictionary

|  |  |  |
| --- | --- | --- |
| **Item** | **Item Name** | **Description** |
| 1 | Project plan | In this phase, entire project plan is developed that contains clear overview about the neds and requirements of the project. |
| 2 | Conducting security testing | Security testing is conducted in the requirement phase for identifying the security issue that the organization s facing |
| 3. | Multiple security layers | Multiple security layers are designed in order to provide proper security to the organization Equifax |
| 4. | Secure coding practices | Proper coding practices are used for developing the security applications effectively |
| 5. | Testing | Proper testing needs to be done in order to make sure that the system is working effectively. |
| 6. | Security review | Security review is done for ensuring that the security application is able to provide proper facility related security or not. |

# 3. Stakeholder management

**List of important stakeholders**

The list of stakeholders are listed below:

* Project manager
* Project planner
* Workers
* Designer
* IT manger
* IT tester
* Coder
* Reviewer

**Stakeholder register**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Position** | **Internal/external** | **Roles** |
| <Please Fill> | Project manager | Internal | Helps in managing the project. |
| <Please Fill> | Project planner | Internal | Creates proper project plan |
| <Please Fill> | Worker | Internal | Works so that the security application can be developed successfully. |
| <Please Fill> | Designer | Internal | Deigns the entire security application system |
| <Please Fill> | IT manager | Internal | Manages the development of security application |
| <Please Fill> | IT tester | Internal | Testing the application that was developed |
| <Please Fill> | Coder | Internal | Reviews the coding that are used |
| <Please Fill> | Reviewer | Internal | Reviews the entire project |

**Stakeholder management strategies**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Project manager | Developer | Tester | Designer |
| Name/ Organization | Equifax | Equifax | Equifax | Equifax |
| Level of Interest | High | High | High | High |
| Level of Influence/Power | High | High | Low | High |
| Current Engagement | Yes | Yes | Yes | Yes |

# 4. Time management

**Project schedule**

The schedule of the project is provided below:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **WBS** | **Task Name** | **Duration** | **Start** | **Finish** |
| **0** | **Development of security application** | **111 days** | **Mon 10-12-18** | **Mon 13-05-19** |
| **1** | **Initiation phase** | **10 days** | **Mon 10-12-18** | **Fri 21-12-18** |
| 1.1 | Analyzing the needs of the business | 3 days | Mon 10-12-18 | Wed 12-12-18 |
| 1.2 | Project plan | 4 days | Thu 13-12-18 | Tue 18-12-18 |
| 1.3 | Feasibility analysis | 3 days | Wed 19-12-18 | Fri 21-12-18 |
| 1.4 | Milestone 1: Completion of initiation phase | 0 days | Tue 18-12-18 | Tue 18-12-18 |
| **2** | **Requirement analysis stage** | **12 days** | **Mon 24-12-18** | **Tue 08-01-19** |
| 2.1 | Employing use and misuse cases | 4 days | Mon 24-12-18 | Thu 27-12-18 |
| 2.2 | Conducting security testing | 5 days | Fri 28-12-18 | Thu 03-01-19 |
| 2.3 | Application of risk profile | 3 days | Fri 04-01-19 | Tue 08-01-19 |
| 2.4 | Milestone 2: Completion of requirement analysis phase | 0 days | Tue 08-01-19 | Tue 08-01-19 |
| **3** | **Design stage** | **27 days** | **Wed 09-01-19** | **Thu 14-02-19** |
| 3.1 | Least privilege | 5 days | Wed 09-01-19 | Tue 15-01-19 |
| 3.2 | Privilege separation | 6 days | Wed 16-01-19 | Wed 23-01-19 |
| 3.3 | Complete meditation | 7 days | Thu 24-01-19 | Fri 01-02-19 |
| 3.4 | Multiple Security layers | 5 days | Mon 04-02-19 | Fri 08-02-19 |
| 3.5 | Secure failure | 4 days | Mon 11-02-19 | Thu 14-02-19 |
| 3.6 | User-friendly failure | 0 days | Thu 14-02-19 | Thu 14-02-19 |
| **4** | **Development phase** | **37 days** | **Fri 15-02-19** | **Mon 08-04-19** |
| 4.1 | Secure development defend software | 12 days | Fri 15-02-19 | Mon 04-03-19 |
| 4.2 | Secure coding practices | 10 days | Tue 05-03-19 | Mon 18-03-19 |
| 4.3 | Development of security application | 15 days | Tue 19-03-19 | Mon 08-04-19 |
| 4.4 | Milestone 3: Completion of development phase | 0 days | Mon 18-03-19 | Mon 18-03-19 |
| **4.5** | **Code review** | **7 days** | **Tue 19-03-19** | **Wed 27-03-19** |
| 4.5.1 | Fixing vulnerabilities | 4 days | Tue 19-03-19 | Fri 22-03-19 |
| 4.5.2 | Provide guidance about the vulnerabilities | 3 days | Mon 25-03-19 | Wed 27-03-19 |
| **5** | **Testing phase** | **7 days** | **Thu 28-03-19** | **Fri 05-04-19** |
| 5.1 | Penetration testing | 4 days | Thu 28-03-19 | Tue 02-04-19 |
| 5.2 | Testing of the software | 3 days | Wed 03-04-19 | Fri 05-04-19 |
| 5.3 | Milestone 4: Completion of testing phase | 0 days | Fri 05-04-19 | Fri 05-04-19 |
| **6** | **Production stages** | **15 days** | **Mon 08-04-19** | **Fri 26-04-19** |
| 6.1 | Creating incidence response plan | 4 days | Mon 08-04-19 | Thu 11-04-19 |
| 6.2 | Security review | 1 day | Fri 12-04-19 | Fri 12-04-19 |
| 6.3 | Achieving final product | 5 days | Mon 15-04-19 | Fri 19-04-19 |
| 6.4 | Executing incidence response plan | 5 days | Mon 22-04-19 | Fri 26-04-19 |
| 6.5 | Milestone 5: Completion of production phase | 0 days | Fri 26-04-19 | Fri 26-04-19 |
| **7** | **Closure phase** | **11 days** | **Mon 29-04-19** | **Mon 13-05-19** |
| 7.1 | Project review | 4 days | Mon 29-04-19 | Thu 02-05-19 |
| 7.2 | Stakeholder sign off | 3 days | Fri 03-05-19 | Tue 07-05-19 |
| 7.3 | Documentation | 4 days | Wed 08-05-19 | Mon 13-05-19 |
| 7.4 | Milestone 6: Completion of closure phase | 0 days | Mon 13-05-19 | Mon 13-05-19 |

**Important project milestones**

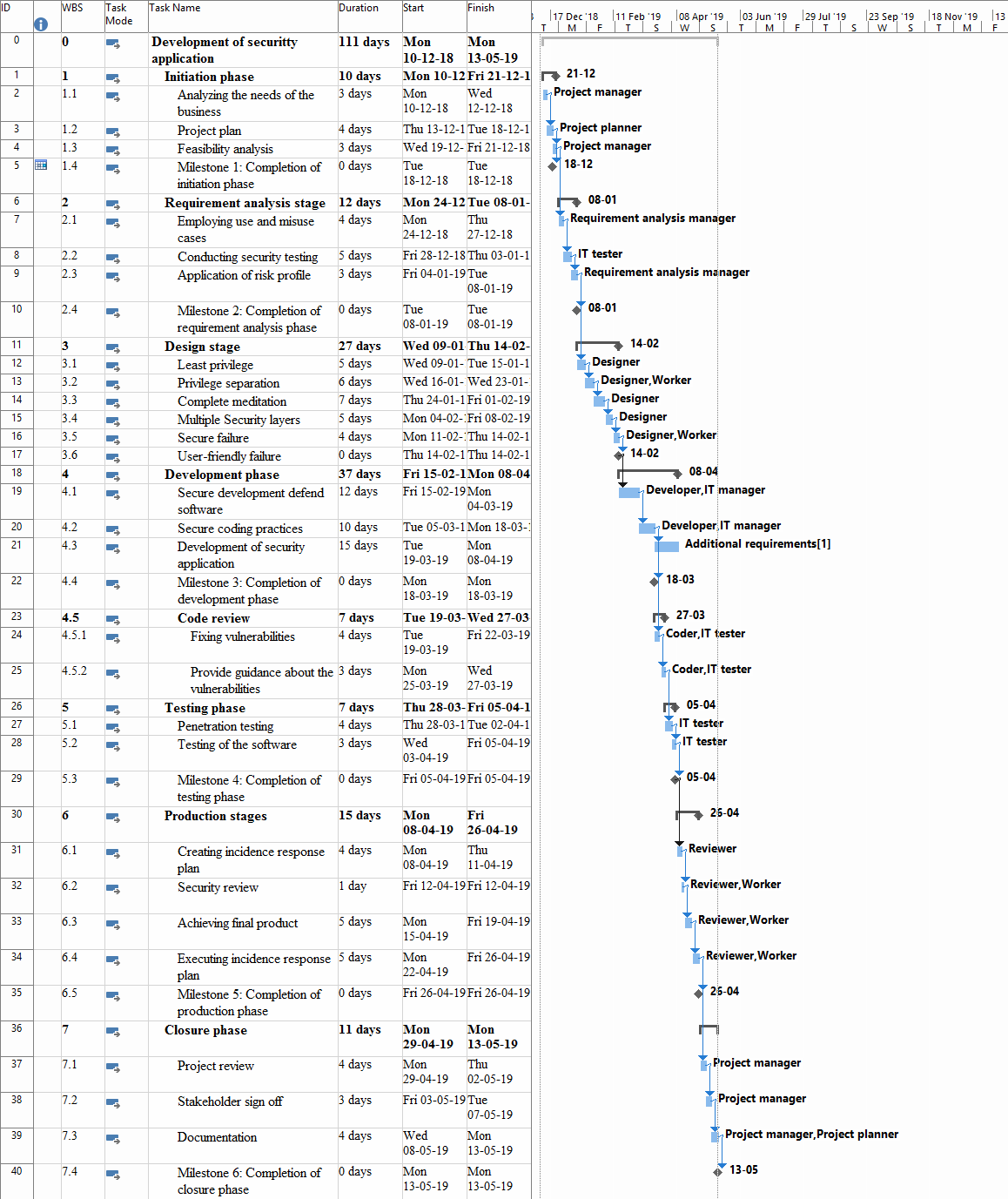
The important project milestones are given in the below table:

|  |  |
| --- | --- |
| **Milestone** | **Completion date** |
| Milestone 1: Completion of initiation phase | Tue 18-12-18 |
| Milestone 2: Completion of requirement analysis phase | Tue 08-01-19 |
| Milestone 3: Completion of development phase | Mon 18-03-19 |
| Milestone 4: Completion of testing phase | Fri 05-04-19 |
| Milestone 5: Completion of production phase | Fri 26-04-19 |
| Milestone 6: Completion of closure phase | Mon 13-05-19 |

**Specific constrains in time management**

It is found that the project needs to be completed within the time that is approved by following the project schedule and therefore sometimes, it become quite difficult to manage the time of the project as per the project schedule. However, if the project is not finished within the expected time then completion date of the project can be extended.

**Gantt chart**

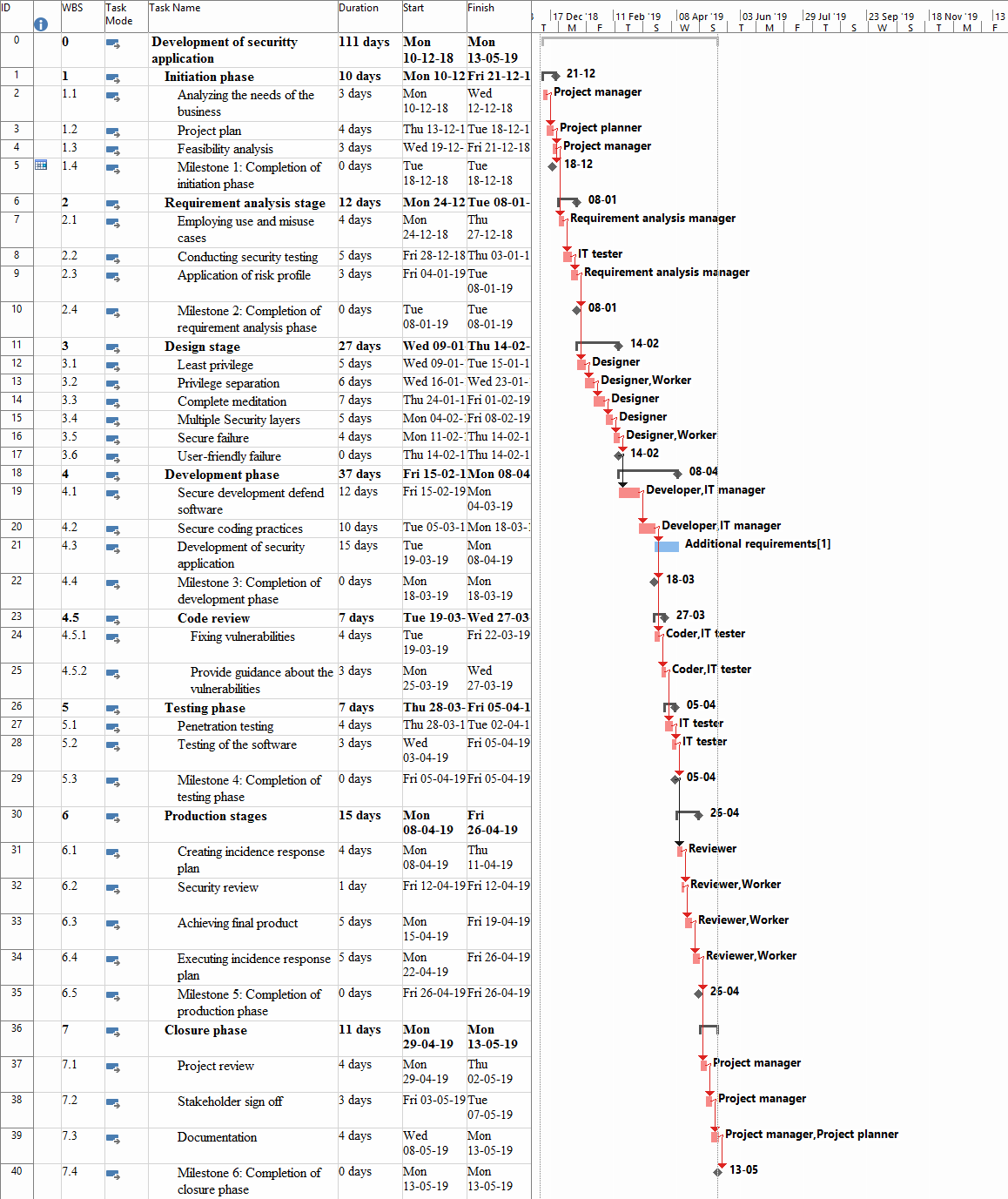
****

**Figure 1: Gantt chart**

(Source: Created by Author)

## 4.2 Project schedule analysis

**Critical path analysis**

****

**Figure 2: Critical path**

(Source: Created by Author)

**Project sack analysis and findings**

The table that is provided below reflects on the total slack of the project.

|  |  |  |  |
| --- | --- | --- | --- |
| **WBS** | **Task Name** | **Duration** | **Total Slack** |
| **0** | **Development of security application** | **111 days** | **0 days** |
| **1** | **Initiation phase** | **10 days** | **0 days** |
| 1.1 | Analyzing the needs of the business | 3 days | 0 days |
| 1.2 | Project plan | 4 days | 0 days |
| 1.3 | Feasibility analysis | 3 days | 0 days |
| 1.4 | Milestone 1: Completion of initiation phase | 0 days | 104 days |
| **2** | **Requirement analysis stage** | **12 days** | **0 days** |
| 2.1 | Employing use and misuse cases | 4 days | 0 days |
| 2.2 | Conducting security testing | 5 days | 0 days |
| 2.3 | Application of risk profile | 3 days | 0 days |
| 2.4 | Milestone 2: Completion of requirement analysis phase | 0 days | 89 days |
| **3** | **Design stage** | **27 days** | **0 days** |
| 3.1 | Least privilege | 5 days | 0 days |
| 3.2 | Privilege separation | 6 days | 0 days |
| 3.3 | Complete meditation | 7 days | 0 days |
| 3.4 | Multiple Security layers | 5 days | 0 days |
| 3.5 | Secure failure | 4 days | 0 days |
| 3.6 | User-friendly failure | 0 days | 0 days |
| **4** | **Development phase** | **37 days** | **0 days** |
| 4.1 | Secure development defends software | 12 days | 0 days |
| 4.2 | Secure coding practices | 10 days | 0 days |
| 4.3 | Development of security application | 15 days | 25 days |
| 4.4 | Milestone 3: Completion of development phase | 0 days | 40 days |
| **4.5** | **Code review** | **7 days** | **0 days** |
| 4.5.1 | Fixing vulnerabilities | 4 days | 0 days |
| 4.5.2 | Provide guidance about the vulnerabilities | 3 days | 0 days |
| **5** | **Testing phase** | **7 days** | **0 days** |
| 5.1 | Penetration testing | 4 days | 0 days |
| 5.2 | Testing of the software | 3 days | 0 days |
| 5.3 | Milestone 4: Completion of testing phase | 0 days | 0 days |
| **6** | **Production stages** | **15 days** | **0 days** |
| 6.1 | Creating incidence response plan | 4 days | 0 days |
| 6.2 | Security review | 1 day | 0 days |
| 6.3 | Achieving final product | 5 days | 0 days |
| 6.4 | Executing incidence response plan | 5 days | 0 days |
| 6.5 | Milestone 5: Completion of production phase | 0 days | 11 days |
| **7** | **Closure phase** | **11 days** | **0 days** |
| 7.1 | Project review | 4 days | 0 days |
| 7.2 | Stakeholder sign off | 3 days | 0 days |
| 7.3 | Documentation | 4 days | 0 days |
| 7.4 | Milestone 6: Completion of closure phase | 0 days | 0 days |

# 5. Cost management

## Work element costing

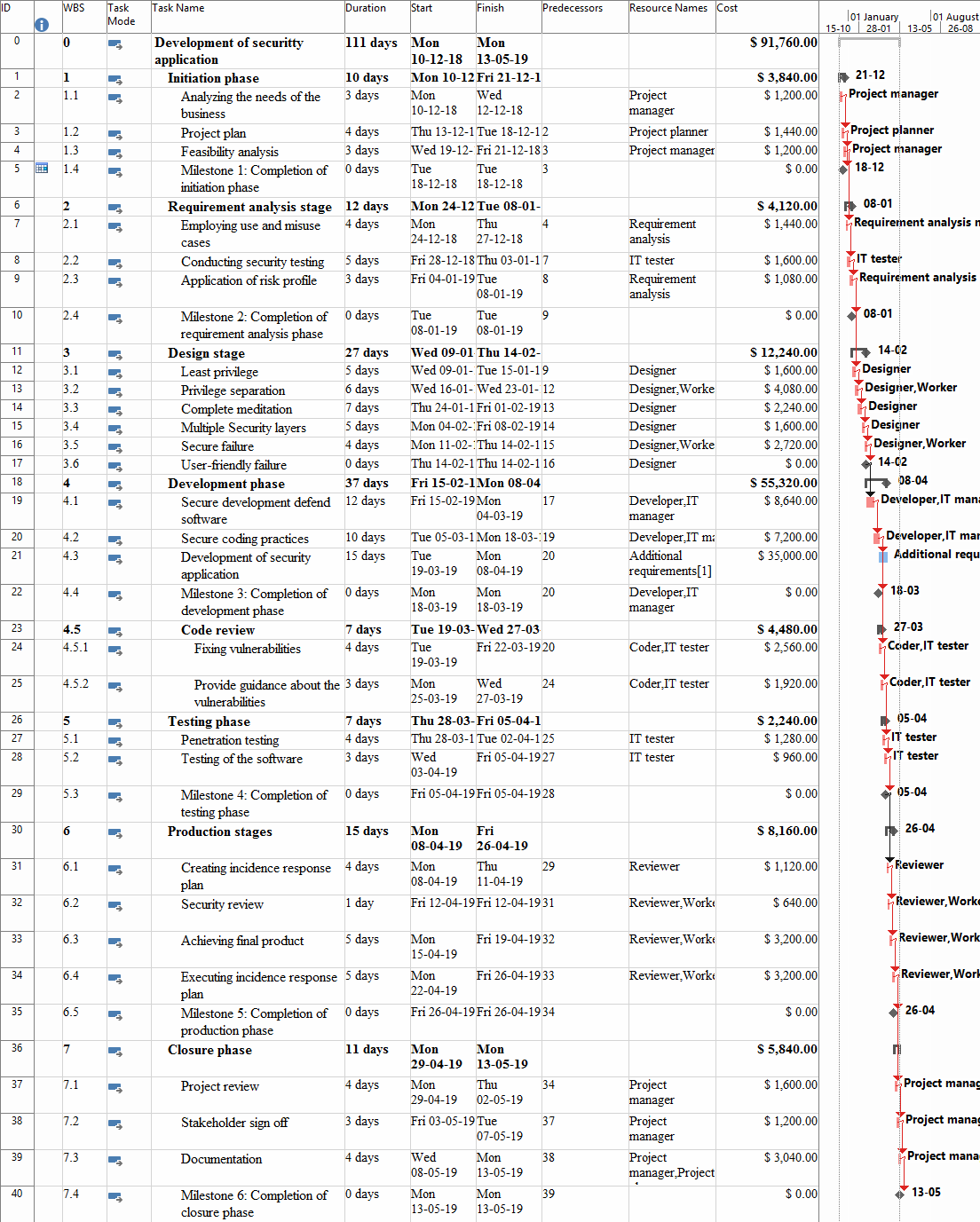
|  |  |  |  |
| --- | --- | --- | --- |
| **WBS** | **Task Name** | **Duration** | **Cost** |
| **0** | **Development of security application** | **111 days** | **$ 91,760.00** |
| **1** | **Initiation phase** | **10 days** | **$ 3,840.00** |
| 1.1 | Analyzing the needs of the business | 3 days | $ 1,200.00 |
| 1.2 | Project plan | 4 days | $ 1,440.00 |
| 1.3 | Feasibility analysis | 3 days | $ 1,200.00 |
| 1.4 | Milestone 1: Completion of initiation phase | 0 days | $ 0.00 |
| **2** | **Requirement analysis stage** | **12 days** | **$ 4,120.00** |
| 2.1 | Employing use and misuse cases | 4 days | $ 1,440.00 |
| 2.2 | Conducting security testing | 5 days | $ 1,600.00 |
| 2.3 | Application of risk profile | 3 days | $ 1,080.00 |
| 2.4 | Milestone 2: Completion of requirement analysis phase | 0 days | $ 0.00 |
| **3** | **Design stage** | **27 days** | **$ 12,240.00** |
| 3.1 | Least privilege | 5 days | $ 1,600.00 |
| 3.2 | Privilege separation | 6 days | $ 4,080.00 |
| 3.3 | Complete meditation | 7 days | $ 2,240.00 |
| 3.4 | Multiple Security layers | 5 days | $ 1,600.00 |
| 3.5 | Secure failure | 4 days | $ 2,720.00 |
| 3.6 | User-friendly failure | 0 days | $ 0.00 |
| **4** | **Development phase** | **37 days** | **$ 55,320.00** |
| 4.1 | Secure development defends software | 12 days | $ 8,640.00 |
| 4.2 | Secure coding practices | 10 days | $ 7,200.00 |
| 4.3 | Development of security application | 15 days | $ 35,000.00 |
| 4.4 | Milestone 3: Completion of development phase | 0 days | $ 0.00 |
| **4.5** | **Code review** | **7 days** | **$ 4,480.00** |
| 4.5.1 | Fixing vulnerabilities | 4 days | $ 2,560.00 |
| 4.5.2 | Provide guidance about the vulnerabilities | 3 days | $ 1,920.00 |
| **5** | **Testing phase** | **7 days** | **$ 2,240.00** |
| 5.1 | Penetration testing | 4 days | $ 1,280.00 |
| 5.2 | Testing of the software | 3 days | $ 960.00 |
| 5.3 | Milestone 4: Completion of testing phase | 0 days | $ 0.00 |
| **6** | **Production stages** | **15 days** | **$ 8,160.00** |
| 6.1 | Creating incidence response plan | 4 days | $ 1,120.00 |
| 6.2 | Security review | 1 day | $ 640.00 |
| 6.3 | Achieving final product | 5 days | $ 3,200.00 |
| 6.4 | Executing incidence response plan | 5 days | $ 3,200.00 |
| 6.5 | Milestone 5: Completion of production phase | 0 days | $ 0.00 |
| **7** | **Closure phase** | **11 days** | **$ 5,840.00** |
| 7.1 | Project review | 4 days | $ 1,600.00 |
| 7.2 | Stakeholder sign off | 3 days | $ 1,200.00 |
| 7.3 | Documentation | 4 days | $ 3,040.00 |
| 7.4 | Milestone 6: Completion of closure phase | 0 days | $ 0.00 |

## Constraints in project cost management

It is found that it is necessary to finish the entire project within the approved budget but if any scope creep occurs within the project, there will be requirement of additional budget for finishing the project. Thus, it is quite difficult to finish the project within budget if any scope creep occurs.

## 5.2 Project cost budgeting and control

**Integration of cost into Gantt chart**

****

**Figure 3: Integration of cost into Gantt chart**

(Source: Created by Author)

# 6. Human resource management

## 6.1 Project human resource planning

**Project organization chart**

Project manager

Project planner

Developer

IT manager

Designer

Tester

Reviewer

Worker

**Figure 4: Organizational chart**

(Source: Created by Author)

**Roles and responsibilities**

|  |  |
| --- | --- |
| **Roles** | **Responsibilities** |
| Project manager | The project manager is mainly responsible of managing the project quite successfully. |
| Project planner | They are generally responsible of developing the project plan. |
| Worker | Works so that the security application can be developed successfully. |
| Designer | Deigns the entire security application system |
| IT manager | They generally take the responsibility of finishing the project work |
| IT tester | Testing the application that was developed |
| Coder | They take the responsibility of checking the codes that are used for application development |
| Reviewer | They are responsible of reviewing the entire project successfully. |

**Specific constraints in human resource management**

It is found that the human resources who are engaged with the project are specific in number however, if project delay occurs and there will be a need of more stakeholders for finishing the project.

## 6.2 Human resource estimation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Resource Name** | **Type** | **Max. Units** | **Std. Rate** | **Base Calendar** |
| Project manager | Work | 100% | $ 50.00/hr | Standard |
| Project planner | Work | 100% | $ 45.00/hr | Standard |
| Requirement analysis manager | Work | 100% | $ 45.00/hr | Standard |
| Worker | Work | 100% | $ 45.00/hr | Standard |
| Designer | Work | 100% | $ 40.00/hr | Standard |
| Developer | Work | 100% | $ 45.00/hr | Standard |
| IT manager | Work | 100% | $ 45.00/hr | Standard |
| IT tester | Work | 100% | $ 40.00/hr | Standard |
| Coder | Work | 100% | $ 40.00/hr | Standard |
| Reviewer | Work | 100% | $ 35.00/hr | Standard |
|  |  |  |  |  |
| Additional requirements | Material |  | $ 35,000.00 |  |

**6.3 Resource loading and levelling**

It is found that after resource levelling, proper overview off resources are reflected with the help of diagram that is provided blow:

**Figure 5: Resource overview**

(Source: Created by Author)

# 7. Quality management

## 7.1 Project quality planning

**Introduction of quality goals**

The main quality goals are to complete the development of security application for the organization Equifax by maintaining the various quality standards.

**Quality metrics**

The quality metrics are listed below:

* Low failure rate
* High customer service
* Proper quality service
* Low defect rate

**Project quality checklist**

|  |  |  |
| --- | --- | --- |
| **Criteria** | **Yes/No** | **Remarks** |
| Does proper quality standards are followed in the project? | Yes | Yes, proper quality standards are followed |
| Does the project help in providing proper quality service? | Yes | Proper quality service is provided |
| Does the hardware that are used for developing the application security are good in quality? | Yes | Proper quality of hardware used |
| Does the client is satisfied with the development of new application software? | No | Client want some changes. |

**Roles and responsibilities**

It is found that the quality manager is mainly responsible of managing the quality of the project so that proper quality standards can be maintained within the project and the project can be completed within the assumed time and budget.

**Specific constraints**

It is quite necessary to follow proper quality standards however if budget shortfall occurs then it will be quite difficult to keep the same quality standards while executing the project.

## 7.2 Project quality assurance

**Quality assurance procedure**

Quality assurance procedure is mainly defied as one of the systematic process that helps in determining whether the security services that are provided with the development of security application are meeting the requirements or not.

**Quality assurance checklist**

|  |  |  |
| --- | --- | --- |
| **Criteria** | **Yes/No** | **Remarks** |
| Does proper quality assurance are maintained? | Yes | Yes, proper quality assurance is maintained |
| Does the standards as well as procedures refers to the material? | Yes | Yes, the standards generally refer to the consumer defined standards. |
| Does the standards and procedures are in place prior to the commencement of work? | Yes | Yes, standards and procedures are place prior to the tasks. |

# 8. Communication plan

## 8.1 Project communication planning

**Communication content and method**

The content on which communication will be done are elaborated below:

**Budget shortfall:** The budget related issues that occur within the project s discussed with the project manager and project sponsor by conducting a meeting.

**Progress report:** The progress report of the project is forwarded to the project manager in order to provide information about progress with the help of E-mail.

**Technical problem:** The technical problem that occur within the project due to improper design of the application will be discussed by undertaking a meeting with the project stakeholders

**Specific constraints**

If the workers of the project do not have proper communication channel then they will not be able to communicate their problems or views ad as a result due to the communication plan, project progress can be affected.

## 8.2 Stakeholder communication and requirement analysis

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Stakeholders | Document Name | Document Format | Contact Person | Due Date |
| Project leader | Progress report | Pdf file | Project manager | 08-12-18 |
| Financial manager | Financial report | Pdf File | Project manager | 20-1-19 |
| Project planner | Schedule | Ms project | Project manager | 08-12-18 |
| Comments: N/A | | | | |

# 9. Risk management

## 9.1 Project risk management planning

**Methodology**

It is found that number of methodologies are utilized within the risk management plan. It is identified that the methodologies are generally implemented in the prospects as well as concerns of the threats towards the success of the security application development.

**Roles and responsibilities**

The risk manager is mainly responsible of identifying, analyzing, as well as prioritizing the risks and challenges that are associated with the project. In addition to this, they are also responsible of providing proper response plan so that the risks and challenge can be mitigated quite easily.

## 9.2 Risk identification

**Risk categories**

The categories of the risks are listed below:

**Project risk:** If the schedule of the project is not managed then schedule slippage can occur.

**Budget risk:** If the entire project cannot be completed within budget then financial risk can occur.

**Technical risk**: If the design for the security application is not developed properly the technical risk can occur.

**Risk documentation**

It is found that proper risk documentation is generally created which generally contains proper information about the risk and challenges that are associated with the project. In addition to this, the risk documents contain proper information as well as details about the probability of occurrence as well as risk category.

## 9.3 Qualitative and quantitative risk analysis

**Probability/impact analysis**

Probability is generally dependent on the assessment of the risk manager with the help of the input that is provided by the team members.

|  |  |
| --- | --- |
| **Probability of occurrence** | **Risk category** |
| >70% | High |
| 30% to 70% | Medium |
| <30% | Low |

**Quantitative analysis**

Proper quantitative analysis is done on the risk in order to analyze the reason as well as cause of the project occurrence so that the project risk can be mitigated quite successfully.

## 9.4 Risk prioritization

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ranking** | **Name** | **Potential risk** | **Category** | **Owner** |
| 1 | Improper design | If the design for the application is not properly developed then technical risk occurs. | Technical risk | Designer |
| 2 | Budget shortfall | If the budget of the project is not managed then it causes number of financial issues. | Financial risk | Financial manager |
| 3 | Schedule slippage | If the schedule of the project is not manged then it is quite difficult to finish the project on time. | Project risk | Project manager |

## 9.5 Risk response plan

**Risk 1: Technical risk**

***Root cause***: If the design of the project is not properly developed then it can cause number of challenges.

***Trigger:*** Improper skills of the designers is mainly raising the problem.

***Risk response plan:*** It is quite necessary to hire experienced designers so that they can be able to design the application quite effectively.

**Risk 2: Budget shortfall**

**Root cause:** The main cause of this risk is improper management of resources.

**Trigger:** Due to improper management and rising cost of resources, the risk is increasing.

**Risk response plan:** It is quite necessary to manage the resources of the project effectively.

**Risk 3: Schedule slippage**

**Root cause:** The main cause of the schedule slippage is improper management of the project schedule.

**Trigger:** The risk is mainly occurring due to improper skills of the project manager.

**Risk response plan:** It is quite necessary to track the schedule on a regular basis so that the project can be completed on time.