# Cybersecurity Project

# Project Finalisation retrospective report

**For further information:**

Steve Gale

Business and ICT

Email: [sgale@gordontafe.edu.au](https://d.docs.live.net/7503200b517357fd/2020-Teaching/Python%20ADCSE2/2020%20new%20Handouts/sgale@gordontafe.edu.au),

# Guide

## Monthly Project tracking meetings

Refer to Trello and **Gant Chart**

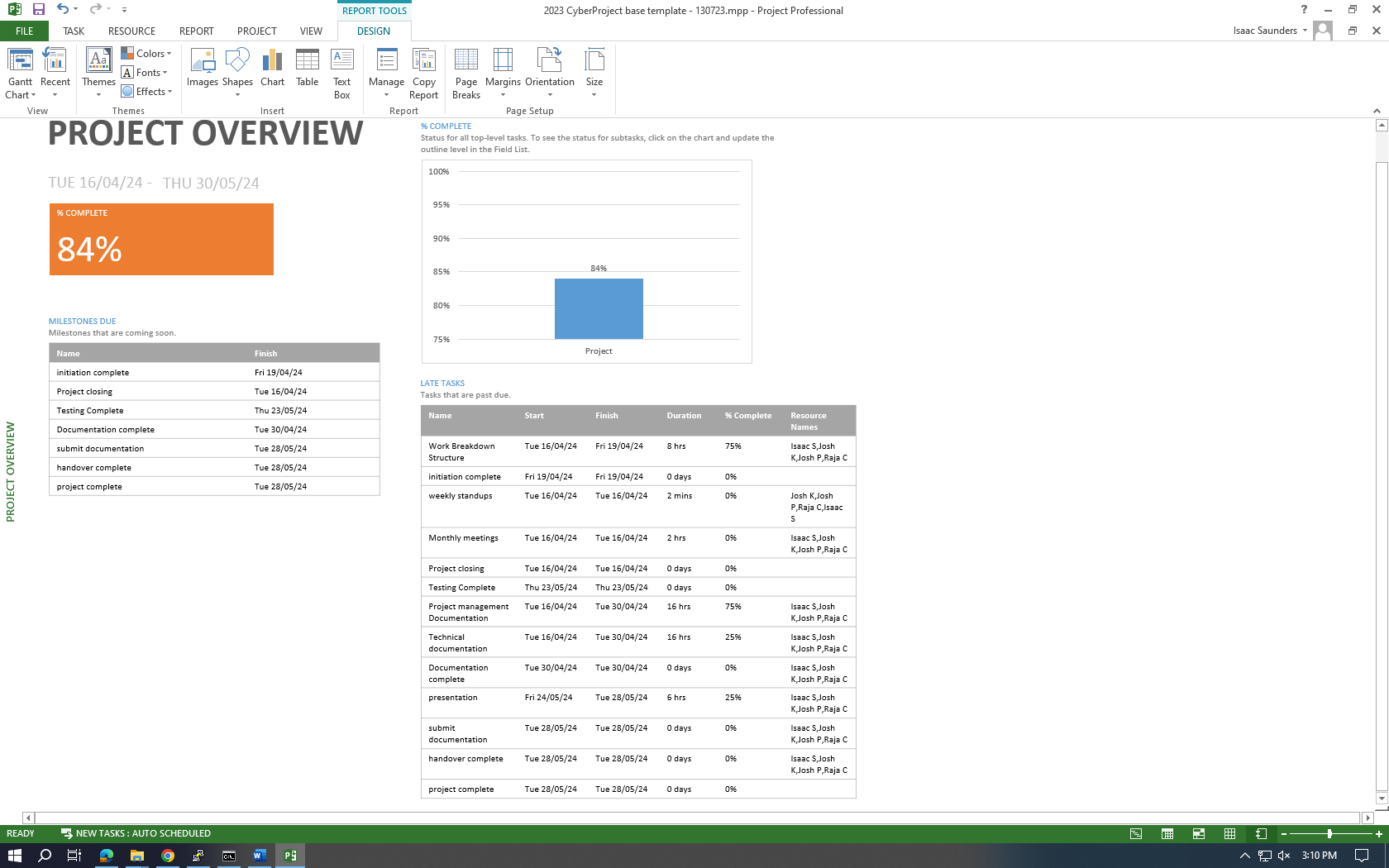
Meeting 15 minutes

* referring to Trello board and Gant chart
* Monitor progress and track:
  + Procurement
  + Project progress to timelines
  + Identify and document variations
  + Monitor risks – update risk register
  + Quality - Verify Prototype is meeting project technical requirements
  + Budget progress relative to projections
  + Critical path analysis
* Meeting minutes
* Documentation

## Procurement progress and tracking

* N/A

## Project progress to timelines

* 
* The project is on time to finish, as all that is left to do is finish the documentation. All configuration and testing is complete.

## Identify and document variations

* DOS attacks for testing DMZ
* Could not install GVM

**Monitor risks – update risk register**

| Id | Description of Risk | Impact or consequence | Likelihood/ Seriousness | Grade | Change | Mitigation Actions  (Preventative or Contingency) | Individual/Group Responsible for Mitigation Action | Timeline for Mitigation Action |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ~~CP1~~ | ~~Availability of resource like MS Project~~ | ~~H~~ | ~~Medium~~ | ~~C~~ |  | ~~Work at College premises~~ | ~~Group~~ |  |
| ~~CP 2~~ | ~~Availability of resource Memory in laptop~~ | ~~H~~ | ~~Medium~~ | ~~B~~ |  | ~~Get a PC with required memory~~ | ~~Individual~~ | ~~Sooner~~ |
| ~~CP 3~~ | ~~Logs from server not transfering~~ | ~~H~~ | ~~Medium~~ | ~~B~~ |  | ~~Redo server~~ | ~~Group~~ |  |

**Quality - Verify Prototype has met project technical requirements**

* Paragraph testing summary refer to prod documentation for more detail.

**Final Budget relative to projection**

* A screenshot of a computer

  Description automatically generated
* While the project may have been late, the status shows that the project is not far off the baseline cost. This means that we have caught up on lost time and the cost should be close to the quoted price.

**Critical path analysis**

* A screenshot of a computer

  Description automatically generatedThe critical tasks shows that every task on the critical path is complete. While a lot ahs been late, this shows that progress has caught up.

### Questions:

1. What were the responsibilities of your team members

Isaac worked on the Switch and Firewall installation in addition to managing the DMZ and Windows Server 2022. Zoey worked on the SIEM, Kali Purple and Firewall with Isaac. Raja and Josh worked on the Prototype and Red and Blue team testing.

1. How did your team perform relative to meeting project milestones, costs and timeline

We quickly became ahead of schedule in the beginning, which gave as some extra time to work on milestones we had trouble with, nearing the end of the project we are completely on schedule. As such costs should line up neatly with the estimates.

1. What final project outcomes did your team achieve

In this project we successfully created and configured interconnected virtualised machines, configured a PaloAlto firewall and secured the network with Intrusion detection and prevention systems, configured and set up a SIEM on a kali machine, End Point Protection, and red team blue team testing.

1. How did you estimate and analyse cost and time through the project

We estimate cost based on how far or behind schedule we were by using a GANTT chart in MS Project.

1. What experience did your team gain from this project

Our team gained firsthand experience with creating and monitoring a network with real traffic flowing through it. We also gained experience working with firewall and switch hardware as before it was all simulated lab environments. Doing this all from scratch gave us a better understanding of how the systems interact with each other as we needed to troubleshoot and find solutions.

1. What lessons did you learn, what would you do different next project

We learned that it is important to ensure every component is fully updated as it could lead to compatibility issues when enrolling other machines. When trying to enrol the DMZ server and Windows Server to the fleet they were unable to send logs to the SIEM even though its was enrolled. It took us hours of trouble shooting to realize that we had to update the fleet server directly, in addition to Elastic. Attempting this again, we’d make sure that the agents are running the last version before enrolling anything to the fleet.

1. What processes did you use to monitor team performance

We had weekly stand-up meetings and a monthly meeting where we went over what each team member was working on during the week/month and to gauge any risks and variations on the project and the plan, and how close we are following the timeline set in the GANTT chart in MS Project

1. What project-management methods and tools were used, which did you find most useful

We used MS-Project, a GANTT chart with waterfall diagrams in MS-Project, Trello, weekly and monthly meetings. The most usefull was the weekly and monthly meetings as we got a chance to speak as a group about how we were going and the things we were having trouble with, as well as a chance to talk with the project owner.

### References:

Critical path - <https://support.microsoft.com/en-us/office/show-the-critical-path-of-your-project-in-project-desktop-ad6e3b08-7748-4231-afc4-a2046207fd86>

MS Project cost totals - <https://support.microsoft.com/en-us/office/view-project-cost-totals-0d3a2451-fb1e-4ba0-826e-20ee3b3d60cc>

Baseline – MSProject - <https://support.microsoft.com/en-us/office/create-or-update-a-baseline-or-an-interim-plan-in-project-desktop-7e775482-ac84-4f4a-bbd0-592f9ac91953>

**MS project reports**

Project > project Information > Statistics

Report > dashboard > Project Overview

Report > costs > task cost overview

Report > In progress > Milestone report

Report > resources > resource Overview

**Key to Risk Rating Symbols used:**

|  |  |  |  |
| --- | --- | --- | --- |
| Rating for Likelihood and Seriousness for each risk | | | |
| L | Rated as Low | E | Rated as Extreme (Used for Seriousness only) |
| M | Rated as Medium | NA | Not Assessed |
| H | Rated as High |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Grade: Combined effect of Likelihood/Seriousness | | | | | |
|  | Seriousness | | | | |
| Likelihood |  | low | medium | high | EXTREME |
| low | N | D | C | A |
| medium | D | C | B | A |
| high | C | B | A | A |

|  |  |
| --- | --- |
| Recommended actions for grades of risk | |
| Grade | Risk mitigation actions |
| A | Mitigation actions to reduce the likelihood and seriousness to be identified and implemented as soon as the project commences. |
| B | Mitigation actions to reduce the likelihood and seriousness to be identified and appropriate actions implemented during project execution. |
| C | Mitigation actions to reduce the likelihood and seriousness to be identified and costed for possible action if funds permit. |
| D | To be noted - no action is needed unless grading increases over time. |
| N | To be noted - no action is needed unless grading increases over time. |

|  |  |  |  |
| --- | --- | --- | --- |
| Change to Grade since last assessment | | | |
| NEW | New risk | ¯ | Grading decreased |
| — | No change to Grade | ­ | Grading increased |