

[Date]

# Assessment Task 2

## Develop ICT Solution

Wells College

NATALIA 18171

Name of Student	Natalia Büttner	ID	18171
-----------------	-----------------	----	-------

## CONTENTS

Case scenario .....	<b>Error! Bookmark not defined.</b>
Heaven Systems internal IT Service Agreement .....	<b>Error! Bookmark not defined.</b>
Task 1: Prepare team support and monitor .....	6
Task 2: Review client support .....	9
Task 3: Submit both report to your trainer for approval.....	10
<b>Search Index</b> .....	
<b>REFERENCE:</b> .....	

# Assessment 2 – Case Study

## Instructions:

This is a group of 2 student assessment.

You need to analyse a case scenarios and complete tasks mentioned after scenario.

You need to demonstrate your develop ICT solution ability to identify the solution, determine client support and manage the team in development an awareness of cyber security in workplace.

## Duration:

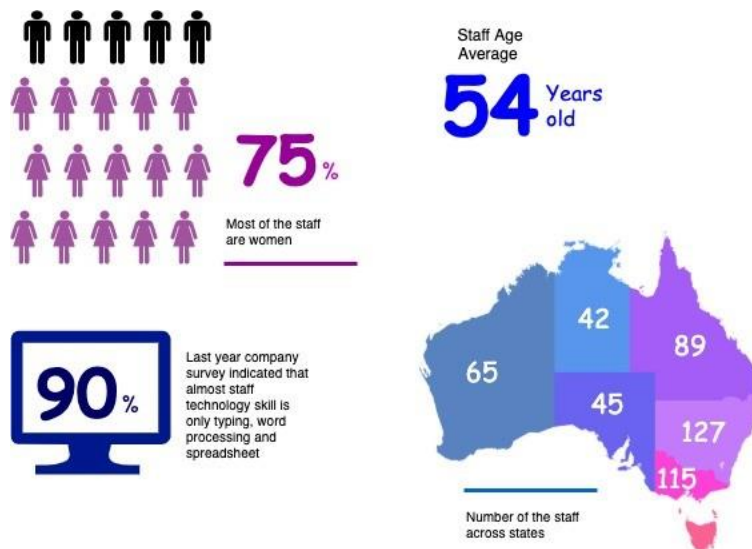
Trainer will set the duration of the assessment.

## Evidence required:

Tasks	Evidence	Submission
Supporting Plan Report	A complete report on team supporting and monitoring team performance, and client support for the case study.	In printing

## Case scenario

Established in 1999 with offices located throughout the western Sydney, Heaven Systems is a world-class, full-service provider of residential, commercial, and logistics-based transportation solutions for businesses and individuals. Many of the world's largest, most respected corporations rely on the company's unwavering commitment to innovation, quality, and customer service to move their employees, offices, and industrial facilities—domestically and internationally—anywhere in the world. Heaven Systems was experiencing an increase of phishing emails that were reaching employee inboxes and introducing the risk of a data breach. As phishing attacks increased, productivity slowed down while end users waited for IT to investigate the suspicious emails. "Phishing emails were getting more specific and sophisticated, and we worried that an employee might open one and cause serious damage," said David Potter, IT Director at Heaven Systems. While there are multiple layers of security to filter email as it enters Heaven Systems' network, it's still possible for some targeted phishing emails to slip through and get into employee in-boxes. For this reason, IT must rely on end users to determine whether an email is safe to open. But it's not always easy to tell. "For instance," said Potter, "one area of the company was getting phishing emails that looked legitimate. They appeared to come from a customer, but the attachment was malicious." Refer to employee background statistic show below:



To help employees identify phishing emails, IT holds annual training to show them what red flags to look for. Then, IT sends mock phishing attacks to test them. If a user clicks on a couple simulated phishing emails, they're required to take the security training again. Human nature being what it is, some users were ignoring legitimate email because they didn't want to make a mistake that would require them to take the training again. Others decided to play it safe and send every questionable email they received to IT to see if it was OK. While IT recognized the obvious threats, even they had to question some of the attachments. "You can imagine the amount of time we spent investigating emails," said Potter. "It took about an hour per email to copy the attachment to a USB drive and then spin up a machine to test the file off network," he explained. "That's valuable time that IT could spend doing other things."

You are work as an IT project manager assigned by Potter to handle this problem in the company. The company decide to use the system to detect a Spear-Phishing. To accelerate suspicious email analysis and response, Heaven Systems implemented MailMon, an automated phishing incident reporting and response service that empowers end users to report suspicious emails directly from the inbox. MailMon runs on Microsoft Exchange 2013 or newer and Office365; it is deployed to end users as an Outlook plug-in, including Outlook App for Android and iOS devices.

You and your friend are 10 years' experience staff in the company. After you evaluate the MailMon, it generates a report in the complex form, many of the staff including a current IT department are not familiar

with the system. Potter approved on new project team recruitment, and HR organised 3 **new graduated** IT staffs joining your team. Potter would like your team to gain more awareness on this cyber security incidence

Project	
Name	Heaven Systems IT Service by 18171
Organization	Wells International College
Web Link	
Description	<p>We are going to analyse a case scenarios and complete tasks mentioned after scenario.</p> <p>I need to demonstrate the company develop ICT solution, and ability to identify the better solution, and determine client support and manage the team in development, also an awareness of cyber security in workplace.</p> <p>Help Heaven System Company make better performance.</p>



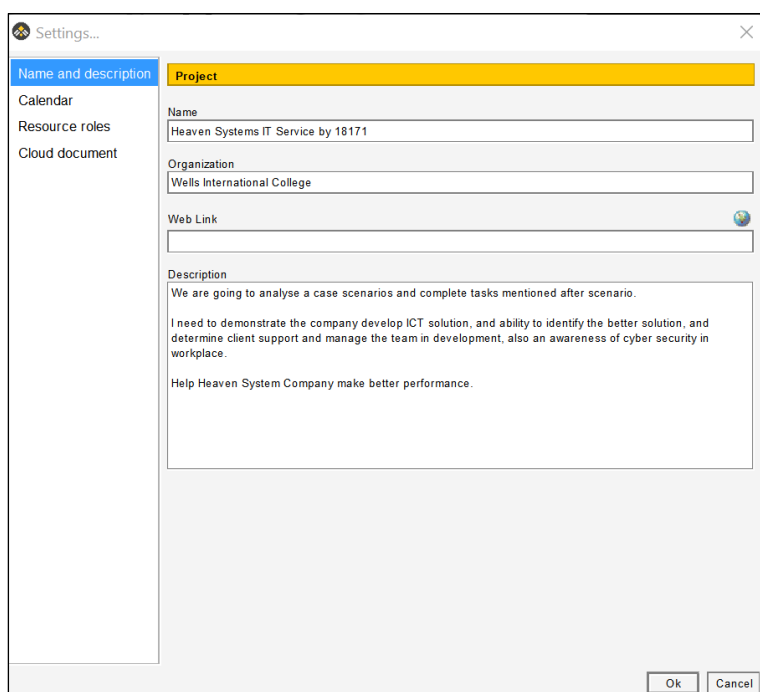
Figure: MailMon Monitoring Sample

## Heaven Systems internal IT Service Agreement

Severity Level	Description	Target Response
1 (Outage)	Entire Company Server down	Immediately
2 (Critical)	Entire Department Server down	Within 15 Minutes
3 (Urgent)	Staff computer down	Within 1 hours

4 (Important)	Staff computer not work properly or potential for interrupt their routine work	Within 3 hours
5 (General)	Upgrade software Training request	Within 48 hours

Learn how to using GanttProject: [https://www.youtube.com/watch?v=5FukJpd\\_VNs&t=1242s](https://www.youtube.com/watch?v=5FukJpd_VNs&t=1242s)



The screenshot shows the 'Settings...' dialog box in GanttProject. The 'Project' tab is selected. The 'Name and description' section contains the following fields:

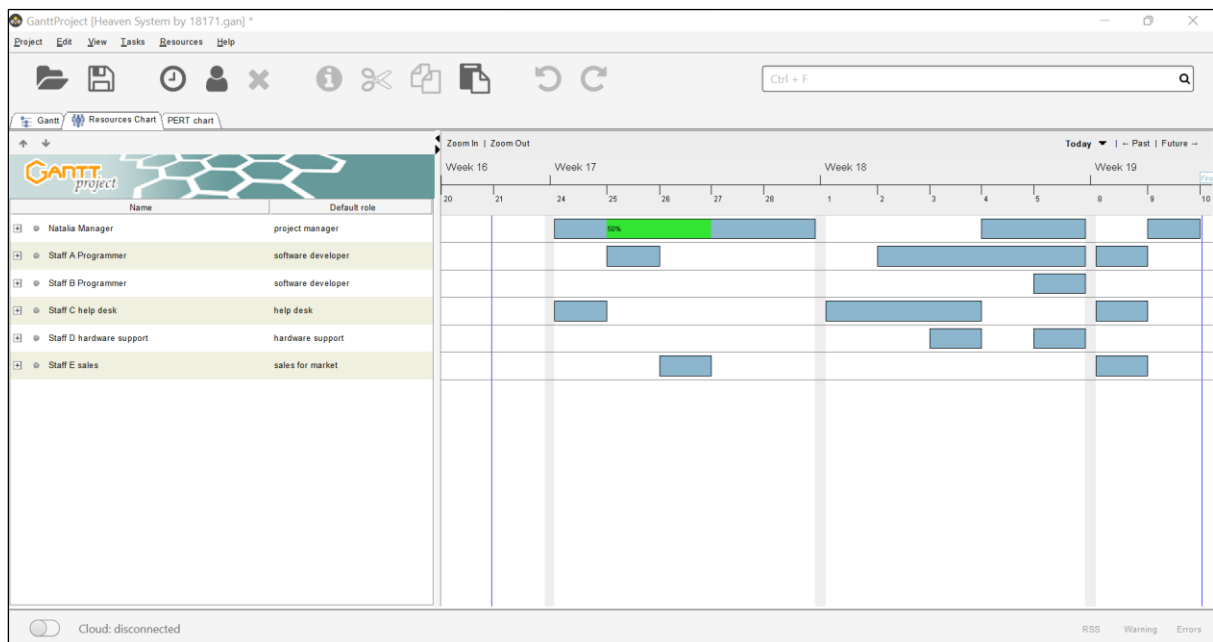
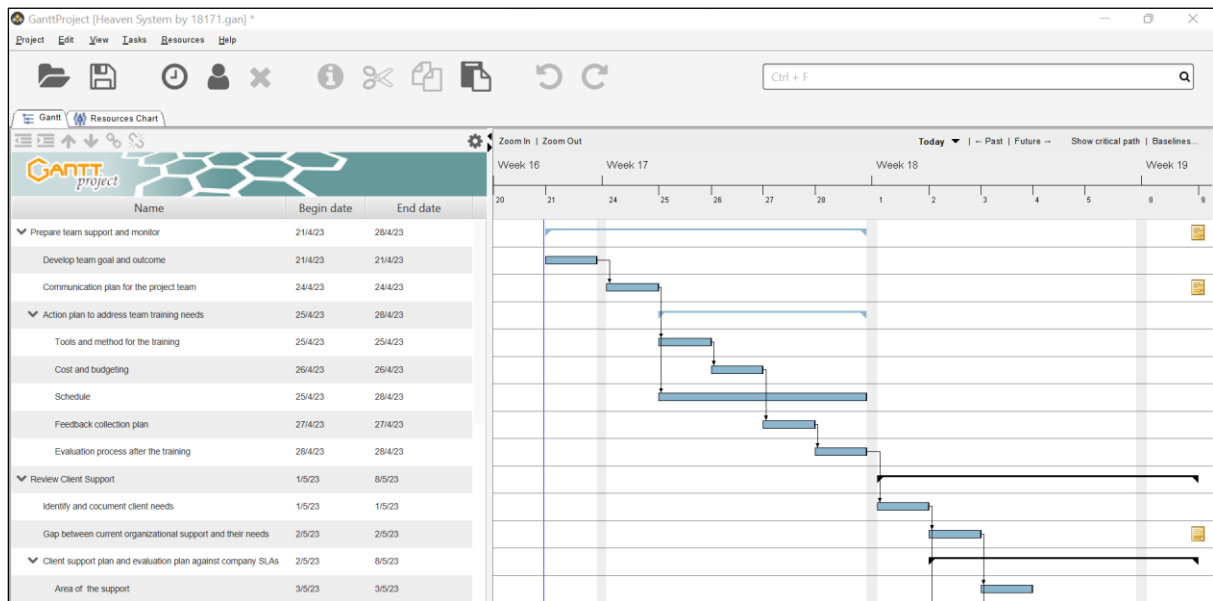
- Name:** Heaven Systems IT Service by 18171
- Organization:** Wells International College
- Web Link:** (empty field with a globe icon)
- Description:**

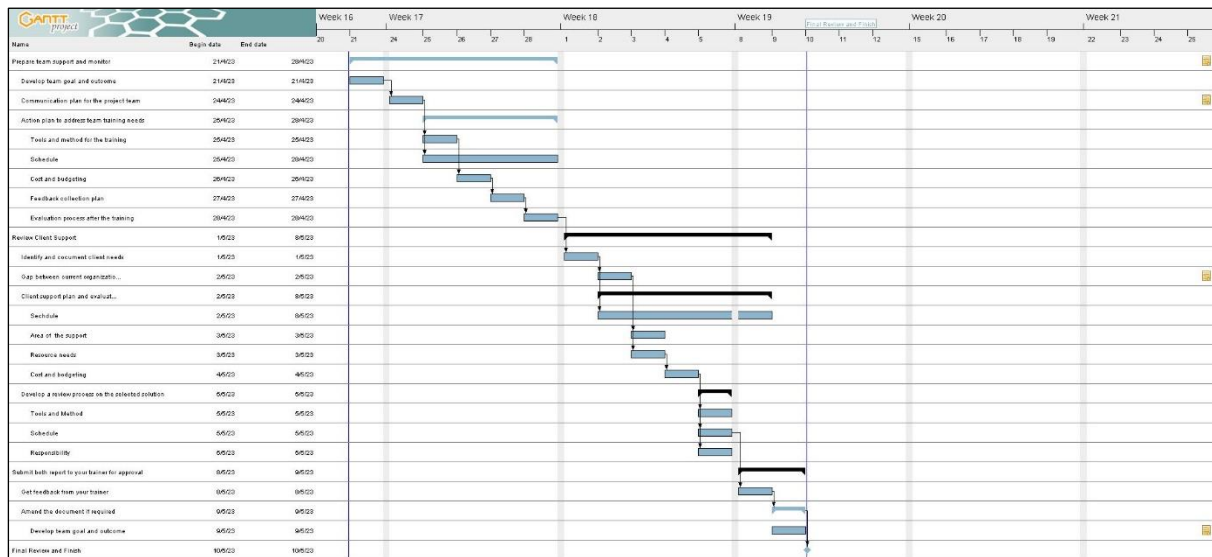
We are going to analyse a case scenarios and complete tasks mentioned after scenario.

I need to demonstrate the company develop ICT solution, and ability to identify the better solution, and determine client support and manage the team in development, also an awareness of cyber security in workplace.

Help Heaven System Company make better performance.

At the bottom right, there are 'Ok' and 'Cancel' buttons.

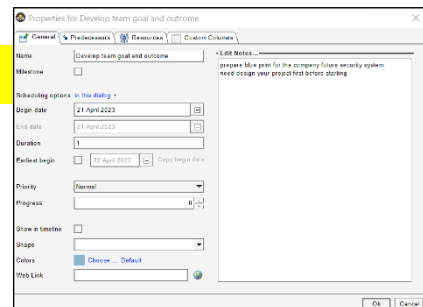




## Task 1: Prepare team support and monitor

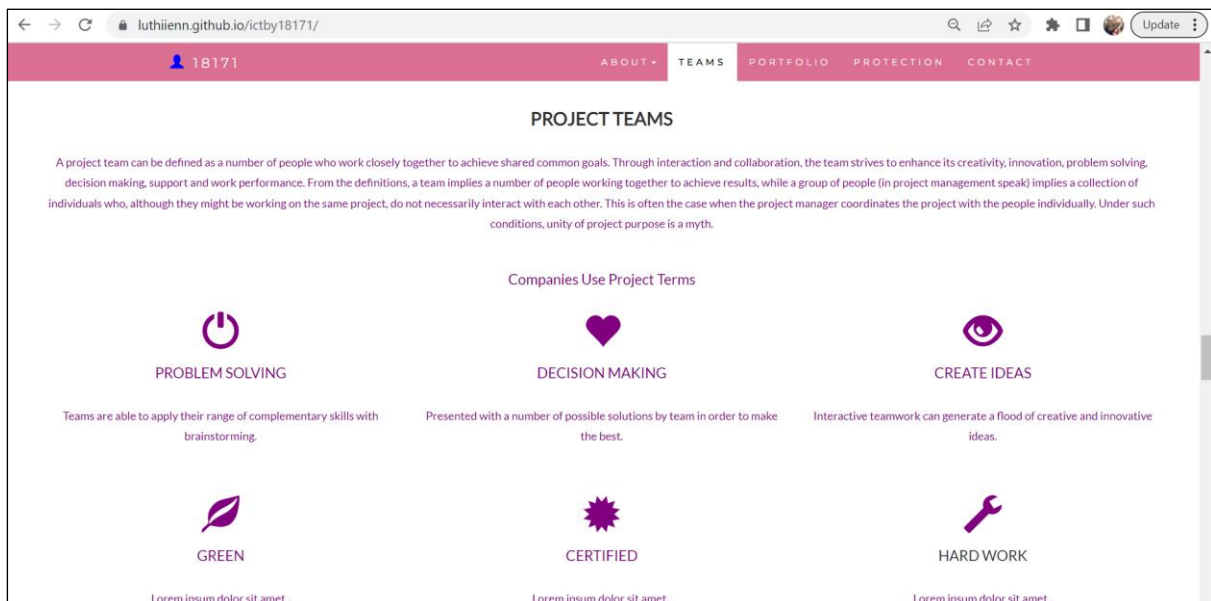
### 1. Develop team goal and outcome

prepare blue print for the company future security system  
need design your project first before starting



Develop communication plan for the project team, please refer:

<https://luthienn.github.io/ictby18171/#services>

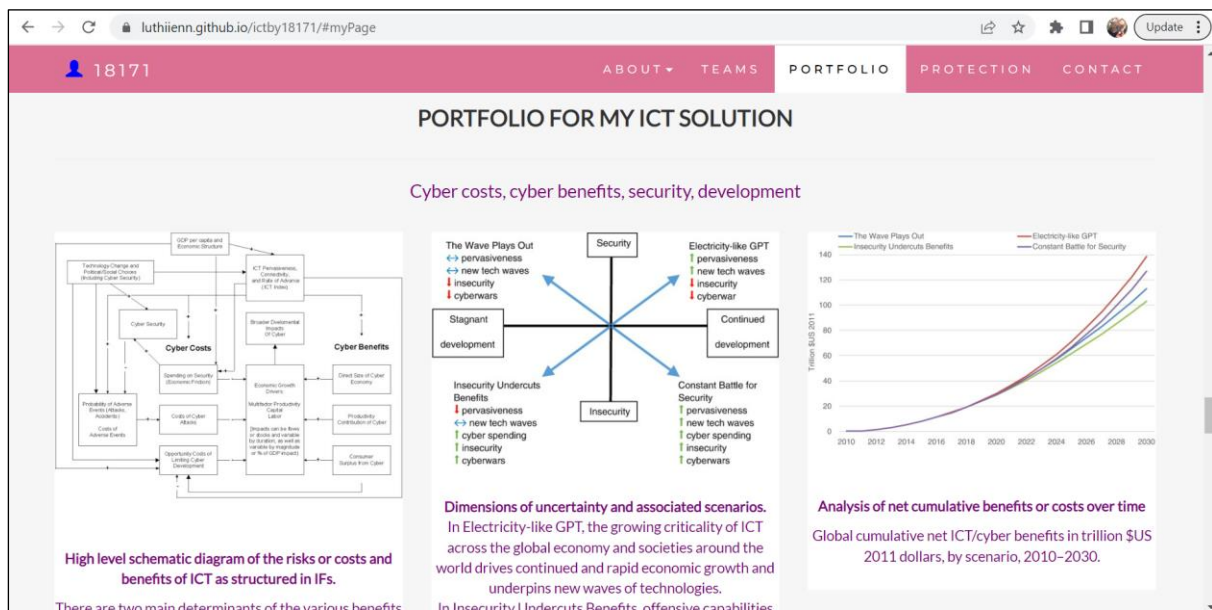
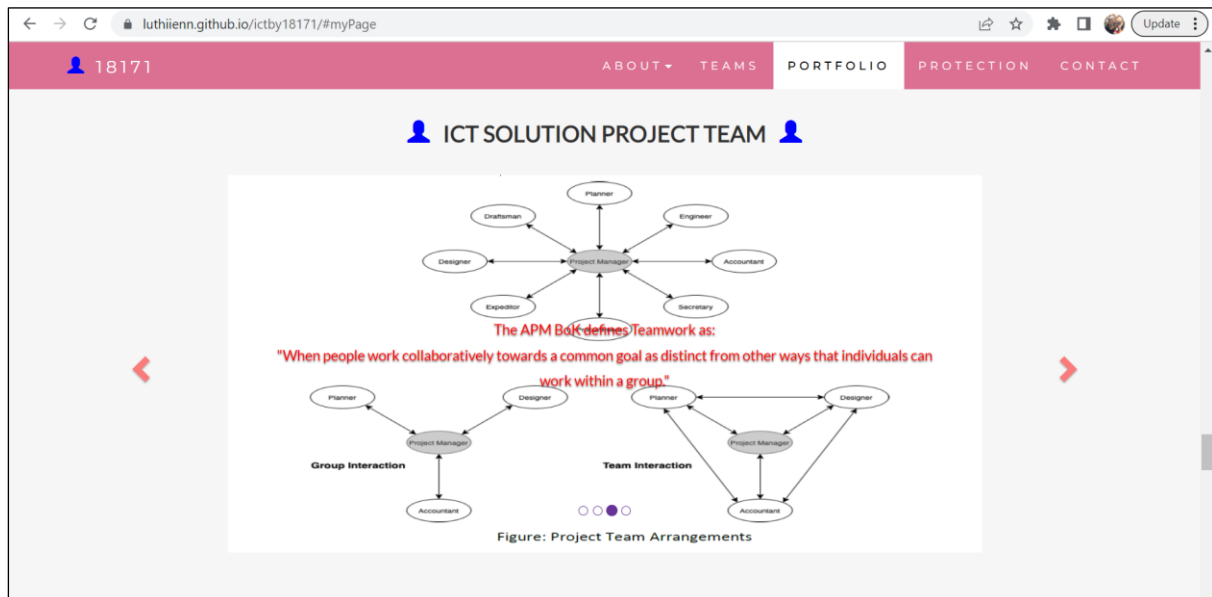


**PROJECT TEAMS**

A project team can be defined as a number of people who work closely together to achieve shared common goals. Through interaction and collaboration, the team strives to enhance its creativity, innovation, problem solving, decision making, support and work performance. From the definitions, a team implies a number of people working together to achieve results, while a group of people (in project management speak) implies a collection of individuals who, although they might be working on the same project, do not necessarily interact with each other. This is often the case when the project manager coordinates the project with the people individually. Under such conditions, unity of project purpose is a myth.

**Companies Use Project Terms**

- PROBLEM SOLVING**  
Teams are able to apply their range of complementary skills with brainstorming.
- DECISION MAKING**  
Presented with a number of possible solutions by team in order to make the best.
- CREATE IDEAS**  
Interactive teamwork can generate a flood of creative and innovative ideas.
- GREEN**  
Lorem ipsum dolor sit amet.
- CERTIFIED**  
Lorem ipsum dolor sit amet.
- HARD WORK**  
Lorem ipsum dolor sit amet.

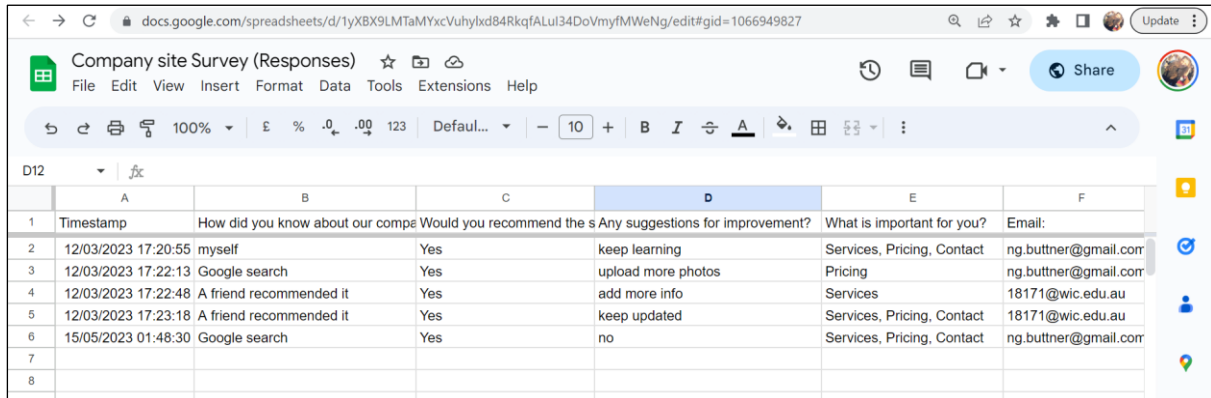


## 2. Develop team KPI and action plan to address team training needs

- Tools and Method for the training
- Cost and budgeting
- Schedule
- Feedback collection plan
- Evaluation process after the training

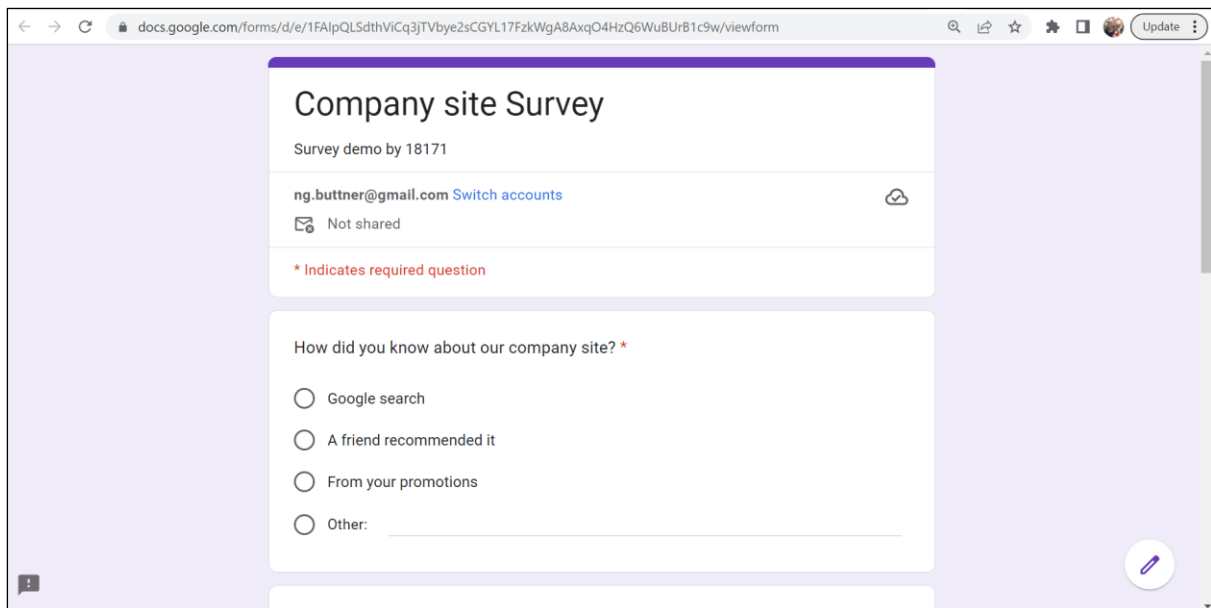
Here are my feedback results for collection





	A	B	C	D	E	F
1	Timestamp	How did you know about our company site?	Would you recommend the site?	Any suggestions for improvement?	What is important for you?	Email:
2	12/03/2023 17:20:55	myself	Yes	keep learning	Services, Pricing, Contact	ng.buttner@gmail.com
3	12/03/2023 17:22:13	Google search	Yes	upload more photos	Pricing	ng.buttner@gmail.com
4	12/03/2023 17:22:48	A friend recommended it	Yes	add more info	Services	18171@wic.edu.au
5	12/03/2023 17:23:18	A friend recommended it	Yes	keep updated	Services, Pricing, Contact	18171@wic.edu.au
6	15/05/2023 01:48:30	Google search	Yes	no	Services, Pricing, Contact	ng.buttner@gmail.com
7						
8						
9						

The design like:



**Company site Survey**

Survey demo by 18171

ng.buttner@gmail.com [Switch accounts](#)

Not shared

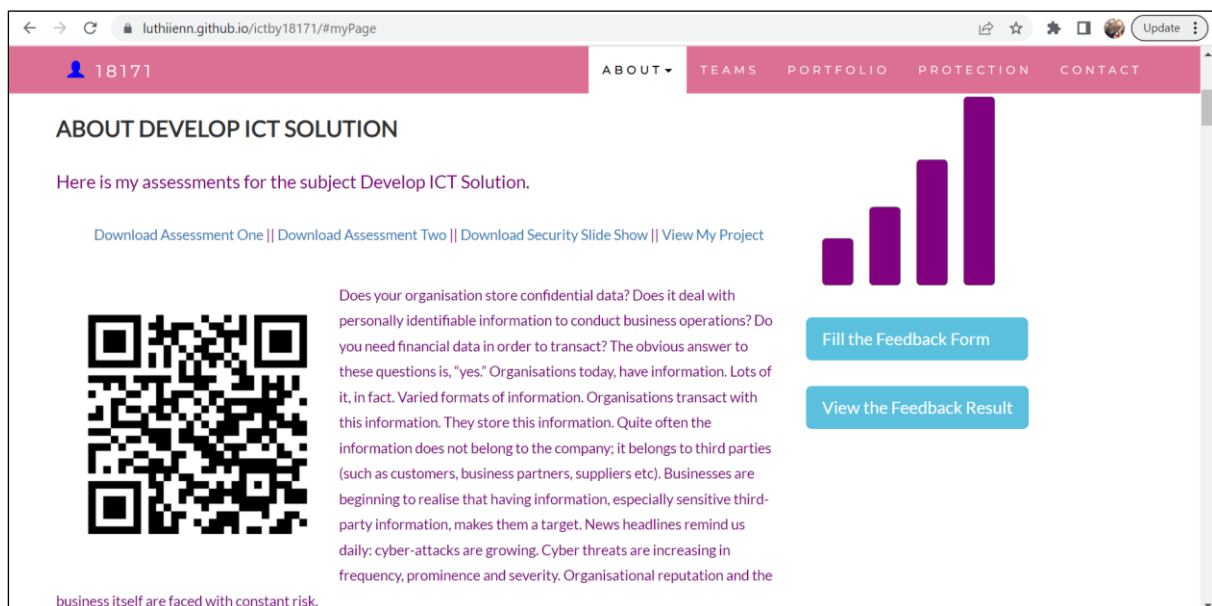
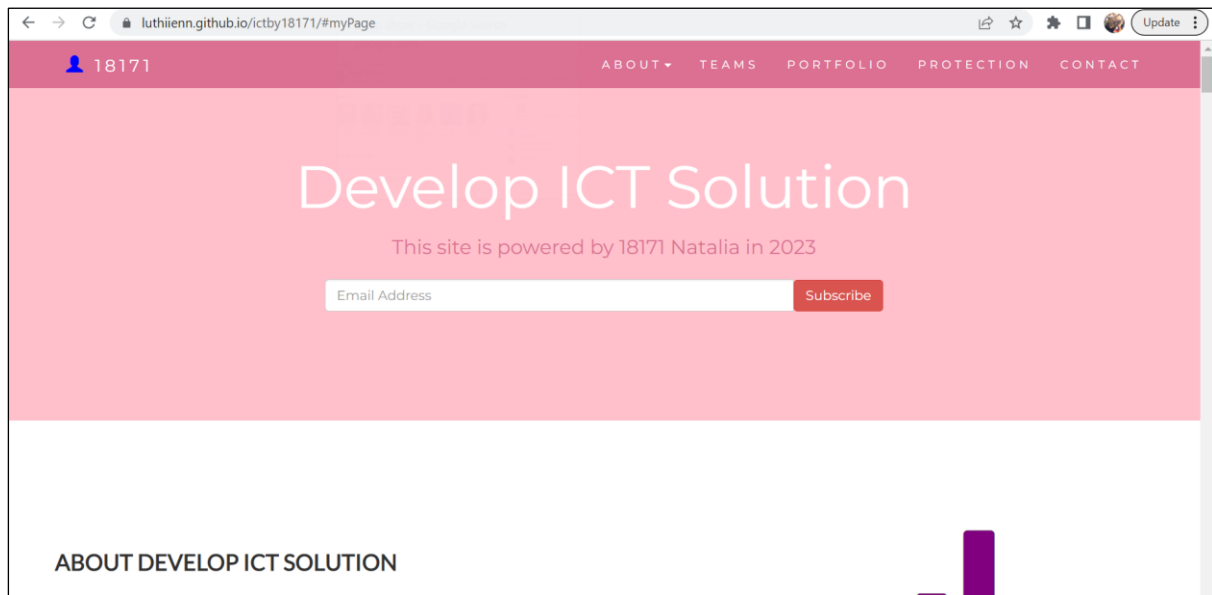
\* Indicates required question

How did you know about our company site? \*

☐ Google search  
☐ A friend recommended it  
☐ From your promotions  
☐ Other: \_\_\_\_\_

Above site could be access by my web support site:

<https://luthiienn.github.io/ictby18171/#myPage>



We could learn about web feedback form from: <https://www.youtube.com/watch?v=BtoOHhA3aPQ&t=15s>

## Task 2: Review client support

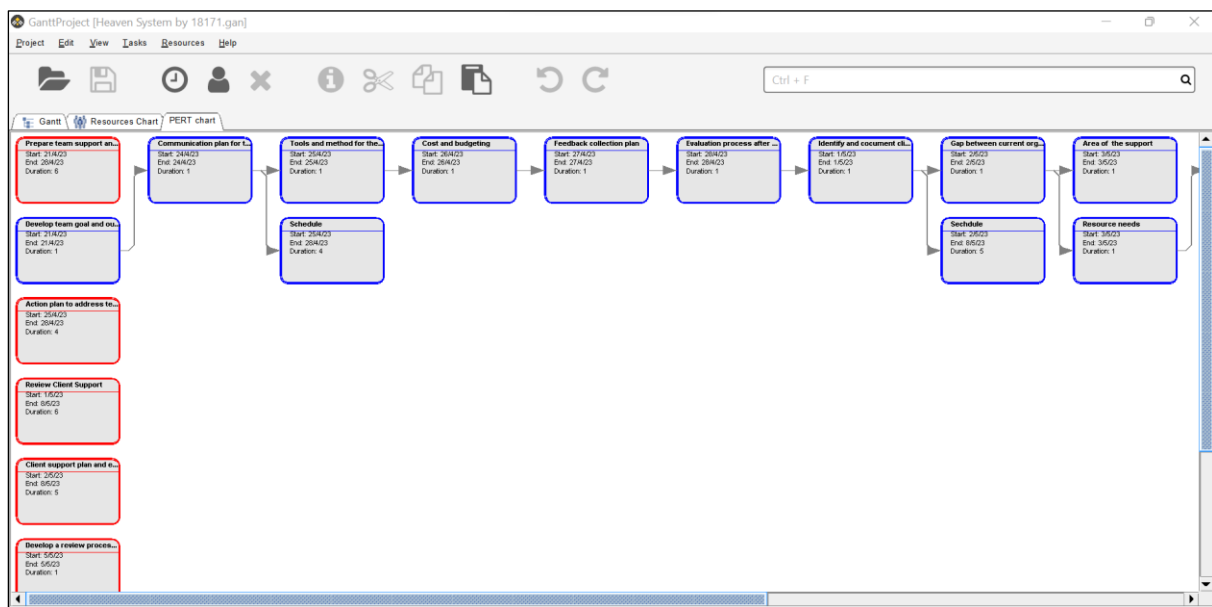
1. Identify and documenting client needs
  - Gap between current organizational support and their needs
2. Develop a client support plan and evaluation plan against company SLAs
  - Area of the support
  - Resources needs
  - Cost and budgeting
  - Schedule

### 3. Develop a review process on the selected solution

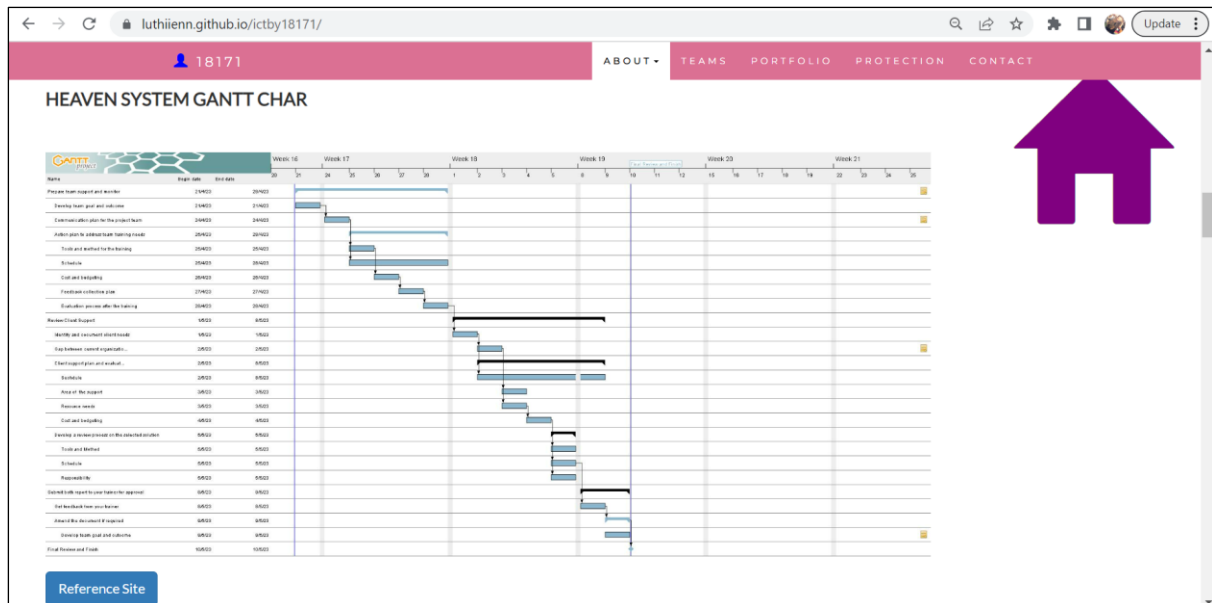
- Tools and Method
- Schedule
- Responsibility

## Task 3: Submit both report to your trainer for approval

1. Get feedback from your trainer
2. Amend the document if required



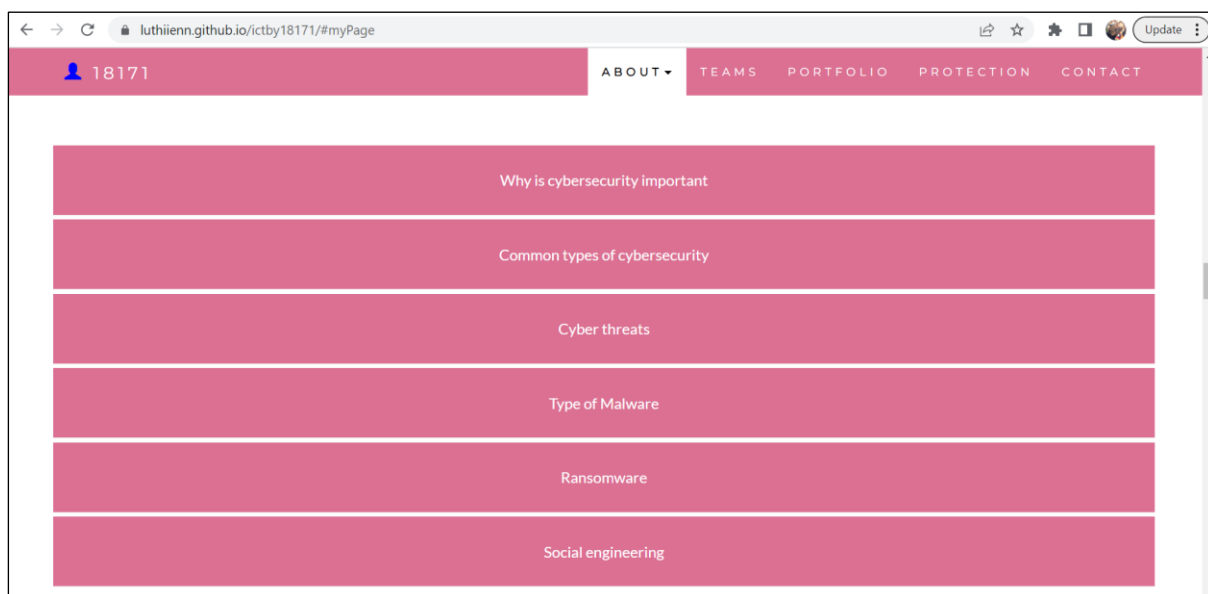
My Subject Web Site: <https://luthiienn.github.io/ictby18171/#myPage> already showing linked above project.





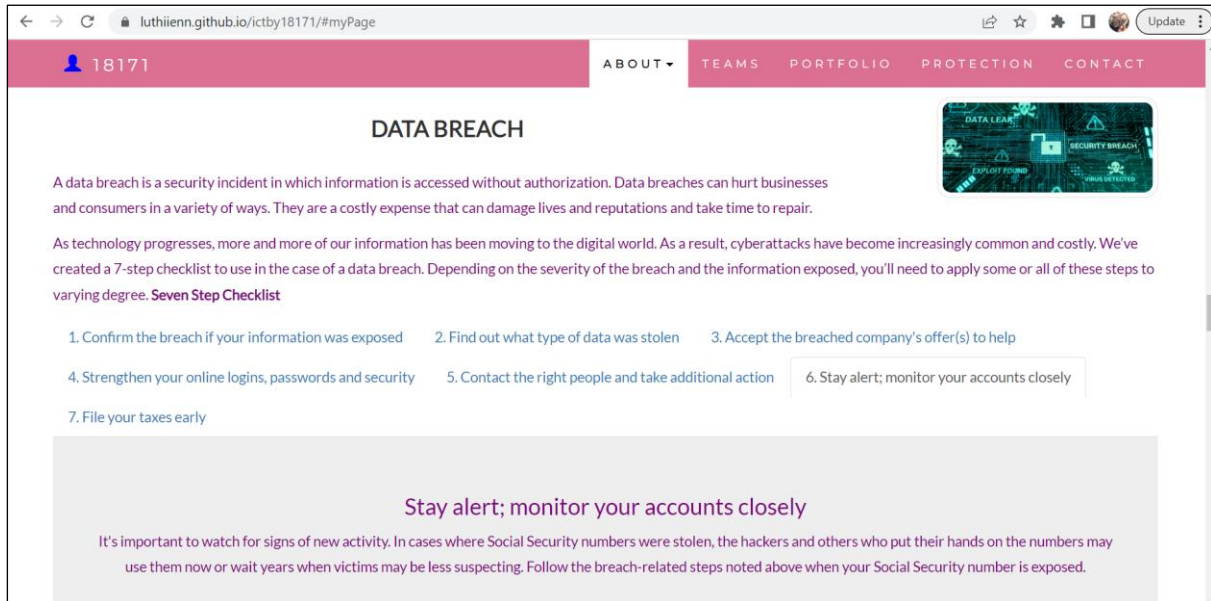
The screenshot shows a web page with a pink header and navigation menu. The main content area features a table with 10 rows of information about working in ICT business. A large purple house icon is positioned to the right of the table.

Good for ICT	Hard for ICT	Comments
Good Salaries	-	Start 60000 Up to 200000
Working Remote	-	Work at home, Save time on the way
Demand	-	Thousands of open positions today
Mobility	-	Easy to move to another company
Business knowledge	-	It can lead to promotions or change departments
-	Long time to work	In order to solve problems
-	Change so quick	Keep to learn your whole life
-	Prepare for change	Some is too hard to keep going
-	Tight deadlines	Some deadlines cant be changed
-	Stress and burnout	Long hours and stress can lead to burnout



The screenshot shows a web page with a pink header and navigation menu. The main content area displays a list of six cybersecurity topics, each in a pink rectangular box.

- Why is cybersecurity important
- Common types of cybersecurity
- Cyber threats
- Type of Malware
- Ransomware
- Social engineering



The screenshot shows a web browser displaying a page titled "DATA BREACH". The page has a pink header with navigation links: ABOUT, TEAMS, PORTFOLIO, PROTECTION, and CONTACT. The main content area includes a definition of a data breach, a 7-step checklist, and a section titled "Stay alert; monitor your accounts closely".

## DATA BREACH

A data breach is a security incident in which information is accessed without authorization. Data breaches can hurt businesses and consumers in a variety of ways. They are a costly expense that can damage lives and reputations and take time to repair.

As technology progresses, more and more of our information has been moving to the digital world. As a result, cyberattacks have become increasingly common and costly. We've created a 7-step checklist to use in the case of a data breach. Depending on the severity of the breach and the information exposed, you'll need to apply some or all of these steps to varying degree. **Seven Step Checklist**

1. Confirm the breach if your information was exposed
2. Find out what type of data was stolen
3. Accept the breached company's offer(s) to help
4. Strengthen your online logins, passwords and security
5. Contact the right people and take additional action
6. Stay alert; monitor your accounts closely
7. File your taxes early

### Stay alert; monitor your accounts closely

It's important to watch for signs of new activity. In cases where Social Security numbers were stolen, the hackers and others who put their hands on the numbers may use them now or wait years when victims may be less suspecting. Follow the breach-related steps noted above when your Social Security number is exposed.