CONFIDENTIAL

FORTIFY

Connect, Assess and Secure

BUSINESS PLAN

Trimester 3, 2022

TABLE OF CONTENTS

Executive Summary **3**

Business Objectives and services **4**

Marketing Analysis **5**

Competitors 5
Clients 7
Advertisement and recruitment strategy 9
SWOT analysis 10
Strengths 11
Weaknesses 11
Opportunities 12
Threats 12

Operational Plan **13**

Operational Procedures **14**

Marketing 14
Questionnaire 16
Matchmaking 19
Strategic Formulation 21
Strategic formulation example - backups 22
Strategic implementation 24
User case example: backups 25
Monitoring 25
Feedback 27

Market and production milestones **28**

Conclusion **29**

Executive Summary

The Fortify project is an innovative initiative that provides a work-integrated volunteering opportunity for graduates, students and IT professionals and connects them to small businesses and non-profit organisations that do not have the adequate resources to effectively manage their cybersecurity risks. Fortify facilitates and monitors the volunteer-company cooperation by creating the platform for the clients, setting clear guidelines for the volunteers and oversighting the process of collaboration. Fortify aims to fill the gaps in the labour and IT market by giving the volunteers an opportunity to build valuable experience to raise their employability, and by giving small organisations a hand in building their cyber security strategy. This report aims to serve as an outline of intentions, i.e., a plan for the near and distant future of Fortify, with an explanation of means and methods of action to achieve the assumed goals. This paper presents a market analysis that assesses the business idea and serves as the baseline for the creation of informed business decisions, utilising a SWOT analysis and survey data analysis. The technical part of the report aims to clearly describe the required organisational structure of Fortify – consisting of roles, teams and employees – that is essential in the long-term planning of the company. Operational procedures in the report serve as a description of the business operations – from start to finish – with justifications of the chosen methods. The report will describe the market and production milestones to clarify the long-term goals of Fortify.

Business objectives and services

01 Prior to the commencement of operations, it is intended to find partners, such as educational institutions, with the goal of cooperation in volunteer recruitment.

02 During 2023, Fortify aims to develop a mentoring program involving at least 5 mentors from our company's volunteer alumni group. The program will offer mentors the development of management and leadership skills, while simultaneously filling the gaps in the organisational structure of Fortify and the provision of assistance to new clients.

03 Fortify aims to increase the customer satisfaction by 25% within the first term of operations with the use of client feedback and satisfaction surveys, by readapting the structure of the website to the client's needs.

04 The platform aims to build trust and a closer connection with clients by creating useful and valuable content targeting the customer's needs and demands that showcases business cases of prior clientele and their satisfaction rating.

Services:

- Partnership with educational institutions to provide volunteering opportunities for students and graduates
- Recruitment of clientele and the facilitation of the matchmaking for volunteers/businesses based on a questionnaire.
- Development and management of a website-based platform for clients.
- Facilitation for the cooperation between clientele and provision of oversight of the operations.
- Development and management of a mentoring program to provide assistance to new volunteers and companies.

Marketing analysis

This marketing analysis serves as a thorough evaluation of the market. It includes prospective customers and competitors. Marketing analysis aims to reduce business risks, effectively connect with the target audience, provide the right products, and services and align with market trends. An analysis of marketing data is needed as it provides strategic information about the market Fortify is going to enter. In addition, analysis of marketing data is also useful for those who are already present in the market as it serves as a comprehensive report on how the business is performing and provides insights on what improvements can be made to enhance the performance.

Competitors

There are several volunteering services online which provide support to various industries. Only a select few of them focus on a niche group of underrepresented organisations with poor cyber security awareness. Our mission at Fortify is to matchmake these organisations with respective volunteers who can guide them with resilience through the cyber space. Nonetheless, there are similar competitors which operate in a similar respect globally, but in Australia, Fortify is the only non-for-profit organization with this focus. Below is a listing of similar platforms to Fortify in the Australian market.

Deakin Freelancing Hub:

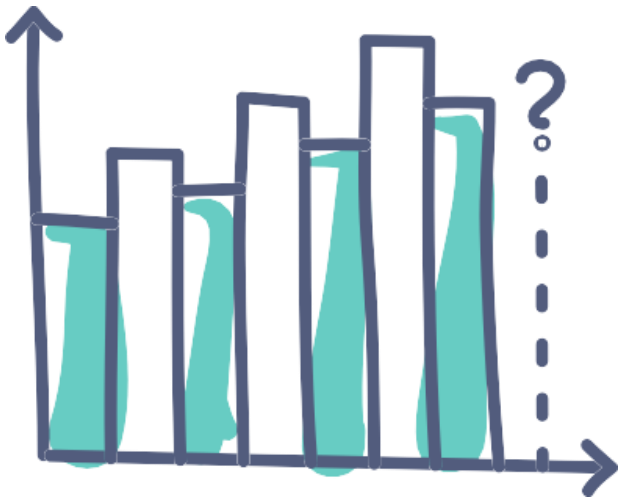
This platform enables interns to experiment with working for themselves as a professional freelancer inside a co-working environment while acquiring important employability skills such as communication, cooperation, creativity, and critical thinking. The Deakin Hub is very similar to Fortify from a volunteering perspective where students can be exposed to industry like projects to help expand their workplace experience, but it focuses on a wide range of volunteers. This means

while the core process is similar, the focus is completely different from that of providing cyber safety to small and underprivileged organisations. Also, we not only assist victims but also unaffected organisations. We believe in assessing an organisations network early on to help identify weaker entry points before a disaster. This gives us an opportunity to build a database of information early on which we can use when trying to matchmake potential volunteers.

CyberV19:

This platform was created as a non-for-profit organisation in Australia during covid. They use volunteers to assist healthcare organisations in identifying, protecting, detecting, and responding to present and new cyber threats. This is because during the pandemic there was an increase of cybercrimes, especially targeted towards Healthcare & Response Services. CyberV19 is different to Fortify as well since its focus is on a specific industry. Once again, Fortify aims to assist all small organisations. Although, CybereV19 is similar in the sense that it provides the healthcare sector access to proper cyber security services.

Based on this findings, it is important to note that Fortify's greatest similarity with other volunteering platforms is that all of them recognise that volunteering is a great pathway for full-time employment where one can expand on their skills and further their experience. Fortify is amongst the only cybersecurity services based in Australia with a focus on aiding the community to become more resilient to the world of online threats.



Clients

A survey has been conducted to serve as the baseline for marketing analysis pertaining to potential clients at Fortify. The collected data is based on facts. The survey was shared amongst students & assessors via Microsoft Teams and other members via online Discord servers. The purpose of running this survey is so that we can measure the demand of Fortify. We already know based on the above market analysis for competitors in Australia that we are the only non-for-profit charity which matchmakes between the organisation and the volunteer. This also signifies that we can fill a gap in the market. Therefore, we have used our collected quantitative data to show areas in which Fortify can expand as well as areas which affirm our company is heading in the right direction. Originally, we highlighted that our potential volunteers would students and/or graduates scouting the job market for employability opportunities. They recognise the difficulties associated with attempting to secure a job with little to no experience. Therefore, we have developed Fortify in a way that helps them to register to volunteer, so that they can almost prove their knowledge and skills in a workplace environment. It allows them the opportunity to aid the community and further their cybersecurity abilities. Our potential target audience would be small organisations who usually do not have the adequate funding and/or knowledge to identify threats in their everyday operations and those who have been victims to cybercrimes and are unaware on how to recover.

From the survey results (page 8) we can conclude that there is clear evidence on both the volunteering side and target audience side which highlights that Fortify not only fits a need in the market, that of assisting smaller organisations but it also creates opportunities that allow an individual to become more experienced, increase their employability and build their network portfolio. All of which can increase Fortify website traffic and awareness. This will all come full circle once we prove what we can do together. We are different because our platform and services bridge between two problems: lack of employability and lack of resources. The true matchmaking tool for experience!

Survey results

Questions	Responses
Which best describes you?	Student (70%) Graduate (35%) Self-Taught IT Pro. (10%)
Do you find it difficult to find volunteering opportunities in the Cyber/IT Industry?	Yes (45%) No but I haven't volunteered before in the IT industry (45%) Maybe but I have volunteered before in the IT industry (10%)
Do you believe volunteering helps enhance your industry experience?	Strongly Agree (45%) Agree (45%) Neither agree nor disagree (5%) Disagree (0%) Strongly disagree (5%)
Fortify aims to support and safeguard technologically vulnerable organizations. Do you believe there is a shortage of volunteering opportunities in the Cyber/IT Industry?	Yes (90%) No (10%)
In your opinion, are smaller organizations more disadvantaged when it comes to understanding their online responsibilities?	Always (30%) Usually (35%) Sometimes (30%) Rarely (5%) Never (0%)
Do you believe smaller organizations tend to be underrepresented and are unable to properly source Cyber/IT guidance?	Yes, they do not have adequate funds or knowledge to source help (95%) No, they are usually well protected (5%)
Have you assisted such organizations in the past? If no, would you be willing to assist?	Yes (90%) No (5%) Lightly (5%)
What excites you about volunteering for such organizations?	None-Monetary Incentives/Perks (0%) Build a network portfolio (20%) For the experience (55%) I struggled to find employment in my industry (15%) I am not excited about working for free (5%) Satisfaction and sense of achievement (5%)

Advertisement and recruitment strategy

Cybersecurity is a very competitive market and Fortify will face a strong competition from already established cybersecurity service providers and vendors. Many of these companies have been operating in the market for a long time employing strong sales and marketing teams with resources at their disposal and have created a very competitive market discouraging new start-ups. But our core values, business strategy and objective in providing a free service to small business entities though volunteers will allow us to have a strong foothold in the market. There is a very high demand for cybersecurity professional in current market, therefore recruiting and retaining volunteers is challenging. But our recruitment strategies such as partnerships with universities and vocational training institutes and internship programs are designed to overcome this situation. The volunteers have the opportunity work in real business environments engaging with business and industry leaders for unique experience to enhance their prospect to become a leader in the industry.

For Fortify to sustain in very competitive cybersecurity market, we must maintain a very strong volunteer recruitment program and we also must maintain a retention program for experienced cyber security professional who are willing to volunteer with us and to mentor junior volunteers. In order to achieve our recruitment goals we must maintain robust marketing and advertisement campaign targeting every sector. Following are our main recruitment campaign methods we focus on:

- Fortify website: who we are, what we are doing and our success stories.
- Partnerships with universities and Vocational Training Institutes.
- Partnerships with Cybersecurity vendors.
- Refer a friend.
- Social Media campaigns.
- Media engagements, news articles, cybersecurity journals and news boards
- Cyber Security Forums.
- Partnerships with large retailors for incentive and discount programs.

SWOT analysis

	Positive	Negative
Internal	**Strengths** • Services provided by volunteers – very cost effective. • Can operate as a non-for-profit. • Volunteers range from 18 – 65+ & can provide a range of experience and training. • Professional consultants with broad skills in cybersecurity. • Self-assessment tools available. • Online Australian based company that links matchmakes organisation to volunteer. • Fully functional website. • Fortify solely operates online.	**Weaknesses** • Organisation in early stages – needs to mature in its operations. • Very few registered volunteers. • Very few registered organisations. • Organisation could become redundant; all volunteer work halts. • Volunteers could leave if they find a better opportunity. • No marketing tactics have been developed or employed.
External	**Opportunities** • Platform fills a gap in the market for small organisations that generally cannot afford good cybersecurity services. • Optimize website and employ marketing tactics to drive more traffic. • Create a database to query all volunteers as per skills, expertise etc. • Very few competitors, virtually zero in Australia. • Provides an opportunity for employment, and experience. • Able to create safer & more communities.	**Threats** • Other platforms similar to Fortify may expand their services to Australia to compete with us. • Legal responsibilities and duty of care on Fortify if volunteer does something wrong. • Volunteers may share confidential information with their peers. • Volunteers could pose as black hat hackers to gain insider information. • May heavily rely on donations to continue operations. • May expand too quickly and need more resources to operate.

Strengths

The Strengths listed in the SWOT table show that Fortify works as a non-profit organisation, thrives on diversity, and is accessible globally through its strictly remote servicing. These key strengths indicate that Fortify should continue optimising its online servicing system and continue to focus on their volunteer diversity allowing clients to feel more inclined to reach out to Fortify's staff for help. Although Fortify can reach overseas, the company should continue to focus on its locals and build that relationship with Australia for the most efficient and effective growth in name, popularity, and revisiting clients / customers. With Fortify's developing feedback system, Fortify can gauge where it lacks customer satisfaction allowing the company to prioritise its time and resources to build and better service for its clientele.

Weaknesses

The weaknesses listed above are very much time induced, this is due to the fact Fortify is still in its development stage and its services and work processes are unique to other generic cybersecurity consulting companies. Combating these weaknesses (as listed), starts with marketing, with a grounded marketing plan and strategy implementation, Fortify can efficiently spread its name through online sources such as social media, radio, emailing, and paid promotions on Google etc. in due time, lack of registered volunteers and organisations will be redundant respectively. It is expected that volunteers are to come and go throughout Fortify's lifecycle, however, Fortify strives to educate volunteers of all knowledge levels with training programs run by senior / experienced cybersecurity enthusiasts. Doing so will entice the younger generation to get on-board with volunteer work which in-turn, aids with diversity as well as the lack of registered volunteer, as listed.

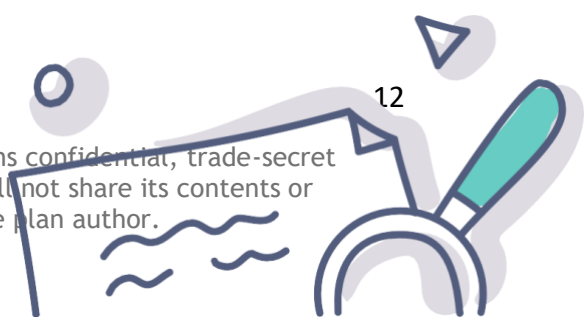
Opportunities

Taking full advantage of the current opportunities listed above may be difficult in these early development stages. Fortify's advantage, however, is the unique service it provides to its clientele, this results in the opportunity to take lead in a small market with large growth potential. Along with this, Fortify can target market ploys

toward small businesses and education institutions with a focus on being a viable, affordable, and business changing service taking specific advantage of those smaller businesses that are not cyber aware with no security implementations in their businesses. Fortify's training scheme creates opportunities for volunteers' self-growth in terms of knowledge, communication, and professionalism, making the volunteer role a great opportunity for graduates as well as seniors looking to grow their networks via helping others.

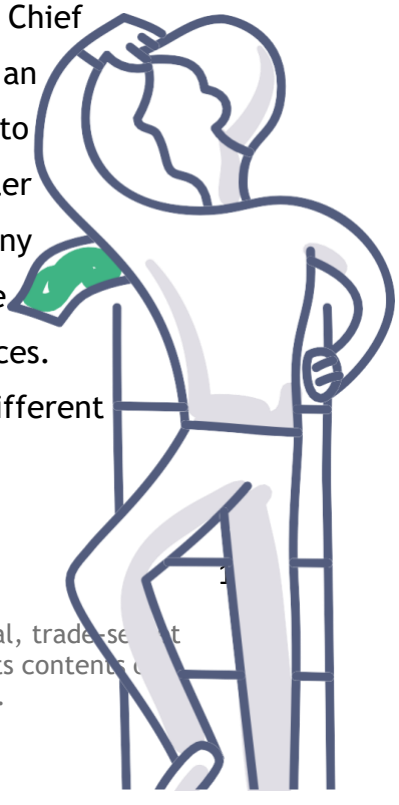
Threats

Threat response and monitoring should be among Fortify's top priorities. Legal threats such as the legal responsibilities volunteers undertake, and confidential information volunteers are exposed to whilst at Fortify can be safe guarded through extensive sign-on contracts explicitly mentioning the criminal act of sharing confidential information or using confidential information for self-benefit will result in legal action taken against the user. To combat against inexperienced volunteers making mistakes, Fortify has developed an escalation system allowing for a second available volunteer (with more experience) to become in the job case, this is to prevent a waste in time, resources, or any legal implications / accidents caused by the volunteer if they are unsure on the "next step". Fortify being a non-profit organisation, has contracting with the government in relation to funding and resources, If Fortify's growth is exponential and an increasing rate, the organisation can yes, rely on donations, but also apply for further government grants to fund growth such as employment and equipment. Fortify will continue to grow its marketing footprint through extensive design and research, this will help Fortify stay relevant and competitive in the case of other organisations join the share market. Fortify's sole focus on its local community and home country will allow it to have that step ahead against international organisations seeking to advertise in Australia.



Operational plan

Fortify's operational plan outlines the process of engagement that organisations required to follow to ensure correct resources are assigned for assistance with their cybersecurity needs. The operation plan also highlights the step taken by Fortify in engaging with these recognitions and delivering the required services. Following the registration process and completion of a questionnaire, Fortify will sit as the consulting body between the customer (company) and the volunteer to create pairings of skills from a pool of retained volunteers to the customer requirements. Depending on the customer requirements, a matchmaking tool will generate a scoring suggestions to the clientele, that aims to ease the selection processes and facilitate for the communication process between a volunteer and a company. On completion of work between the clients, the volunteer would be allowed to develop a portfolio of work done to showcase in their resume. The Volunteers will be assessed on skills from the questionnaire provided as well as developing an understanding of what they wish to get out of the pairing and any upskilling or education that could help them progress their own career. This could be in cross volunteer workshops (senior volunteers/Fortify consultants teaching or mentoring a junior) or from tasking requiring personal research and development to complete the company's requirements. Fortify as an operating organisation will need a number of full-time personnel to see to the day-to-day operations during the initial period of Fortify's operation. The team structure will require a Chief Executive Officer (CEO), a Chief Financial Officer (CFO) and an Administration Officer (AO) as a minimum senior leadership team to achieve continued viability. Below these personnel will be a smaller team of operating consultants (OC) in charge of volunteer / company pairing and supervision of tasking and workloads than will later be exchanged with volunteer alumni to minimise the cost of resources.
At the bottom layer sit the Volunteer IT professionals (V), all at different levels of expertise.



Operational procedures

Marketing

Fortify's marketing strategy will focus on the innovative and unique services Fortify have to offer. The company's marketing strong point should focus on Fortify being a non-profit organisation that thrives and prides itself on hiring volunteer cybersecurity enthusiasts with all different skill-levels and skillsets. To implement a successful marketing strategy, Fortify must clarify / identify their goals. The main marketing goal is to attract and complete sales, whilst this is common in most companies, Fortify must focus on different aspects such as growth, volunteer attraction, and client attraction.

At this point in time Fortify is strictly an online remote service, therefore the majority of its advertising will be conducted there. To ensure the most is made out of the time and resources spent for online advertisement, Fortify need to optimise some key aspects to get the name and service known.

- Optimise web design (as this is Fortify's main platform).
- Search engine optimisation (Investment to improving ranking in searches).
- Pay-per-click advertising (Investment to place ads in google searches).
- Social media marketing (Connect to target and non-target audiences of all generations).
- Content marketing (Marketing interesting information that may pull new clients or audiences in).
- Email Marketing (Reliable / direct marketing to target specific potential clients)

Whilst our target audience is likely to predominantly engage with us through online forums as listed above, we may still utilise more traditional advertising platforms. This could be completed through the following:

- Attending industry specific conventions to discuss implementation of Fortify within other organisations.
- Pitching directly to institutions such as Universities and advertising at campus events.
- Informative flyers and pamphlets.
- Business cards.

Fortify's advertising strategy has a specific focus on the target audience of small businesses and institutions with a need for improvement of their cyber security infrastructures and upskilling in such areas. By focusing the strategy design on online forums, we are able to reach the target audience through widespread and efficient techniques. The utilisation of social media, search engines, and email advertising allows Fortify to be discoverable at any convenient time or location for its desired clientele. This strategy also requires industry specific marketing by making physical connections with those in our target audience. By making personable connections and being provided with platforms to pitch our company ideals, we are able to grab the attention of prospective clientele.

Fortify is planning on monitoring paid advertisements through social medias such as Facebook, Linked In, Instagram, Twitter, YouTube and Google in which we will utilise analytics through their websites where we can monitor the success of individual posts. Fortify will review the analytics on a quarterly basis, to identify which social media posts are having the most effective outcomes. Each quarter, the marketing team will discuss the following –

- Which posts are receiving the most single-page visits.
- What posts are resulting in the use of Fortify's services.
- Revisit of individual advertisements and what impact this is having on attracting both individual users and companies.
- What changes, if any, need to be made.

Furthermore, Fortify will also optimise search engines to increase its visibility and ensuring reviews, and ratings in Google will be monitored regularly to improve

services. Fortify will implement and optimise its current marketing plan through the use of a Customer Relationship Management Database which allows data to be sorted into three categories.

- Operational – Streamlines sales, marketing, and service tasks.
- Analytical – Improves future planning and aids in decision making of how to best serve customers.
- Strategic – Shared data and information systems across business units.

This will allow Fortify to reorganise and optimise costs and resources efficiently, therefore progressing the company forward and allowing for appropriate planning to occur in future so that it is clearly identifiable as to what is working and what needs adjustment.

Questionnaire

The organisation questionnaire is designed based on guidance from The Australian Cyber Security Centre (ACSC). Based on responses, the survey questionnaire will produce maturity level data, “0” for very week cybersecurity maturity to level 3 with excellent cybersecurity maturity. This date will then be used to ‘match make” capabilities required from our volunteer consultant to assist the organisation with their needs. The questionnaire consists of three blocks of questions:

Block 1 – has eight sections which are as per the ACSC Essential 8 maturity model
Q1 - "Application control" - Do you/your organisation control who and how software is installed and managed on your devices?"
Q2 -"Patch applications" - Do you check of out-of-date unsupported version of your application/software and update on a defined regular basis?
Q3 - "Configure Microsoft Office macro settings" - Has your organisation Disabled Microsoft Office macros in documents, spreadsheets and other Office products?"
Q4 - "User Web Application Hardening" - Does your organisation have centralised access to identify and/or disable Web Application CVEs (Common Vulnerabilities & Exposures)?

Q5 - "Restrict Administrative Privileges" - Does your organisational structure limit system and data access only to authorised members?
Q6 - "Patch Operating Systems" - Do you have an update/patching schedule for your Operating Systems (e.g. Windows), Servers and back-end systems?"
Q7 - "Multi-Factor Authentication" - Do you have basic secure processes in place to authenticate who is trying to login?
Q8 - "Regular Backups" -Do you keep a record of all data using correct naming conventions and dates to be accessed when necessary?

Block2 – covers the organisation's understanding and needs on Prevention, Governance and Audit. The areas covered in questions for this block are:

- Penetration Testing Scoping
- Development Cybersecurity Policies
- Development Cybersecurity Strategy
- Delivering Cybersecurity awareness e.g. Phishing emails, Social engineering awareness
- Produce Cybersecurity Compliance Reporting
- Cybersecurity advisory - high Level (e.g.) assist with completing questionnaire

Block 3 – covers questions on organisation capability to respond to critical cybersecurity incidents and covers the areas of:

- Ransomware attack - restoring services e.g. from backup
- Website compromised - restore website back to normal and fix vulnerability
- User account compromised & systems accessed - clean-up user account and block/reset compromised account
- Data loss /theft - Forensic analysis of what was lost and how to inform authorities
- Vulnerabilities in the environment such as malware - detect and clean-up

Example of survey data output:

Survey questionnaire questions	Survey questionnaire maturity Level	Help required
Q1	2	
Q2	1	X
Q3	3	

"While no set of mitigation strategies are guaranteed to protect against all cyber threats, organisations are recommended to implement eight essential mitigation strategies from the ACSC's Strategies to Mitigate Cyber Security Incidents as a baseline. This baseline, known as the Essential Eight, makes it much harder for adversaries to compromise systems."

Source: (ACSC)

Essential 8 Maturity Model is a prescriptive set of standards developed by Australian Cyber Security Centre (ACSC). These 8 areas of focus provide accurate guidance on what organizations need to do to improve their maturity and posture in cybersecurity. These mitigation strategies help organizations protect themselves against various cyber threats. See Appendix 1 to view the questionnaire.

At Fortify we selected Essential 8 as our core platform to assess organizations' needs to uplift their cybersecurity posture. The reason for selecting Essential 8 versus another framework or set of standards is:

- ACSC developed the model based on their experience in producing cyber threat intelligence, responding to cyber security incidents, and conducting penetration testing.
- They are based on Australian governance compliance and requirements
- They cover better than 85% of cybersecurity risk mitigation

- ES8 provides a set of measurements, procedures, rules and guidelines to measure progress
- Essential 8 provides the basis for Fortify to build a questionnaire and ask organizations consistent questions toward assessing their cybersecurity requirements
- Essential 8 provides the basis for Fortify to build a list of skill requirements and associated selection criteria for our volunteers

Matchmaking

Fortify provides organisations with recommendations for a suitable cybersecurity volunteer consultant based on their need and the consultant professional skills. To assess the organisation's cybersecurity capabilities, Fortify formulated a set of questions based on Essential 8. Data accumulated from the questionnaire will be used for a Fortify volunteer-to-organisation "matchmaking" process. The companies and volunteers will be able to see other profiles as well, but the matchmaking tool will facilitate for easier cooperation. The questionnaire is designed to produce

maturity level data, the data will be used to match suitable volunteer consultants to work on required cybersecurity gaps and technical solutions.

Data matching example:

Survey questionnaire questions	Survey questionnaire maturity Level	Help required	Volunteer 1 Skill level 0 to 3	Volunteer 2 Skill level 0 to 3	Volunteer 3 Skill level 0 to 3
Q1	2		3	1	2
Q2	1	X	0	3	1
Q3	3		2	2	2
Qx					

In this example Volunteer 2 is most suitable to assist as they would have the highest level of skill for their gap requirement as identified by the self-assessment survey.

The Volunteers consultants will be asked questions aligned with those of the self-assessment questionnaire provided to the organisations. For example, for Block 1, “Essential 8” the following skill level questions will be asked to our volunteers:

1. “Application Control” - Ability to configure user access rights centrally managed by group policy
2. "Patch Applications - Ability to work with application vendors and ensure latest software versions are installed and maintained including patching and vulnerability management.”
3. "Microsoft Office Macro Settings - Ability to configure Microsoft Office macros in documents, spreadsheets and other Office products are disabled"
4. "User Web Application Hardening" - Ability to analyse different CVEs, what they mean, where to find them and how to disable them.
5. "Restrict Administrative Privileges" - Ability to implement just-in-time (JIT) or PIM or Palm and or other mechanisms and processes to Restrict administrative privileged access to IT systems

6. "Patch Operating Systems" - Ability to Patch operating systems and run and action items found by Vulnerability scanners
7. "Multi-Factor Authentication" - Ability to Implement and test Multi-factor authentication systems and services Such as Cisco DUO, Okta and Microsoft
8. "Regular Backups" - Ability to set up, configure, implement and test backup and DR systems to ensure reliable recovery in a Crypto lock or systems loss.

Strategic formulation

***Note**: This shows the process after the volunteer and company have chosen to cooperate.*

Following the matchmaking process, which aligns our volunteer cybersecurity professionals with the organization needs identified in the questionnaire, there are some additional steps prior to the official engagement.

1 – Fortify, the volunteer associated with the work and the organisation sing a non-disclosure agreement (NDA). This ensures there is a clear understanding that information of cybersecurity gaps and the assistance provided to resolve issues does not go outside this engagement circle.

2 – Scope is developed, and which clearly outlines the objectives and deliverables of the engagement and the project. The scope will need to be signed by authorised executives from the organisation and Fortify and the organisation.

3 – Although Fortify is a not-for-profit organisation, there may be nominal costs associated with the project, for example solutions that require procurement of software. This may require a commercial agreement which outlines associated costs and terms of payment. The agreement will need to be signed by authorised executives from the organisation and Fortify and the organisation.

4 – Project timelines will be set and agreed upon. The Agile project methodology will be used, and objectives will be delivered in aligned sprints. End of sprits reports will be provided to the organisation's executives

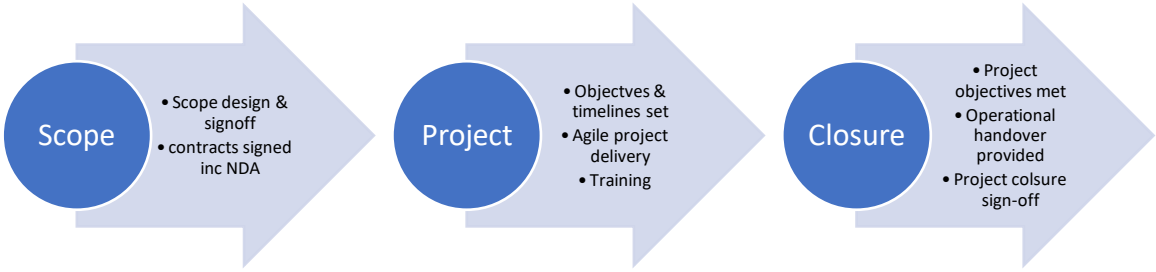
5 - Management by exception will be agreed at 3% of project costs and resource allocation. Should project costs or resources allocations exceed 3%, a management

by exception report will need to go to the organisation's board for approvals of any additional founding or resources.

6 – Project will proceed as per agree scope and as per agreed deliverables, however in the duration of the works, there may be additional vulnerabilities identified which require additional objectives to be met. If these additional works don't fall within the cost allocation of 3% contingency reserves, the organisation's board will need to above additional scope.

7 – Fortify consultants will provide necessary training for a new cybersecurity solution or for any new or changed business process. This will be part of operational handover of project deliverables.

8 - Upon completion of the works as per scope and schedule, a full project closure report will be presented to the executive and board for project signoff and closure.



Strategic formulation example – backups

The following step guide is an example of the implantation of the strategic formulation guide. This is the process post to the client and volunteer making official contact and the job ticket is accepted.

1) Fortify, the volunteer associated with the work and the organisation sign a non-disclosure agreement (NDA). This ensures there is a clear understanding that information of cybersecurity gaps and the assistance provided to resolve issues does not go outside this engagement circle. In this case, ensuring that company data is secure in terms of privacy and integrity. Fortify does not hold data but simply guide and ensure the process of the project / case is carried out to Fortify's standards. This step applies to any / all cases and job tickets as part of Fortify's legal policies.

2) Scope of the project is to successfully backup all Company X data including server, desktop, and laptop data owned by the company using Microsoft Azure's cloud backup service. The timeframe of this process is to take an estimate 31 days (possibly more days during the monitoring or migration phases).

3) External costs are required for the services of a third-party vendor servicing in on-site / off-site data backups. It is estimate average monthly payments for such service are between $500 - $1500 AUD (this may vary depending on data amount and data consumed monthly). This may require a commercial agreement which outlines associated costs and terms of payment. The agreement will need to be signed by authorised executives from the organisation and Fortify and the organisation.

4) A timeframe of 31 days has been allowed to complete the project. The Agile project methodology will be used, and objectives will be delivered in aligned sprints. End of sprits reports will be provided to the organisation's executives.

Times may vary due to unexpected delays (timeframes are based on average time taken in similar cases).

5) Standard Fortify project contingency is 2% - 5%. This is to prevent delays in service fees and extra potential costs for data that was not audited / assessed at the beginning of the project. If resources exceed agreed limit and the contingency plan is put into play, an exception / approval report will be sent to Company X's executives for additional resources.

6) Project progress review to revise / reiterate scope and deliverables agreed upon in contract. Consultation on any newly developed deliverables or project changes is to be discussed, ie: data amount to be backed up, encrypted data to be backed up, change in backup services (VM, SQL databases, on / off-premises databases etc). Contingency plan may be re-evaluated is resources are at limits.

7) Fortify standard training requirements to provide all necessary awareness, advisory, and practical training to ensure all members are educated in data backups, data security, data placement, and data consumption, as well as software training in relation to Microsoft Azure logging and backup processes.

8) Project progress is compared against project scope and deliverables to ensure the project is complete to a satisfactory standard on both sides (client and volunteer). A full project closure report is provided to Company X executives to be signed and dated for completion and closure.

9) Post project monitoring may take place to ensure post project processes are running smoothly and there are no technical / knowledge issues present.

Strategy implementation

Once the analysis and approach, formulation process is complete, an appropriate implementation plan as part of a project will be developed. The plan will include deliverables required for the success of the engagement.

For the backup user case example, the project implementation plan will include the following populated template:

User case example: Back-ups

PROJECT NAME	Fortfy Backup / Migration for Company X			**PROJECT MANAGER**	Volunteer ID: A2453
PROJECT LOCATION	Burwood			**PROJECT DELIVERABLE**	Backup client data
PROJECT SCOPE	To backup Company X data to a secondary location (cloud)				
COMPANY	Company X				
CONTACT NAME	Andrew Smith				
MAILING ADDRESS	123 Example Rd, Melbourne 3000				
EMAIL	ASmith@CompanyX.com			**PHONE**	0412 456 789
START DATE	12/1/2022	**END DATE**	12/31/2022		

SL. No.	ACTIVITY/ TASK NAME	RESOURCE ASSIGNED	START DATE	END DATE	DURATION (in days)	TASK COMPLETE
1	Audit / Assess Company X environment		12/1/2022	12/5/2022	5	Y / N
2	Report on data amount and type		12/6/2022	12/11/2022	5	Y / N
3	Consult Company X with results		12/12/2022	12/17/2022	5	Y / N
4	Contact / Contract with Azure (confirm pricing and backup solutions)		12/18/2022	12/22/2022	5	Y / N
5	Implementation of backup strategies to Company X		12/23/2022	12/27/2022	5	Y / N
6	Monitor results and report on completion of project		12/28/2022	12/31/2022	5	Y / N

Strategy monitoring

Upon completion the project Fortify will provided a benefits realisation analysis which will include the objectives delivered and the value they have added to the organisation.

Benefit Description – The organization and Fortify will define the benefit that will be delivered by the project as per the agreed engagement.

In this case for example, it will be to ensure the "last line of defense i.e., back of critical data" is at optimal levels to allow the organization to recover from a major catastrophic event.

List of benefits – in this example the list of benefits will include:

- Reliable infrastructure solutions are implemented and tested to ensure data is baked up and be able to be recovered
- Risk mitigation process is in place and available should the organization need to revoke disaster recovery
- Audit and reports can be generated providing the organization's board with assurances that the business is able to recover form a critical event
- Having reliable back and recovery systems implements provides the opportunity for less costly cybersecurity insurance (cost reduction in operations)

Benefit Measures

The table below provides an example of the benefits delivered by the backup improvement project for the organization. The table includes the expected benefits, measurements, frequency, baseline and target measures.

Benefit Measurement Plan

Benefit	Measurement Metric	Measurement Technique	Measurement Frequency	Baseline Value	Target Value
Reliable infrastructure	Test reports generated of successful backups	% of success or failure of backups with reliable data	Monthly	90%	100%
Risk mitigation process	DR plans incorporate updated process	Documents are implemented and tested in playbook scenario	Six monthly	85%	98%
Audit and reports	Data restoration reports are provided to audit and risk committee	Report with charts indicating quality of data at percentage levels	Monthly	90%	100%
cybersecurity insurance cost reduction	Costs in terms of budget	Percentage of savings	Annual	$15,000.00	$10,000.00

Client feedback

Project closure report will be provided to the organisation. The project closure will include all elements of handover to the organisation which included training and RACI matrix (Roles & Responsibilities) to support processes and solutions in operations. As part of project closure a lessons learned report will be generated which will include customer feedback via a survey and will incorporate sign-off of benefits realisation. The customer feedback and associated data will be stored in Fortify's "lessons learned" register and will be used towards improvements on delivery of services.

Market and production milestones

First term (first 6 months of Fortify's Operations):

- Start the cooperation with 3 major educational institutions to promote the volunteering opportunities with Fortify.
- Provide oversight for all commenced projects and gather responses from clients to improve the services.
- Launch advertising campaigns to attract customers
- Create selection criteria for mentoring program and use survey responses from first term to determine mentors and training program for future terms
- Gather comprehensive feedback clients to improve websites and services

Second term (First 12 months of Fortify's Operations):

- Create a portfolio of previous customers to attract investors
- Analyse client data to better distribute volunteers amongst clients
- Launch mentoring program that will reduce resources needed for the operations while simultaneously improving performance.

Conclusion

All work presented has been developed by:
Paulina Katarzyna Wesolowska, Bill Petridis, Luke Newton, Muhammed Khudruj, Ranjan Weerasinghe, Manav Lath, Kevin Kidd and Aayush Talwar.

Executive Summary written by Paulina Wesolowska
Business objectives and services written by Paulina Wesolowska
Marketing Analysis (Competitors and clients) written by Muhammed Khudruj with Manav Lath and Paulina Wesolowska as contributors.
Marketing Analysis (Advertisement and recruitment strategy) written by Ranjan Weerasinghe, Aayush Talwar and Paulina Wesolowska.
Marketing Analysis (SWOT analysis) written by Muhammed Khudruj and Luke Newton with Bill Petridis as contributor.
Operational Plan written by Kevin Kidd, Bill Petridis and Paulina Wesolowska.
Operational procedures (marketing) written by Luke Newton
Operational procedures (questionnaire) written by Bill Petridis
Operational procedures (matchmaking) written by Bill Petridis
Operational procedures (Strategic formulation) written by Luke Newton and Bill Petridis
Operational procedures (Strategic implementation) written by Bill Petridis
Operational procedures (monitoring) written by Bill Petridis
Operational procedures (feedback) written by Bill Petridis
Market and Production Milestones written by Paulina Wesolowska
Conclusion, formatting and design made by Paulina Wesolowska

This document has summarised and outlined the developed work surrounding Fortify's planned operations. Fortify's GitHub repository includes all work and documents such as:

Questionnaire for volunteers and clients can be found under **Volunteer/Consultants Assessment**.

Details on Essential 8 and other frameworks can be found under **ESS8 VS NIST**.

User case for back-ups can be found under **Fortify Backup Process Draft and User Case - Backup example**.

The marketing strategy, developed in trimester 2 and 3 can be found under **Fortify Marketing Plan V 1.1**.

Guidelines for volunteers in case of an incident response scenario can be found under **Incident Response Plan and Guidance**.

User case for incident response can be found under **Incident Response Scenarios**.

User case for cyber awareness can be found under **Awareness About Cyber**.

User case for 2-factor authentication can be found under **Use Case - 2-factor Authentication**.

User case for penetration test scoping can be found under **Penetration Test scoping**.

User case for system hardening can be found under System Hardening based on **Ess 8**.

User case for cybersecurity advisory can be found under **Cybersecurity Advisory**.

The emailing templates can be found under **email templates**.

Details and survey questions for the feedback post-op system can be found under **post-op system feedback**.

Work completed in previous trimesters is available in GitHub Repository of Hardhat.