School of Computing and Information Systems
SWEN90016 – Software Processes and Management, Semester 2, 2022
Dr. Andrew Valentine

Assignment 1: Individual Submission

Assignment Release Date:	**05th August 2022 4:00 PM AEST** (End of Week 2, Refer to Subject Handbook)
Assignment Submission Date:	**26th August 2022 4:00 PM AEST** (End of Week 5, Refer to Subject Handbook)
Assignment Weight:	20% of Total Subject Score (Refer to Subject Handbook)

Overview:

This is an individual assignment focusing on Project Management and Software Development Life Cycles (SDLCs) topics. This assignment aims to develop understanding of various SDLCs and their relationship to other project aspects described in the Case Study given in Appendix A.

Learning Outcomes:

By a thorough analysis of the project described in the case study, students will demonstrate the ability to:

- Identify the goals of the project
- Identify the key characteristics of the project
- Identify the risks in the project as evident at the start of the project
- Justify the choice of an appropriate software development lifecycle (SDLC) model for the project

Submission Instructions:

Read and analyze the case study 'Resilienza Business Continuity Services' in Appendix A, and answer the questions related to the software product to be developed. Make sure to mention the question numbers properly for the answers. Your answers must have the appropriate justifications and citations where appropriate; use IEEE citing and referencing (More information on referencing - recite (unimelb.edu.au)). While references in the case study have been given from general sources to facilitate a better understanding of the case study as a whole, remember to use only academic references in your arguments and not general sources from the internet. An excellent source to search for any academic articles is Google Scholar.

Submit your work using the Turnitin link on the Assignment tab on Canvas. From the SWEN90016 CANVAS page, select Assignments – Assignment 1 submission link from the menu. Follow the instructions and upload only a PDF file containing your responses to the assignment questions.

You must include your *Name and Student ID* in your submission.

Late Submissions:

If you need an extension for the project, please email the Subject Coordinator explaining your situation with supporting documentation (medical certificate, academic adjustment plan, etc.).

The assignment submission is due at 4:00 pm AEST sharp. Any submissions received past this time (from 4:01pm onwards) will be considered late unless an extension has been granted. There will be no exceptions. There is a mark penalty of 10% for a late project, plus an additional mark penalty of 10% per 24 hours.

Academic Misconduct:

Academic misconduct by students is not permitted in any form. Work submitted by students for assessment must be their independent work. The University Policy and Procedures for Academic Misconduct can be found at: https://academichonesty.unimelb.edu.au/#policy.

Word Count:

As a guide, the approximate length expected for this assignment is around 1750 – 2000 words (about 4 to 4.5 pages). This is an approximate estimate based on normal spacing in Microsoft Word, using Sans-Serif type face fonts such as Calibri or Times New Roman size 11, and about 500 words per page). Word limit excludes the cover page and references that are used in support of the arguments.

The suggested word limit guidelines are to give you an estimate about the expected length for arguments. While a good argument that exceeds the suggested word limit by a small margin will not be penalized, be mindful of not going way off the suggested limits which may incur a penalty. Precise writing is a skill you develop as a part of academic endeavor, and it is a good practice to be concise in expressing your arguments.

Assignment Assessment Criteria:

This assignment is used to demonstrate your Intended Learning Outcomes (ILO's) 1 – 5, as specified in the Subject Handbook. The assessment will be evaluated based on the quality of analysis and overall arguments. You must use a combination of the core learning areas expected to address this assignment, PLUS demonstrate your depth of understanding in terms of the applicability of these core areas to the given case study. A sample assessment rubric for this Assignment can be found along with the Assignment Specifications in CANVAS.

Assignment 01 Questions

Section 1: Short Research Questions

Q1 (2 Marks) - Identify the business case (need) for the project. (Suggested Word Limit: 50 – 100 words)

Section 2: Extended Research Questions

Q2 (4 Marks) Identify three project constraints from this case study, that would make this project difficult to execute. Briefly explain why each of these constraints are important in the context of this case study. Clearly explain how each of the three constraints independently apply to the Case Study. (Suggested Word Limit: 450 – 500 words)

- *At most*, only two of the three constraints may be from the generic PMBoK (Project Management Body of Knowledge) constraints of scope, cost, or schedule.
    - You don't have to use scope, cost, or schedule at all if you don't want to. You just cannot use these for more than two of the three constraints.
- *At least one* of the three constraints must be something other than from the generic PMBoK constraints of scope, cost, or schedule.
- If you only identify the three generic PMBoK constraints of scope, cost, and schedule, your marks for this section will be capped at a maximum of 2 out of 4.

Note: Constraints identify the limiting factors that can impact the quality and overall success of the project.

Q3 (4 Marks) Identify three things that could go wrong in this project – otherwise known as *Risks*, resulting in the project not achieving the intended goal/s. Clearly mention the *Justification* and *Impact* that each of these risks could have on the project. (Suggested Word Limit: 250 – 300 words)*

- Ensure that you identify risks that are *unique to the characteristics of this case study*, rather than generic risks that can occur in any project.

For example, generic risks that can occur in any project include project members leaving the project, or project running out of budget before completion (to name a couple).
* - For both Q2 and Q3, ensure that your arguments are clear enough to differentiate constraints / challenges (Q2) are not risks (Q3) and vice – versa.

Section 3: Discussion

Q4 (10 Marks) Discuss two possible Software Development Lifecycle models (SDLCs) that you would consider for this case study. This should include the pros and cons of each of your choices, referring to specific project characteristics as outlined in the case study. Use at-least two external references to support your argument. (Suggested Word Limit: 1000 – 1100 words)

Note: Identifying the SDLC models as described in the lectures will not address the requirements of this question, and will attract a low mark. Be clear and specific about how the characteristics/capabilities offered by the SDLC model *apply to the characteristics / constraints / challenges of this case study*. i.e. avoid giving generic definitions or statements about the SDLC – you need to directly link what you write to the case study.

Appendix – A

Resilienza Business Continuity Services

Case Study Background - A Brief Overview of Business Resilience:

Business disruptions to organizations is not a new phenomenon. They happen for a variety of reasons that impacts the continuity of the business to serve their customers. Disruptions can also create a challenge to the existence and survivability of the business in the long run, based on the nature of the disruption. One such reason for the disruption is the challenge for organizations to protect their confidential and intellectual knowledge assets in an ever-changing technology landscape. A key driver in this scenario is the threat of cyber-attacks to the organization's infrastructure. A cyber-attack is usually an unwanted and unauthorized intrusion or offensive manoeuvres on the information technology systems of organizations, usually comprised of a network of computers. These activities are unwelcome assaults that are primarily aimed to create an adverse impact to the source of the attack – such as stealing, altering, or exposing sensitive, private and confidential information from these systems through unauthorized access. This can also be viewed as a targeted set of actions performed by external actors to exploit vulnerabilities in the technology infrastructure and computer data networks, to gain illegal access with a malicious intent. Some of the common types of cyber-attacks are Malware, Phishing, Distributed Denial of Service, SQL Injection and Zero Day exploits (to name a few)[1]. While the cost of mitigating a cyberattack such as a data breach rose to about 4.24 million dollars in the United States[2], it has been reported that the average cost to address a cybercrime attack for a business in Australia is about $276,000[3].

Business disruptions can also be triggered due to natural disasters that are driven by long terms shifts in temperature and weather patterns (climate change). The economic costs to businesses and their infrastructure due to natural disasters are staggering, as discussed in multiple research reports[4][5].

Key decision makers specially at medium and large-scale businesses, are now acknowledging the criticality of disaster planning for business resilience and continuity, as an indispensable function in the administration of a business. This is primarily driven by research studies attesting to the importance of planning business continuity, wherein it has been found that about 80% of companies that have not managed to have a viable disaster recovery plan will fail within a year of encountering a major disaster[6].

Business continuity is not only a focus area of few large-scale organizations, but they also form an important organizational planning area across diversified domains such as healthcare and manufacturing organizations. For example, healthcare organizations have been a chosen target for ransomware attacks. The paramount nature of their operations with an infamous appreciation for IT security in this industry motivate ransom ware actors to target this industry. The ransomware attack on Ireland's health care system[7], City of Atlanta's IT systems[8], and mass infection of computers at a UK hospital network[9] are some of the examples that made front page headlines. Addressing these critical issues is one of the key focus areas of business resilience planning activities.

Resilienza Business Continuity Services

Resilienza Business Continuity Services (hereafter referred to as 'Resilienza') is a company founded in January 2002, in the aftermath of September 11 attacks in the United States. The company has its headquarters in Santa Clara, California, United States, and focussed on providing IT business production and business resilience services[10][11] to organizations. This is to ensure business continuity for the clients in the aftermath of natural or man-made business disruptions. Resilienza has over 3000 employees working from offices across 15 countries, with an annual turnover of 300 million dollars. The company uses its core expertise in business resilience to serve clients safeguard their business interests, by designing and building backup production environments that are resilient and available always in the face of challenges with business continuity. The company manages over 50 mobile facilities staged in strategic locations in the United States and Europe, that are served by guarded data centres and work place facilities that are connected by a redundant and a robust global dedicated backbone of network and infrastructure services. The services of the company have been well received by its clients in the last two decades. The company recently received multiple awards as well as one of the highest scores for its 'Disaster-Recovery-As-A-Service' offerings, as reported in multiple research studies.

While the company is expanding its client base at a rapid pace due to the advent of multiple business disruption scenarios across the world in the past few years, the expansion is severely limited by the existing IT systems and infrastructure that were designed in 2002. The current IT systems have been designed to be used only by the internal customer service staff of the organization, when designing business resilient networks for their clients. For example, any new business that wishes to partner with Resilienza to explore business resilience services have to talk to a dedicated customer representative to explain their needs. Specifically, a new client needs to discuss their explicit needs for business continuity over telephone (in the event of a disruption at their main offices due to natural or man-made disaster scenarios, wherein the company employees will continue with their daily work at Resilienza' s mobile facilities, till the disruption can be addressed). During the call with the customer service engineer, they can provide their explicit business continuity needs - such as the number of remote seating locations, total laptops needed, desktop and server environments to handle specialized data processing needs, different types of printers (such as dot thermal, LED, Business Inkjet, Multifunction, 3D and laser printers, both in black and white and color printing configurations), explicit licensed software's that need to be run on these machines, and the bandwidth for networks and infrastructure support. The customer service engineer then designs the explicit configuration using the internal IT systems. This process is a pain point for both Resilienza as well as its customers for multiple reasons, the chief of them being (i) Customers need to spend long periods of time over the telephone to explain their explicit resilience needs to the customer support engineer, (ii) Customer service engineers need to present too many configurable options to customers over the telephone that can be very confusing to understand (such as different models of laptops with varying amounts of RAM and hard drive storage, and varying server grade configurations that can be chosen - to name a couple), and (iii) new technological offerings (such as laptops, printers and other IT equipment that Resilienza buys from external vendors to serve its customers) are only updated once a month in the IT systems. This also means that the customer support team has to reach out to their existing customers multiple times every month to advise them of new hardware and technology offerings that they can choose for no additional (or a small cost) for the upgrade.

In order to work around the limitations of the existing IT system and make the customer experience more meaningful, the leadership team at Resilienza have decided to revamp their existing IT system by building a new IT platform '*ConquerIT*' that is customer centric. A key feature of this new platform '*ConquerIT* 'is that all the services provided by Resilienza to its clients can be directly configured by the customers themselves, instead of spending considerable time speaking to a customer representative. At the heart of the new functionality for '*ConquerIT*' is a 'Guided Buying and Selling' engine, which helps new customers to seamlessly answers non-technical questions on the user interface and present them with the most appropriate options to select for their business continuity needs. As an example, one of the questions during the configuration process for laptops could

be 'What is the primary usage for the laptop?' – with options 'Office Documentation', 'Video Editing and Production' and 'Heavy Content Editing' for selection. If the user were to choose 'Video Editing and Production', the engine will automatically hide laptop configurations with less than 16 GB RAM from being shown on the next UI for selection by the end user. In addition, to complement the 'Guided Buying and Selling' engine to perform effectively, a new 'Business Rules Configuration' engine also needs to be developed. For example, if the user has chosen 'Video Editing and Production' as the primary use for a laptop, when the user is presented options to choose the hard drive storage for the laptop, the rules engine triggers a rule only to show Solid State Drives with a storage capacity over 256 GB for the user to select (considering video files are very huge and the fetch time latency from the hard drive needing to be very less during video editing, traditional spinning hard drives are prevented from being shown to the end user for selection, and only Solid State Drives are presented). Depending on the varying hardware options available for configuration, the business rules engine can get extremely complex with too many rules to be handled. Therefore, one of the core business needs of '*ConquerIT*' is to have a configurable 'Rules Design User Interface'. This module can accommodate new business rules that are to be created with new hardware and IT offerings that come to the market regularly, as well as deprecate rules for those IT offerings and hardware infrastructure that are obsolete. Needless to say, the 'Rules Design User Interface' module is only available to the customer service engineers of Resilienza to configure the rules for new hardware configurations that they wish to offer to their customers. The outcome of the rule changes triggers seamlessly when new or existing clients of Resilienza use the system to configure their business continuity needs.

In addition, the current IT system is severely limited when existing customers of Resilienza need to make changes or upgrades to the existing business continuity configurations that they have chosen. This scenario can primarily happen in two instances - (i) When technological advances make an existing IT hardware or service redundant, and an advanced solution offering is available at the same price point as the old solution (Example - a new advanced processor or storage offering available for the same price as an old processor or low storage capacity for which the customer was initially paying for) or (ii) Business Requirements of the customer change and they wish to make modifications to the existing configuration, that could be offered at the same price or a higher price (E.g.: For the new configuration chosen, Resilienza may be willing to absorb the higher costs to maintain its preferred relationship with the customer). In both these cases, existing customers have to call up Resilienza to discuss the changes to be done and the customer service engineer makes the required configuration and price adjustments (as applicable) changes using their existing IT systems. This activity gets more complex specially for the first scenario of technological advancements. In this case, the customer service engineers of Resilienza have to reach out to each of their existing customers individually and advise them of better technology offerings being available now for the original price the customer paid, and make the changes to their configurations as needed. This is an extremely time-consuming process and to mitigate this pain point, it is also expected of the new IT platform '*ConquerIT*' that a separate 'Configuration Change' Engine be present. The 'Configuration Change' Engine essentially exposes a 'Self Service' option for each customer of Resilienza to make changes to their existing configurations seamlessly for both the instances described above. Specifically, for the first scenario of technological advancements, an automated mail is triggered from the new IT system for all the customers individually tailored to address their specific needs, and advising them about the new hardware or infrastructure capabilities in the market. In doing do, customers can harness the new technological advancements using the 'Self Service Options' at no additional cost. This can serve Resilienza well in the long run because, increased customer satisfaction can result in repeat or extended business for these service offerings in the future.

Moreover, it is very convenient to ignore the challenges of data and configuration migration from the existing IT systems to the new IT system '*ConquerIT*'. Currently Resilienza serve over 200 customers with about 3000 specific configurations to meet their business continuity needs. Each of these unique configurations with their underlying rules needs to be mapped and migrated to the new IT platform '*ConquerIT*'. Considering that the entire business of Resilienza is built to support business continuity in disaster scenarios, it is extremely critical that there are no data migration issues (and thereby preventing this new project itself becoming a disaster scenario when trying to

address the business resilience needs of the customers). Therefore, it is also envisioned that the new IT platform '*ConquerIT*' not only has a new 'Configuration Migration Engine' to migrate the existing configurations to the new system, but also has an integrated 'Configuration Health Check' Engine to validate the configurations after the migration and alert the administrators for any failed scenarios for manual intervention.

To continue, the sales and marketing team at Resilienza have also reported that since January 2022, there has been an fivefold increase in customer leads and enquiries that have been asking for specific 'Fixed Configuration Offerings' that can serve to address the needs of small businesses at a lower price point. For example, as a business continuity 'Fixed Offering' solution for a small home office web design business, Resilienza could offer a pre-configured solution with (i) one laptop with Microsoft office and standard web design software preinstalled (like Adobe Creative Cloud), (ii) a small Black and White laser printer and, (iii) data restoration from the backups on the laptop - for the small business owner to continue work in the event of a business disruption. While there are no configuration capabilities here, this configuration can be offered at a very low price point as compared to specific configuration needs for business continuity that can serve to be expensive for small businesses. In other words, to take care of this new and emerging market in business resilience, the new IT platform '*ConquerIT*' should have 10 'Fixed Configuration Offerings' to serve a variety of small business domains such as Web Design, Media Consumption, Accounting Firms and Hospitality Services (to name a few). Based on future demand, the new IT platform '*ConquerIT*' should also support creating new 'Fixed Configuration Offerings' or modifying existing 'Fixed Configuration Offerings' to serve new and existing clientele.

Finally, considering over 50 existing customers of Resilienza have moved their entire business operations to the cloud (with many existing customers in the process of moving their business operations to the cloud in the next 5 years), Resilienza wishes to offer its existing and new customers a new service called 'Cloud Recovery'. As a part of this new service, Resilienza wishes to offer solutions that would safeguard clients against disruptions to their cloud services caused by network infrastructure and outages that are natural or man-made (such as power outages due to storms, network outages or even due to nefarious reasons such as cyberattacks). To this effect, '*ConquerIT*' should have capabilities to perform backup and recovery from existing cloud computing infrastructure of clients and use this data in the business resilience configurations of the clients, should the need arise.

Case Study References:

[1] "What Are the Most Common Cyber Attacks", *CISCO*, 2022. [Online]. Available: https://www.cisco.com/c/en_au/products/security/common-cyberattacks.html#~types-of-cyber-attacks [Accessed: 25- July- 2022].

[2] "How much does a data breach cost?", *IBM.com*, 2017. [Online]. Available: https://www.ibm.com/security/data-breach [Accessed: 25- July- 2022].

[3] "THE COST OF CYBERCRIME TO AUSTRALIA", *Infrastructure Australia*, 2022. [Online]. Available: https://www.infrastructure.gov.au/sites/default/files/Cost%20of%20cybercrime_INFOGRAPHIC_WEB_published_08102015.pdf [Accessed: 25- July- 2022].

[4] "Building Australia's resilience to natural disasters", *Deloitte Access Economics*, 2021. [Online]. Available: https://www2.deloitte.com/au/en/pages/economics/articles/building-australias-natural-disaster-resilience.html [Accessed: 25- July- 2022].

[5] Sands, Dale, "The state of disaster resilience of small businesses: 'Natural hazard' or 'disaster'", *United Nations Office for Disaster Risk Reduction*, 2019. [Online]. Available: https://www.undrr.org/publication/state-disaster-resilience-small-businesses-natural-hazard-or-disaster [Accessed: 25- July- 2022].

[6] "Business as Usual: Maximising Business Resilience to Terrorist Bombings", *U. S. Department of Justice - OFFICE OF JUSTICE PROGRAMS*, 1999. [Online]. Available: https://www.ojp.gov/ncjrs/virtual-library/abstracts/business-usual-maximising-business-resilience-terrorist-bombings [Accessed: 25- July- 2022].

[7] "Inside Ireland's Public Healthcare Ransomware Scare", *KrebsonSecurity*, 2021. [Online]. Available: https://krebsonsecurity.com/2021/12/inside-irelands-public-healthcare-ransomware-scare/ [Accessed: 25- July- 2022].

[8] Theo Douglas, "What Can We Learn from Atlanta?", *Government Technology*, 2018. [Online]. Available: https://www.govtech.com/security/what-can-we-learn-from-atlanta.html [Accessed: 25- July- 2022].

[9] Kelsey D Atherton, "The biggest ransomware attack in history is crippling UK hospitals", *Popular Science*, 2017. [Online]. Available: https://www.popsci.com/ransomware-hack-affects-hospitals/ [Accessed: 25- July- 2022].

[10] "What is Business Continuity?", *BCI - Leading the way to resilience*, 2021. [Online]. Available: https://www.thebci.org/knowledge/introduction-to-business-continuity.html [Accessed: 25- July- 2022].

[11] Erin Sullivan, "What is business continuity and why is it important?", *TechTarget – Disaster recovery planning and management*, 2022. [Online]. Available: https://www.techtarget.com/searchdisasterrecovery/definition/business-continuity [Accessed: 25- July- 2022].