QUESTION 1 **(Total: 40 marks)**

a) What is one benefit of shifting static security analysis earlier in development?

(2 marks)

b) What is one advantage and one disadvantage of releasing multiple variants of a feature to experiment with user reactions (e.g. "The Spotify Model")?

(4 marks)

c) What are two disadvantages of common lean and agile processes (e.g. Scrum and Kanban)?

(4 marks)

d) Why is functional safety important in software engineering?

(4 marks)

e) Why does software quality management focus on the development process and not on the software product?

(4 marks)

f) Explain how to use the defect amplification model to determine at which stages of development to invest resources in defect detection, and how much effort should be put into defect detection at each of these stages.

(6 marks)

g) Explain how developer productivity affects software estimates. What can an organisation do to take into account developer productivity when estimating time to complete development work?

(4 marks)

h) Consider an organisation that is following all aspects of the Spiral process for software projects in a disciplined manner. What do you believe would be the highest CMMI level at which this organisation could be rated? Justify your answer. Explain which aspects of the Spiral process contribute to your rating.

(6 marks)

i) Would formal Fagan inspections be an appropriate verification technique to use in a team following Large Scale Scrum? Justify your answer. Identify two characteristics of Fagan inspections and explain why these make it suitable (or unsuitable) to apply in Large Scale Scrum? (Your answer to this last part of the question will depend on your answer to the first part of the question.)

(6 marks)

a) What is one benefit of shifting static security analysis earlier in development?

It is more useful to use static security analysis earlier in development as it does not require a working application to perform. One benefit is that it allows developers to identify vulnerabilities early in the project, and resolve those issues early instead of resolving them later, which is much more

expensive as it could result in breaking builds, or a complete restructure of the software.

- Code is shorter so you can be more thorough
- Detect errors earlier
- **Google:** SAST helps integrate security into the early stages of the software development lifecycle. This enables security testers to detect vulnerabilities in the proprietary code in the design stage or the coding stage when they are relatively easier to mitigate.

b) Pro and con of Spotify model

1. Pro: Allows users to directly influence design decisions by offering them alternatives to given software, they can specify which option they prefer (and why) which gives insight into the usability of the different variants of the software
2. Con: Can be expensive to produce different variants of features, if this testing method is overused, it can make the testing much more expensive.

Advantages:
- Allows devs to get user data for each different form of the feature
- General Public opinion
- Unbiased empirical data

Disadvantages:
- Wasted resources if
- May be annoying for users
- **Google said it not me:** creating an inconsistent **experience** for the **user**.

c) 2 cons of scrum and kanban

Not sure if the question wants us to talk about lean and agile in general, or the specific processes that are listed. I guess ill go with the latter

Scrum:

1. One disadvantage of Scrum is that it requires experienced team members to carry out. The constant feedback that team members (or scrum masters) give must be done by experienced team members, lack of knowledge or expertise can break down the project.
2. Another issue with scrum is that it can be hard to scale up to large projects. As each team is quite small, executing it on a large scale requires precise coordination, which is often complex and hard to understand.

Kanban

1. One disadvantage of Kanban is that it is not used as an independent process, and is a methodology that can't be applied without it being merged with another software process such as scrum.
2. Another disadvantage of Kanban is that the boards can become too complex if there are too many interconnected activities or tasks needed to be carried out. The over-complexity can mitigate its effectiveness, especially if tasks pile up and are left uncompleted.

Lean Disadvantages:

- Lack of time – needs time and planning upfront
- A lack of strategy – losing sight of the bigger picture while trying to focus on Lean tactics
- Cutting things too fine – only the highest priority work is delivered so if there is a bottleneck on resources then delays can start occurring.
- Not enough buy-in – teams need to work independently without too much direction.

Reference:

G. Guthrie, "Lean management: the pros, cons, and everything in-between", Backlog. 14-Feb.-2020. [Online]. Available: backlog.com/blog/lean-management-pros-cons-everything/. [Accessed: 9-June-2022].

Agile Disadvantages:

- Customer availability may not be possible.

- Teams should be experienced to follow the rules of the method.``
- Team is expected to have estimation skills and negotiation skills.
- Team should have effective communication skills.
- New teams may not be able to organize themselves.
- Requires discipline to develop and deliver in time-boxed iterations.

d) Why is functional safety important in software engineering?

For systems that are used in safety-critical situations such as airplanes, functional safety is important as it seeks to eliminate risks that are ethically unacceptable (e.g. personal injury).

“Software is increasingly used in safety-critical product development — such as automobiles, planes, and medical devices. And that software needs to be safe, secure, and reliable. That’s why there are safety standards designed for embedded systems developers in several industries.”

“What Is Functional Safety? | Software”, Perforce. [Online]. Available: www.perforce.com/resources/qac/what-is-functional-safety. [Accessed: 9-June-2022].

e) Why does software quality management focus on the development process and not on the software product?

The quality of the software product is hard to determine early in the project. By focussing on the development process, we can ensure that quality is met throughout the project instead of at the end of the development cycle. Corrections as a result of bad quality are more easily made during the development of the product, as oppose to only at the end. Also by ensuring that the development process is in line with quality guidelines, this prevents quality issues that could have been present in the final product (better to prevent that to cure).

f) Explain how to use the defect amplification model to determine at which stages of development to invest resources in defect detection, and how much effort should be put into defect detection at each of these stages.

The defect amplification model shows the impact of previous defects of earlier stages and allows a clearer understanding at where the defects begin to impact the project. The defect detection should be implemented as early as possible where a moderate amount of defects can occur. This is because earlier stages have a bigger impact due to the amplification of these defects throughout the development process. The stages with large amounts of new defects should also be invested heavily into as if they are passed through and amplified can result in an unmanageable amount of defects.

g) Explain how developer productivity affects software estimates. What can an organisation do to take into account developer productivity when estimating time to complete development work?

The developer's productivity affects the software estimates as this impacts how quickly they are able to complete a task. The organization can account for this by using the team's velocity instead of individual developers and also use past projects as a reference to determine the velocity of the team as well as the time needed for development.

h) Consider an organisation that is following all aspects of the Spiral process for software projects in a disciplined manner. What do you believe would be the highest CMMI level at which this organisation could be rated? Justify your answer. Explain which aspects of the Spiral process contribute to your rating.

Level 2

I guess it doesn’t really keep track of time estimates as each spiral can theoretically continue indefinitely. Some spirals may be more complex than others.

Level 2, the spiral process doesn't focus much on improvement for its process. However it does have the basic project management and a repeatable process needed for level 2.

i) Would formal Fagan inspections be an appropriate verification technique to use in a team following Large Scale Scrum? Justify your answer. Identify two characteristics of Fagan inspections and explain why these make it suitable (or unsuitable) to apply in Large Scale Scrum? (Your answer to this last part of the question.)

"No" – Squidward

1. Fagan inspections are very time consuming, and if performed in a large-scale project can restrict the speed of development. The meetings meticulously examine code, and if the project is large-scale, a lot of code needs to be reviewed which can be infeasible in a large-scale environment.

They are only used to find defects in the software, and cannot be used to determine whether the software meets the clients needs, or the requirements specified. Large-Scale Scrum is user-focused. +1

QUESTION 2 (Total: 60 marks)

Consider a project that is developing a "personal academic record" application for the Australian government. The application will record results from your tertiary studies. This will include a breakdown of your results for each course you complete at an Australian university, where a degree programme is comprised of many courses. This breakdown will record the learning objectives for each course and the mark you achieved against each learning objective. The intent is that it will allow students to transfer easily between universities and to gain credit for courses completed at different universities.

At the end of each study period (e.g. a semester) universities will upload student results to the application. This will require that universities follow standardised descriptions of learning objectives. All the assessments in a course will need to be mapped to the course learning objectives so that marks can be allocated to the learning objectives.

Universities will be able to query a student's results to determine what credit to give the student if they transfer into a degree programme at the university. Students would be able to use the application to check what credit they would receive if they transferred to another university. Students would also be able to determine if they completed a course at another university, if it could be used as credit towards the degree they are currently studying.

Employers would be able to query the application to get a detailed breakdown of the results achieved by those who have applied for a position in the organisation. Students would have to give permission for the employer to access their personal record.

Students would be able to generate a summarised or detailed breakdown of their results for degree programmes that they have completed or have not yet completed. These could be used to meet certification requirements or to determine equivalency of qualifications if the student applied for work outside of Australia.

There will be a web application and a mobile application for students to review and manage their personal record. (e.g. Check their results and to allow employers or universities to access their record.) Employers will be able to use a web application to access a student's results. Universities will use an API so that their systems could interact with the application.

A risk has been identified that an unauthorised agent could use the API interface to modify a student's results. The cost of this risk has been assessed as being $15,000,000, based on potential damage to an individual's reputation and compensation costs. The probability of this risk occurring has been assessed as being 0.01 percent.

Two strategies are being considered to reduce the risk of unauthorised modification of results. One strategy is for the government to develop and supply the API communication module to all universities. The cost of developing this module is estimated to be $850,000. It is expected that this will reduce the risk to 0.002 percent.

The second strategy is to use SQC's quantum computation and communication technology to secure the communication between universities and the application. The cost of implementing this strategy is estimated to be $5,500,000. It is expected that this will reduce the risk to 10^{-6} percent.

a) Which of these two risk reduction strategies is the better option? Provide calculations, that show your working out of the results, to support your answer. Also provide a descriptive explanation of your answer. Explain why it is better to choose one of these risk reduction strategies, or why it is better to not use either strategy.

(6 marks)

Re = 15,000,000 * 0.01 = 150,000

1) ReAfter = 15,000,000 * 0.002 = 30,000

R = (150,000 - 30,000)/850,000 = 0.14

2) ReAfter = 15,000,000 * 10^-6 = 15

R = (150,000 - 15) / 5,500,000 = 0.027

Choose 1, as it has a higher value which is better.

It is overall better not to choose either strategy, as generally speaking, only a value >= 1 is worth doing (according to lecture slides).

However, since the risk has a high severity (this is subjective, since it's not specified in the example), might consider implementing option 1 anyway.

Didn't use percentage shouldn't it be 0.002% = 0.00002? And 10^-6% = 0.0000001. Powerpoint examples use percentage, not decimal equivalent. Nah bruh they use % sign in the equation to signify the decimal equivalent e.g. RE = 80%×$147,200 = $117,760 i.e. RE = 0.8*147,200 not 80*147,200 +1

Re = 15,000,000 * 0.01 = 150,000

1) ReAfter = 15,000,000 * 0.00002 = 300

R = (150,000 - 300)/850,000 = 0.176

2) ReAfter = 15,000,000 * 0.0000001 = 1.5

R = (150,000 - 1.5) / 5,500,000 = 0.027

[+1]

b) Identify one additional risk for the originally planned personal academic record application, and one risk for each of the two risk reduction strategies. The risks for the risk reduction strategies need to be new risks introduced by that strategy. Categorise each risk's impact and probability, using NASA's risk matrix. For each risk, justify your selection of the impact and probability.

(6 marks)

1 -> identify

1 -> mark

1 -> justify

1st strategy:

API communication module is poorly integrated within the system.

2nd strategy:

Unable to hire qualified staff to manage the complexity of the quantum computation.

c) Select a software engineering process that would be suitable for this project. Provide an explanation as to why your selected process would be suitable. Your explanation should provide at least two reasons for your choice. Explain why the process model (i.e. plan driven, incremental, agile, lean, formal), to which your selected process belongs, would be a better choice than each of the other four process models.

(8 marks)

I guess the requirements are well defined and very detailed, you could probably pick waterfall in this example. It doesn't seem that the example is exposed to changing requirements either.

But I would still be in favor of agile as there are many components of the software that are independent and can be developed in small teams.

d) Identify a requirements elicitation technique that would be appropriate for this project. Provide a justification as to why you have selected this technique.

(4 marks)

I would say something like observations as you can give users set tasks and determine whether each user can complete the set requirements given in an example. You can also calculate the amount of time it takes for a user to complete a set task in order to give insight into the usability of the system.

Workshops:

Structured meeting

- formal roles
- clear goals

Multiple stakeholders

- resolve conflicting requirements
- quickly gather broad system usage

e) Write two user stories for the functionality of the originally planned personal academic record application. These will be assessed based on their relevance to the project description above, and their quality in terms of INVEST.

Can't we literally just copy the example?

As an employer I want to see an applicant's academic record so that I can determine whether they are suitable for the position.

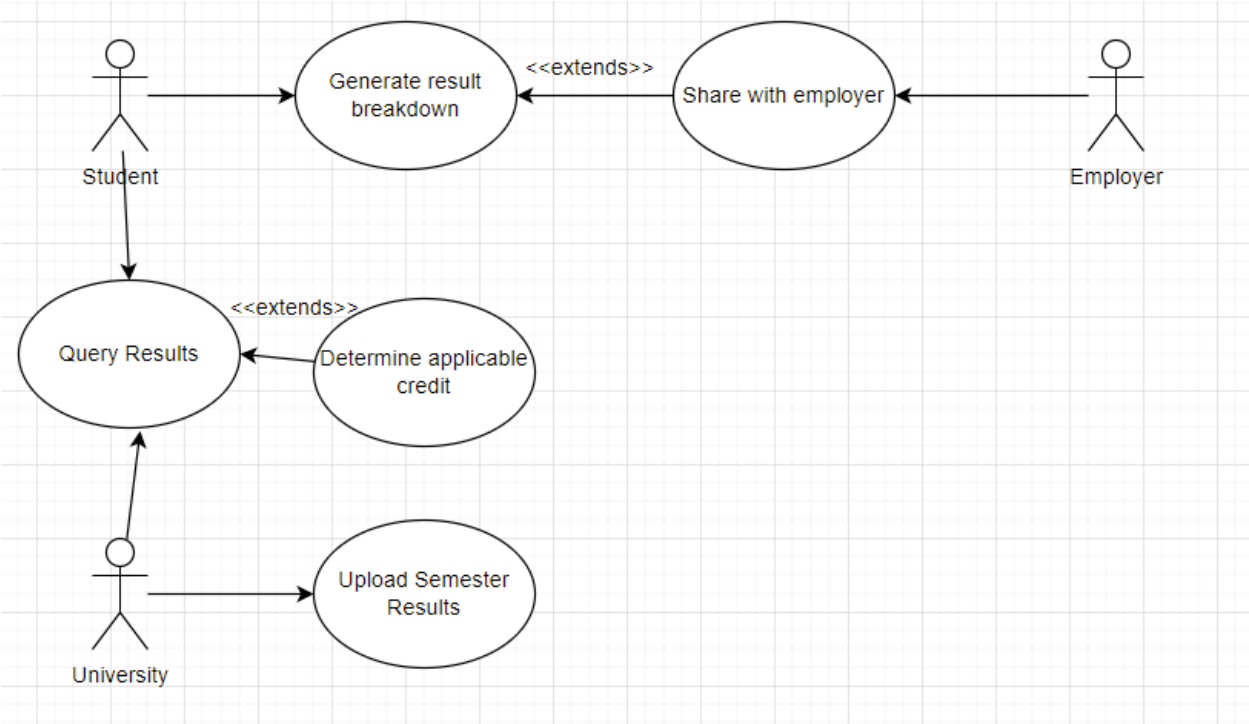
As a university I want to be able to see a student's academic record so that I can determine what credits I can give.

Do we assess these ourselves? I guess these aren't independent as they both need to see academic records. Also the "I can determine what credits I can give" is probably a separate story and not a result.

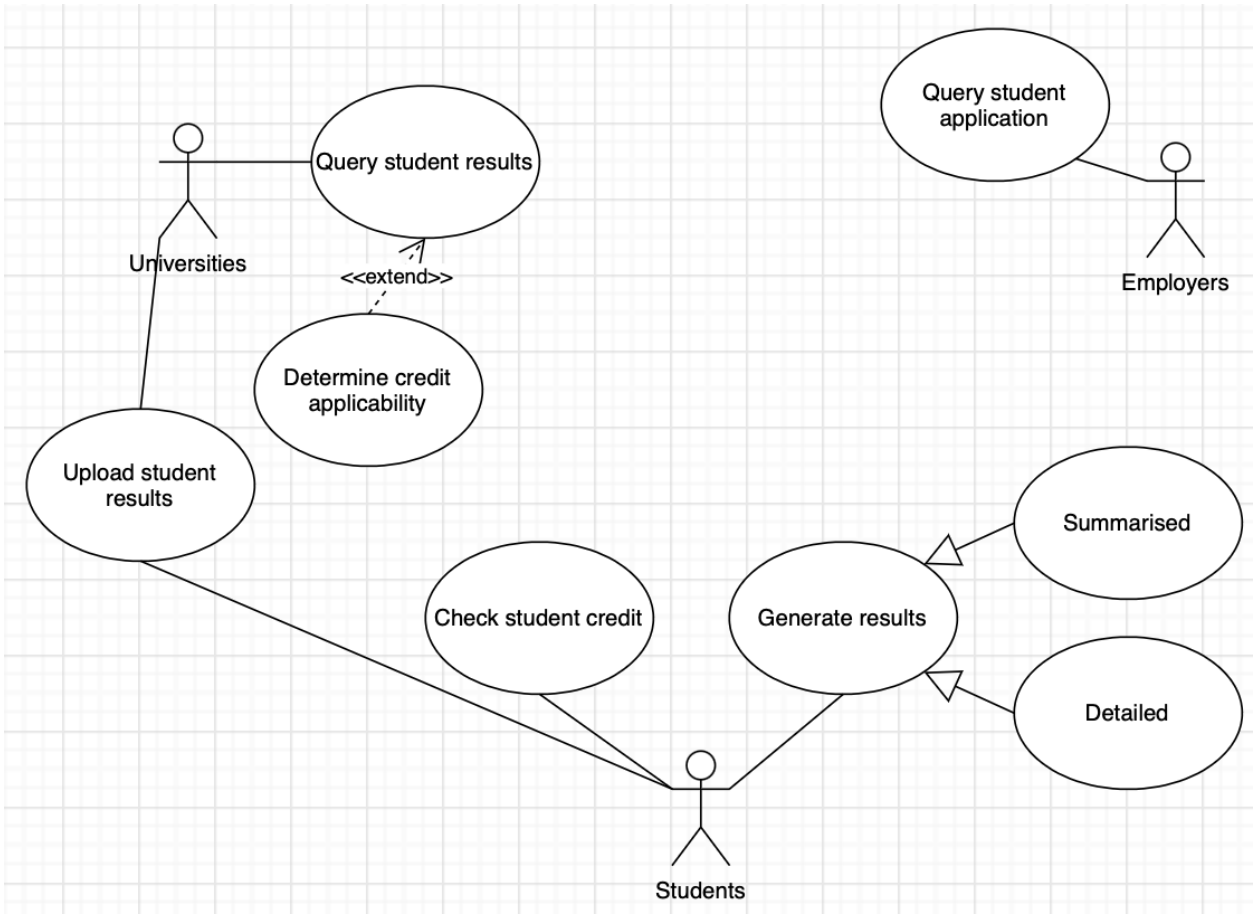
f) Draw a use case diagram for the originally planned personal academic record application. This diagram should show any obvious include or extends relationships in the model. Actor and use case names need to clearly describe the role or functionality.

Only 8 marks for this monstrosity of a question

I had something like this but probably missing something



Determining applicable credit could also be separate and not an extension of querying results.



g) Provide a detailed description for the typical scenario of the use case that includes the functionality of a student checking to see if they could obtain credit towards their current degree for a course from another university. This will involve selecting the university and course and getting a result indicating whether it could be used as credit or not. If this use case includes other use cases or is extended by other use cases, indicate where this occurs in the description. Use the table format from the use cases project to describe the steps involved in performing the scenario. As a reminder of the format, the headings for the table columns are provided below.

Actor Stimulus	System Response
1) Student selects a university within the system	2) System successfully locates university within the system 3) System prompts input for the course that they are seeking credit for.
4) Student inputs a course code	5) System successfully locates course within the system

	6) System checks course against credit database 7) System successfully locates approved credit for the selected course 8) System presents approved course message 9) System prompts user for input of current degree
10) Student views approved course message 11) Student inputs current degree	12) System cross-checks approved course for applicable credit in degree 13) System displays results to the user
14) User views degree applicability result	

Cross-checking an approved course for degree applicability should maybe be a separate use case, this one is very large (above 10 steps).

1.1. Student identifies themselves. 1.2. Student selects a university within the system.	2.1. System successfully locates university within the system 2.2. System prompts input for the course that they are seeking credit for.
3. Student inputs a course code	4.1. System checks course against credit database 4.2. System successfully locates course within the database. 4.3. System presents approved course message

	4.4 System prompts user for input of current degree
5.1. Student views approved course message 5.2. Student inputs current degree	6.1. System cross-checks approved course for applicable credit in degree 6.2. System displays results to the user
7. User views degree applicability result	

h) Identify one alternative scenario for the use case described in part (g). Provide a short single sentence description of the alternative and identify at which step(s) it would occur in the typical scenario.

(2 marks)

At step 2 system can't locate the university within the system, displays an error message which the user can view.

Could also have done the reject message at step 8, which terminates the scenario after the user views the message.

System could not locate the course within the database at step 4.2.

i) Describe two non-functional requirements (NFR) for the personal academic record application. Each NFR must be from a different category. Provide an explanation as to why the NFR is an important consideration for the project.

(6 marks)

1) The web application must be navigable and easy to use.

This is important as it directly influences the usability of the system blah blah blah

2) The academic records must be secure and kept confidential

This is important as privacy is an ethical concern that is important blah blah blah

j) Explain one purpose of performing scenario testing. Write a detailed usage scenario that would test the typical scenario for the use case described in part (g). List all the system features that are tested by the scenario.

(8 marks)

Scenario testing can be used to test specific scenarios that are applicable in the system. One purpose is that it is commonly used to test the functionality of a particular use case.

How is the test scenario different to the use case scenario? Can someone who did the presentation on this do the answer?

A usage scenario is a long textual description of a user's interaction with the system. It includes heaps of context about when they use it, why they use it, how they use it, and exactly what they do when they use it.

Scenario testing is using this scenario to test how well the system works for this use scenario. It is about going through this person's use of the system and figuring out which features they interact with (and therefore which features are tested).

k) An extension has been proposed for the personal academic record application. The proposal is that the government would check student results to determine how well they are doing in their degree programme. The government would use the results to determine whether to increase, decrease or cancel the government allowances being paid to the student.

Describe one ethical issue of this proposal. For the issue, provide an argument as to why the proposal is ethically appropriate or inappropriate. Marking will be based on your argumentation, not on whether your answer is correct.

(4 marks)

Infringes on student privacy of results. There may be medical conditions or surrounding circumstances which are attributing to the students poor academic performance. This essentially means that the government would be discriminating against students because of these conditions, which would later lead to anarchy and complete destruction of societal infrastructure. Basically an all out apocalypse. Pray for us.