**Phil Feain** - Hello and welcome to the VCE Software Development Unit 4 School-based Assessment on-demand video on the Unit 4 Outcome 2 SAC for 2022. The purpose of Video 3 is to support teachers with understanding how to plan for the Unit 4 Outcome 2 SAC task for Software Development. My name is Phil Feain and I'm the Curriculum Manager for Digital Technologies with the VCAA. The purpose of this session is to: build capacity to develop compliant, rigorous and engaging VCE assessment tasks in line with the VCE assessment principles and to provide an overview of the Unit 4 Outcome 2 School-assessed Coursework task.

This presentation will cover: Unit 4 Outcome 2, key knowledge, key skills, the assessment task, resources including: Task development template - blank and the Task development template - plan. Over the next few slides, we'll go through Unit 4 Outcome 2.

Let's have a look at the Outcome statement. On completion of this unit the student should be able to respond to a teacher provided case study to examine the current software development security strategies of an organisation, identify the risks and the consequences of ineffective strategies and recommend a risk management plan to improve current security practises. You need to ensure the SAC task meets this. Here's the Key knowledge. These can be used to help develop the case study. The scenario for the case study should only reference these dot points.

And here are the Key skills. You develop your assessment task to enable students to meet these. You want students to be able to: analyse and discuss the current security controls to protect software development practises and to protect software and data, identify and discuss the potential risks to software and data security with the current security strategies, propose and apply criteria to evaluate the effectiveness of the current security practises, identify and discuss the possible legal and ethical consequences to an organisation for ineffective security practises and recommend and justify an effective risk management plan to improve current security practises.

Next is the assessment task itself. The student's performance will be assessed using one of the following: structured questions, a report in written format and a report in multimedia format. It must be out of 100 marks. Over the remaining slides we will look at planning the Unit 4 Outcome 2 SAC task.

This slide shows six useful VCAA resources that will help you with planning the assessment task. On the left we have the Applied Computing Study Design that includes the Software Development Unit 4 Outcome 2. Then we have the Advice For teachers with Sample approaches to developing an assessment task and the Unit 4 Outcome 2 performance descriptors. This is followed by three resources on the study page: The Unit 4 Outcome 2 SAC Template. The Unit 4 Outcome 2 Assessment task development template - Blank and The Unit 4 Outcome 2 Assessment task development template - Plan.

This slide shows a resource that I've put together of a template showing how the key knowledge, key skills and performance descriptors link together. The purpose of this resource is for you to put down your ideas or notes in the blank space linking back to the performance descriptors, key skills and key knowledge. You can use this resource to help you plan for the assessment task. This can be downloaded from the Software Development study page. I'll go through this in detail over the next few slides.

The first part of the document links the following three key knowledge bullet points to the key skill of - analyse and discuss the current security controls to protect software development practises and to protect software and data. These link to the performance descriptor - Comprehensive analysis and discussion of the current security controls used to protect software development practises and to protect software and data.

When planning to meet this key skill or performance descriptor, these are the three key knowledge bullet points that need to be addressed. In the case study students are analysing and discussing the current security controls to protect the organisation's software development practises and to protect their software and data.

The next part of the document links the following five key knowledge bullet points to the key skill of - identify and discuss the potential risks to software and data security with the current security strategies. These link to the performance descriptor - Comprehensive identification and discussion of the potential risk to software and data security.

When planning to meet this key skill or performance descriptor, these are the five key knowledge bullet points that need to be addressed. Using the case study, students are identifying and discussing the potential risk to software and data security with the current security strategies of the organisation.

The next part of the document links the following key knowledge bullet point to the key skill of - propose and apply criteria to evaluate the effectiveness of the current security practises. This links to the performance descriptor - Comprehensive set of relevant evaluation criteria to measure the effectiveness of the current security practises are proposed and applied.

When planning to meet this key skill or performance descriptor, this is the key knowledge bullet point that needs to be addressed. Using the case study, students are to propose and apply criteria to evaluate the effectiveness of the current security practises of the organisation.

The next part of the document links the following two key knowledge bullet points to the key skill of - identify and discuss the possible legal and ethical consequences to an organisation for ineffective security practises. These link to the performance descriptor - Comprehensive understanding of the possible legal and ethical consequences of ineffective security practises.

When planning to meet this key skill or performance descriptor, these are the two key knowledge bullet points that need to be addressed. Using the case study, students are identifying and discussing the possible legal and ethical consequences to an organisation for their ineffective security practises.

The final part of the document links the following key knowledge bullet point to the key skill of - recommend and justify an effective risk management plan to improve current security practises. These link to the performance descriptor - Comprehensive recommendations are made and justified to improve the current security practises as part of an effective risk management plan.

When planning to meet this key skill or performance descriptor, this is the key knowledge bullet point that needs to be addressed. Using the case study, students are recommending and justifying an effective risk management plan to improve the organisation's current security practises.

This slide shows a resource that I've put together of a template showing how the key knowledge, key skills and performance descriptors link together with an explanation of how to create the assessment task on the right. The purpose of this resource is to assist teachers with planning the assessment task to ensure it links back to the performance descriptors, key skills and key knowledge. You can use this resource to help you write the assessment task. This can be downloaded from the Software Development study page. I'll go through this in detail over the next few slides.

This slide is about planning the case study or the scenario for the assessment task. Create a fictitious organisation that is real-world with a reasonable level of complexity. Media articles can assist with this. A case study for this task needs to involve an organisation that develops software and has some security strategies in place that can be analysed and discussed. The information system must not be a manual system and must be an existing system, not proposed. Have issues in what the organisation is doing. Write the case study for the organisation. Key content within the case study should be based on the targeted key knowledge and key skills.

To meet the following key skill, content to be included in the case study should introduce students to the background of the organisation. This could include the setting of the organisation, what they do in terms of software development and their goals and objectives. Details regarding the physical and software security controls used to protect their software development practises and how they protect their software and data including any software auditing and testing strategies to minimise risks should be included. Issues should be included within the case study for students to pick up on and write about in their analysis and discussion. These could include a lack of security controls and strategies.

To meet the following key skill, content should be included in the case study to enable students to identify and discuss the potential risk to software and data security. Students will need to consider the types of vulnerabilities in the key knowledge for this outcome: data breaches, lack of version control, poor user authentication practises, irregular software updates, man-in-the-middle attacks, social engineering, or lack of encryption, the types of web application risks and managing risks with software acquired from third parties. While there is no requirement for teachers to include all of these vulnerabilities within the case study, there should be some reference to the types of vulnerabilities selected by the teacher. Data integrity is also affected by vulnerabilities and risks and these need to be identified within the case study to determine the impact on the organisation.

To meet the following key skill, the content above should enable students to evaluate the effectiveness of the organisation's current security practises by considering how vulnerabilities may pose a risk to their development practises and how they reduce the effectiveness of their development practises. The case study could include strategies that they follow. The organisation should have some weaknesses in these practises and strategies. This will enable students to propose and apply evaluation criteria to measure the effectiveness of the current security practises.

To meet the following key skill, content should be included in the case study for students to be able to clearly identify the relevant legislation impacting the organisation. This could be the Copyright Act 1968, the Privacy Act 1988, the Health Records Act 2001 or the Privacy and Data Protection Act 2014. Therefore, students could be given information on the type of organisation, the amount the organisation earns each year, the location of the organisation, whether it is a government or private organisation, and how the ineffective security practises may be impacted by the relevant legislation. Details describing how the organisation controls the collection, storage and communication of their data should be included. Students should be able to clearly identify some legal and ethical issues involving the software development process and the use of the software solution.

And to meet the following key skill, the content above should enable students to make recommendations and to justify improvements to the organisation's security practises through an effective risk management plan. This presentation covered: Unit 4 Outcome 2, key knowledge, key skills, the assessment task, resources including: Task development template - blank and the Task development template - plan.

Thank you for following this presentation. If you have any questions regarding this presentation, you can contact Phil Feain, the Digital Technologies Curriculum Manager, at the contact details below.

[Copyright Victorian Curriculum and Assessment Authority](https://www.vcaa.vic.edu.au/Footer/Pages/Copyright.aspx) 2022