Who do I need to send my Contract Compliance Statement (CCS) to?
The first section of the CCS indicates who needs to approve the form.

The lead SCU researcher should sign first, then forward the form to the next person on the approval list.

Once all approvals are received, the CCS should be emailed to research.services@scu.edu.au

Why are some fields mandatory?
Some fields are mandatory because there is a minimum amount of information required about a project to enable the approver to review and authorise the project.

If this information isn’t available, then there is not sufficient information for HOS/Centre Director to approve the project or for the Office of Research to progress the agreement.

Why do I need to fill out a CCS?
The CCS is a valuable tool for the research team, your work unit and the Office of Research, as the CCS gives the researcher and the HOS/Centre Director the chance to review and approve the ‘final deal’ for a project, including the commitment of SCU resources (cash/in- kind) to the project.

The Contract Compliance Statement stage is the last chance to review and flag any concerns or issues before the research funding agreement is signed. This includes any changes that have been made since the original Project Pre-Approval and during agreement negotiation.

How do I create my electronic signature?
All Office of Research electronic forms will require digital signatures. You will only need to create your signature once, after that, documents requiring a digital signature will ask you for a signature password.

Follow these steps when creating your digital signature:

Check “A new digital ID I want to create now”, then press ‘Next’.
Add or create a digital ID to sign and encrypt documents. The certificate that comes with your digital ID is sent to others so that they can verify your signature. Add or create a digital ID using:

- **My existing digital ID from:**
  - A file
  - A roaming digital ID accessed via a server
  - A device connected to this computer

- **A new digital ID I want to create now**
Select “New PKCS#12 digital ID file”, then press ‘Next’

- **New PKCS#12 digital ID file**
  
  Creates a new password protected digital ID file that uses the standard PKCS#12 format. This common digital ID file format is supported by most security software applications, including major web browsers. PKCS#12 files have a .pfx or .p12 file extension.

- **Windows Certificate Store**

  Your digital ID will be stored in the Windows Certificate Store where it will also be available to other Windows applications. The digital ID will be protected by your Windows login.
Complete the form with your ‘Name’, ‘Organisation Unit’ etc and press ‘Next’.

Add Digital ID

Enter your identity information to be used when generating the self-signed certificate.

Name (e.g. John Smith): 
Organizational Unit: 
Organization Name: 
Email Address: 
Country/Region: AU - AUSTRALIA

Enable Unicode Support

Key Algorithm: 1024-bit RSA
Use digital ID for: Digital Signatures and Data Encryption

Cancel  < Back  Next >
Confirm the local path to store your certificate and add a ‘strong password’, then press ‘Finish’.

You have now created a local digital signature.

This signature will be inserted each time you ‘sign’ an electronic document. Remember your password as you will need this to ‘sign’ future documents.