Cyber Essentials Plus Assessment Report

Assessment of: SHJ Hospital Pipelines Ltd

Assessed by (Certification Body): d83d9f602bd6be968881deb5981d25941a861f7c4548882cc1b03ddc9cafa68d

Assessed By (Assessor Name): Tharun Jagathish Udayasankar

Assessed By (Lead Assessor name): Jake Hazelwood

Date of assessment visit: 16/01/2025

Date of Report: 28/1/2026

Cyber Essentials Plus certification can only be issued by a licensed Certification Body.

You can confirm the authenticity of this report by contacting IASME Consortium

+44 (0)3300 882752

1. About this report

Cyber Essentials Plus is the audited version of the Cyber Essentials information security standard.

Cyber Essentials requires organisations to have a number of technical and procedural controls in place to improve their information security in order to mitigate common internet-borne cyber attacks. Cyber Essentials Plus is a series of tests that provide a further level of assurance that these technical controls have been successfully implemented within an organisation.

This report is a record of the Cyber Essentials Plus audit of SHJ Hospital Pipelines Ltd against the Cyber Essentials standard that has been carried out by Tharun Jagathish Udayasankar of the Certifying Body d83d9f602bd6be968881deb5981d25941a861f7c4548882cc1b03ddc9cafa68d.

Cyber Essentials provides assurance that a number of key information security controls are in place within an organisation. For further assurance, the IASME information security standard provides a broader set of controls that enable good information security governance across an organisation.

1.1 Summary of findings

The assessor has concluded that SHJ Hospital Pipelines have passed the required tests and should be awarded the Cyber Essentials Plus certification. All systems tested conformed to the required specifications of the Cyber Essentials Plus and provided an adequate level of security against threats.

The assessor has concluded that SHJ Hospital Pipelines Ltd has passed the required tests and should be awarded the Cyber Essentials Plus certification.

The Certificate Number is 3c418ef4-b023-4270-85e6-d59712ace0e6 and can be found at https://registry.blockmarktech.com/certificates/3c418ef4-b023-4270-85e6-d59712ace0e6/

If a test has not been passed successfully, the assessor has provided feedback within the relevant section.

Evidence of activities

In carrying out the audit, the assessor will have carried out a number of technical tests and have seen documentary evidence. This evidence forms a basis for the assessor's recommendations and where appropriate has been included in this report.

Scope of CE+ Audit

The following networks and locations were considered in the scope of this assessment:

SHJ operate from their office and network in Bucks.Private IP Range: 10.0.0.0 10.0.1.254, 192.168.100.0 192.168.101.254Public IP: 80.79.141.106, 81.143.114.158, 82.147.31.130

Any areas that were excluded from the audit are listed below:

Company Website excluded because located with cloud hosting provider and as such not required part of Cyber Essentials Plus scoping requirements.

Remote Vulnerability Assessment

The purpose of this test is to test whether an Internet-based opportunist attacker can hack into the applicant's system with typical low-skill methods.

Each external IP address that is in scope has been scanned to identify any services that are open to the internet. All open services are tested to confirm that they have met the requirements of Cyber Essentials.

Remediations for Remote Vulnerability Assessment
No remediation is required. There were no non compliances encountered during the test performed.

Internal Testing

A suitable set of devices that was selected at random by the assessor that is representative of 100% of the applicant infrastructure.

A summary of the breakdown of this sample is as follows:

SHJ pipeline confirmed to have the below listed quantity of devices in scope.
27 X Android 16, 1 X Windows Server 2016, 5 X Windows Server 2019, 18 X Windows Server 2022, 43 X Windows 11 Enterprise 25H2.

We randomly sampled and audited the below listed quantity of devices.
4 X Android 16, 1 X Windows Server 2016, 3 X Windows Server 2019, 4 X Windows Server 2022, 4 X Windows 11 Enterprise 25H2.

Authenticated vulnerability scan of devices

The purpose of this test is to identify missing vulnerability fixes within the defined CE+ test scope that could be exploited within the bounds of the CE threat model. Vulnerability fixes include patches, updates, registry fixes, configuration changes, scripts or any other mechanism prescribed by the vendor to fix a known vulnerability.

This test was awarded PASS by the assessor.

The following vulnerabilities were discovered that scored 7 or higher on CVSS v3 and had a security update available that had been released by the vendor 14 or more days ago:

Weak Windows Service Permissions High
Windows Missing Security Patches High

The assessor has confirmed that these issues have been remediated and the required update applied during the remediation period.

Remediations for Authenticated Vulnerability Scan
No remediation is required. There were no non compliances encountered during the test performed.

Check Malware Protection

This test checks the sampled devices to confirm that all devices in scope benefit from a basic level of malware protection.

All devices and virtual desktop environments should either be using anti malware software or application allow listing.

This test was awarded PASS by the assessor.

All sampled devices have been tested and the assessor who has confirmed that they benefit from a basic level of malware protection.

For all devices using anti-malware software it has been confirmed that the software is functional and is being updated in line with vendor recommendations.

For devices using application allow listing, the assessor has confirmed that the application allow list is configured correctly.

Remediations for Malware Protection Check
No remediation is required. There were no non compliances encountered during the test performed.

Remediations for Anti-Malware Software
No Remediation works were required. There were no non compliances encountered during the test performed.

Remediations for Allow-Listing
No remediation is required. There were no non compliances encountered during the test performed.

Check Multi-Factor Authentication (MFA) Configuration

All cloud services must be configured to authenticate using MFA. This test is in place to confirm that all cloud services that have been declared in the scope with MFA available are authenticating using MFA.

The assessor has checked the user of each sampled device against every cloud service that they use.

At least one administrator account and one standard user account has been checked for each cloud service.

This test was awarded PASS by the assessor

All users for sampled devices were observed authenticating to cloud services which they use as an organisational service and confirmed that they were authenticating using MFA.

At least one administrator and one standard user for each cloud service was tested.

Remediations for MFA Configuration
No remediation is required. MFA is confirmed to be enabled on all cloud services for both admins and standard users.

Check Account Separation

This test is conducted to ensure that account separation is in place and that standard users can not conduct administrator tasks.

Elevating privileges is not an acceptable alternative to using separate accounts.

This test was awarded PASS by the assessor

The assessor has confirmed that all users of the sampled devices had standard user accounts and could not carry out an administrative task without entering credentials of a separate admin account.

Remediations for Account Separation

No remediation is required. There were no non compliances encountered during the test performed.

Applicant Answers

	Applicant Answers	Assessor Score
A1.1 Organisation Name? What is your organisation's name? The answer given in A1.1 is the name that will be displayed on your certificate and has a character limit of 150 including spaces. Where an organisation wishes to certify subsidiary companies on the same certificate, the organisation can certify as a group and can include the subsidiaries' name on the certificate as long as the board member signing off the certificate has authority over all certified organisations. For example: The Stationery Group, incorporating The Paper Mill and The Pen House It is also possible to list on a certificate where organisations are trading as other names. For example: The Paper Mill trading as The Pen House.	SHJ Hospital Pipelines Ltd	Compliant
A1.2 Organisation Type What type of organisation are you? “LTD” – Limited Company (Ltd or PLC) “LLP” – Limited Liability Partnership (LLP) “CIC” – Community Interest Company (CIC) “COP” – Cooperative “MTL” – Other Registered Mutual (Community Benefit Society, Credit Union, Building Society, Friendly Society) “CHA” – Registered Charity “GOV” – Government Agency or Public Body “SOL” – Sole Trader “PRT” – Other Partnership “SOC” – Other Club/ Society “OTH” – Other Organisation	LTD - Limited Company (Ltd or PLC)	Compliant

A1.3 Organisation Number What is your organisation's registration number? Please enter the registered number only with **no spaces or other punctuation**. Letters (a-z) are allowed, but you need at least one digit (0-9). There is a 20 character limit for your answer. If you are applying for certification for more than one registered company, **please still enter only one organisation number**. If you have answered A1.2 with Government Agency, Sole Trader, Other Partnership, Other Club/Society or Other Organisation please enter "none". If you are registered in a country that does not issue a company number, please enter a unique identifier like a DUNS number.	01089049	Compliant
A1.4 Organisation Address What is your organisation's address? Please provide the legal registered address for your organisation.	UK Custom Fields: Address Line 1: Unit 4, Anglo Business Park Address Line 2: Asheridge Road Town/City: Chesham County: Bucks Postcode: HP52QA Country: United Kingdom	Compliant
0.1 Assessment Scope Have you verified that the scope for this CE+ assessment is the same as the scope for the applicant's CE verified self assessment (VSA)?	Yes	Compliant

0.2 Networks and Locations in Scope Provide a brief summary of the networks and locations in scope for this CE+ assessment.	SHJ operate from their office and network in Bucks. Private IP Range: 10.0.0.0 10.0.1.254, 192.168.100.0 192.168.101.254 Public IP: 80.79.141.106, 81.143.114.158, 82.147.31.130	Compliant
0.3 Excluded Items If you have chosen to exclude any items, please provide a summary. For example: "Company Website is excluded because it is located with the cloud hosting provider, and as such not required, as per the Cyber Essentials Plus scoping requirements". If anything is excluded from the verified self assessment (VSA) in this CE+ assessment, then the VSA will need to be assessed again or the issue remediated within the prescribed 30 day window.	Company Website excluded because located with cloud hosting provider and as such not required part of Cyber Essentials Plus scoping requirements.	Compliant
0.4 Organisation Name What is the name of the applicant? Please provide the organisation's full name, to match that provided for their CE verified self assessment.	SHJ Hospital Pipelines Ltd	Compliant
0.5 CE VSA Certification Number What is the CE verified self assessment (VSA) Blockmark certificate number for the applicant? Please provide the certificate number for the client's CE self assessment questionnaire.	4b361af6-b297-41b6-8a5d-ac687739b4c2	Compliant

0.6 CE VSA Date What date did the client pass their verified self assessment (VSA)? Provide the date that the client passed their verified self assessment. Cyber Essentials Plus must be completed within 90 days of the date of certifying for Cyber Essentials. The 30 day remediation period is inclusive of the 90 days. The CE+ assessment should be completed as close as possible to the date of the Cyber Essentials verified self assessment certification date, and sufficient time must be allowed for the remediation period within the 90 days. Extensions will only be granted in extreme circumstances. This does not include Christmas, Easter or other publicly notified holidays, the dates of which are static or known in advance.	06-11-2025	Compliant
0.7 CE+ Certification Date On what date/s was the CE+ assessment carried out? Please enter the date that the CE+ testing was carried out.	16/01/2025	Compliant
0.8 Scope Description What is the scope description that should appear on the CE+ certificate? The CE+ Scope must match the CE verified self assessment scope. This must be the same scope description as the organisation's CE verified self assessment certificate. If the scope is the whole organisation please enter "Whole organisation".	Whole organisation	Compliant
0.9 CE+ Test Platform Which CE+ Testing platform have you used, to run the email audit tests?	The test platform which as used is the portal - scan.cyberessentials.live	Compliant
0.10 Audit Location Was the CE+ audit carried out remotely or onsite?	remotely	Compliant
0.11 Scanning Tool Which vulnerability scanning tool was used for the external and internal audit? Was it supplied by the Certification Body or the applicant?	All devices were scanned with a Tenable Nessus and Nessus Agent by the SHJ Pipeline and certification body performed scan on a server and External IP addresses.	Compliant

1.1.1 Scan Recommended Ports Have you scanned all external IP addresses for the client on all TCP and UDP ports?	Yes	Compliant Assessor Notes: Public IP was scanned using a Nessus full TCP/UDP scan.
1.1.1.2 External Addresses Have you checked all external addresses against the networks and network devices in the CE VSA? You must check against the answers given in Section 2 of the VSA. Please list the quantity of external IPs tested. Where it is unclear how many external IP addresses were tested, the quantity should be clarified with the applicant.	In scope networks, network devices and locations checked against CE VSA. External IPs tested:3	Compliant Assessor Notes: The applicant is a fully remote company. For the purpose of this assessment one homeworker network was elected as the primary place of business, the external IP address of this network was then used to conduct the external vulnerability scan.
1.1.2 Identify Critical and High Risk Vulnerabilities Did you identify any vulnerabilities that were scored 7 or higher on CVSS v3? The CVSS v3 score is taken from the base score, and temporal scoring should not be taken into account.	No	Compliant
1.1.3 Other Vulnerabilities For each Internet-accessible service you discover you must use the flow diagram in the Cyber Essentials Plus Test Specification document. Did the flow chart highlight any vulnerabilities to be identified as a fail?	No	Compliant
1.1.4 Remediation Details Please provide information about any remediations carried out including the date that they were retested.	No remediation is required. There were no non compliances encountered during the test performed.	Compliant
2.1.1 Sample Device Identification Has a suitable sample of all end user devices, servers and IaaS instances been identified, in line with Cyber Essentials Plus scheme guidance? The sample must be selected by the CE+ assessor not the applicant. The sample must be 100% representative of the applicant's infrastructure.	Yes	Compliant Assessor Notes: Sampled devices based on CE End User Devices, Thin Clients, Servers, Mobile Devices and checked against and updated asset list from the client. Sampled according to assessor guidance.

2.1.2 Details of Sampling You must provide a brief summary of your device sampling decision. Sample calculation data must be retained by the certifying body for the lifetime of the certificate.	SHJ pipeline confirmed to have the below listed quantity of devices in scope. 27 X Android 16, 1 X Windows Server 2016, 5 X Windows Server 2019, 18 X Windows Server 2022, 43 X Windows 11 Enterprise 25H2. We randomly sampled and audited the below listed quantity of devices. 4 X Android 16, 1 X Windows Server 2016, 3 X Windows Server 2019, 4 X Windows Server 2022, 4 X Windows 11 Enterprise 25H2.	Compliant Assessor Notes: The changes were confirmed with the point of contact in Technical verification.
2.1.3 Authenticated Vulnerability Scan Has a full authenticated vulnerability scan been conducted on all devices in your sample?	Yes	Compliant Assessor Notes: All devices were scanned with a Tenable Nessus Agent.
2.1.4 Internal Vulnerability Scores Did you identify any vulnerabilities for the tested devices that were scored 7 or higher against CVSS v3 scoring? The CVSS v3 score is taken from the base score, and temporal scoring should not be taken into account.	Yes	Compliant
2.1.4.1 Internal Vulnerability Assessment Do any of the vulnerabilities identified in the internal vulnerability scan relate to issues for which a vulnerability fix has been made available by the software vendor (and was released more than 14 days ago)? Only vulnerabilities for which the vendor has released a vulnerability fix, and the client has failed to install the fix will cause a fail for this test. If you identify a high risk or critical vulnerability for which a vulnerability HAS NOT been released, you should answer NO to this question (which will result in a PASS for the client).	Yes	Compliant
2.1.4.2 List of Vulnerabilities Identified Please list the vulnerabilities for which a vulnerability fix has been released. When vulnerabilities have been identified, a summary list must be provided.	Weak Windows Service Permissions High Windows Missing Security Patches High	Compliant

2.1.4.3 Applicant Addressed Vulnerabilities Has the applicant applied the vulnerability fixes to address the identified vulnerabilities? Please provide notes on what happened. If there are vulnerabilities identified, the client must remediate the vulnerabilities and the identified service must be retested by the CE+ assessor within the 30 day remediation window.	Yes	Compliant
2.1.5 Remediation Details Please provide information about any remediations carried out including the date that they were retested.	No remediation is required. There were no non compliances encountered during the test performed.	Compliant
3.1.1 Sample Confirmation Has a suitable sample of all end user devices, servers and IaaS instances that provide a user-interactive desktop been identified in line with Cyber Essentials Plus scheme guidance? You must use the same devices as picked in the sample for the authenticated vulnerability scan. VDI Servers, Virtual desktop servers, DaaS servers must be tested. All other servers do not need to be tested.	Yes	Compliant
3.1.2 Malware Protection Method For all end user devices in the sample, have you identified which method of preventing malware is in use? Please select every method that is in use at this organisation. The methods of preventing malware available are: A - having anti-malware software installed or B - limiting installation of applications to an approved set (i.e. using an App Store and a list of approved applications)	0: A - having anti-malware software installed, 1: B - limiting installation of applications to an approved set (i.e. using an App Store and a list of approved applications)	Compliant
3.1.3 Email Domains Which email domain/s have been tested? List the email domains.	Max.Griffiths@shj.co.uk	Compliant
3.1.4 Email Addresses How many individual email addresses have been tested? List the quantity per email domain tested.	3 Email addresses were tested	Compliant Assessor Notes: One user was on sick leave during the audit day so tested with admins user account.

3.1.5 Remediation Details Please provide information about any remediations carried out including the date that they were retested.	No remediation is required. There were no non compliances encountered during the test performed.	Compliant
3.2.1 Anti-Malware Software Installed For all devices in the sample relying on A - anti-malware software, is antivirus software installed on all end user devices or virtual desktop environments?	Yes	Compliant
3.2.2 Anti-Malware Software Testing For all devices in the sample relying on A - anti-malware software, determine whether the test files will work for the testing purpose. Test files must be used to test all anti malware software that uses signature based scanning. Determine whether the test files should be triggered using the software installed and then answer one of the following options: A - Test files work on all sampled devices B - Test files do not work on any device within the sample set C - Test files work on some of the devices in the sample set	A - Test files work on all sampled devices	Compliant
3.2.3 Email Delivery Test For all end user devices in your sample using anti malware software that should defend against the test files, have you tested email delivery by sending a test email with no attachments and verified the receipt of the email?	Yes	Compliant Assessor Notes: A test email was sent to each device within the sample using scan.cyberessentials.live
3.2.4 Email Test Files Have you sent a suitable set of test files by email to each device in the sample (this should include "malware" test files and "executable" test files)? You must use the standard test files provided by IASME to carry out this test. You only need to send a subset of these files that would be appropriate to the device operating system (for example, Windows devices do not need to be sent the .dmg file, which is a macOS file). There are two types of test files - "malware" and "exectuable". Both types must be sent to every device in the sample. If in doubt, please verify your list of test files with IASME. You should send one email per file.	Yes	Compliant Assessor Notes: A full set of malware test files were sent to every device in the sample using scan.cyberessentials.live.

3.2.5 All Attachments Blocked Were all of the email attachments containing malware blocked by all of the end user devices in your sample? You should answer No if you were able to open any of the malware attachments.	Yes	Compliant Assessor Notes: All malware test files sent via email were blocked by all end user devices
3.2.6 Test Files - Email - Binary Files Test Did all of the end user devices in your sample produce a warning or an opportunity to cancel before opening the email attachments containing executable (non-malware) files? You should answer no if you were able to open an executable attachment without a warning or opportunity to cancel.	Yes	Compliant Assessor Notes: All the emails attachments were either blocked or the emails did not arrive in the user inbox, with the exception of the following emails which displayed the following behaviour: .dmg Attachment Blocked by email App .msi Attachment Blocked by email App .ps1 Attachment Blocked by email App .sh Attachment Blocked by email App .py Attachment Blocked by email App
3.2.7 Test Files - Web Delivery For all devices in your sample using anti malware software that should defend against the test files, have you attempted to open both "executable" and "malware" test files using a web browser? You must use a standard user account for this test (not an administrator account). You must use the standard test files provided by IASME to carry out this test. You only need to send a subset of these files that would be appropriate to the device operating system (for example, Windows devices do not need to be sent the .dmg file, which is a macOS file). There are two types of test files - "malware" and "exectuable". Both types must be sent to every device in the sample. If in doubt, please verify your list of test files with IASME. You should send one email per file.	Yes	Compliant Assessor Notes: A standard account was used to attempt to open a sample of both executable and EICAR malware files on every device in the sample
3.2.8 Test Files - Web - Malware Blocked Test Files - Web - Malware Blocked Were all of the downloads containing malware blocked by all of the end user devices in your sample? If you identify a configuration issue, the client may be given an opportunity to address the issue and have a retest of a specific device carried out.	Yes	Compliant Assessor Notes: **The EICAR malware files were blocked by AV or security policies in place.**

3.2.9 Test Files - Web - Malware Warning Did all of the end user devices in your sample produce a warning or an opportunity to cancel before opening the downloads containing executable (non-malware) files? If the browser prompts the user to decide whether to "run" or "save as" then this is classed as a pass for this test.	Yes	Compliant
3.2.12 Anti-Malware Software Updated For all devices in your sample using anti malware software, have you confirmed that the software has been updated in accordance with the vendor’s configuration instructions?	Yes	Compliant
3.2.13 Remediation Details Please provide information about any remediations carried out including the date that they were retested.	No Remediation works were required. There were no non compliances encountered during the test performed.	Compliant
3.3.1 Application Allow List Testing For all devices in the sample relying on B - certificate based application allow listing, have you confirmed that the list of trusted root certificates are provided by the operating system manufacturer?	Yes	Compliant
3.3.3 Unsigned Executables For all devices in the sample relying on B - certificate-based application allow listing, has it been confirmed that an unsigned executable and executables with a certificate that does not chain to a trusted certificate will not run on the end user device?	Yes	Compliant
3.3.4 Code Signing For all devices in the sample relying on B - certificate-based application allow listing, have you confirmed that operating system policy settings are in place to ensure that code signing applies to all of the applicable file formats to the relevant device?	Yes	Compliant

3.3.5 All Devices Protected Are you satisfied that every device in your sample is protected from malware using one of the methods described in Q3.1.2? If NO, please add notes to explain why.	Yes	Compliant
3.3.6 Remediation Details Please provide information about any remediations carried out including the date that they were retested.	No remediation is required. There were no non compliances encountered during the test performed.	Compliant
4.1.1 Cloud Sample Identification Provide a list of all cloud services used by the applicant that provides an authentication service. A list of all cloud services tested must be provided. Any cloud service that has been declared in the verified self assessment as not providing MFA does not need to be tested. Where a cloud service authenticates through another cloud service, only the authentication service needs to be tested in the sample. (For example if an organisation authenticates 10 x cloud services via Azure SSO, only the Azure would need to be tested).	Mimecast	Compliant
4.1.2 Check MFA configuration of sampled users Were all users challenged with an MFA prompt prior to a successful login using an incognito browser or untrusted device? Notes required -result must be recorded for each cloud service tested. Observe the users trying to log in with their standard user accounts to each cloud service that they use. This test is carried out against the user accounts belonging to the user that would use each sampled device to carry out their daily tasks. If the user is also an administrator for that service, ask them to login with their administrator account using the same method. Answer No if an MFA prompt wasn't provided and the user successfully logged into the cloud service.	Yes	Compliant

4.1.3 Confirmation that all cloud services have been checked Have all cloud services as listed in the verified self-assessment been checked to confirm that MFA has been applied? All cloud services listed in the verified self-assessment that have not been declared as ‘not providing MFA in A7.15’ must have their authentication method checked. All authentication methods must have been checked with one Administrator and one standard user. If any of the cloud services were not checked as part of the sample an additional administrator and / or user must be checked. Where an organisation does not have any standard users, please provide notes to detail this. Where an organisation does not have any standard users, please provide notes to detail this.	Yes	Compliant
4.1.4 Remediation Details Please provide information about any remediations carried out including the date that they were retested.	No remediation is required. MFA is confirmed to be enabled on all cloud services for both admins and standard users.	Compliant
5.1.1 Confirm Standard User Account Details Has every user account on the sampled devices confirmed to you they are logged in with a Standard User account? This test is carried out on all sampled end user devices and/or desktop environments with the account/s that the standard user/s that would normally use that device would use for their daily tasks. You should check the name associated with each account to confirm the sample is true and representative.	Yes	Compliant Assessor Notes: This was evidenced when installing the Nessus agent, an admin elevation window was displayed on all devices.
5.1.1.1 Quantity of Accounts Provide the quantity of accounts tested per sampled device.	1 account per sampled device. 4 accounts in total over all sampled devices.	Compliant
5.1.2 Confirm Account Separation For all end user devices and the accounts, when observing a standard user attempting to run a process, were they asked to enter administrator credentials? If the user was not prompted for an additional login to a separate administrator account, answer No and describe what happened.	Yes	Compliant Assessor Notes: A separate administrator account and standard were used on all devices.

5.1.3 Remediation Details Please provide information about any remediations carried out including the date that they were retested.	No remediation is required. There were no non compliances encountered during the test performed.	Compliant
6.1.1 Executive Summary Provide a summary of your findings here – ideally one or two paragraphs to give a flavour of the report. Briefly mention locations and scope. You should also highlight any notable anomalies and action points, pointing the reader to the appropriate section of the report for more information.	The assessor has concluded that SHJ Hospital Pipelines have passed the required tests and should be awarded the Cyber Essentials Plus certification. All systems tested conformed to the required specifications of the Cyber Essentials Plus and provided an adequate level of security against threats.	Compliant
6.1.2 Lead Assessor Details A Lead Assessor must review and sign off the findings of this assessment and confirmed that they agree with them. Please provide the name of the Lead Assessor for this assessment. If you are a Lead Assessor, please enter your own name (you will not require a second person to sign off the assessment). A Lead Assessor is an assessor that holds one of the qualifications in List A of the Assessor Requirements document. A Lead Assessor must review and agree with the findings of any CE+ assessments issued by a CB. If the person carrying out the assessment is already a Lead Assessor, you will not require a second person to sign off the assessment.	Jake Hazelwood	Compliant