It is possible to achieve Conditional Certification if all the controls assessed as NOT MET in an official L2 Assessment (misunderstood, incorrectly implemented, documentation out of date, etc.) are eligible for the Plan of Actions & Milestones:

§ 170.21 Plan of Action and Milestones requirements.
(a) POA&M. For purposes of achieving a Conditional CMMC Status, an OSA is only permitted to have a POA&M for select requirements scored as NOT MET during the CMMC assessment and only under the following conditions: (summarized below)

- Only 1-point controls according to DoDAM (except FIPS)
- No L1 controls can be on the POA&M
- SC.L2-3.13.11 CUI Encryption may be included on a POA&M if encryption is employed but it is not FIPS-validated, which would result in a point value of 3
- Max of 22 controls permitted on POA&M to receive conditional certification

All open POA&Ms must be closed within 180 days of conditional certification. There must be a close-out assessment on those controls, resulting in a Final Certification.

Following is the list of controls which **are** eligible for POA&M. If you fail any controls other than these, or if you fail more than 22 of these, you will fail your assessment.

Practice ID	Practice Description
AC.L2-3.1.3	Control the flow of CUI in accordance with approved authorizations.
AC.L2-3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
AC.L2-3.1.6	Use non-privileged accounts or roles when accessing non-security functions.
AC.L2-3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.

AC.L2-3.1.8	Limit unsuccessful logon attempts.
AC.L2-3.1.9	Provide privacy and security notices consistent with applicable CUI rules.
AC.L2-3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.
AC.L2-3.1.11	Terminate (automatically) a user session after a defined condition.
AC.L2-3.1.14	Route remote access via managed access control points.
AC.L2-3.1.15	Authorize remote execution of privileged commands and remote access to security- relevant information.
AC.L2-3.1.21	Limit use of portable storage devices on external systems.
AT.L2-3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.
AU.L2-3.3.3	Review and update logged events.
AU.L2-3.3.4	Alert in the event of an audit logging process failure.
AU.L2-3.3.6	Provide audit record reduction and report generation to support on-demand analysis and reporting.
AU.L2-3.3.7	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.
AU.L2-3.3.8	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.
AU.L2-3.3.9	Limit management of audit logging functionality to a subset of privileged users.
CM.L2-3.4.3	Track, review, approve or disapprove, and log changes to organizational systems.
CM.L2-3.4.4	Analyze the security impact of changes prior to implementation.
CM.L2-3.4.9	Control and monitor user-installed software.
IA.L2-3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.
IA.L2-3.5.5	Prevent reuse of identifiers for a defined period.
IA.L2-3.5.6	Disable identifiers after a defined period of inactivity.
IA.L2-3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.
IA.L2-3.5.8	Prohibit password reuse for a specified number of generations.
IA.L2-3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.
IA.L2-3.5.11	Obscure feedback of authentication information.
IR.L2-3.6.3	Test the organizational incident response capability.
MA.L2-3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI.
MA.L2-3.7.6	Supervise the maintenance activities of maintenance personnel without required access authorization.
MP.L2-3.8.4	Mark media with necessary CUI markings and distribution limitations.
MP.L2-3.8.5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.
MP.L2-3.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
MP.L2-3.8.9	Protect the confidentiality of backup CUI at storage locations.

PE.L2-3.10.6	Enforce safeguarding measures for CUI at alternate work sites.
RA.L2-3.11.3	Remediate vulnerabilities in accordance with risk assessments
SC.L2-3.13.3	Separate user functionality from system management functionality.
SC.L2-3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.
SC.L2-3.13.7	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).
SC.L2-3.13.9	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period ofinactivity.
SC.L2-3.13.10	Establish and manage cryptographic keys for cryptography employed in organizational systems.
SC.L2-3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.*
SC.L2-3.13.12	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.
SC.L2-3.13.13	Control and monitor the use of mobile code.
SC.L2-3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.
SC.L2-3.13.16	Protect the confidentiality of CUI at rest.