



Cyber Essentials (CE) and
Cyber Essentials Plus (CE+)

Danzell Service
Offerings 2026



Background

URM Consulting Services Ltd (URM) offers a range of Cyber Essentials (CE) and Cyber Essentials Plus (CE+) service offerings to ensure your organisation receives the appropriate level of advice, guidance, and assurance to achieve a successful certification outcome.

The introduction of the Danzell update reflects the evolving cyber threat landscape and introduces tighter scheme controls to preserve the value of CE and CE+ certificates as mechanisms of independent, external assurance.

The Danzell update also provides greater clarity on organisational scoping, helping to ensure that legal entities, group structures and technical boundaries are accurately declared.

For CE+, if an organisation fails the authenticated vulnerability assessment on the first sample set of devices, URM must select a second sample set. If the vulnerabilities that caused the original failure are also identified in the second sample set, this will result in an immediate failure and revocation of the CE certificate, in line with scheme rules. The second sample set is designed to ensure that organisations remediate detections across their entire IT estate rather than only within the devices selected for the first sample.

The sections below outline each service offering. URM's recommended route to CE and CE+ certification is the Assured route, which is designed to reduce avoidable risk, delays, rework and unforeseen or increased cost. URM's Account Management Team will be pleased to help you select the most appropriate option for your organisation.



Contents

Cyber Essentials (CE)
Service Offerings 4

Cyber Essentials Assured.5
Cyber Essentials Guided8
Cyber Essentials Self-Managed10
CE Offerings Comparison Table12

Cyber Essentials PLUS (CE+)
Service Offerings 13

Cyber Essentials PLUS Assured.14
Cyber Essentials PLUS Guided18
Cyber Essentials PLUS - Self-Managed21
CE+ Offerings Comparison Table23

URM's Cyber Essentials (CE) Service Offerings



Cyber Essentials Assured

Cyber Essentials Assured is our recommended route for organisations seeking the smoothest and most straightforward path to CE certification, with the assurance of confirmed compliance at every stage. It combines targeted advisory support with additional activities focused on areas that, based on our assessors' experience, most commonly present challenges during assessment.

This offering includes the scope verification checks required for Cyber Essentials Plus and is the recommended option for organisations intending to progress to CE+.

PLATFORM ACCESS AND INITIAL QUESTIONNAIRE COMPLETION

You are provided with access to URM's Abriska platform, which includes embedded advice and guidance within the questionnaire to support a simplified and clearer process.

SCOPE VERIFICATION WORKSHOP

Early in the process, we will conduct a scope verification workshop with you. The Danzell questionnaire places much greater emphasis than previous questionnaires on correct scoping, particularly where certification covers an entity within a wider group. This workshop ensures that your CE scope is accurate and correctly reflects any group structures or legal entities, while providing an opportunity to agree the proposed certification boundaries before the assessment begins, in line with NCSC requirements.

It also confirms that the scope is suitable for a future CE+ assessment if you intend to progress to CE+ certification.

As part of the workshop, the assessor will work with you to agree:

- Devices in scope
- Networks in scope
- Any segregation arrangements
- Parent, child, or wider group relationships.

The logo features the letters 'CE' in a large, bold, sans-serif font, with the word 'ASSURED' in a smaller, bold, sans-serif font directly beneath it. The text is white and is centered within a dark blue circular background. This circle is surrounded by several concentric, glowing blue lines that resemble a stylized globe or a digital interface, with small blue dots and dashes scattered along these lines.

Technical considerations, such as the presence of hypervisors or other relevant infrastructure elements, are also identified and discussed where applicable.

This process helps identify potential issues at an early stage, including unsupported devices, high numbers of out-of-date systems, or non-compliant segregation arrangements.

QUESTIONNAIRE COMPLETION AND FEEDBACK REVIEW

Before the scope verification workshop, you will complete an initial draft of the questionnaire to the best of your ability, using the built-in guidance to support accurate and complete responses. This gives the assessor the opportunity to review your proposed scope, organisational structure and technical environment in advance of the workshop, helping to make the discussion as focused and productive as possible.

Following the workshop and any agreed amendments to the scope or questionnaire responses, you will submit the questionnaire for

formal review. An experienced URM assessor will then conduct an in-depth review of all responses and arrange a structured 1-hour feedback session via Microsoft Teams to discuss any areas of non-compliance and the actions required before resubmission.

During this feedback session, the assessor will help you clearly demonstrate your compliance, supporting you in addressing ambiguous responses that could otherwise be interpreted as not fully meeting CE requirements. Included follow-up support can be used as needed to discuss, address, and resolve any outstanding issues, ensuring the submission fully aligns with the agreed scope and clearly evidences compliance with CE requirements.

If your organisation is intending to proceed to CE+, the assessor will also capture the agreed scope information as evidence, such as obtaining exports or screenshots, in line with the Technical Scope Verification (TSV) requirements of the CE+ scheme. Once agreed, the outcome of the review forms part of the evidence used during your formal CE+ assessment.

The logo features the letters 'CE' in a large, bold, sans-serif font, with the word 'ASSURED' in a smaller, bold, sans-serif font directly beneath it. The text is white and is centered within a dark blue circular area. This central area is surrounded by several concentric circles and arcs, some of which are dashed and others solid, creating a sense of motion or a digital interface. Small blue dots and rectangular markers are scattered along these lines, further enhancing the technological aesthetic.

FINAL SUBMISSION AND CYBER ESSENTIALS ASSESSMENT

Once the questionnaire has been finalised, you will submit it for assessment through the Abriska platform, where it will be marked by an experienced URM assessor. Where minor inaccuracies are identified, these are resolved through the included support before the final submission is made.

Once a compliant submission has been achieved, the nominated senior management contact will be notified via Abriska and asked to sign off the assessment. This ensures that sign-off is required only once the questionnaire has been confirmed as accurate and compliant.

CYBER ESSENTIALS ASSURED SUMMARY:

- Our recommended CE route.
- A scope verification workshop included at an early stage to ensure your assessment is correctly scoped.
- A comprehensive questionnaire review, including a structured 1-hour Microsoft Teams session with an experienced and accredited assessor. This will also incorporate the full Technical Scope Verification (TSV) if you are progressing to CE+.
- Follow-up advisory support included as required to resolve issues and confirm compliance.
- Designed to reduce risk, rework, delays and unforeseen cost during later TSV and CE+ assessment stages.



CE
ASSURED

Cyber Essentials Guided

A guided route if you require some support with Cyber Essentials certification. An assessor will review your questionnaire, provide structured feedback, and help you understand why your responses are non-compliant and what actions you need to take before resubmission.

This service is designed for organisations that require some assessor guidance throughout the certification process, but do not need the additional scope verification and consultancy support provided through our *Cyber Essentials Assured* offering. This option is typically chosen by organisations that do not intend to proceed to CE+ but recognise the value of review, advice and guidance before submitting their assessment to support a successful CE outcome.

Cyber Essentials Assured remains our recommended offering for organisations seeking the highest level of support, confidence and assurance throughout the certification process.

QUESTIONNAIRE COMPLETION AND FEEDBACK REVIEW

With the *Cyber Essentials Guided* offering, you will gain access to the Abriska platform with embedded question guidance to help you complete the CE questionnaire. Once you have completed and submitted it for review, the experienced URM assessor will conduct a review of all responses and arrange a structured 1-hour questionnaire feedback session via Microsoft Teams.

During this session, the URM assessor will help you clearly demonstrate your compliance, supporting you in avoiding ambiguous responses that could otherwise be interpreted as not fully meeting CE requirements.

The logo features the letters 'CE' in a large, bold, sans-serif font, with the word 'GUIDED' in a smaller, bold, sans-serif font directly beneath it. The text is white and is centered within a dark blue circular area. This circle is surrounded by several concentric, glowing blue lines that resemble a stylized globe or a digital interface. The lines are composed of small segments and dots, giving it a sense of motion or data flow. The overall design is modern and tech-oriented.

FINAL SUBMISSION AND CYBER ESSENTIALS ASSESSMENT

Having attended the questionnaire feedback session, you can make any changes required and submit it for assessment through the Abriska platform, where it will be marked by an experienced URM assessor.

Up to 4 submission attempts are included, in line with the NCSC scheme managed by IASME. If you are still non-compliant after the third attempt, you will have the opportunity to take part in a 10-minute call with a URM assessor to discuss specific issues within the questionnaire.

Once a compliant submission has been achieved, the nominated senior management contact will be notified via Abriska and asked to sign off the assessment. This ensures sign-off is required only once the questionnaire has been confirmed as accurate and compliant. At any stage, you may convert to the Assured offering to access the recommended level of support for the smoothest Cyber Essentials certification experience.

CYBER ESSENTIALS GUIDED SUMMARY:

- Limited-support route
- A questionnaire review, including a structured 1-hour Microsoft Teams feedback session with an accredited assessor
- 4 total attempts included in line with NCSC guidelines
- Includes 10-minute call with assessor after the third failed attempt
- No scope-definition support included.

The logo features the letters 'CE' in a large, bold, white sans-serif font, with the word 'GUIDED' in a smaller, bold, white sans-serif font directly beneath it. The text is centered within a dark blue circular area. Surrounding this central circle are several concentric, glowing blue lines and arcs, some of which are dashed, creating a sense of motion and technology. Small blue dots and rectangular markers are scattered along these lines, resembling a digital or orbital path.

Cyber Essentials Self-Managed

A self-managed route for organisations that only require CE certification and wish to complete the questionnaire independently, without any assessor support. This offering includes access to URM's Abriska platform, which provides embedded question guidance and contextual advice.

QUESTIONNAIRE SUBMISSION AND CYBER ESSENTIALS ASSESSMENT

You complete the questionnaire independently and submit it through the Abriska platform, where it will be marked by an experienced URM assessor.

Where non-compliant responses are identified, feedback will be provided directly within the Abriska platform. This allows you to review, update, and resubmit the questionnaire as required. As with the *Cyber Essentials Guided* offering, up to 4 submission attempts are included.

If the submission remains non-compliant on the fourth attempt, the assessment will be recorded as a fail, and a new CE application will be required to restart the process.

Once a compliant submission has been achieved, the nominated senior management contact will be notified via Abriska and asked to sign off the assessment. This ensures that sign-off is required only once the questionnaire has been confirmed as accurate and compliant.

At any stage of the assessment, you have the option to upgrade to the *Cyber Essentials Guided* or *Assured* offerings if you decide you will benefit from speaking directly with an assessor and receiving tailored advice and guidance. Our objective is to support your success at every stage.

A large, stylized graphic on the right side of the page. It features a dark blue circular background with concentric circles and glowing blue lines, resembling a digital or network interface. In the center, the text 'CE' is written in large, bold, white letters, with 'SELF-MANAGED' written below it in smaller, bold, white letters.

CE
SELF-MANAGED

This option is intended for organisations that wish to manage the certification process independently with minimal assessor support. It is not URM's recommended route to certification, as our experience shows that even organisations with a

strong understanding of the scheme can encounter avoidable delays, rework, assessment failures and additional cost when undertaking the process without assessor guidance.

CYBER ESSENTIALS SELF-MANAGED SUMMARY:

- Self-managed route
- Access to Abriska platform question guidance
- 4 submission attempts included, in line with NCSC guidance
- No advisory, scope definition or questionnaire feedback support included.



CE
SELF-
MANAGED

CE Offerings Comparison Table

Service / Activity	CE ASSURED	CE GUIDED	CE SELF-MANAGED
Access to Abriska platform including question advice and guidance	✔	✔	✔
Applicant completes questionnaire	✔	✔	✔
Scope verification workshop including: • Scope-definition support • Review of device, networks segregation, group structure • Gathering of evidence for the Technical Scope Verification (TSV) requirements of the CE+ scheme.	✔	✘	✘
Detailed questionnaire review with a structured 1-hour feedback session with an assessor	✔	✔	✘
Assessor marks submission	✔	✔	✔
CE questionnaire submission attempts included	Unlimited	4 As per NCSC guidance	4 As per NCSC guidance
Follow-up support to ensure the CE submission meets requirements	Unlimited	Limited 10-minute feedback call	✘

URM's Cyber Essentials PLUS (CE+) Service Offerings



Cyber Essentials *PLUS* Assured

This is our recommended route for organisations seeking the most straightforward and reliable path to Cyber Essentials (CE) and Cyber Essentials Plus (CE+) certification, supported by ongoing compliance assurance.

It includes targeted advisory support and key activities focused on areas that, based on our assessors' experience, most commonly create challenges during assessment. Vulnerability management and patching account for around 90% of CE+ assessment failures and, without additional preparation, fewer than 5% of applicants pass first time. To address this, *Cyber Essentials PLUS Assured* provides ongoing monthly scanning to help you maintain compliance, together with enhanced scanning during the CE+ assessment process.

This offering includes *Cyber Essentials Assured* ([See Page 5](#)), 1 year of access to the Abriska CE+ Assured module, a half-day sample-based CE+ pre-assessment, the formal CE+ assessment, and 1 follow-up test within the NCSC remediation window, in line with the Danzell scheme's

remediation process. It also includes:

- An additional half day of ad hoc advisory time
- Additional scans in the 3 days immediately preceding the CE+ assessment
- Daily internal vulnerability scans (on all assets) if the initial assessment is not successful
- Unlimited CE/CE+ certification attempts* if you fail the CE+ assessment.

Because this offering includes *Cyber Essentials Assured*, your journey benefits from the Scope Verification Workshop and Technical Scope Verification activities completed during the Cyber Essentials certification process.

*Further support and guidance are available for additional certification attempts, provided that all URM guidance and recommendations have been followed. Charges may apply where an additional attempt results from a scope change, the same vulnerabilities have not been addressed, or URM's advice and guidance have not been followed. Once you have undertaken a CE+ assessment, you have 30 days to remediate all issues and complete a follow-up test that includes a second sample.



This ensures your certification scope is defined fully and accurately before the CE submission is finalised and that any issues likely to cause problems later in the certification journey are identified as early as possible.

ABRISKA CE+ ASSURED MODULE

Your 1-year access to the Abriska CE+ Assured module provides:

- Monthly compliance scans of up to 20 external IP addresses in scope for CE**
- Monthly compliance scans of all servers and end-user devices in scope***
- An interactive view of the assets and vulnerabilities that could cause a compliance failure
- Actionable recommendations aligned to CE and CE+ requirements
- 1 daily authenticated internal Qualys scan of all assets in the 3 working days before the official CE+ assessment
- 1 daily authenticated internal vulnerability scan of all assets if the initial CE+ assessment is not successful until the scheduled follow-up test date within the NCSC remediation window.

CE+ PRE ASSESSMENT AND ADVISORY SUPPORT

A sample-based CE+ pre-assessment is typically scheduled within the 2 weeks before your official CE+ assessment. This pre-assessment tests a small, representative sample of your devices, identifies likely failure points before the formal assessment, and provides initial advice on any issues identified.

In addition, half a day of advisory time is included. This can be used to review pre-assessment findings, discuss required remediation actions, answer questions, or provide targeted advice ahead of the formal CE+ assessment.

To provide further assurance immediately before the official CE+ assessment, this offering also includes daily internal vulnerability scans for all in-scope devices during the 3 working days before the assessment.

** Additional external IP addresses can be included – please speak to your account manager.

***You are responsible for ensuring all in-scope devices are correctly enrolled. URM can provide scan results only for devices that have been correctly enrolled.



CE+
ASSURED

These scans are designed to provide visibility of vulnerabilities that could result in a failed assessment, helping you address issues before testing takes place and improve your chances of first-time success. Compliance can then be monitored throughout the period immediately preceding the assessment, reducing the likelihood of unforeseen issues.

TECHNICAL SCOPE VERIFICATION (TSV)

In most cases, the Technical Scope Verification is conducted separately from the CE+ assessment and must be passed at least 7 working days before the assessment start date. For this *Cyber Essentials PLUS Assured* offering, the TSV is typically conducted as part of the scope workshop included within *Cyber Essentials Assured* ([See Page 5](#)).

This approach significantly reduces the risk of booking CE+ assessment time that cannot be used due to issues with the declared scope. Any factors that could prevent a successful CE+ assessment are identified and addressed early in the process.

For some small or micro-organisations (e.g., where the whole organisation is in scope and only a very small number of devices are involved) it may be

possible to agree that the TSV is performed at the start of the CE+ assessment rather than as a separate activity in advance.****

FOLLOW-UP TESTING AND CERTIFICATION ATTEMPTS

If the CE+ assessment identifies failing items or vulnerabilities that have not been addressed, URM will test a second sample set in line with the Danzell scheme's remediation process.

If the authenticated vulnerability assessment of the first sample set is unsuccessful, adopting this route will enable you to monitor compliance of all your assets via the daily vulnerability scans included immediately ahead of your second test.

****Performing the TSV on the day of the CE+ assessment may reduce cost and administrative effort, but it increases risk. If issues are identified that cannot be immediately resolved, the CE+ assessment time will need to be either repositioned as advisory activity or postponed, and postponement charges will apply. By choosing this option, you acknowledge that passing the TSV is a prerequisite for proceeding with the formal CE+ assessment and that this approach carries a higher risk.



You should be aware that under the Danzell remediation rules, if the second sample set fails because the same vulnerabilities identified in the first sample set are identified again, your CE certificate will be revoked and the entire CE and CE+

process will need to be restarted. The guidance and support provided during the Assured process are designed to mitigate the risk of this occurring.

CYBER ESSENTIALS PLUS ASSURED SUMMARY:

- Recommended CE+ route
- Includes *Cyber Essentials Assured*
- 1 year of access to the Abriska CE+ Module (Assured)
- Monthly internal device scans included
- Monthly external IP scans included
- Daily compliance scans of all assets in the days immediately before the CE+ official assessment and, if the initial assessment is unsuccessful, until the scheduled follow-up test date within the NCSC remediation window
- Sample-based CE+ pre-assessment included
- Half-day advisory support included
- Includes testing of a second sample set in line with the Danzell scheme remediation process.

The logo for Cyber Essentials Plus Assured. It features the letters 'CE' in a large, bold, sans-serif font, with a plus sign integrated into the 'E'. Below this, the word 'ASSURED' is written in a smaller, bold, sans-serif font. The entire logo is set against a dark blue background with glowing, concentric circular lines and small dots, suggesting a digital or technological theme.

Cyber Essentials PLUS Guided

A guided route if you want structured support across both the CE and CE+ assessments. This offering includes all the benefits of the *Cyber Essentials Guided* offering, together with additional preparation ahead of the official CE+ assessment.

This offering includes *Cyber Essentials Guided*, a Vulnerability Check Workshop, the formal CE+ assessment, and 1 included follow-up test within the NCSC remediation window, in line with the Danzell scheme's remediation process. Your assessor will also help to validate the proposed certification scope and complete the Technical Scope Verification activities required ahead of the CE+ assessment. This helps ensure the scope is appropriate and any potential issues are identified as early as possible.

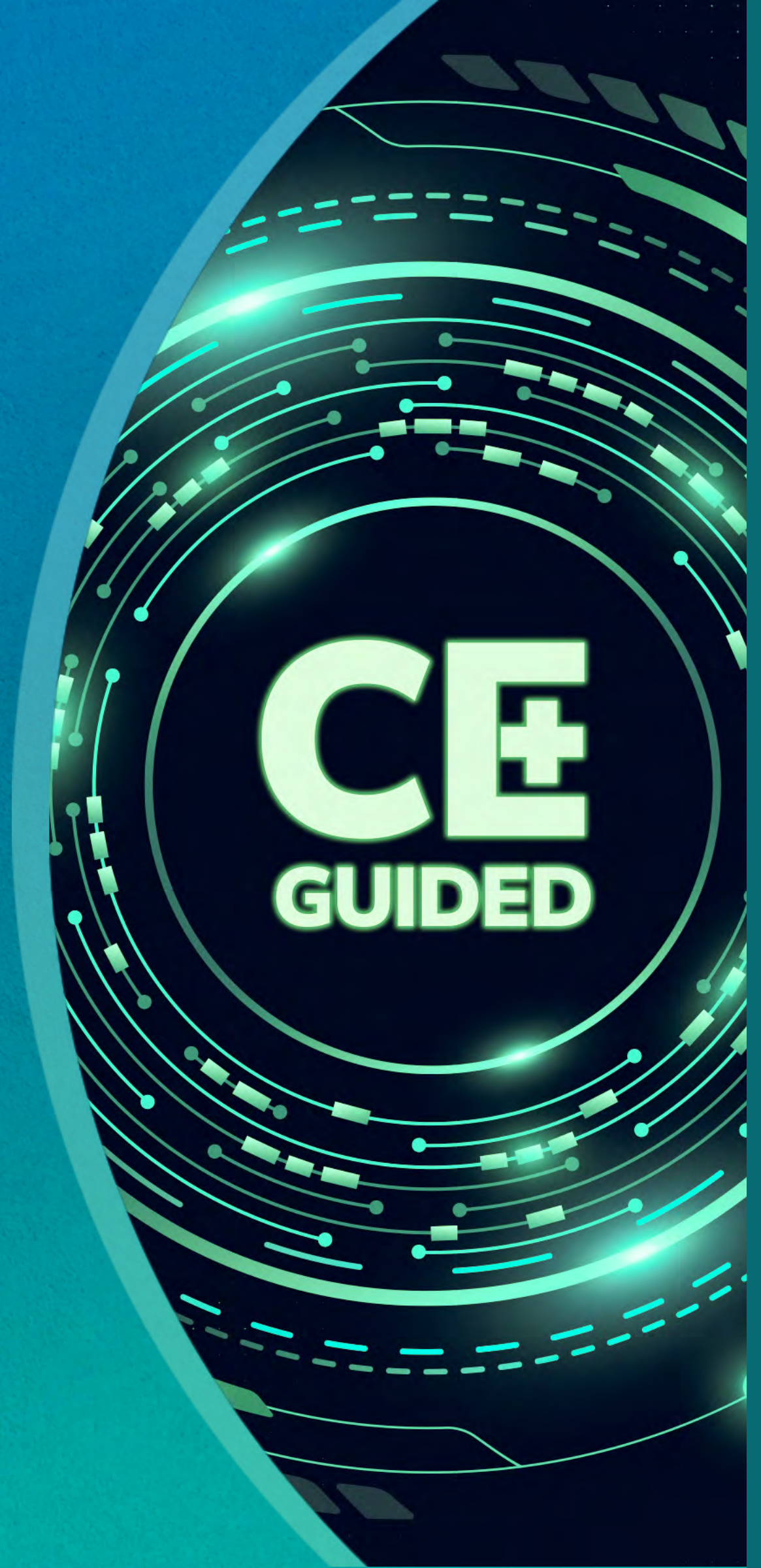
This offering does not include access to the Abriska CE+ Assured module, which provides vulnerability scanning and compliance assurance services both ahead of and after the CE+ assessment. Organisations selecting *Cyber Essentials PLUS*

Guided should therefore already have an established vulnerability scanning capability and mature patch management processes. If you do not have these capabilities, *Cyber Essentials PLUS Assured* will provide the most appropriate level of support.

VULNERABILITY CHECK WORKSHOP

The internal authenticated vulnerability scan is the single most common reason for failing a CE+ assessment, and under new Danzell requirements, multiple vulnerability reports are no longer acceptable.

To help reduce the risk of assessment failure, *Cyber Essentials PLUS Guided* includes a vulnerability check workshop ahead of the official CE+ assessment. The workshop is designed to provide visibility of vulnerabilities that could result in a failed assessment, helping you address issues before testing takes place and improve your chances of first-time success.



If your organisation already has a vulnerability scanning solution, we will ask you to perform a scan prior to the workshop and review the results with one of our assessors. Where a scanning capability is not available, URM can provide Qualys agents for installation on applicable devices and conduct the scan on your behalf. Please note that only devices with an installed agent can be assessed.

During the workshop, your assessor will review the scan findings, highlight any vulnerabilities that could prevent a successful CE+ assessment, and provide guidance on the remediation actions required before testing begins. All detections should be remediated before the CE+ assessment.

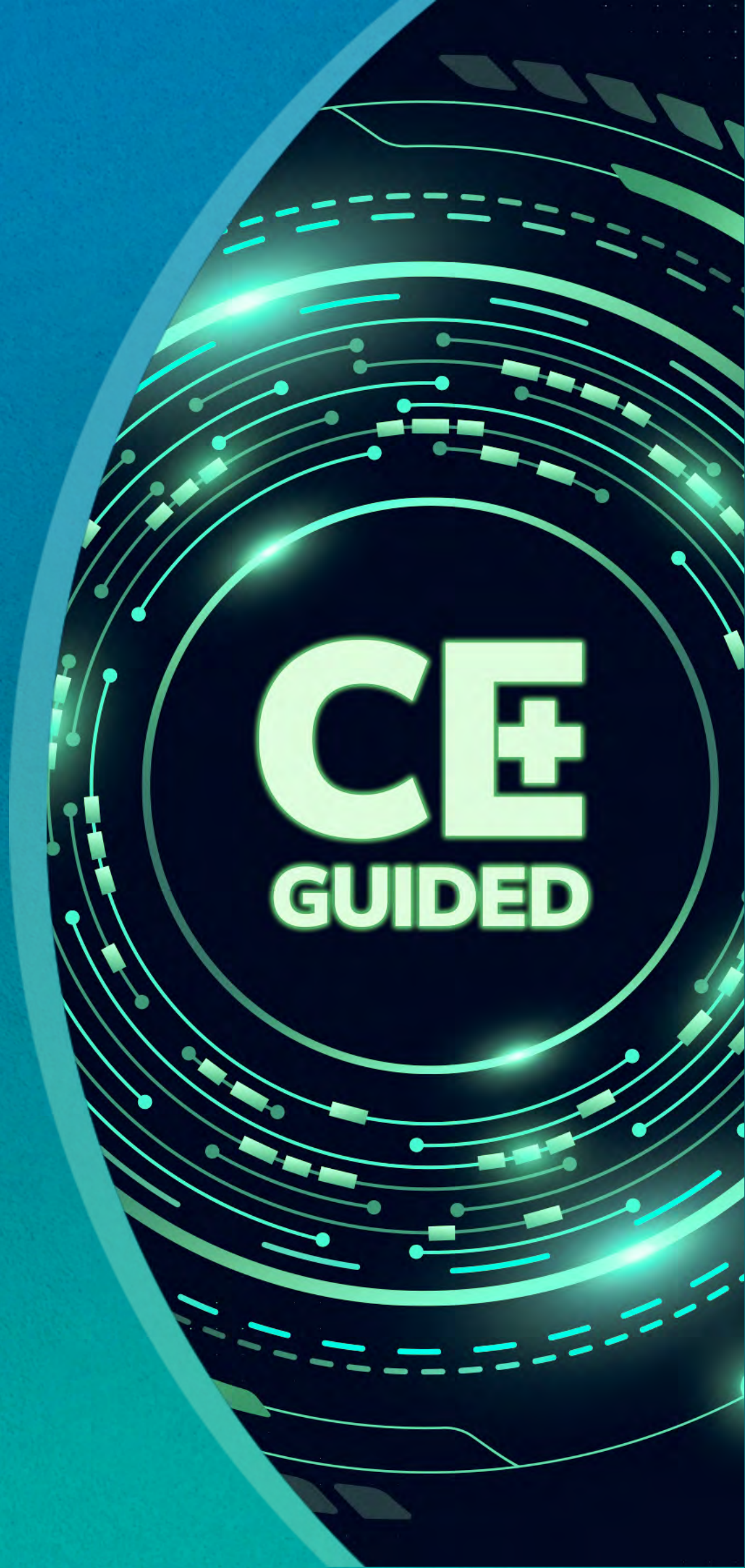
The workshop provides a point-in-time assessment of your vulnerability status; organisations remain responsible for ensuring compliance is maintained between the workshop and the formal CE+ assessment, and following certification. If you do not have an established vulnerability scanning capability and mature patch management processes, *Cyber Essentials PLUS Assured* remains our recommended option.

SCOPE VERIFICATION WORKSHOP AND TECHNICAL SCOPE VERIFICATION (TSV)

In most cases, the Technical Scope Verification is conducted separately from the CE+ assessment and must be passed at least 7 working days before the assessment start date. For this *Cyber Essentials PLUS Guided* offering, the TSV will typically be conducted as part of a scope verification workshop. During the workshop, your assessor will review the proposed certification scope with you to help ensure that it accurately reflects your organisation, is suitable for CE+, and does not contain issues that could prevent the assessment from proceeding.

This approach significantly reduces the risk of booking CE+ assessment time that cannot be used if issues are later identified with the declared CE scope. Any factors that could prevent a successful CE+ assessment are identified and addressed early in the process.

For some small or micro-organisations (e.g., where the whole organisation is in scope and only a very small number of devices are involved) it may be



CE+
GUIDED

possible to agree that the TSV is performed at the start of the CE+ assessment rather than as a separate activity in advance.*

FOLLOW-UP TESTING

If the TSV passes successfully, but the CE+ assessment identifies failing items, you may book 1 follow-up test in line with [NCSC guidance and the Danzell remediation process](#). A second sample set must be selected for this test. If the same vulnerabilities are identified again, you will fail the CE+ assessment and your CE certificate will be revoked in accordance with scheme rules.

To reduce this risk and achieve the smoothest possible path to CE and CE+ certification, you may wish to consider the *Cyber Essentials PLUS Assured* offering, which includes additional scanning, advisory support, and assurance designed to identify and resolve issues earlier.

* Performing the TSV on the day of the CE+ assessment may reduce cost and administrative effort, but it increases risk. If issues are identified that cannot be immediately resolved, the CE+ assessment time will need to be either repositioned as advisory activity or postponed, and postponement charges will apply. By choosing this option, you acknowledge that passing the TSV is a prerequisite for proceeding with the formal CE+ assessment and that this approach carries a higher risk.

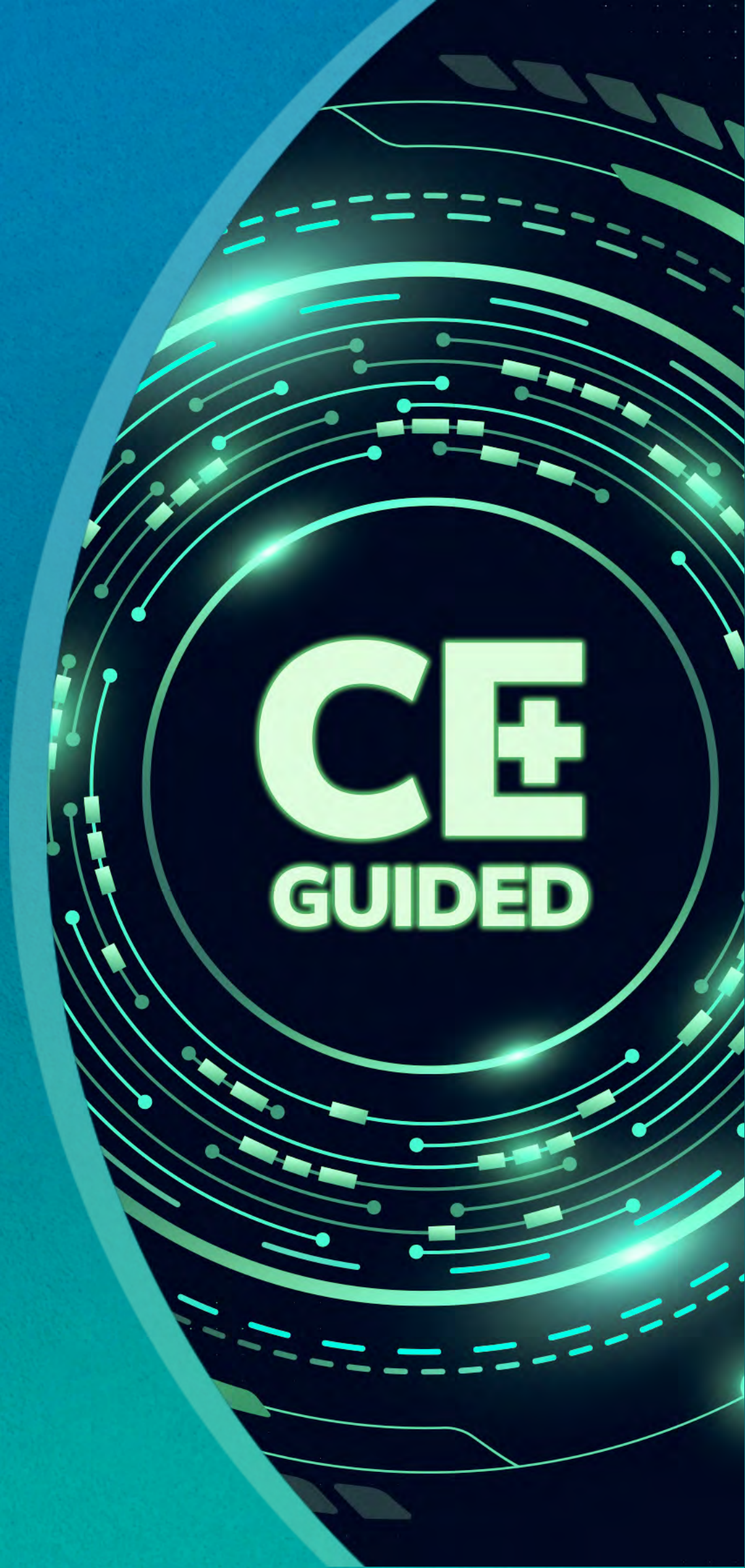
CYBER ESSENTIAL PLUS GUIDED SUMMARY:

- Includes *Cyber Essentials Guided*
- Vulnerability check workshop ahead of the assessment
- Includes testing of a second sample set in line with the Danzell scheme remediation process.

Unlike *Cyber Essentials PLUS Assured*, this offering includes:

- No monthly internal device scans
- No monthly external IP scans
- No daily scans in the final 3 working days before the official CE+ assessment
- No remediation scans following a failed assessment
- No sample-based CE+ pre-assessment included
- No option for unlimited CE+ certification attempts

In addition, any ad hoc advisory time outside the structured Guided offering is chargeable.



CE+
GUIDED

Cyber Essentials *PLUS*

- Self-Managed

An assessment-only route for organisations that already hold a valid CE certificate and now require the formal CE+ assessment.

This offering includes the CE+ assessment only. It includes 1 follow-up test in line with [NCSC guidance and the Danzell remediation process](#).

It includes the required assessment prerequisites and instructions but excludes a CE offering, a scope verification workshop, any pre-assessment activity, advisory time, and access to the Abriska CE+ Assured module. The Abriska CE+ Assured module provides monthly compliance scans alongside CE+ preparation and remediation scans, which are not included in the self-managed offerings.

This offering is available only to organisations that already hold a valid CE certificate and includes the mandatory Technical Scope Verification (TSV). The purpose of the TSV process is to confirm that the declared CE scope accurately reflects the organisation and technical environment to be assessed for CE+.

As the Self-Managed offering does not include the scope verification workshop, organisations selecting this option are responsible for ensuring that their declared scope accurately reflects the organisation and complies with CE and CE+ scheme requirements. Even organisations with previous Cyber Essentials experience can encounter scope-related issues. If such issues are identified at the TSV stage, this may prevent the CE+ assessment from proceeding and, in some cases, may require a new CE certification before CE+ can be achieved.

TECHNICAL SCOPE VERIFICATION (TSV)

In most cases, the TSV is conducted separately and must be passed at least 7 working days before the CE+ assessment start date. This reduces the risk of booking assessment time that cannot be used if issues are identified with the declared scope.

If the TSV identifies issues that prevent the assessment from proceeding, you may need to revisit your CE scope and, in some cases, carry out a



new CE assessment before continuing with CE+.

For some small or micro-organisations (e.g., where the entire organisation is in scope and only a very small number of devices are involved) it may be possible to agree that the TSV is performed at the start of the CE+ assessment rather than as a separate activity in advance.*

FOLLOW-UP TESTING

If the TSV passes but the CE+ assessment identifies failing items, you may book 1 follow-up test in line with the [Danzell scheme's remediation process](#).

A second sample set must be selected for the retest. If the same vulnerabilities are identified in

this test, you will fail the CE+ assessment and your CE certificate will be revoked in accordance with scheme rules.

To reduce this risk and to follow the smoothest path to CE and CE+ certification, it is strongly recommended that you consider the *Cyber Essentials PLUS Assured* offering. This is designed to identify and address potential issues earlier in the certification process.

* Performing the TSV at the start of the CE+ assessment may reduce cost and administrative effort, but it increases risk. If issues are identified that cannot be immediately resolved, the CE+ assessment time will need to be either repositioned as advisory activity or postponed, and postponement charges will apply. By choosing this option, you acknowledge that passing the TSV is a prerequisite for proceeding with the formal CE+ assessment and that this approach carries a higher risk.

CYBER ESSENTIALS PLUS SELF-MANAGED SUMMARY:

- Assessment-only CE+ route
- Existing valid CE certificate required
- Mandatory TSV required
- TSV is usually conducted separately and in advance. For some very small organisations, it may be performed at the start of the CE+ assessment by agreement
- Passing a separate TSV at least 7 working days before the CE+ assessment reduces the risk of late cancellation charges
- If a same-day TSV fails, the CE+ assessment cannot proceed
- No advisory or preparation support included
- Includes testing of a second sample set in line with the Danzell scheme remediation process.



CE+
SELF-MANAGED

CE+ Offerings Comparison Table

Service / Activity	CE+ ASSURED	CE+ GUIDED	CE+ SELF-MANAGED
CE offering included	Cyber Essentials Assured	Cyber Essentials Guided	
TSV required before CE+ can proceed	Covered through Cyber Essentials Assured path	Covered during CE process	
TSV timing approach	Usually conducted ahead of CE assessment as part of scope verification workshop, for some very small organisations may be conducted at the start of CE+ by agreement	Usually conducted ahead of CE assessment as part of scope verification workshop, for some very small organisations may be conducted at the start of CE+ by agreement	Usually conducted separately in advance; for some very small organisations may be conducted at the start of CE+ assessment by agreement
Scope verification workshop included			
0.5-day sample-based CE+ pre-assessment			

CE+ Offerings Comparison Table

Service / Activity	CE+ ASSURED	CE+ GUIDED	CE+ SELF-MANAGED
0.5-day advisory time			
1-year access to Abriska CE+ Assured module			
Final assessment readiness checks	Daily internal vulnerability scans of all in-scope devices in the 3 working days ahead of assessment	Single, point-in-time vulnerability scan ahead of CE+ assessment and Vulnerability Check Workshop with assessor to discuss findings	
Formal CE+ assessment			
1 follow-up test in line with Danzell scheme remediation process			
Unlimited daily internal authenticated scans after fail (max 1/day, until retest date)			



T: 0118 206 5410

E: info@urmconsulting.com

www.urmconsulting.com

