URM
PART OF COOPER PARRY

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.

Improved clarity has also been introduced across both schemes regarding organisational scoping, ensuring that legal entities, group structures, and technical boundaries are accurately declared.

For CE+, if an organisation fails its initial assessment, a single retest may be arranged. A new sample set must be selected by URM. If the vulnerabilities that caused the original failure remain present during the retest, this will result in an immediate failure and revocation of the CE certificate, in line with scheme rules.

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, delay, and rework. URM's account management team will be pleased to help you select the most appropriate option for your organisation.

Contents

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 CE + and is therefore the default CE offering within URM's CE+ services.

PLATFORM ACCESS AND INITIAL QUESTIONNAIRE COMPLETION

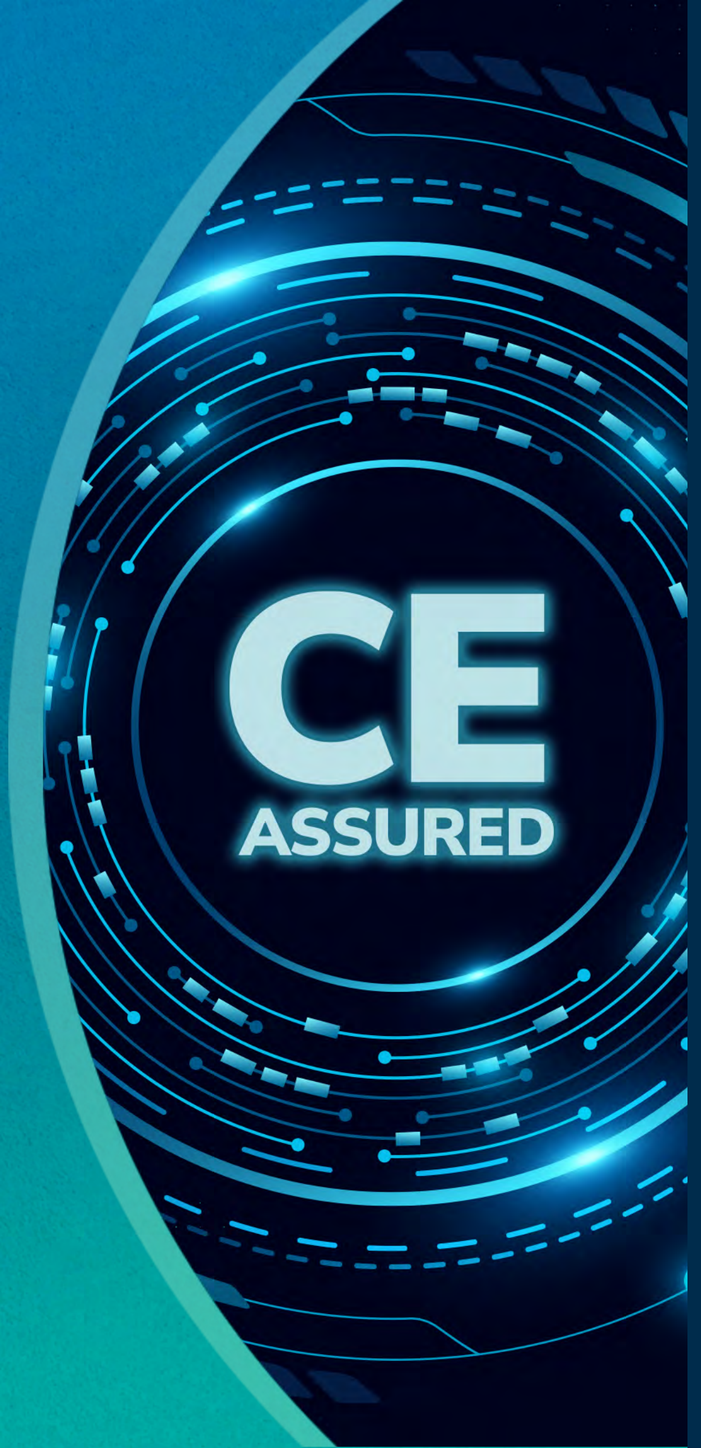
You are provided with access to the Abriska platform, which includes embedded advice and guidance within the questionnaire.

SCOPE VERIFICATION WORKSHOP

Early in the process we will run a scope verification workshop with you. The Danzell questionnaire provides a much greater focus than previous questionnaires on correct scoping, particularly if your certification is for an entity within a wider group. This workshop ensures that your CE scope is accurate and correctly reflects any group structures or legal entities. It also confirms that the scope is suitable for a future CE+ assessment, if you are moving onto CE+.

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



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

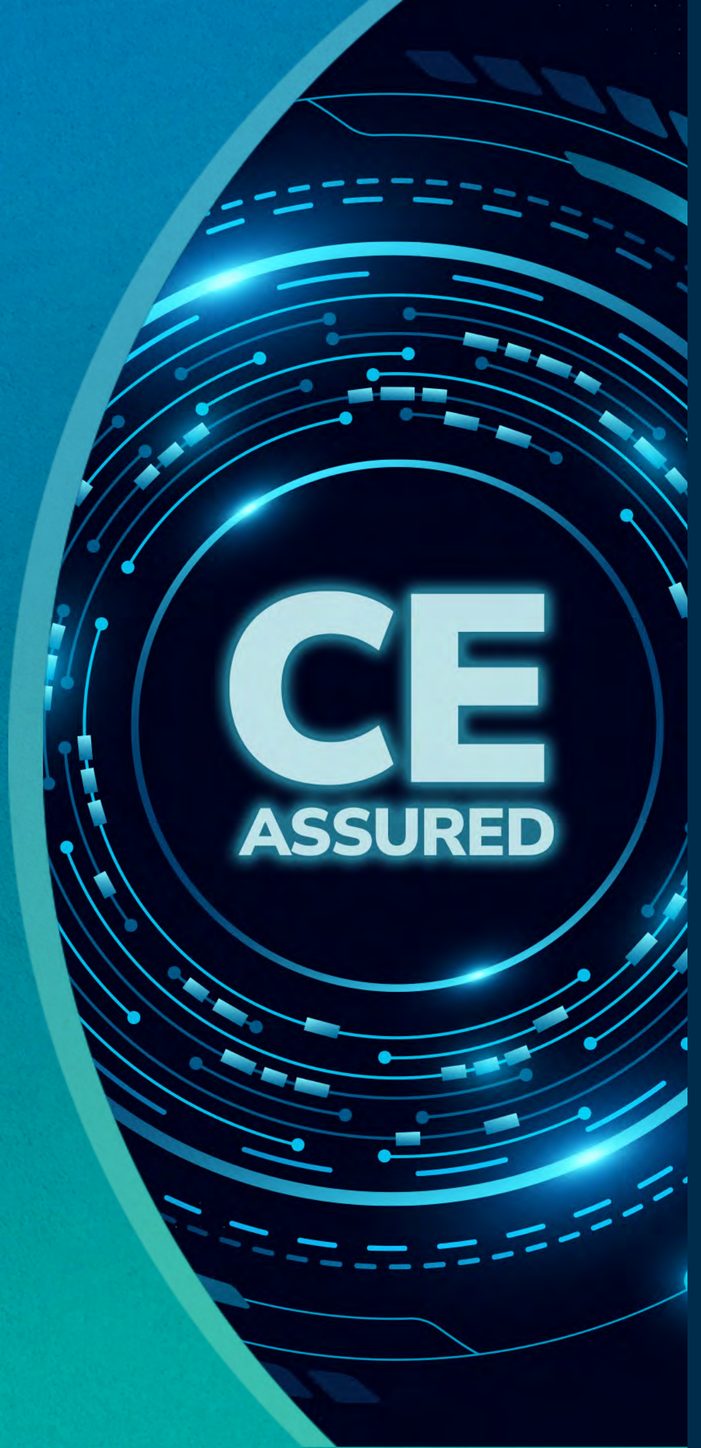
This process helps identify potential issues at an early stage, including unsupported devices, high numbers of out-of-date systems, or ineffective segregation arrangements.

QUESTIONNAIRE COMPLETION AND FEEDBACK REVIEW

Following 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. You will then submit the questionnaire for review. Once submitted, an experienced URM assessor will conduct an in-depth review of all responses and arrange a structured 1-hour questionnaire feedback session via Microsoft Teams.

For organisations 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.

During this 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.



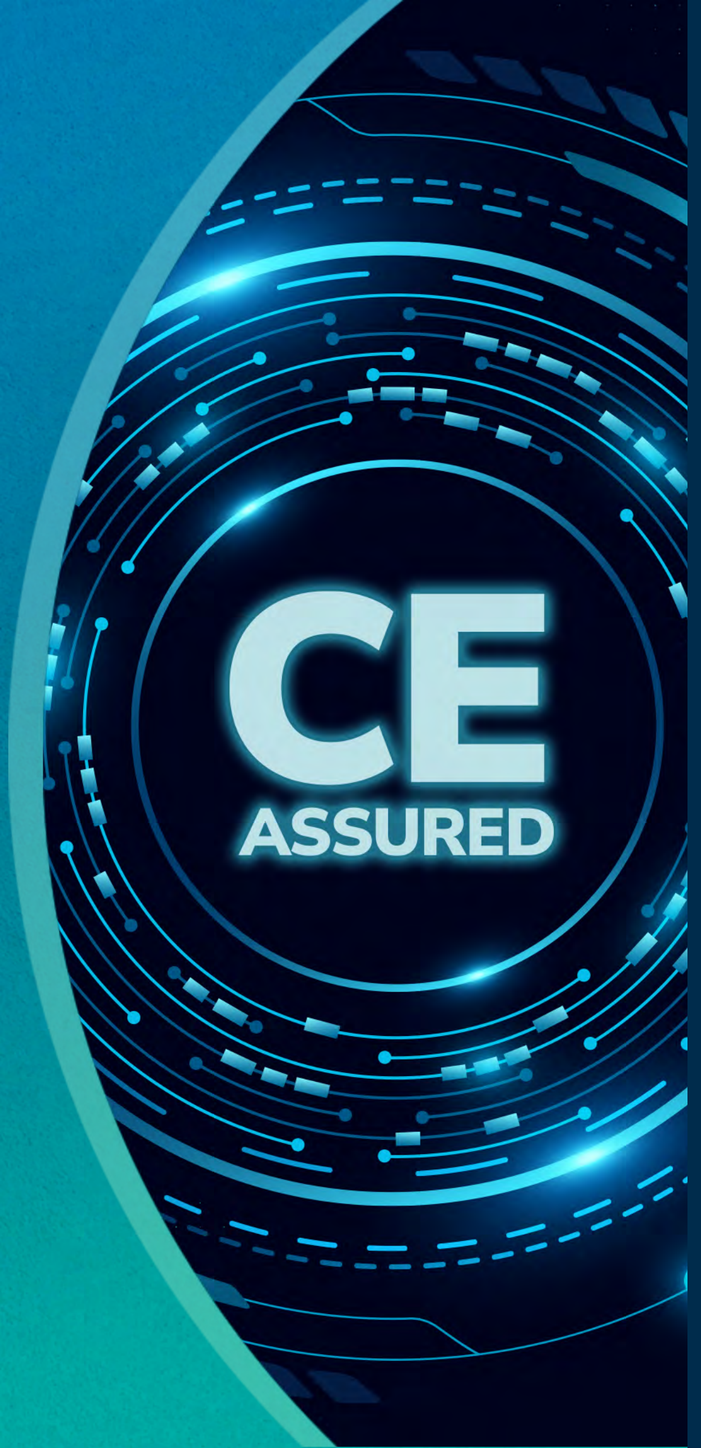
FINAL SUBMISSION AND CYBER ESSENTIALS ASSESSMENT

Once the questionnaire has been finalised, you submit it 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, you will be notified via Abriska and can arrange senior management sign off. This ensures sign off is only required once the questionnaire is confirmed to be accurate and compliant.

CYBER ESSENTIALS ASSURED SUMMARY:

- Our recommended CE route and a prerequisite for organisations intending to progress to CE+.
- 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 moving on to CE+.
- Follow-up advisory support included as required to resolve issues and confirm compliance.
- Designed to reduce risk, rework, and delays during later TSV and CE+ assessment stages.



Cyber Essentials Guided

A guided route for your organisation if you only require CE certification and want an assessor to 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 offering does not include the scope definition support required for CE + assessments and is therefore suitable for CE certification only. If seeking CE+, please refer to URM's *Cyber Essentials PLUS Assured* offering.

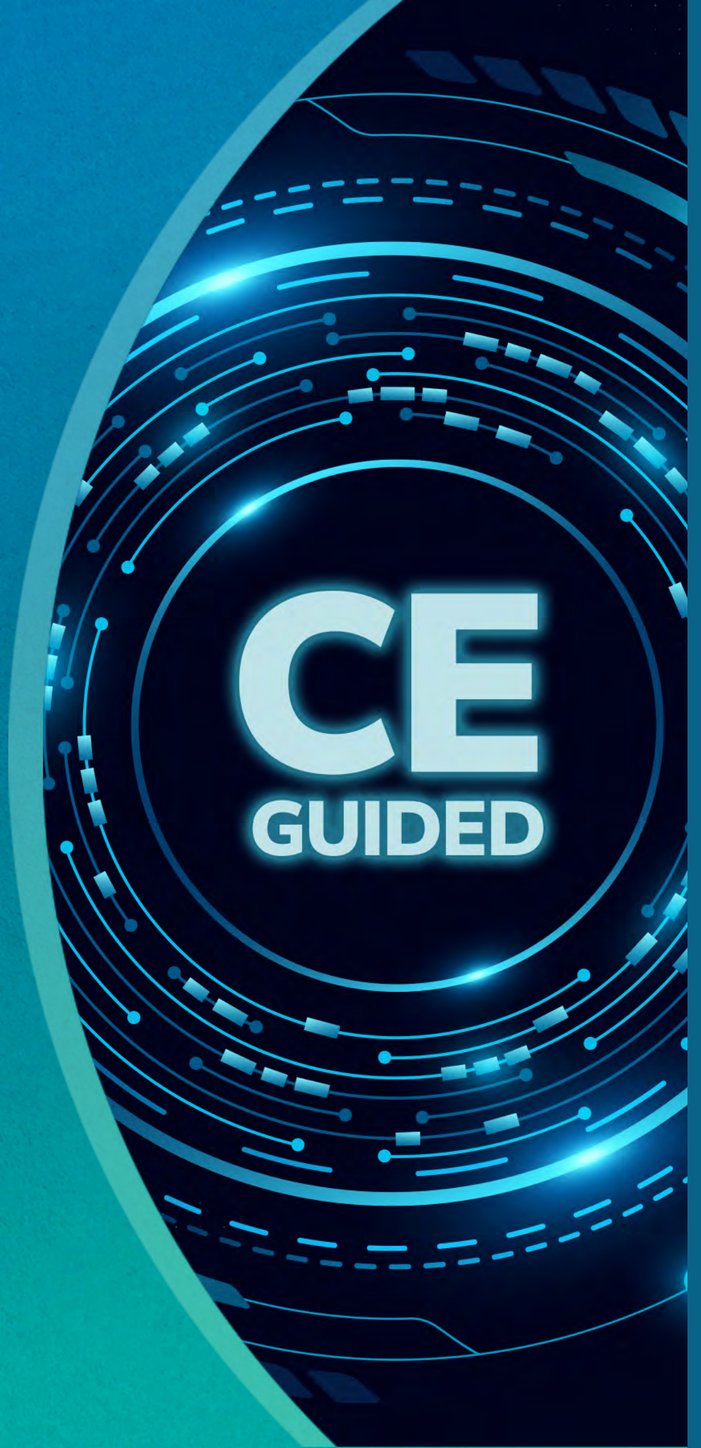
QUESTIONNAIRE COMPLETION AND FEEDBACK REVIEW

With the *Cyber Essentials Guided* offering you can 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 an in-depth 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.

FINAL SUBMISSION AND CYBER ESSENTIALS ASSESSMENT

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

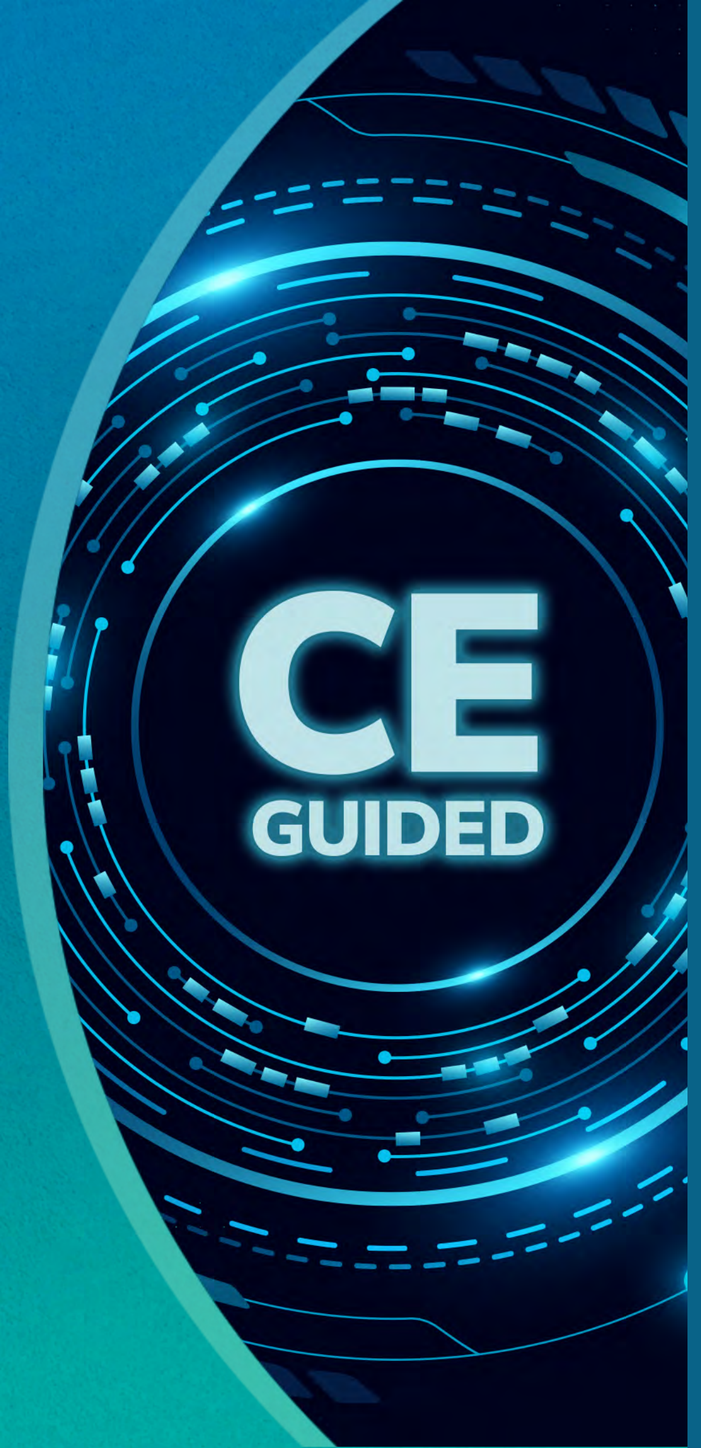


Up to 4 submission attempts are included, in line with the NCSC scheme which is managed by IASME. If you are still non-compliant after the third attempt, you will have the opportunity to take part in a 10 minute call with the URM assessor to discuss specific issues within the questionnaire.

Once a compliant submission has been achieved, you will be notified via the Abriska platform and can arrange senior management sign off. This ensures sign off is only required once the questionnaire is confirmed to be 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 comprehensive 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 3rd failed attempt
- No scope-definition support included.



Cyber Essentials Self-Managed

A self-managed route for organisations that only require CE certification and are confident completing 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 Guided offering, up to 4 submission attempts are included. If the submission remains non-compliant on the 4th attempt, the assessment will be marked as a fail and a new CE application will be required to restart the process.

Once a compliant submission has been achieved, you will be notified via the Abriska platform and can arrange senior management sign off. This ensures sign off is only required once the questionnaire is confirmed to be 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.

This option is only intended for experienced applicants who do not expect to progress to CE+. It does not include advisory meetings, scope definition support, or assessor led questionnaire feedback sessions.

CYBER ESSENTIALS SELF-MANAGED SUMMARY:

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

*National Cyber Security Centre's (NCSC) delivery partner for the CE scheme

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 if you want the smoothest 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. It also 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 included retest within the NCSC remediation window in line with the Danzell scheme's remediation process, plus:

- 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+ certification attempts* within 3 months of your CE certification date.

Because this offering includes *Cyber Essentials Assured*, your journey includes both the initial scoping workshop and the Technical Scope Verification where evidence will be captured. 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.

* If additional retests are as a result of a scope change or the same vulnerabilities are identified and not addressed or URM's advice and guidance is not followed then charges may apply. Please note that once you have undertaken a CE+ assessment you have 30 days to remediate all issues and for there to be a retest including a second sample.

ABRISKA CE+ ASSURED MODULE

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

- Monthly compliance scans of all 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 prior to the official CE+ assessment
- 1 daily authenticated internal vulnerability scan of all assets if the initial CE+ assessment is not successful until the scheduled retest date within the NCSC remediation window.

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

CE+ PRE ASSESSMENT AND ADVISORY SUPPORT

A sample-based CE+ pre assessment is typically scheduled within the 2 weeks prior to 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 prior to assessment. This allows compliance to be monitored in the days preceding the assessment and avoids any 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 seven working days before the assessment start date. For this *Cyber Essentials PLUS Assured* offering, the TSV is typically conducted as part of the review 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.***

RETESTS AND CERTIFICATION ATTEMPTS

If the CE+ assessment identifies failing items or vulnerabilities that have not been addressed, URM will perform 1 retest in line with the Danzell scheme's remediation process.

If the initial CE+ assessment is unsuccessful due to vulnerabilities identified through authenticated scanning, adopting this route will enable you to monitor compliance of all your assets via the daily vulnerability scans included immediately ahead of your retest.

You should be aware that under the Danzell remediation rules, if the retest using a second sample set fails due to the same vulnerabilities, your CE certificate will be revoked and the whole CE and CE+ process will need to be restarted.

*** 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 Essentials PLUS Assured

***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 and after the CE+ official assessment
- Sample based CE+ pre assessment included
- Half day advisory support included
- 1 retest included in line with the Danzell scheme remediation process.

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 Assured* offering, together with additional preparation ahead of the official CE+ assessment.

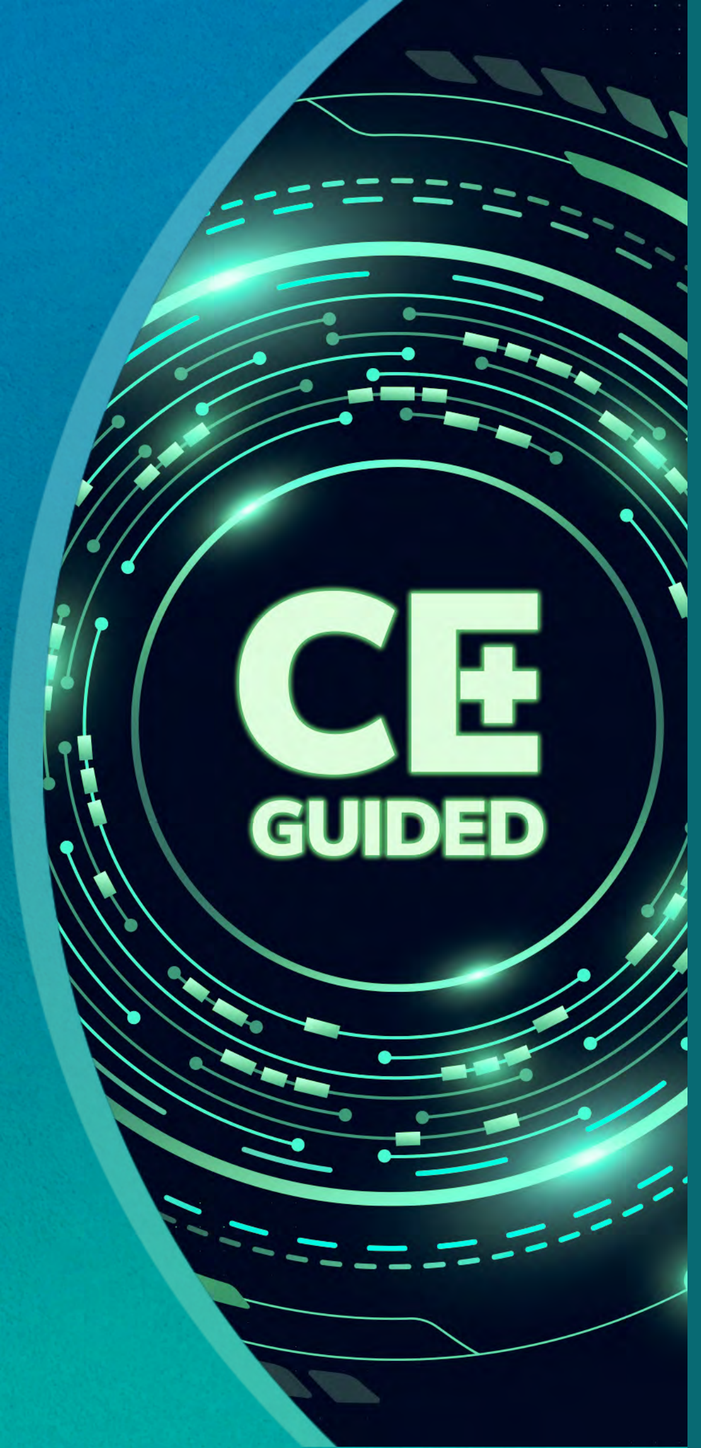
This offering includes *Cyber Essentials Assured*, 1 year of access to the Abriska CE+ *Guided* module, a half-day sample-based CE+ pre assessment, the formal CE+ assessment, and 1 included retest within the NCSC remediation window in line with the Danzell scheme's remediation process.

Because this offering includes *Cyber Essentials Assured*, your journey includes both the initial scoping workshop and the **Technical Scope Verification** where evidence will be captured. 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+ GUIDED MODULE

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

- Monthly compliance scans of all 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 lead to a compliance failure
- Actionable, prioritised recommendations tailored to CE and CE+ requirements.



CE+ PRE ASSESSMENT

A sample-based CE+ pre assessment is typically scheduled within the 2 weeks prior to your official CE+ assessment. This half-day pre-assessment tests a small, representative sample of your devices, identifies likely points of failure before the formal assessment, and provides initial advice on any issues identified so they can be addressed in advance.

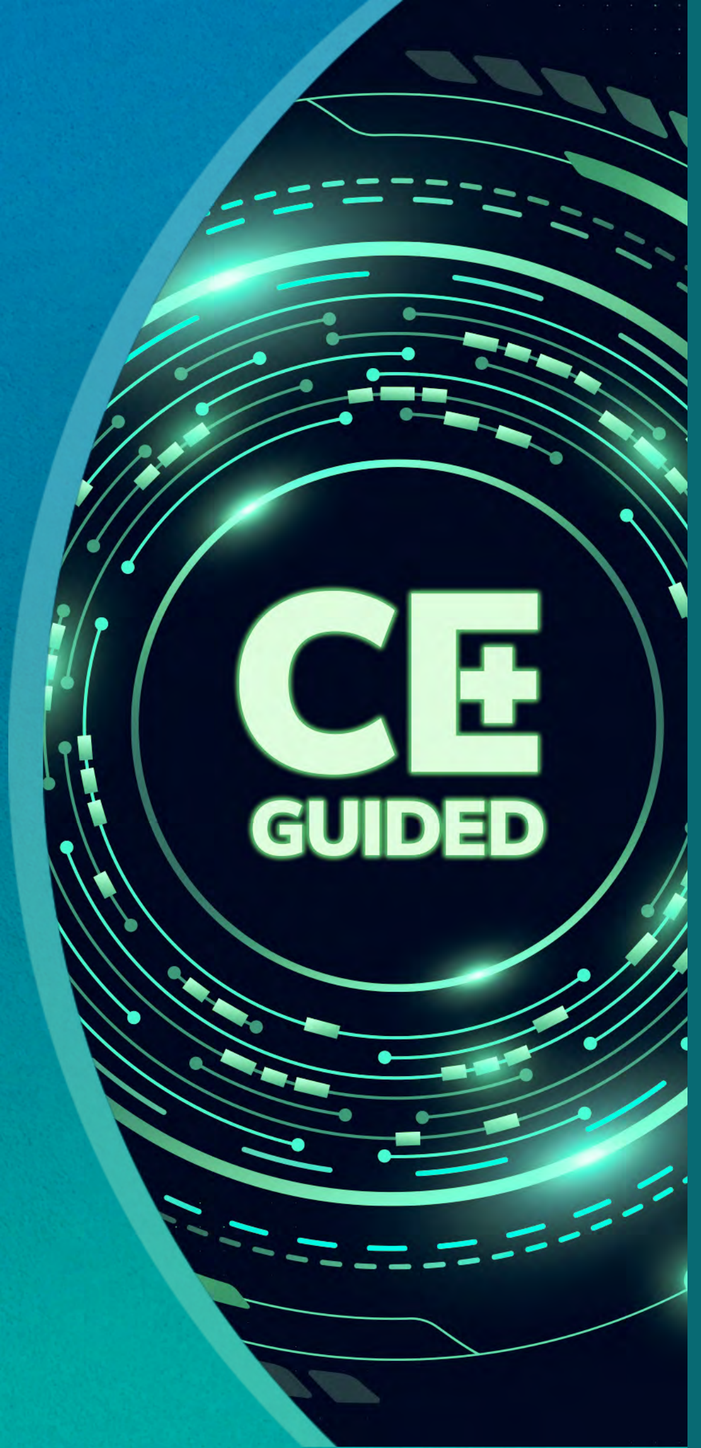
TECHNICAL SCOPE VERIFICATION (TSV)

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

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

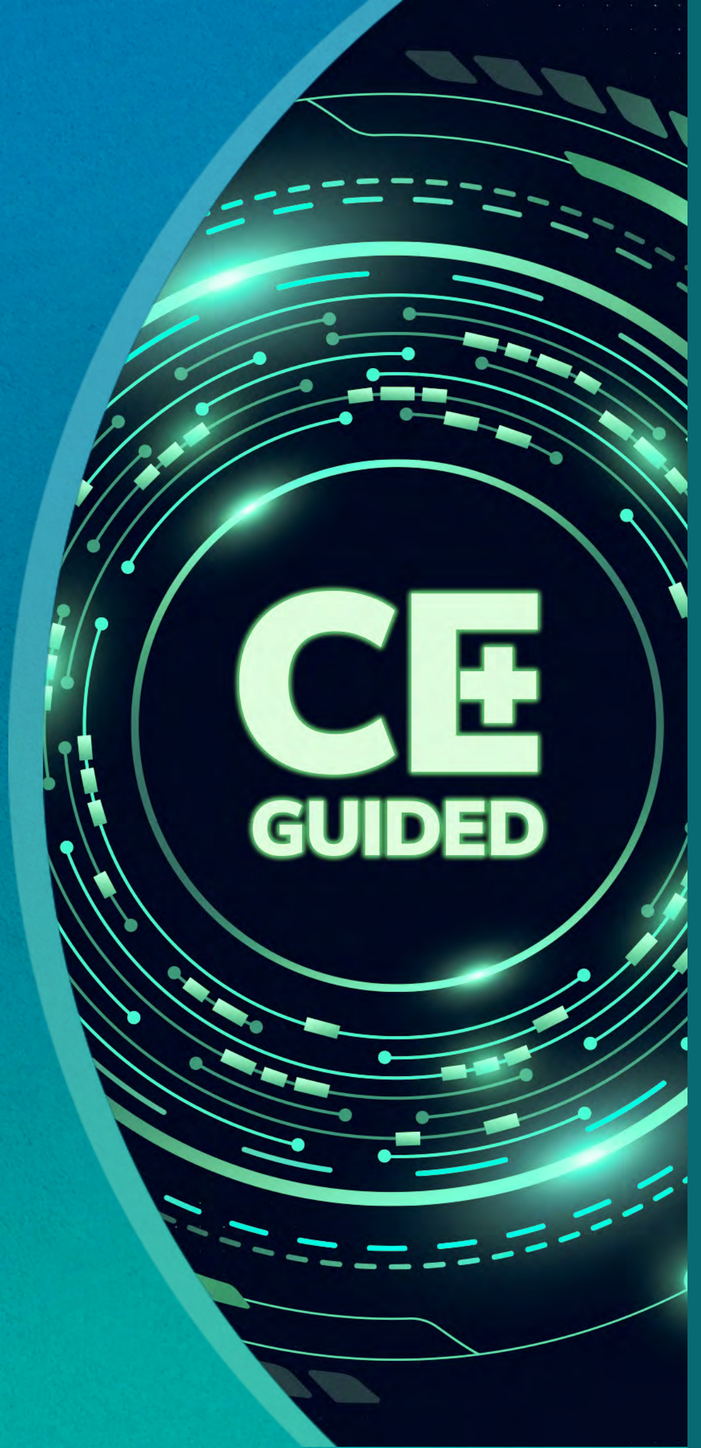
* Performing the TSV on the day of the CE+ assessment may reduce cost and administrative effort, but it increases risk. If issues are identified that cannot be immediately resolved, the CE+ assessment time will need to be either repositioned as advisory activity or postponed, and postponement charges 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



RETESTS

If the TSV passes successfully, but the CE+ assessment identifies failing items, you may book 1 retest in line with NCSC guidance and the Danzell remediation process. A 2nd, different sample set must be selected for the retest. If the same vulnerabilities are identified again, 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.



CYBER ESSENTIAL PLUS GUIDED SUMMARY:

- Includes *Cyber Essentials Assured* 1 year of access to the Abriska CE+ Module (*Guided*)
- Monthly internal device scans included
- Monthly external IP scans included
- Half-day sample-based CE+ pre assessment included
- 1 retest available in line with the Danzell scheme remediation process

Unlike the *Cyber Essentials PLUS Assured*, there are

- No daily scans in the final 3 working days before the official CE+ assessment
- No remediation scans following a failed assessment
- No option for unlimited CE+ certification attempts

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

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 retest 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+ module. The Abriska CE+ 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 matches the actual activities.

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, it is important that the applicant has a strong understanding of the CE and CE+ scheme requirements and scoping rules. If scope 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.*

RETESTS

If the TSV passes but the CE+ assessment identifies failing items, you may book 1 retest in line with the Danzell scheme's remediation process.

A 2nd sample set must be selected for the retest. If the same vulnerabilities are identified in the retest, 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

***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 seven 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
- 1 retest available in line with the Danzell scheme remediation process.

CE+ Offerings

Service / Activity	CE+ ASSURED	CE+ GUIDED	CE+ SELF-MANAGED
CE offering included	*Cyber Essentials Assured*	*Cyber Essentials Assured*	✗
TSV required before CE+ can proceed	Covered through *Cyber Essentials Assured* path	Covered through *Cyber Essentials Assured* path	✓
TSV timing approach	Usually conducted ahead of CE assessment as part of scope verification workshop included within *Cyber Essentials Assured*; 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 included within *Cyber Essentials Assured*; 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+ by agreement
Scope verification workshop included	✓	✓	✗
0.5-day sample-based CE+ pre-assessment	✓	✓	✗

Service / Activity	CE+ ASSURED	CE+ GUIDED	CE+ SELF-MANAGED
0.5-day advisory time	✓	✗	✗
1-year access to either Abriska CE+ *Assured* Module or *Guided* Module	✓	✓	✗
Daily scans in the 3 working days prior to official CE+ assessment	✓	✗	✗
Formal CE+ assessment	✓	✓	✓
1 retest 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