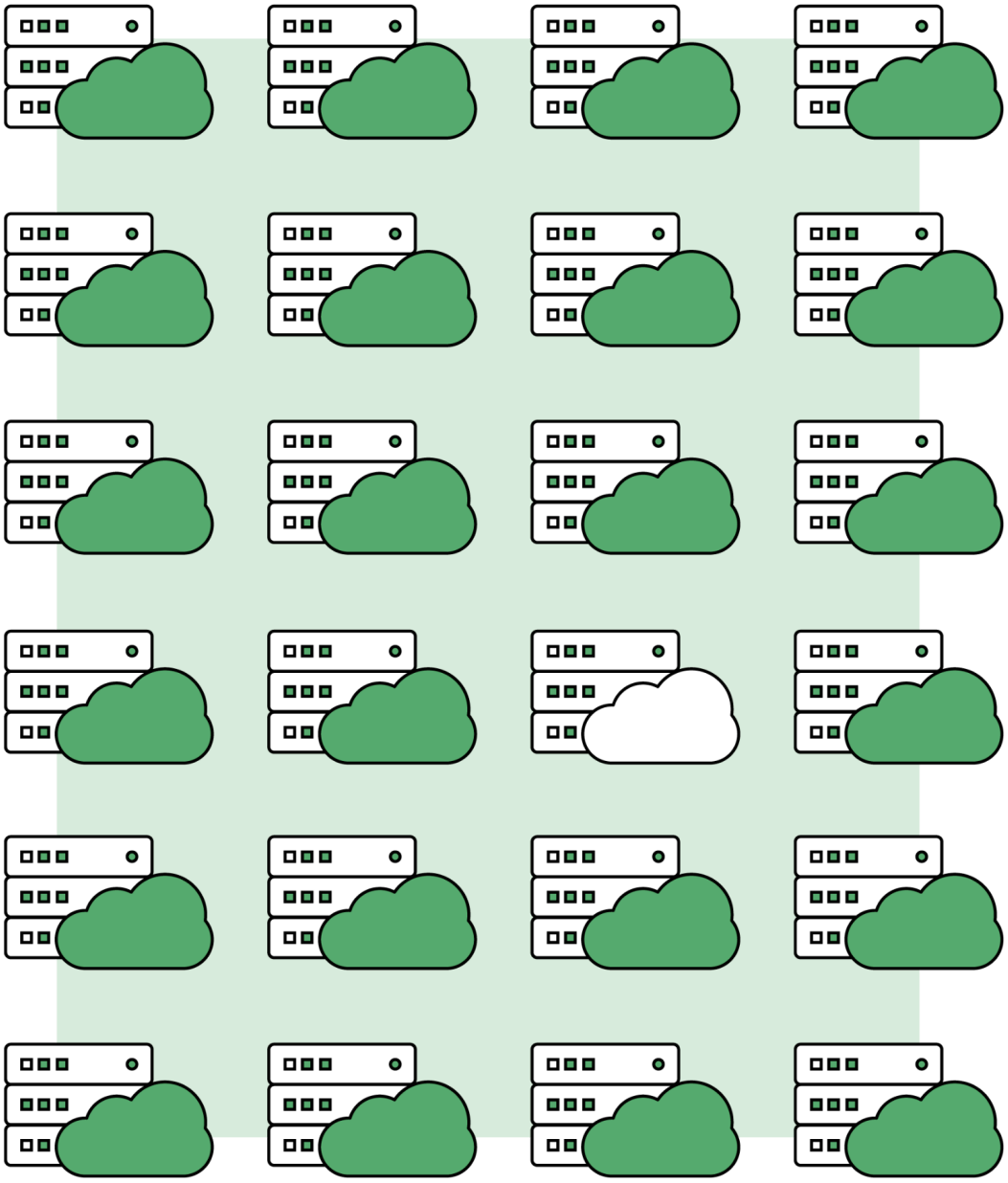

TCO Certified Cloud

TCO Certified Cloud — the sustainability certification for cloud resources

Our reliance on cloud services is growing rapidly — and so are the sustainability challenges. Behind every cloud service is a complex physical infrastructure that requires large amounts of energy, water and other natural resources. The climate impact of the cloud sector is significant, harmful substances may be present, and linear practices generate growing volumes of electronic waste.

TCO Certified Cloud — the world's first global sustainability certification for cloud resources — helps tackle these challenges. With mandatory, science-based criteria and rigorous follow-up of compliance, it is designed to drive sustainable development in the cloud industry. The certification focuses on Infrastructure as a Service (IaaS) cloud resources — the foundation of the cloud ecosystem, where the potential for impact is greatest. The criteria cover four key areas: climate, substances, circularity and supply chain.

TCO Certified Cloud is a third-party certification, independent of both industry and buyers. Compliance is independently verified both before and after certification, throughout the full validity period of each certificate, to support credible, lasting progress. As part of the compliance process, sustainability data aligned with international standards is collected and independently verified, enabling a more reliable assessment of the impacts connected to cloud resources.

TCO Certified Cloud is developed and managed by TCO Development, building on more than 30 years of certification work to advance more sustainable IT. The certification complies with ISO 14024 Type I ecolabel requirements and have been approved through the GENICES peer-review process of the Global Ecolabelling Network.

How to apply for certification
The certification process for TCO Certified Cloud is designed to be clear, structured and reliable. This criteria document explains the requirements that must be fulfilled and the evidence needed to demonstrate compliance. Before a certificate is issued, independent, accredited verification organizations review the required documentation and evidence to confirm that all criteria are met.

Our certification team is here to help. To get started, or if you have questions about the process, contact us at certification@tcodevelopment.com.

How to use this document
This is the criteria document for TCO Certified Cloud, released in June 2026. The criteria cover all key aspects needed to provide the certified cloud resource, including:

- the cloud resource itself
- the IT hardware providing the cloud resource (servers, data storage and network equipment)
- the data center facility
- the software and operations necessary for providing the certified cloud resources.

Additional services that are not an integral part of the core cloud resource offering are not covered by the criteria.

Five criteria areas
The criteria document is divided into five chapters, each representing a criteria area. Each chapter begins with an introduction that briefly presents the sustainability challenges addressed and provides an overview of the included criteria. This is followed by the full criteria.

How the criteria are structured
Each criterion includes the following sections:
Background: Describes the sustainability challenge that the criterion addresses.
Mandate: States the requirement that must be fulfilled, and the proof needed to demonstrate compliance.
Clarification: Provides additional explanations and guidance.

Where relevant, a criterion may also include:
Applicability: Lists any specific limitations or conditions, in addition to the scope described above.
Definitions: Explains relevant terms used in the criterion.

Key terms
This section defines key terms used in TCO Certified Cloud. Understanding these terms clarifies the scope of the criteria and how certified cloud resources are identified.

Cloud resource: An IT resource that is provided through a network, usually the internet. It may include computing capacity, such as CPU and RAM, data storage and network capacity. Cloud resources are normally virtualized, meaning that they are created from physical IT hardware such as servers, storage equipment and network equipment. In some cases, the cloud resource is provided directly on dedicated physical IT hardware. This is often referred to as “bare metal”.

Offering name: The name, model number, configuration description, or similar identifier used by the cloud resource provider at the point of sale to identify a specific configuration of a cloud resource. It typically describes the resources included, such as CPU, type and amount of RAM, type and amount of data storage, and amount of network traffic

Cloud resource provider: The organization that offers cloud resources. The cloud resource provider may operate its own data center facility or lease space in a facility owned by another party. The provider may also own or lease the IT hardware used to provide the cloud resources.

Data center facility: The physical facility where the IT hardware used to provide cloud resources is located. It may be a standalone building or part of a building.

Cloud resource identifier: The identifier for a certified cloud resource. It's the unique combination of the offering name, cloud resource provider and data center facility

Cloud resource instance: The specific cloud resource purchased by a customer as a standalone product. It is managed through a cloud resource management console provided by the cloud resource provider.

IT hardware: IT hardware means the physical equipment used to provide the cloud resource, including servers, data storage equipment and network equipment.

Asset management system (AMS): A system for maintaining an accurate inventory of the IT hardware used to provide a cloud resource. The system typically includes information such as asset identification, status, location, ownership, and lifecycle information, and enables traceability and effective management throughout the asset's operational life.

Editions of TCO Certified Cloud

New editions of the criteria document may be released to improve the precision of mandates, test methods or clarifications. If criteria levels are raised, this will be considered a new generation of TCO Certified Cloud.

Table of contents

1 Cloud resource and sustainability information

Cloud infrastructure is complex, with different actors responsible for different parts of the service. Sustainability data is often difficult to find, inconsistent and self-declared, which creates a high risk of greenwashing and unfair competition between cloud resource providers. Verified, comparable information is needed to help both cloud resource providers and purchasers make informed decisions and measure progress toward their sustainability goals.

Criteria in chapter 1 focus on:

- Identification of certified cloud resources and IT hardware.
- User information about TCO Certified Cloud.

1.1 Cloud resource identifier

Background
A lack of transparency and access to verified information can make it difficult to evaluate and improve the sustainability aspects of cloud offerings. To support transparency and traceability, all certified cloud resources must be clearly identifiable.

1.1.1 Mandate

The cloud resource provider must ensure that the certified cloud resource is identified by a unique combination of the following:

- Offering name
- Name of cloud resource provider
- Name of data center facility

The cloud resource provider must define the scope of IT hardware (servers, data storage, network equipment) that may be used for providing the certified cloud resource. The scope may be defined using one or more of the following:

- Product models
- Resource pools
- Racks
- Other appropriate grouping

Submit the following to an approved verifier:

- The cloud resource identifier to be certified.
- The scope of IT hardware that may be used for providing the certified cloud resource.

For the first certified cloud resource and annually at the end of August

- Provide access to, or a printout from, the asset management system showing that at least all IT hardware (servers, data storage, network equipment) that has been, and is planned to be, provisioned for providing the certified cloud resource are identified with the necessary information required in TCO Certified and is linked to the certified cloud resource identifier.

The following is submitted to TCO Development and may be published:

- A copy of the verification report(s) from a verifier approved by TCO Development.
- The cloud resource identifier

1.1.2 Clarification

- A grouping of offering names may be certified together under a family name as long as all offering names sold under this family fulfills TCO Certified Cloud. *(A family name often indicates that all the cloud resource offering names in the same family are provided from the same pool of hardware resources. However, family groupings may be done by other means.)*
- All IT hardware (servers, data storage, network equipment) that has been provisioned for providing the certified cloud resource must be included and identified in the asset management system until the certificate expires irrespective of if it was purchased, self-built, leased or otherwise has been added.
- If several cloud resources are certified at the same time and are supported by different parts of a shared hardware pool, the AMS must contain information identifying the hardware used for each cloud resource.
- Hardware that has been provisioned for providing the certified cloud resource and later decommissioned must remain in the system and labelled with the decommission date during the validity of the certificate.
- For each IT hardware asset provisioned for providing the certified cloud resource the following information must be available in the Asset Management System if applicable:
    - Asset model name
    - Supplier name
    - Year of purchase/commission date
    - Compliance with EU Ecodesign Regulations; or Energy Star®
    - Repair history
    - Upgrade history
    - Asset status (Commissioned/decommissioned)

  If decommissioned:
    - Decommission date
    - Actual life length
    - End of life treatment
        - Refurbishment provider/ Recycling provider
- It is not mandatory but can be helpful to follow ISO55001 when implementing and managing the asset management system (AMS).
- For cloud providers who use leased hardware or shared datacenters to provide a certified cloud resource, it is recommended to have a leasing contract including a clause to share the necessary information required in TCO Certified.

On-site factory inspection initiated by TCO Development (spot checks).
TCO Development may request audit reports or commission on-site inspections at data centers and providers offering certified cloud resources, limited to verifying compliance with the criteria. If an inspection cannot be carried out, this may affect the certificate's validity.

Spot check audits are financed by TCO Development. If non-conformities are found and further investigations are necessary, the license holder must cover this cost to keep their certificate.

1.2 Information to end customers

Background
When sustainability information is missing, it can be difficult for purchasers and users to make informed choices. To support more sustainable decisions, information about certified cloud resources must be available when and where purchasing decisions are made. It must be possible to identify which cloud resources are certified, where they are located, and which sustainability attributes they include.

1.2.1 Mandate

The cloud resource provider must ensure the following:

- The country and city of the data center location are displayed together wherever the certified cloud resource is sold and managed.
- The TCO Certified logo, with an embedded link to https://tcocertifiedcloud.com/, is displayed next to the offering name wherever the certified cloud resource is sold and managed.
- The “About TCO Certified Cloud” text is presented on the cloud resource provider's website.

Submit the following to an approved verifier:

- A link to the cloud resource provider website where the certified cloud resource will be sold, with a description of where the TCO Certified logo will be displayed.
- A link to the page on the cloud resource provider’s website(s) where the “about TCO Certified Cloud” text is presented.

The following is submitted to TCO Development and may be published:

- A copy of the verification report(s) from a verifier approved by TCO Development.
- A link to the cloud resource provider website where the certified cloud resource will be sold.

1.2.2 Clarification

Rules if the links change during the certificate validity
If any of the links referred to in this criterion change during the validity period of the certificate, the new link must be sent to the verifier and to TCO Development.

2 Climate

Cloud services have a considerable and increasing climate impact. Data centers require large amounts of electricity to power servers and cooling systems. Many cloud providers still depend on fossil-fuel-based energy sources, leading to substantial greenhouse gas emissions. As the demand for cloud services continues to rise, the number of data centers is also increasing. Consequently, the sector's climate footprint is expected to grow in the coming years. To begin reducing the climate impact of cloud services, we need to improve energy efficiency and increase the share of renewable energy used to power data centers.

Criteria in chapter 2 focus on:

- Energy efficiency of data center facilities.
- Energy efficiency of IT hardware.
- Renewable and non-fossil energy use.
- Climate footprint transparency.

2.1 Maximum PUE of data center facility

Background
PUE (Power Usage Effectiveness) is a key metric for assessing the energy efficiency of a data center. It is calculated by dividing the facility's total electricity consumption by the electricity used solely for the IT equipment: servers, storage, and networking devices that perform the actual computing. A lower PUE indicates a more efficient data center with a lower climate impact. This can be achieved by improving the efficiency of supporting systems such as cooling, power distribution, and lighting.

2.1.1 Mandate

- The cloud resource provider must ensure that the data center facility used to provide the certified cloud resource does not exceed a monthly PUE (Power Usage Effectiveness) value of 1.4.

Submit the following to an approved verifier:

- Annually, at the end of August, a report calculating the PUE of the data center facility used for providing the certified cloud resource. The report must cover the previous calendar year and present the PUE value for each month.

The following is submitted to TCO Development

- A copy of the verification report(s) from a verifier approved by TCO Development.
- A report calculating the PUE of the data center facility used for providing the certified cloud resource. The report must cover the previous calendar year and present the PUE value for each month.

2.1.2 Clarification

Definition of PUE

A monthly PUE of 1.4 means that, over that month, energy used for facility overhead — such as cooling, power distribution losses and other support systems — must not exceed 40% of the IT equipment energy use.

Accepted standards for calculating PUE values
PUE values must be calculated in accordance with ISO/IEC 30134-2 or EN 50600-4-2.

Timeframe for reporting
Calculations must be based on data from the previous calendar year. However, if it is the first time a cloud resource is certified at a data center facility that has not previously been used to provide certified cloud resources, the reporting period must start in the month when the first cloud resource is certified and end in December of the same year. For all following years, calculations must cover the full previous calendar year.

Documentation of data used in calculations
The data used to calculate the PUE value must be documented and stored in a way that allows it to be reviewed during an on-site audit.

Data center facilities that have been in operation for less than one year
If the data center facility has been in operation less than one year, the report must include the monthly PUE values from the first month of operation and for each following month.

2.2 Energy efficiency of IT hardware

Background
IT hardware (servers, data storage, and network equipment) uses a lot of energy, which makes it a significant contributor to the climate impact of cloud resources. To reduce this impact, cloud resource providers must select energy-efficient IT hardware.

Applicability
All commercially manufactured IT hardware, purchased less than five years ago and not pre-owned when purchased.

2.2.1 Mandate

The cloud resource provider must ensure that all IT hardware (servers, data storage, network equipment) used to provide the certified cloud resource meets one of the following requirements:

- The energy efficiency requirements of the applicable product-specific EU Ecodesign implementing regulation; or
- The energy efficiency requirements of the applicable Energy Star requirements.®

Submit the following to an approved verifier:
As part of the certification application, and annually at the end of August, provide the following for all IT hardware (servers, data storage and network equipment) used to provide the certified cloud resource:

- Documentation showing compliance with the applicable product-specific EU Ecodesign implementing regulation; or
- A test report showing compliance with Energy Star, issued by a laboratory accredited according to ISO 17025; or
- An invoice proving that the IT hardware is homebuilt, was pre-owned when purchased, or was purchased more than five years ago.

Submit the following to TCO Development:

- A copy of the verification report(s) from a verifier approved by TCO Development.

2.2.2 Clarification

Identification in the asset management system
In the asset management system, it must be possible to identify that the IT hardware used for providing the certified cloud resource meets the energy efficiency requirements of the applicable product-specific EU Ecodesign implementing regulation or Energy Star.

Applicable EU Ecodesign implementing regulations
For EU Ecodesign, the applicable regulation is the product-specific EU Ecodesign implementing regulation in force for the relevant product category at the time of verification. Current applicable regulations include, where relevant: Commission Regulation (EU) 2019/424 for servers and data storage products.
If new or revised EU Ecodesign implementing regulations enter into force for IT hardware covered by this criterion, the applicable requirements in those regulations must be met.

Proving non-applicability
Claims that IT hardware is homebuilt, pre-owned when purchased, or is more than five years old, must be proven by invoices or other documentation.

Accepted versions of Energy Star
When Energy Star is used to show compliance, the IT hardware must be tested according to the standard and version of Energy Star applicable to the product category that applied on its manufacturing date, or according to a newer version.

2.3 Low-carbon electricity

Background

Data centers use large amounts of electricity and, in many regions, this electricity is generated from fossil fuels. To reduce climate impact, fossil-based electricity must be replaced with renewable or other non-fossil sources. Renewable electricity is preferred, since it can increase demand for Renewable Energy Certificates (RECs), which in turn drive investments in new renewable electricity generation.

Definitions

Fossil-free: Fossil-free electricity means electricity generated from renewable sources accepted under this criterion or from nuclear power. Electricity generated from coal, oil, natural gas, peat, or fossil-derived waste fractions is not accepted.

2.3.1 Mandate

1. The cloud resource provider must ensure that the electricity used to produce the certified cloud resource meets one of the following requirements:

- At least 30% is procured and/or generated from renewable sources; or
- At least 60% is procured and/or generated from fossil-free sources.

2. The cloud resource provider must report the Renewable Energy Factor (REF) in accordance with ISO/IEC 30134-3 or EN 50600-4-3.

Submit the following to an approved verifier:

Annually, at the end of August, provide the following for the data center facility used to provide the certified cloud resource:

- Documented proof of the total electricity used, in MWh, for the previous calendar year.
- Documented proof of the fossil-free or renewable electricity ratio used to produce the certified cloud resource, in percent, for the previous calendar year.
- Documented proof of the Renewable Energy Factor (REF), calculated in accordance with ISO/IEC 30134-3 or EN 50600-4-3.

The following is submitted to TCO Development:

- A copy of the verification report from a verifier approved by TCO Development.

Annually, at the end of August, provide the following for the data center used to provide the certified cloud resource:

- The total electricity used, in MWh, for the previous calendar year.
- The fossil-free or renewable electricity ratio used to produce the certified cloud resource, in percent, for the previous calendar year.
- The Renewable Energy Factor (REF), calculated in accordance with ISO/IEC 30134-3 or EN 50600-4-3.

2.3.2 Clarification

Reporting frequency and reporting responsibility
The cloud resource provider is responsible for ensuring that the required reporting is submitted to TCO Development within the specified time, the last reporting occasion is one year after the certificate has expired. The reporting must cover the previous calendar year and the production period must be stated on the REC cancellation statements or in the proof of fossil-free electricity.

Temporal correlation
The production period of the Renewable Energy Certificates (the period during which the renewable electricity was generated) referenced in the cancellation statements must be the same month as it was consumed. This means that at the yearly reporting:

- The provider must calculate the electricity consumption on a monthly basis for the previous calendar year.
- The provider must then purchase renewable electricity that was generated during the same month that it was consumed.
- No single month must have a lower ratio of renewable electricity than the mandated level.

Example:
Reporting submitted in 2026 must be received by 31 August 2026. It must cover electricity consumption from 1 January 2025 to 31 December 2025. The renewable energy claims must be supported by REC cancellation statements covering RECs produced during each month that electricity was consumed.

Exception for new providers
When a provider applies to certify a cloud resource at a data center for the first time, the provider is exempt from this mandate for that calendar year if the certification takes place after August 31. Then the provider must instead fulfill the mandate from the following calendar year and onward.

If reporting is done for the whole data center (the easiest alternative)
Cloud resource providers may choose to report either for the entire data center or for their share of electricity. Reporting on the whole data center level is generally simpler. In this case, all cloud resources generated at the data center are assigned the same share of renewable or fossil free electricity as the data center.

If reporting is done for the whole data center, the cloud resource provider must submit the following, covering the previous calendar year:

- Documented proof of the total electricity consumption of the data center (X)
- All REC cancellation statements designated to the data center (with the data center name) for the renewable electricity (Y) generated or purchased by the data center during this period, OR A cancellation summary report signed by an agent approved by TCO Development.

OR

- Documented proof of the ratio of the total electricity used (X) that was fossil-free.

Calculations:

- The ratio of renewable electricity by the data center ($R_F = Y/X$).

If reporting is done for a cloud provider's share of electricity (more detailed information)
If the data center does not comply with the renewable electricity mandate or if the cloud resource provider wishes to demonstrate a higher share of renewable or fossil free electricity than the data center as a whole, the cloud resource provider may report its own share of electricity.

If reporting is done for a cloud resource provider's share of the generation, the cloud resource provider must report the following, covering the previous calendar year:

- All REC cancellation statements assigned to the data center (with the data center name) for the renewable electricity (Y) generated or purchased by the data center during this period.
- All REC cancellation statements assigned to the data center and cloud resource provider (with the data center name and cloud resource provider's name) for the generation of certified cloud resources for the cloud resource provider at the data center (S).
- Documented proof of the electricity consumption (E) of at least the hardware generating the certified cloud resource multiplied with the average annual PUE.

OR

- Documented proof of the ratio of the electricity used to generate certified cloud resource (E) that was fossil-free.

Calculations:

- Ratio of renewable electricity for the whole data center ($R_F = Y/X$).
- Ratio of renewable electricity only for the generation of certified cloud resource ($R_B = S/E$)
- Total ratio of renewable electricity for the generation of certified cloud resource ($R_T = R_F + R_B$)

Fossil free energy
For fossil-free electricity claims, the provider must submit cancelled or redeemed Energy Attribute Certificates, Guarantees of Origin, EECS Disclosure certificates, or equivalent registry-based documentation showing the electricity source, production period, volume in MWh, beneficiary, cancellation or redemption status, and issuing registry. The documentation must demonstrate that the claimed electricity was generated from non-fossil sources and was not double counted.

Where no accepted registry-based certificate system exists for the relevant fossil-free electricity source in the relevant market, the provider may submit alternative evidence. This must include a signed supplier attestation, the electricity supply contract, invoices or metering records, fuel mix disclosure, and evidence that the claimed fossil-free attributes have not been sold, allocated, or claimed elsewhere. This alternative evidence must be assessed and accepted by the approved verifier.

Renewable electricity must be generated from:
Renewable electricity must be generated from wind, solar, geothermal, hydropower (pumped hydro storage is only accepted if the amount of grid-imported electricity used to run the pumps is specified on the submitted REC and deducted from the generated electricity) or biomass (agricultural waste and residues, forest biomass, biofuels plants).

Renewable energy certificates (RECs)
Renewable electricity used by data centers may be either purchased or self-generated. Generation facilities may be on-site or off-site, grid-connected or off-grid.

All renewable electricity must be issued with Renewable Energy Certificates (RECs). data centers or providers may:

- Consume electricity directly from their own renewable generators, retain the RECs, and claim the use of renewable electricity.

  OR
- Sell electricity to the grid, retain the RECs, and claim the use of renewable electricity.

REC registries prevent double-counting by tracking each unit of renewable electricity. Canceled RECs can be independently verified in the registry to confirm exclusive ownership and use claims.

RECs must be sourced and purchased within the same national region as the data center that uses the electricity. The renewable electricity production facility from which the RECs originate must also be located within the same national region. The national region defines the market boundary for transacting and claiming renewable electricity attributes.

To claim the renewable electricity for a specific beneficiary, cancellation statements are issued by the registry or issuing body when RECs are canceled by an end-user (e.g., a company).

Accepted agents

To simplify the purchase and verification of RECs, cloud resource providers may engage an agent accepted by TCO Development.

Accepted agents may:

- Assist in purchasing RECs across different markets
- Confirm REC cancellation statements
- Issue a “cancellation summary report”

Accepted agents have access to certain REC registries that may otherwise be difficult for independent verifiers to access. A current list of accepted agents is available on the TCO Certified website.

Exception for a high market price of RECs

When REC prices are significantly above average in a given market, partial sourcing from neighboring regions is allowed under the following conditions:

- If the market price of all accepted RECs in the relevant market is above 10 USD/MWh, up to 30% of the renewable electricity purchased may be covered by RECs from neighboring markets.
- If the market price is above 30 USD/MWh, up to 70% of the renewable electricity purchased may be covered by RECs from neighboring markets.

Under this rule, RECs for factories in Taiwan may be sourced from China, Japan, the Philippines, South Korea, or Vietnam.

Only RECs recognized as “**Accepted REC systems”** by TCO Development are valid as proof of compliance. Additional countries or credible REC systems may be added to this list following independent expert review and formal acceptance by TCO Development.

Country	Accepted REC systems
Belgium	I-REC, National Guarantees of Origin (regional systems for Brussels, Flanders, Wallonia)
Brazil	I-REC
Canada	I-REC, REC (MRETS, NAR, ERCOT, WECC)
China	I-REC, GEC
Czech Republic	I-REC, National Guarantees of Origin
Denmark	I-REC, National Guarantees of Origin
Egypt	I-REC
Finland	I-REC, National Guarantees of Origin
France	I-REC, National Guarantees of Origin
Germany	I-REC, National Guarantees of Origin
Hungary	I-REC, National Guarantees of Origin
India	I-REC, TIGR
Japan	I-REC, J-Credit, FIT-NFC
Malaysia	I-REC, TIGR
Mexico	I-REC
Netherlands	I-REC, National Guarantees of Origin
Norway	I-REC, National Guarantees of Origin
Poland	I-REC, National Guarantees of Origin
Portugal	I-REC, National Guarantees of Origin
Singapore	I-REC, TIGR
South Korea	I-REC, Korean national REC system, TIGR
Sweden	I-REC, National Guarantees of Origin
Switzerland	I-REC, National Guarantees of Origin
Taiwan	I-REC, T-REC, TIGR, (CPPA is not an REC but allowed)
Thailand	I-REC, TIGR

USA	I-REC, REC (MRETS, NAR, ERCOT, WECC)
Vietnam	I-REC, TIGR

Verification guidelines for cloud resource providers and data center data
Three aspects need to be verified:

1. The claimed electricity consumption,
2. The authenticity of cancellation statements, and
3. The coverage of renewable electricity claims.

Claimed electricity consumption.
Verify that the submitted documentation supports the reported electricity consumption and includes correct calculations.

The documentation must:

- Cover the total electricity consumption for the previous calendar year, and
- Clearly show that the electricity consumption covers the entire business license (address) under which the data center is registered. It must not be limited to individual buildings, assembly lines, or partial operations.

Examples of documentation to verify a data center's annual electricity use include:

- Energy bills
- Metering records
- Energy audit reports
- Monitoring system data

If reporting is done for a provider's share of the generation of certified cloud resource instead of the whole data center, the share of the data center's electricity consumption for, which the provider is accountable, must also be verified with documentation showing units generated cloud resource or revenue for both the data center and the cloud provider.

Examples of documentation examined to verify a cloud provider's share of a data center's annual total revenue or volume of generated cloud resources include:

- Cloud resource generation records
- Production and sales logs
- Internal financial documents
- External audit reports
- Contractual agreements

All records submitted must be verifiable copies or digital system outputs that can be checked during an on-site audit. The verified data center, or cloud resource provider's share of electricity consumption, is reported to TCO Development and only needs to be verified once per data center, cloud resource provider, and year.

Authenticity - Verification of cancellation statement authenticity:

Verify that a cancellation statement is authentic by confirming that the information on the cancellation statement matches the information listed in the registry of the issuing body. This must be done in one of the following:

- **A.** Verifier accesses the issuing body registry from the QR-code on a cancellation statement or gets an account login at the issuing body registry and verifies the authenticity of the cancellation statements.
- **B.** Verifier gets a signed confirmation that the submitted cancellation statement is authentic from either the issuing body or an accepted agent.
- **C.** Verifier gets a signed “cancellation summary report” from an accepted agent.

Coverage - Verification of correct coverage of cancellation statements:
Verify correct coverage and compliance with the TCO Certified mandate by confirming that:

- The beneficiary is the data center only, to count for the data center's renewable electricity share, OR that the beneficiary is the data center and provider, to count for the provider-specific renewable energy share in the data center (for REC systems that do not allow this type of specific beneficiary a “purpose” of “free text” field may be used to add this information).
- The total MWh canceled matches the claimed consumption
- The REC production period falls within 6 months before and up to 3 months after the previous calendar year in line with the TCO Certified mandate.
- The energy source is of an accepted type (see criteria document).

For more information on how to verify renewable energy, see supporting documentation.

Renewable Energy Factor (REF)

If sufficient data is not provided to calculate and verify the REF in accordance with ISO/IEC 30134-3 or EN 50600-4-3, the REF must be reported as 0 for the purposes of TCO Certified reporting. The reported value must be marked as not supported by verified REF data.

2.4 Transparency of climate footprint

Background
To make informed decisions that reduce the climate impact of cloud services, customers need access to accurate information. Carbon footprint estimates help users understand climate impacts and choose cloud services with lower greenhouse gas emissions. Organizations can also use these estimates in sustainability reporting and to track and reduce the impact of the cloud services they rely on.

2.4.1 Mandate

- The cloud resource provider must ensure that end customers have access to monthly reports on the estimated climate footprint associated with that customer's use of the certified cloud resource. These reports should be available wherever the cloud resource is managed.
- Historical reports must remain accessible to the end customer for a rolling period of 24 months.

Submit the following to an approved verifier:

- Documentation showing that end customers have access to monthly reports on the estimated climate footprint associated with the certified cloud resources they purchase and use. The documentation should also prove that these reports are accessible wherever the certified cloud resource is purchased and managed.
- A description of how the climate footprint has been measured and calculated, including details of the methodology, key assumptions and data sources.

The following is submitted to TCO Development:

- A copy of the verification report(s) from a verifier approved by TCO Development.

2.4.2 Clarification

Changes to the reporting system that affect compliance with this mandate must be reported to the verifier for re-evaluation.

Methodology for reporting to end customers

- The reported climate footprint estimates must use the framework specified in the Product Category Rules (PCR) for Data Centre IT Hosting Services and Cloud Services released in 2025.
- This criterion does not require reporting of all environmental indicators included in the PCR. Only the climate footprint estimate must be reported.

Climate footprint calculation tool example
Open-source tools such as CloudAssess may be used to fulfil the reporting requirements, provided that they use real operational data and apply the methodology defined in the Product Category Rule (PCR) for Data Centre IT Hosting Services and Cloud Services.

Each tool must be verified for compliance and approved by TCO Development. The use of the tool must be verified for each provider.

Report specifications
Each report must contain at least the following:

Scope	Identification of the certified cloud resource instance.
Date	Assessment period and date of publication.
Data resolution	A monthly average of the climate footprint estimate.
Methodology used	A statement that the results have been developed according to the Product Category Rule (PCR) for Data Centre IT Hosting Services and Cloud Services.
Responsible for results	The person or organization responsible for the results.
Modifications	Any limitations or modifications applied.
Tools used for calculations	If a tool is used to calculate the climate footprint, the name and version of the software used must be reported.

3 Substances

Substances used for cooling and firefighting in data centers can be harmful to both human health and the environment. They may be carcinogenic, hormone-disrupting, pose other serious health or environmental risks, and have a significant climate impact. Today, there is a lack of transparency regarding which substances are used. To enable a shift toward safer substitutions, we first need to identify the substances currently in use.

Criteria in chapter 3 focus on:

- Transparency of substances used for cooling and fire extinction.

3.1 Transparency of substances

Background

Substances used in both cooling and fire extinguishing systems in data centers can be hazardous to human health and the environment. Refrigerants often have high global warming potential, while fire suppression agents may contain chemicals that are persistent or harmful if released. To reduce chemical risks and climate impact, it is essential to know which substances are used and in what quantities. A consolidated inventory of all refrigerants and fire suppression agents improves monitoring, supports substitution to safer alternatives, and provides a necessary foundation for future reduction efforts.

Definitions

CRAC: Computer room air conditioning

CRAH: Computer room air handler

3.1.1 Mandate

The cloud resource provider must ensure that a complete inventory is maintained for refrigerants used in cooling systems and clean agent fire suppressants used in fire extinction systems. The inventory must cover at least the parts of the data center facility used to provide the certified cloud resource and include the CAS number and annual usage volume for each substance.

Submit the following to an approved verifier:

As part of the certification application, and annually at the end of August:

- A copy of the inventory showing all cooling refrigerants and fire extinguishing agents used in the data center facility that provides the certified cloud resource. The inventory must include the CAS number and annual usage volume for each substance.

The following is submitted to TCO Development

- A copy of the verification report(s) from a verifier approved by TCO Development.
- A copy of the inventory showing all cooling refrigerants and fire extinguishing agents used in the data center facility that provides the certified cloud resource. The inventory must include the CAS number and annual usage volume for each substance.

3.1.2 Clarification

- If there are any changes to the inventory during the validity period of the certificate, an updated inventory must be sent to the verifier for re-evaluation.
- Refrigerants must be recorded for all cooling systems, heating systems and heat exchangers involved in providing the certified cloud resource. This includes CRAC and CRAH systems, air conditioning systems, chillers, humidifiers, heat exchangers and heat pumps.

4 Circularity

Data centers largely operate within a linear model, where IT hardware is manufactured, used for a short period, and then discarded. This short product lifespan depletes natural resources and contributes to climate change, as greenhouse gases are emitted during production. Large amounts of e-waste are generated, and toxins risk leaching out into the natural environment if not handled safely. By equipping data centers with durable, repairable products and adopting circular IT practices, we can significantly reduce both waste and climate impact.

Criteria in chapter 4 focus on:

- IT hardware life length.
- Circular management of IT hardware.

4.1 IT hardware life length

Background

Short product lifespans lead to large greenhouse gas emissions and other negative sustainability impacts. By systematically monitoring the lifetimes of servers, data storage devices, and network equipment, and actively working to extend their use, these impacts can be significantly reduced.

Definitions

IT hardware: servers, data storage, network equipment.

4.1.1 Mandate

The cloud resource provider must ensure that the IT hardware used to provide the certified cloud resource must not be decommissioned before it has been used for at least 5 years.

Submit the following to an approved verifier:

Annually, at the end of August, provide the following covering the previous calendar year (1 January–31 December):

- Provide access to, or a printout from, the Asset Management System showing that no more than 5% of IT hardware provisioned for the certified cloud resource has been decommissioned before being used for at least 5 years.

Submit the following to TCO Development:

- A copy of the verification report(s) from a verifier approved by TCO Development.

4.1.2 Clarification

IT hardware that was pre-owned or decommissioned after being used for at least five years is excluded from the calculation of the 5% limit.

4.2 Circular management of IT hardware

Background

E-waste is the world's fastest-growing waste stream, with more than 60 million tonnes of discarded electronics generated each year. Unsafe handling of this waste leads to pollution, health risks, and the loss of valuable, finite resources. By managing IT devices in a circular manner, for example, by repairing and upgrading products to extend their lifespans, less e-waste is produced.

Definitions

IT hardware: servers, data storage, network equipment.

4.2.1 Mandate

The cloud resource provider must ensure that, for all IT hardware used to provide the certified cloud resource:

- All decommissioned IT hardware is logged and traceable to the receiving refurbishment or recycling provider.
- The receiving refurbishment of recycling providers has a process that prioritizes repair and refurbishment over recycling, or is certified according to the SERI R2 standard for responsible recycling, or an equivalent standard..

Submit the following to an approved verifier:

- A list of all refurbishment and recycling providers contracted to receive decommissioned hardware used to provide the certified cloud resource.
- A valid SERI R2 certificate or documentation proving an equivalent implemented process that prioritizes repair and refurbishment over recycling, for each listed refurbishment and recycling provider.

Annually, at the end of August, provide the following for the previous calendar year (1 January–31 December):

- Access to, or a printout from, the cloud resource provider's asset management system showing that all decommissioned IT hardware used for providing the certified cloud resource has been logged with the receiver.

The following is submitted to TCO Development

- A copy of the verification report(s) from a verifier approved by TCO Development.

4.2.2 Clarification

- To prove that a repair and refurbishment process is equivalent to SERI R2, an independent party approved by TCO Development must carry out a gap analysis that is accepted by TCO Development.
- Outflow of IT hardware includes decommissioned hardware, including at least PSUs, CPUs, RAM, GPUs and storage devices, which must be logged.
- If there are any changes to the list of refurbishment and recycling providers used during the validity period of the certificate, the changes must be sent to the verifier for reevaluation.

Using a process description
When process documentation is used to prove that a refurbishment or recycling provider prioritizes repair and refurbishment over recycling, only official documents are accepted.The documents must describe the process and include dates showing that they are valid at the time of verification. The documentation must prove that the described processes are implemented in the provider’s operations, and should preferably be supported by actual operational data.

5 Supply chain

Cloud resource operations depend on data center facilities, which often have significant environmental impacts. Key risks include high energy consumption and unsustainable water use. The data center location is often unknown to cloud resource buyers and users, making informed sourcing decisions difficult. These impacts must be addressed through structured environmental management and greater transparency, including access to relevant information on water use and data center location.

Criteria in chapter 5 focus on:

- Environmental management systems in data center facilities.
- Freshwater use transparency.
- Data center location transparency.

5.1 Environmental management system

Background
Data centers have a significant environmental impact, including high energy use, pollution, and waste production. Without structured management systems, facilities may lack effective processes to reduce emissions, improve resource efficiency, and minimize their environmental footprint.

5.1.1 Mandate

The cloud resource provider must ensure that the data center facility used to provide the certified cloud resource has an environmental management system that is independently certified to ISO 14001.

Submit the following to an approved verifier:

- An ISO 14001 certificate covering the data center facility used to provide the certified cloud resource.

The following is submitted to TCO Development:

- A copy of the verification report(s) from a verifier approved by TCO Development.

5.1.2 Clarification

- The cloud resource provider must ensure that the data center facility has a valid ISO 14001 certificate at all times.
- Any change to the ISO 14001 certification status of the data center facility, such as expiry or renewal, must be reported to the verifier for re-evaluation.
- The certificate, or an appendix to the certificate, must clearly show that the certification covers the data center facility used to provide the certified cloud resource.
- If the data center facility is not yet certified, the cloud resource provider may request an extension of up to 18 months on behalf of the data center facility. The request must include an implementation plan for achieving ISO 14001 certification and a signed agreement. TCO Development may deny an extension if there is a substantial risk that the data center facility will not achieve ISO 14001 certification within the extended time period.
- The certificate must be issued by a certification body that is accredited by an accreditation body covered by the International Accreditation Forum, iaf.nu, Multilateral Arrangement on Environmental Management Systems.

Reference
https://www.iso.org/standards/popular/iso-14000-family

5.2 Water Usage Efficiency (WUE)

Background
Some data center facilities use freshwater in their cooling systems. In many regions, freshwater is a limited resource, and its use can have environmental and social impacts. To help purchasers make informed decisions, transparent and comparable information on water use is needed. A key first step is to measure and report freshwater use using standardized methods, and to disclose whether potable (drinking-quality) water is used.

Definitions

Freshwater: Water with ≤1,000 mg/L total dissolved solids, sourced from municipal supply, surface water, or groundwater, excluding seawater, reclaimed or reused water. Freshwater is counted when consumed as make-up water within the data center facility boundary for cooling, humidification, or other data-center-critical support systems. Accounting shall follow ISO/IEC 30134-9 (EN 50600-4-9).

Potable water: Freshwater treated to drinking-water quality, typically supplied through municipal water systems.

5.2.1 Mandate

The cloud resource provider must ensure that, for the data center facility used to provide the certified cloud resource, the following are reported annually:

- Water Usage Effectiveness (WUE), Category 1
- Total freshwater use (m^3)
- Potable water use (m^3)

Calculations must follow ISO/IEC 30134-9 and be based on data from the previous calendar year.

Submit the following to an approved verifier:
Annually, at the end of August, provide the following information covering the previous calendar year (1 January–31 December):

- The calculated Water Usage Effectiveness (WUE), Category 1, in accordance with ISO/IEC 30134-9.
- Evidence of total freshwater use (m^3), such as invoices, metering records, or equivalent documentation.
- Documentation showing potable water use (m^3).
- Documentation demonstrating the electricity used to power IT equipment (servers, network equipment, and data storage) in the data center facility (kWh), used as the basis for the WUE calculation.

The following is submitted to TCO Development:

- A copy of the verification report(s) from a verifier approved by TCO Development.
- The WUE value (Category 1) calculated in accordance with ISO/IEC 30134-9.
- The reported total freshwater and potable water use (m^3).

5.2.2 Clarification

- WUE Calculations must follow ISO/IEC 30134-9 and be based on data from the previous calendar year.
- Changes to the measurement methodology, scope, or data sources used to calculate WUE or freshwater use during the validity period of the certificate must be reported to the verifier for re-evaluation.
- Non-freshwater sources, such as seawater, brackish water, reclaimed water, greywater, or harvested rainwater, are outside the scope of this criterion. These sources must not be included in the freshwater use or WUE calculations.
- WUE must be calculated according to ISO/IEC 30134-9 (identical with EN 50600-4-9).
- Only facility-based or site-based water use within the data center facility boundary must be included. This includes water used for cooling and humidification, and water evaporated on-site for energy production or cooling of the data center facility and its support systems.
- The IT equipment energy use (kWh) used as the denominator in the WUE calculation must be the same figure as the one used in the PUE calculation

Timeframe for reporting
Calculations must be based on data from the previous calendar year. However, if it is the first time a cloud resource is certified at a data center facility that has not previously been used to provide certified cloud resources, the reporting period must start in the month when the first cloud resource is certified and end in December of the same year. For all following years, calculations must cover the full previous calendar year.

5.3 Supply chain transparency

Background

The rapid expansion of cloud services has increased reliance on data centers, whose environmental and social impacts vary widely but are often difficult for cloud resource providers to assess. Hosting decisions are often based on cost and performance, while access to verified information on energy use, emissions, resource efficiency, and responsible business practices is limited. This lack of transparency makes it difficult for providers to align sourcing decisions with sustainability goals and growing stakeholder expectations. TCO Certified Accepted Data Center List provides an independent, verified reference of data centers that meet defined environmental and social criteria, supporting more informed sourcing decisions and encouraging improved transparency and performance across the digital infrastructure sector.

5.3.1 Mandate

The cloud resource provider must ensure that

- The data center facility used to provide the certified cloud resource is listed on TCO Certified Accepted Data Center List.
- The country and city of the data center facility location must be provided to TCO Development for publication on the registry of certified cloud resources.

Submit the following to an approved verifier:

- A completed data center template

The following is submitted to TCO Development and may be published:

- A copy of the verification report(s) from a verifier approved by TCO Development.
- The country and city of the data center facility.

5.3.2 Clarification

For each data center included on TCO Certified Accepted Data Center List, the cloud resource provider must submit the following information:

- Name of the data center facility.
- Full address of the data center facility.
- The country where the data center is located.

TCO Certified Accepted Data Center List

All cloud resource providers and verifiers who have a signed agreement with TCO Development may access the TCO Certified Accepted Data Center List. This list includes information such as the compliance levels on data center wide criteria, as well as due dates for submission.

Data center facilities owned by the cloud resource provider

Data center facilities that are owned and operated solely by the cloud resource provider do not need to make their data center facilities visible to other stakeholders in the TCO Certified Accepted Data Center List.

Audit scheduling

The first time a data center is used for providing certified cloud resources, an audit less than 12 months old, showing compliance with TCO Certified Cloud criteria must be presented, or a new one scheduled within one year.