

Trusted Site Infrastructure

Evaluation and Certification of Data Centers
TSI.STANDARD Version 4.6 (incl. EN 50600 & ISO/IEC 22237)



Date of Document: 01.11.2024
Document Vers.: V4.6 (a)

Date of Catalog: 01.11.2024
Catalog Vers.: V4.6

TÜV NORD CERT GmbH
Am TÜV 1, 45307 Essen, Germany

tuev-nord-cert.com

IMPORTANT NOTE:

The list of criteria is the basis for a TSI evaluation and certification. In the form published here it does not claim to be the planning basis for a data center. As a rule, this requires the support of professional planners. Similarly, the classification into the individual levels is only a rough guide. The exact interpretation can only be provided in dialog with TÜV NORD. This paper is intended exclusively for internal company use. The disclosure of the original or copies thereof, including extracts, to third parties is not permitted.

Relevant changes are documented on the TÜV NORD website.

Contents

Structure of the Criteria Catalog	4
Evaluation Levels	6
Requirement Class	7
TSI Certificate	8
TSI certificate with additional “PUE award”	8
Additional TSI Dual Site Certificate	8
Additional EN 50600 certificate	9
Additional ISO/IEC 22237 certificate	11
ENV: Environment	12
CON: Construction	15
FIR: Fire & Extinguishing Systems	24
SEC: Security Systems & Organization	28
CAB: Cabling	33
POW: Power Supply	35
ACV: Air Conditioning & Ventilation	44
ORG: Organization	52
DOC: Documentation	55
DDC: Dual Site Data Center	61
EFF: Energy Efficiency	65
PoC: Proof of Concept	67
Glossary	69
The TSI.ECOSYSTEM	72
About TÜV NORD CERT	73

Structure of the Criteria Catalog

Criteria Sections

The criteria catalog is divided into nine thematically separate evaluation sections. These sections are the following:



ENV: Environment



POW: Power Supply



CON: Construction



ACV: Air Conditioning & Ventilation



FIR: Fire & Extinguishing Systems



ORG: Organization



SEC: Security Systems & Organization



DOC: Documentation



CAB: Cabling

There are three additional optional evaluation aspects, from which supplemental assessment results or where applicable certificates can be derived.



DDC: Dual Site Data Center



PoC: Proof of Concept



EFF: Energy Efficiency

The DDC evaluation aspect allows an availability statement to be made when two equivalent data centers are operated as a dual site.

The EFF evaluation aspect adds an energy efficiency statement to the TSI certificate.

The PoC evaluation section defines requirements for a supplementary procedure to prequalify standardized, modular data center concepts.

Evaluation Criteria

Each section contains evaluation requirements in the form of evaluation criteria. Each evaluation criterion is uniquely identified, has a title, an explanatory text and regulations for the application, that define how the criterion is to be implemented in so called evaluation levels. The identification of the evaluation criterion (criterion-ID) consists of the prefix (belonging to an evaluation section), a main number (assignment to a partial aspect), a sub-number (numbering) and if applicable an ending letter.

The TSI.STANDARD evaluation criteria are a recognized industry standard and already cover a large part of the EN 50600 requirements and the ISO/IEC 22237 requirements. In order to ensure the full compliance with the standard by means of a separate additional certificate, some further criteria have been added. They are marked [EN] and/or [ISO]. These specific extensions can be optionally audited in order to achieve the respective standard conformity. If such an additional criterion is used, it is marked with a final A letter (I=ISO22237, E=EN50600, A=Additional- ISO/EN) in the criterion ID.

ATTENTION:

The criteria-ID are not always consecutive, because with the development of the criteria catalog some evaluation criteria were shifted. Similarly, with the technical development in the past, some evaluation criteria became obsolete and were therefore removed, without a new numbering.

Evaluation Levels

The result of a successful examination is documented by a classification into four different evaluation levels: Level 1 to Level 4. Here, the levels mean:

- Level 1 Average protection requirements/Average availability**
Functional basic supply to ensure the operating conditions of IT server rooms while taking access control and fire protection into account

- Level 2 Extended protection requirements/Extended availability**
Securing the supply through redundancies, consideration of environmental hazards for the IT, access control and fire protection

- Level 3 High protection requirements/High availability**
No single points of failure (SPoF) in the supply, increased intrusion resistance, protection of supply routes, fire control and the monitoring of conditions

- Level 4 Very high protection requirements/Maximum availability**
Dedicated data center building, perimeter security, tolerances for maintenance

- Extended** If all requirements of an evaluation aspect (ENV, CON, FIR, SEC, CAB, POW, ACV, ORG) of the next higher level are fulfilled, these aspects are marked with the attribute “extended” on the certificate.

Requirement Class

Three requirement classes are defined to formulate the application rules for each evaluation criterion. As a rule, they describe the degree and the quality of implementation of the requirements of the four evaluation levels or serve the purpose to distinguish between the variations of requirements in the individual evaluation criteria. The requirements increase in most cases from class A to class C. The requirements of an evaluation criterion are considered fulfilled if the specifications in the explanatory text for the criterion and the specifications in the corresponding requirement class of the selected evaluation level have been implemented.

< . > The evaluation criterion is not taken into account.

Class A The evaluation criterion shall be taken into account in the implementation measures. The measures must implement the required properties and functions according to the description.

Class B The evaluation criterion shall be taken into account in the implementation measures. The measures must implement the required properties and functions in a transparent manner and be effective.

Class C The evaluation criterion shall be taken into account in the implementation measures. The measures must implement the required properties and functions in accordance with the catalog description and be sufficiently effective with regard to availability, protection against attempts to overcome it and enforcement of the measure.

TSI Certificate

Conformity

The TSI Certificate and conformity mark is issued when

- a) all TSI criteria (ENV, CON, FIR, SEC, CAB, POW, ACV, ORG and DOC) are fulfilled) in the selected level without those further marked (EN) or ISO or EN/ISO).

TSI certificate with additional “PUE award”

Conformity

The TSI certificate with additional “PUE award” is issued when

- a) all TSI criteria in the selected level are fulfilled.
b) all EFF criteria are fulfilled.



Additional TSI Dual Site Certificate

Conformity

The TSI certificate and conformity mark is issued when

- a) all TSI criteria are fulfilled for both data centers in the selected level.
b) all DDC criteria in the next higher level are fulfilled.

Additional EN 50600 certificate

Conformity

The EN 50600 certificate and conformity mark is issued when

- a) all TSI criteria in the selected level are fulfilled
- b) all additional criteria marked with an EN field are fulfilled in the selected level (corresponding to the availability classes AC).

References of Standards used for the EN 50600 Conformity Statement

Together with the tagged EN 50600 evaluation criteria, the TSI.STANDARD criteria catalog also serves to check and confirm conformity with the following parts of the standard:

- EN 50600-1 (VDE 0801-600-1), Information technology – Data center facilities and infrastructures – Part 1: General concepts; German version EN 50600-1:2019-08
- EN 50600-2-1 (VDE 0801-600-2-1), Information technology – Data center facilities and infrastructures – Part 2-1: Building construction; German version EN 50600-2-1:2021-09
- EN 50600-2-2 (VDE 0801-600-2-2), Information technology – Data center facilities and infrastructures – Part 2-2: Power distribution; German version; EN 50600-2-2:2019-08
- EN 50600-2-3 (VDE 0801-600-2-3), Information technology – Data center facilities and infrastructures – Part 2-3: Environmental control; German version EN 50600-2-3:2019-08
- EN 50600-2-4 (VDE 0801-600-2-4), Information technology – Data center facilities and infrastructures – Part 2-4: Telecommunications cabling infrastructure; German version EN 50600-2-4:2023-09

Additional EN 50600 certificate

- EN 50600-2-5 (VDE 0801-600-2-1), Information technology – Data center facilities and infrastructures – Part 2-5: Security systems; German version EN 50600-2-5:2021-09
- EN 50600-3-1 (VDE 0801-600-3-1), Information technology – Data center facilities and infrastructures – Part 3-1: Management and operational information; German version EN 50600-3-1:2016-08

The TSI.STANDARD criteria are selected in Level 2–4 in such a way that their fulfillment together with the marked EN 50600 criteria confirm their conformity with the above series of standards. Therefore, Level 2–4 correspond with the availability classes 2 – 4 of the EN 50600.

An EN 50600 certificate in the availability class 1 cannot be issued based on the TSI.STANDARD criteria catalog, the TSI.EN50600 criteria catalog must be applied for this purpose.

Additional ISO/IEC 22237 certificate

Conformity

The ISO/IEC 22237 certificate and mark of conformity is issued when

- a) all TSI criteria in the selected level are fulfilled
- b) all additional criteria marked with an ISO field are fulfilled in the selected level (corresponding to the availability classes AC).

References of Standards used for the ISO/IEC 22237 conformity confirmation

The TSI.STANDARD criteria catalog, together with the marked ISO/IEC 22237 test criteria, is also used to verify and confirm accordance to the following parts of the standard:

- ISO/IEC 22237-1, Information technology - Data center facilities and infrastructures -Part 1: General concepts, 2021-10
- ISO/IEC 22237-2, Information technology - Data center facilities and infrastructures -Part 2: Building construction, 2024-02
- ISO/IEC 22237-3, Information technology - Data centre facilities and infrastructures -Part 3: Power distribution, 2021-10
- ISO/IEC 22237-4, Information technology - Data centre facilities and infrastructures -Part 4: Environmental control, 2021-10
- ISO/IEC 22237-6, Information technology - Data center facilities and infrastructures -Part 6: Security systems, 2024-02

The TSI.STANDARD criteria in Levels 2 - 4 are selected in such a way that their fulfillment together with the criteria identified in ISO/IEC 22237 confirm accordance with the above series of standards. Levels 2 - 4 correspond to the availability classes 2 - 4 of ISO/IEC 22237.

An ISO/IEC 22237 certificate in availability class 1 cannot be issued on the basis of the TSI.STANDARD criteria catalog.

The TSI and ISO criteria are designed to confirm that at least 3 protection classes regarding unauthorized access has been implemented.

At the time of publication of this catalogue, only ISO/IEC 22237-1, -2, -3, -4 and -6 were finally available, therefore conformity is only confirmed for these parts of the standard in the certificate.



ENV: Environment

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
ENV01.01	Avoidance of areas susceptible to flooding and floodplains Areas susceptible to flooding and floodplains are avoided. All infrastructure components are incorporated in the assessment. B: If the site lies within the floodplains of the 100-year flooding level, sufficient structural measures have been taken to protect it against ingress of water. The expected water levels respectively water depths were taken into account. C: The location lies above the 100-year flooding level.	.	B	B	C
ENV02.01	Avoidance of production and storage facilities or pipelines which are at risk of explosion Safety distances are taken into account according to the type and quantity of explosive substances. B: If the safety distance of 250 m is fallen short of, this can be compensated by structural measures. C: A minimum distance of 250 m is ensured.	.	.	B	C
ENV03.01	Avoidance of places, operating and storage facilities with harmful emissions or the release of pollutants A minimum distance of 1 km between the data center and possible pollutant sources in the prevailing wind direction is maintained. Effects of more distant facilities (up to 10 km) are analyzed and structural, technical and/or organizational measures are implemented to minimize risks. C: Implementation is carried out as described in the text above.	.	.	C	C
ENV04.01	Avoidance of sources of electromagnetic interference Strong sources of electromagnetic interference, such as transmission equipment and high-voltage power lines, are avoided or their safety is demonstrated using measurement technology. Depending on the strength of the source of interference, safety distances or possibly measures such as shielding must be ensured which prevent negative effects on operations. C: Implementation is carried out as described in the text above.	.	C	C	C

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
ENV05.01	Avoidance of sources of vibration Sources of vibration are avoided. Any sources in the surroundings, such as rolling and hammer mills, roads with a high volumen of heavy traffic load and railway lines, are avoided, unless constructural vibration isolation is provided. Constructive measures must be taken in seismically active areas. B: Implementation is carried out as described in the text above. C: Seismically active regions above class VII according to EMS-98 are avoided.	.	B	B	C
ENV06.01	Avoidance of transport routes with an increased volume of hazardous materials Transport routes with potentially increased volume of hazardous materials, such as motorways, rail freight lines, waterways and airports, are avoided. B: The following minimum distances are complied with: main roads and railway lines: 75 m, waterways: 150 m, airports: outside the approach and departure sector. Smaller distances can be tolerated if specific measures can compensate for distances which are associated with risks. C: The following minimum distances are complied with: main roads and railway lines: 100 m, waterways: 250 m, airports: outside the approach and departure sector. Smaller distances can be tolerated if specific measures can compensate for distances which are associated with risks.	.	B	B	C
ENV06.01I	Avoidance of transport routes with an increased volume of hazardous materials Transport routes with potentially increased volume of hazardous materials, such as motorways, rail freight lines, waterways and airports, are avoided. B: The following minimum distances are complied with: main roads and railway lines: 75 m, waterways: 150 m, airports: 1.000 m to runway and to flight altitude. Smaller distances can be tolerated if specific measures can compensate for distances which are associated with risks. C: The following minimum distances are complied with: main roads and railway lines: 100 m, waterways: 250 m, airports: 1.000 m to runway and to flight altitude. Smaller distances can be tolerated if specific measures can compensate for distances which are associated with risks.	.	B	B	C

ENV: Environment

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
ENV07.01	Avoidance of properties in the neighborhood which are at risk of being attacked	.	.	C	C
	Properties at risk of being attacked (e.g. fire or explosive attack) in the neighborhood are avoided. Foreign objects at risk of being attacked are not located in the same building or in freely accessible, unprotected neighboring buildings.				
	C: Implementation is carried out as described in the text above.				
ENV08.01	Avoidance of locations near major event sites and their access routes	.	.	C	C
	Meeting places, venues for large events and the position of the properties next to transport routes leading there are avoided. Protection of the property against vandalism is ensured. Measures are taken in order to control temporary barriers with access prevention to the operator's own site.				
	C: Implementation is carried out as described in the text above.				
ENV09.01	Protection against impairment by structures at risk of collapse	.	.	C	C
	The property is located outside the sphere of influence of structures at risk of collapsing.				
	A safety distance to structurally questionable, potentially collapse-endangered objects is guaranteed. This corresponds to at least 105 % of the total height.				
	C: Implementation is carried out as described in the text above.				
ENV10.01	Outside dam drainage and avalanche areas	.	B	B	C
	The property location is outside dam drainage and avalanche areas. If appropriate protective measures are taken, the location in avalanche areas is accepted.				
	B: The location in dam drainage areas is tolerated.				
	C: Implementation is carried out as described in the text above.				
ENV11.01	Avoidance of wildfire hazards	.	C	C	C
	If there are risks from wildfires at the location, these are addressed with appropriate protective measures. These methods including but not limited distance or extinguishing systems. Protective measures are taken in a way to prevent the fire from spreading to the data center building and its provisioning infrastructures.				
	C: Implementation is carried out as described in the text above.				



CON: Construction

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
CON01.01	Inconspicuous, unexposed position of the security area	B	B	C	C
	<p>There is a layered approach with respect to the location of the security area (SA) in the building. There are no indications of the existence and location of the SA.</p> <p>B: Implementation is carried out as described in the text above.</p> <p>C: The SA is located away from visitor traffic, personnel and material flows and has a front area in the form of an entrance area or corridor.</p>				
CON01.02	Avoidance of building areas with potential hazards	.	B	C	C
	<p>IT rooms and singular supply routes are not located in the immediate neighborhood of rooms which represent a danger to the IT rooms or supply routes due to their form of use. Unless their additional risk is compensated for by countermeasures which are evidently suitable. Items which have a high hazard potential are, for example: gas connection or central heating rooms, production areas where there is a risk of explosion or rooms in which highly flammable objects are stored.</p> <p>B: Implementation is carried out as described in the text above.</p> <p>C: The requirement also applies to the technical rooms which are not designed to be redundant.</p>				
CON01.03	Contiguous security areas	.	B	B	C
	<p>A coherent arrangement of primary security areas (IT and telecommunications rooms and their access corridors) is provided to control the flow of people and minimize cable routes. For the secondary security area (supply and security systems as well as control and security centers) a coherent arrangement is to be aimed at.</p> <p>B: Implementation is carried out as described in the text above.</p> <p>C: The IT, telecommunication, technical and functional rooms are arranged in a contiguous security area.</p>				
CON01.04	Meaningful functional room layout with fire protection separation	B	B	C	C
	<p>The principle of the separation of infrastructure (T rooms) and IT systems (IT rooms) is applied.</p> <p>B: The IT room or the IT zone is constructed with a 90 min fire-rating.</p> <p>C: The spatial separation has been consistently implemented for all IT and T rooms. The rooms are constructed with 90 min fire-rating. System-redundant components of a 2n design are located in different rooms separated from one another by constructional/technical fire protection measures.</p>				

CON: Construction

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
CON01.05	Sufficient dimensioning in terms of area, height, structural properties and transportation routes	B	B	C	C

The maintenance of technical components is unhindered.

The room and raised floor heights enable unhindered air circulation and the load-bearing capacity of the unfinished floor slab and any raised floor is designed in such a way that it can also support heavy loads. In the case of technical installations or for risks due to debris, the load-bearing capacity of the ceilings and any roofs is to be taken into account.

B: Implementation is carried out as described in the text above.

C: There is unhindered transport along the transport routes. The load-bearing capacity of the floors of IT and telecommunication rooms is designed for a point load of at least 5 kN (for raised floors according to EN 12825). For other areas, the load specifications according to EN 50600-2-1 are taken into account. Permissible loads must be available at the entrances or in the documentation.

CON01.06	Physical separation of the areas of responsibility for the technical and IT personnel	.	.	B	C
----------	---	---	---	---	---

As a result of the room layout, separate accesses are enabled for the technical and IT rooms.

B: The accesses to the technical rooms and to the IT rooms are designed in such a way that the personnel can only ever enter rooms associated with their area of responsibility. If there is no spatial separation of the CRACs, additional measures are required.

C: The route guidance to the technical rooms and to the IT rooms is designed in such a way that the personnel can essentially only reach rooms of their own area of responsibility.

CON01.08	Securing of the perimeter and front area	.	.	B	C
----------	--	---	---	---	---

The data center is separated from the public by barriers that complicate intruding the security area and its anterooms and facilitate surveillance. If fences or walls are used, they create a space from the building that cannot be crossed with portable means (such as ladders).

B: Implementation is carried out as described in the text above.

C: The front area is implemented as a fenced open space outside the building. A protective barrier against vehicles is provided along the boundary of the property.

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
CON01.09	No parking opportunity along the external walls of IT rooms There are no parking opportunities directly next to, above or under IT rooms. B: There are no parking opportunities directly next to, above or under IT rooms unless additional measures for fire protection, collision protection and vehicle access control are taken. C: There are no parking opportunities in the data processing center building or directly adjacent to the building. Visitor parking lots are located outside an inner enclosure (e.g. protection zone 1).	.	B	B	C
CON01.10A	Access and secure delivery routes, storage and preparation In the event that the main access route for material and personnel to the data center and the site is not available, there is a concept which regulates the alternative access (possibly with restrictions regarding very large transports such as diesel generators). Delivery is provided via a suitable area (a loading area in the case of large installations) outside the security area. Reserved areas suitable for material provision are available. Temporary storage areas are marked and do not represent a risk or impairment of operations. C: Implementation is carried out as described in the text above.	.	C	C	C
EN / ISO					
CON01.11	Areas for temporary installations If the concept of operation provides for the temporary use of technical installations (e.g. mobile chillers or emergency power systems), load-bearing and reserved areas are correspondingly provided. The connections and accessibility of these systems shall be prepared and designed so that the boundaries of the protection zone are not rendered ineffective. C: Implementation is carried out as described in the text above.	.	C	C	C
CON02.01	Rental rights and use of buildings All rooms of the data center building are under the control of the data center operator/data center owner. B: Renting parts of the building to a third party is permitted to a limited extent if the operator/owner holds the rental right. C: The structure comprises exclusively IT rooms and their necessary telecommunications, technical and functional areas. It is used exclusively as a data center.	.	.	B	C

CON: Construction

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
CON03.01	External lightning protection	B	B	C	C
	<p>Data center buildings have a lightning protection system. All roof structures are protected against a direct lightning strike, the separation distances are complied with. Conduction with corresponding grounding is ensured. The lightning protection system is regularly inspected and maintained.</p> <p>B: The system conforms at least to lightning protection class III according to EN 62305 / IEC 62305</p> <p>C: The system conforms to lightning protection class I according to EN 62305 / IEC 62305 (5 x 5 m mesh, conductors every 10 m).</p>				
CON04.01	Protective type of construction using appropriate building materials	B	B	C	C
	<p>Room partitions and ceilings are designed in such a way that they offer fire protection and resistance to intrusion. Building materials and their application are suitable for minimizing, for example, dust emissions, mold and damage from rodents.</p> <p>B: Implementation required as described in the text above.</p> <p>C: In the design of the foundations, location requirements (site survey) have been taken into account.</p>				
CON04.02	Intrusion resistant security boundary for the IT zone	B	B	C	C
	<p>The individual IT rooms or the entire IT zone are designed in terms of their construction – walls, ceilings, doors, windows, ducts – to be intrusion resistant in accordance to resistance classes defined by EN 1627 (Resistance Class (RC)).</p> <p>B: Direct internal and external borders to the public are always of RC2 quality. Borders to the operator’s own rooms with their own personnel (or other co-location tenant), who do not have authorized access to the security area, display intrusion resistant properties, provided that the entire room or area possesses this level of quality all the way round.</p> <p>C: Direct internal and external borders to the public are always of RC3 quality. Alternatively, there are two equivalent RC2 borders with intrusion monitoring. Borders to the operator’s own rooms with their own personnel (or other co-location tenant), who do not have authorized access to the security area, display intrusion resistant properties, provided that the entire room or area possesses this level of quality all the way round. For structural elements with intrusion resistant properties (RCx) there is a test certificate and/or individual installation company certificate available.</p>				

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
CON04.03	Securing the technical zone	.	B	B	C
	<p>The individual T rooms or the entire T zone are secured in terms of their structural design – walls, ceilings, doors, windows, ducts – in accordance with EN 1627. Technical room doors are closed and can only be opened with a locking medium or a token.</p> <p>B: Direct internal and external borders to the public are designed to be intrusion resistant.</p> <p>C: Direct internal and external borders to the public are always of RC2 quality. Borders to the operator’s own rooms with their own personnel (or other co-location tenant), who do not have authorized access to the security area, display intrusion resistant properties, provided that the entire room or area possesses this level of quality all the way round. Furthermore, it is ensured by technical measures that the T rooms – or alternatively the entire T-zone – is locked at all times. For structural elements with intrusion resistant properties (RCx) there is a test certificate and/or installation company certificate available.</p>				
CON04.04	Avoidance of windows in the security area	.	B	B	C
	<p>In IT rooms windows are avoided or specially secured with respect to their disadvantages, depending on their location (opening, intrusion, fire, heat input and view).</p> <p>B: Implementation is carried out as described in the text above.</p> <p>C: Windows in IT rooms are not permitted.</p>				
CON04.05	Tamper and climb-through protection for channels, vertical ducts & exterior openings	.	B	C	C
	<p>All access possibilities for individuals to IT and T rooms, such as ducts and openings which it is possible to crawl through, are secured on the intrusion resistant zone boundary in the same quality, e.g. by means of intrusion resistant grilles (cf. CON04.02). Accessible grills are secured against the attachment of ropes, hooks, etc.</p> <p>B: Implementation is carried out as described in the text above.</p> <p>C: In the case of manholes in the outside area there are safety measures which prevent the intrusion of flying devices, as well as the introduction of items or liquids such as chemicals.</p>				

CON: Construction

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
CON04.06	Protection for the transfer points of supply networks and out-door installations	B	B	C	C

Supply routes, external installations next to access roads, as well as underground facilities under driveways, are protected against mechanical damage.

B: Implementation is carried out as described above in the text.

C: Supply routes in the outside area are also protected against sabotage and are routed into the building with protection against mechanical damage.

CON04.07A	Implementation of a protective zone shell model	.	C	C	C
-----------	---	---	---	---	---

EN / ISO

The security area is divided up into protection zones and uses the shell principle with – as a rule – increasing intrusion protection (protection class). For each protection zone a protection class is defined which specifies the intrusion resistant quality of walls, doors, windows and grilles.

Areas of protection class 3 and 4 are realized in resistance class RC 2 according to EN 1627. The intrusion resistant properties of the other protection classes depend on the risk analysis and are explained in a transparent manner in the security concept.

Areas of protection class 4 are completely surrounded by protection class 3 areas.

C: For white space, telecommunication rooms, mechanical, electrical distribution and fuel supply systems, at least protection class 3 regarding resistance against unauthorized access is realized. Where under control of the premises owner, this also applies to power supply equipment. Pathways which are routed in areas of a lower protection class are monitored for unauthorized access.

CON04.08A	Implementation of the outer protection zone boundaries	.	C	C	C
-----------	--	---	---	---	---

EN / ISO

If fences (or similar) represent the boundaries of protection classes, the following minimum requirements apply:

Boundaries requiring RC2 quality are secured with fencing at least 2 m high, RC3 at least 2.40 m and RC4 at least 2.80 m high, including an extension that makes it difficult to climb over.

The structural design of the fence takes into account the specified resistance times (2 minutes, 5 minutes or 10 minutes for the above resistance classes).

Higher objects that can be used as climbing aids are located horizontally at least 2 m from the fence.

C: Implementation is carried out as described in the text above.

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
CON05.01	Avoidance of combustible finishing materials and furnishings Combustible materials are not used if possible in IT or T rooms. No storage takes place in IT rooms. C: Implementation is carried out as described in the text above.	C	C	C	C
CON05.02	Securing of doors, windows and shutters against fire and smoke according to EN 1634 In the case of doors, windows, fire barriers in technical rooms and IT rooms, fire transmission is prevented for 90 minutes unless the neighboring room is free of fire loads (e.g. corridor) or extinguished (e.g. UPS room). In all other rooms, the elements prevent the fire from spreading for at least 30 minutes if they are connected to a room free of fire loads (e.g. corridor), otherwise for at least 60 minutes. B: Implementation is carried out as described in the text above. C: IT rooms and T rooms with control electronics (e.g. UPS, climate control, BAS) and rooms with very early fire detection are designed to be smokeproof.	B	C	C	C
CON05.03	Proper execution of fire stops For wall, floor and ceiling penetrations and the components to be provided, suitable approved fire stops are used, which are labeled and kept closed at all times. C: Implementation is carried out as described in the text above.	C	C	C	C
CON05.04	Compliance with temperature and humidity limits in the case of ambient fires Either by structural measures or the exclusion of an ambient fire it is ensured that a temperature load across walls or ceilings does not result in the stopping of IT operations. In the case of small connecting surfaces of the endangered room (< 10 % of the ceiling area plus 3 largest wall areas of the IT room) the implementation of walls and ceilings is given in the quality of F90 according to DIN 4102). Hazards from fires in neighboring rooms together with connecting surfaces > 10 % are accepted by an implementation of the elements in F120 according to DIN 4102. B: Implementation is carried out as described in the text above. C: Proof has been provided of the fire protection quality of the walls and ceilings within the meaning of the requirements of this aspect of testing, if the connection area is > 10 %.	.	B	C	C

CON: Construction

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
CON05.05	Fire protection for Lithium-Ion batteries	C	C	C	C
	<p>If Lithium-Ion batteries are used as energy storage for UPS systems, they must be housed in a separate room for each path (separated from their UPS systems). The room must be completely constructed with at least 90 min fire-rating (ceilings, walls, windows, fire dampers, doors). A fire extinguishing concept is available.</p> <p>C: Implementation is carried out as described in the text above.</p>				
CON05.06	Additional protection for photovoltaic systems	.	C	C	C
	<p>If photovoltaic systems are installed on the data center building, protection concepts that limit additional risks from the system (especially fire) have been developed and implemented.</p> <p>This applies to all systems adjacent to IT or singular technical rooms, as well as the protective function of the roof (e.g. tightness after a fire) and the structures on it.</p> <p>Photovoltaic systems are approved by an independent specialist company (e.g. recognition by VdS) or an inspection organization during commissioning and are serviced regularly.</p> <p>C: Implementation is carried out as described in the text above.</p>				
CON06.01	Structural water protection	B	B	B	C
	<p>In the case of water hazards, structural or constructive measures have been taken which prevent the penetration of water into critical rooms – especially IT rooms. Roof openings, e.g. in the form of skylights, have been avoided within IT and plant rooms, or additional safety measures (drainage of possible leaks and their detection) are used.</p> <p>The roof construction allows the drainage of water loads outside IT and technical rooms.</p> <p>B: Implementation is carried out as described in the text above.</p> <p>C: Skylights and roof hatches are not allowed in IT rooms.</p>				

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
CON06.02	Protection against leaking water	B	B	B	C
	<p>Liquid-carrying pipes that do not supply the local air-conditioning systems (e.g. in-row coolers, CRACs) run outside IT, telecommunication and technical rooms. In case of individual pipes, measures have been implemented to prevent the ingress of liquids into critical areas (e.g. switch cabinets, switchgear systems or IT racks), e.g. trays, suitable floor profiles or upstands.</p> <p>In the event of a leak, the quantity of liquid must always be limited by appropriate shut-off devices.</p> <p>B: Implementation is carried out as described in the text above.</p> <p>C: Liquid-carrying third-party pipes in the IT rooms are not permitted.</p>				
CON06.02A	Protection against leaking water	.	B	B	C
EN / ISO	<p>Liquid-carrying pipes that do not supply the local air-conditioning systems (e.g. inrow coolers, CRACs) do not run above electrical equipment, controls, distributions, IT- and networking installations and -cabeling, switchboards, etc. In the case of a leak, the quantity of liquid must always be limited by appropriate shut-off devices.</p> <p>B: Implementation is carried out as described in the text above.</p> <p>C: Additionally liquid-carrying third-party pipes in IT rooms are not permitted.</p>				
CON08.01	Emergency lighting and marked escape routes	C	C	C	C
	<p>The escape routes are marked in the IT rooms, T rooms and all function rooms. In addition, there is emergency lighting which enables safe operation and guarantees the full illumination of the escape routes in such a manner that it is possible for persons to escape at all times in the case of danger.</p> <p>C: Implementation is carried out as described in the text above.</p>				



FIR: Fire & Extinguishing Systems

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
FIR01.01	Use of an advanced and appropriate fire alarm system	B	C	C	C

The fire alarm system enables the division into detector areas and groups and has a secure energy supply. The alarm is given both on site and at a location which is permanently manned. The components, e.g. fire alarm panel, detector or smoke aspiration systems fulfill the EN 54 specifications. The location of the fire alarm control panel is included in the fire monitoring.

B: Implementation is carried out as described in the text above.

C: There is secure transmission to the alarm receiving center.

FIR01.02	Monitoring of IT and technical areas	B	C	C	C
----------	--------------------------------------	---	---	---	---

The IT and telecommunication areas as well as the technical support rooms required to supply the IT and the control center in the data center are monitored for fire.

B: Implementation is carried out as described in the text above.

C: In addition, the rooms through which supply lines are routed are monitored for fire.

FIR01.03	Monitoring of adjacent rooms	.	C	C	C
----------	------------------------------	---	---	---	---

All of the rooms adjoining the IT rooms are monitored for fire. These also include the rooms located above and below them. More remote rooms in the building with high fire risks which are located in the same fire zone as the security area are also monitored.

C: Implementation is carried out as described in the text above.

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
FIR01.04	Sufficient detector density	B	B	C	C
	<p>The individual room detectors cover a maximum defined monitoring area. Within the security area, this is 60 m² per sensor. The requirement can be implemented via point detectors or appropriately designed aspirating smoke detectors.</p> <p>The requirements of any installed fire extinguishing system (e.g. halving the surveillance area) or other reasons for dual detector dependency are also taken into account.</p> <p>Cold or hot aisle containments are taken into account in the monitoring.</p> <p>B: The max. monitoring area of a detector in IT rooms is 30 m², in the raised floor and suspended ceiling 40 m². For other rooms of the security area, the max. monitoring area of a detector is 60 m².</p> <p>C: The max. monitoring area of a detector in IT rooms is 25 m², in the raised floor and suspended ceiling 40 m². For other rooms of the security area, the max. monitoring area of a detector is 60 m².</p>				
FIR01.05	Detector types relative to the form of room use	C	C	C	C
	<p>The detectors used are suitable for the use of the rooms, ensure reliable detection, are fail-safe or malfunctions can be detected, and are equipped with a sensor system with which false alarms are avoided in the area in which they are used.</p> <p>C: Implementation is carried out as described in the text above.</p>				
FIR01.06	Use of very early fire detection systems	.	B	C	C
	<p>Smoke aspiration systems are used in IT rooms for very early fire detection.</p> <p>B: Class B aspirating smoke detectors in accordance with EN 54-20 are used.</p> <p>C: Class A aspirating smoke detectors in accordance with EN 54-20 are used.</p>				
FIR01.07	CO ₂ portable fire extinguisher	C	C	C	C
	<p>For effective and early damage limitation, CO₂ hand-operated fire extinguishers are installed independently of automatic gas extinguishing systems. If the size of the rooms exceeds 150 m², hand-operated extinguishers are also installed in the room, otherwise outside the room. The extinguishing units are stored in accordance with the applicable regulations. EN 3 is complied with.</p> <p>C: Implementation is carried out as described in the text above.</p>				

FIR: Fire & Extinguishing Systems

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
FIR01.08	Fire protection in technical rooms	.	B	C	C
	<p>Technical rooms are incorporated into conventional fire monitoring by means of a fire alarm system. In addition, the fire risk is minimized by additional measures.</p> <p>B: The technical rooms are free of any fire loads. Distributors are inspected annually by means of thermography.</p> <p>C: For LVMD rooms, UPS rooms, main distributions and technical rooms with increased air exchange, (additional) monitoring is carried out with smoke aspiration systems according to EN 54-20 Class B or systems with comparable sensors. Alternatively, extinguishing systems are used.</p>				
FIR02.01	Fire fighting solutions in IT rooms	.	B	B	C
	<p>Depending on the availability requirements and local conditions, suitable fire-fighting solutions are implemented for IT areas. The extinguishing process does not lead to extensive damage to unaffected installations. Aspects of personal safety are taken into account.</p> <p>B: If the IT rooms have low fire load installations, a continuous presence of firefighting trained personnel and on-site extinguishing agent reserve is considered a sufficient solution.</p> <p>C: Automatic extinguishing systems or oxygen reduction systems (in compliance with EN 15004 and EN16750 respectively) are installed for IT areas. The quantity of the extinguishing agent kept on site is adjusted to the volume of the largest extinguishing area and in case of more than 5 extinguishing areas (or poor availability of the extinguishing agent), a 100% reserve of extinguishing agent is available. The necessary tightness of the extinguishing areas and safe release of overpressure are ensured.</p>				
FIR02.02	Monitoring of the extinguishing batteries or the oxygen reduction system	.	B	C	C
	<p>If a gas extinguishing system is used, the extinguishing agent supply is monitored for losses. An oxygen reduction system is monitored to ensure it is functioning correctly.</p> <p>B: The monitoring is carried out by at least one weekly manual check.</p> <p>C: The remote signals are sent to a permanently manned office.</p>				

FIR: Fire & Extinguishing Systems

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
FIR02.03	Installation of the extinguishing agent supply or the oxygen reduction system	.	C	C	C
	Extinguishing batteries or the oxygen reduction system is/are positioned away from hazards in a separate access-protected room, monitored for fire. The room is ventilated.				
	Extinguishing gases with alternative approval, e.g. Novec 1230, may be stored here alternatively in accordance with the authorization.				
	C: Implementation is carried out as described in the text above.				
FIR02.04	Fire protection dampers controlled via a fire alarm system signal	.	C	C	C
	Fire protection dampers in the security area (except for e.g. storage, sanitary rooms) are equipped with a controllable closing mechanism such as spring return actuators.				
	The closing function is maintained even in the case of a power failure. The exclusive use of fusible links is avoided.				
	C: Implementation is carried out as described in the text above.				
FIR02.05A	Control of smoke and gas extraction systems	.	C	C	C
EN / ISO	Smoke and gas extraction dampers can only be triggered manually. The control unit is protected against unauthorised access.				
	C: Implementation is carried out as described in the text above.				
FIR03.01	ORG: Maintenance of fire alarm systems, fire extinguishing systems and fire protection shutters	C	C	C	C
	The fire alarm systems, fire extinguishing systems and fire protection dampers are maintained at least once a year by specialists. Maintenance reports are archived.				
	C: Implementation is carried out as described in the text above.				



SEC: Security Systems & Organization

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
SEC01.01	Access control system: use of an appropriate access control system using advanced technology	B	B	C	C

For access to secure areas an access control system is installed. This has a function monitoring system, tamper monitoring and a secure energy supply, as well as options for logging. Access areas are monitored with respect to their closed condition. In the European environment, EN 60839-11-1 / IEC 60839-11-1 represents the state of the art. The application rules according to EN 60839-11-2 / IEC 60839-11-2 are complied with.

B: At least access to IT rooms must be via the access control system.

C: The access control system controls access to important technical rooms (e.g. LVMD, UPS, main distributions, mechanical room). This is carried out for each individual room or for the security zone as a whole.

SEC01.02	Access control system: protection of the central data base	B	B	C	C
----------	--	---	---	---	---

The access control system center (data base with the access profiles) – if implemented as a dedicated system – is protected against unauthorized access and located in an access-protected room or in an access-protected and monitored enclosure.

B: Implementation is carried out as described in the text above.

C: The room in which the access control system data base is installed has the same intrusion resistance as the IT rooms, is monitored by an alarm and access is controlled via the access control system. The requirement applies analogously to enclosures.

SEC01.03	Access control system: sabotage-protected laying and monitoring of the cables	B	B	C	C
----------	---	---	---	---	---

Insofar as they can be identified, the signal cables are protected against manipulation. Interruptions and short-circuits are detected.

B: Implementation is carried out as described in the text above.

C: Transmission between the concentrators and the access control system's servers takes place either via the operator's own access-protected cables outside the security area or in encrypted form if the IT data network is used. Any tampering that is indicated is handled organizationally in the same way as an alarm from the intrusion detection system.

SEC01.04	Access control system: components with back-up power supply	.	C	C	C
----------	---	---	---	---	---

Technical components of the access security system, such as readers, controllers, door openers, electric locks, are provided with a back-up power supply.

C: Implementation is carried out as described in the text above.

SEC: Security Systems & Organization

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
SEC01.05	Access control system: use of suitable readers The readers are protected against opening, and the input of PIN codes cannot be tracked or observed without being noticed. B: Implementation is carried out as described in the text above. C: The readers have a tamper contact. Any tampering that is indicated is sent to a permanently manned office and handled organizationally in the same way as an alarm from the intrusion detection system.	.	B	C	C
SEC01.06	Access control system: security of the identification device (IDD) The IDD is issued and used on a personal basis. The non-personalized IDD are securely stored. B: Implementation is carried out as described in the text above. C: In addition, the encoding method is deemed to be secure and cannot be compromised.	B	B	B	C
SEC01.07	Access control system: access logging Every access attempt through a door secured with an access control system is logged with at least the IDD code, date and time. B: The data are stored for at least 8 days. C: The data are stored for at least 30 days. Failed attempts are indicated separately by the access control system.	B	B	C	C
SEC01.08	Access control system: identification of the user by means of a second characteristic Besides the possession of the IDD, a further characteristic (knowledge or biometrics) is required for access to the IT rooms or the entire security area. C: Implementation is carried out as described in the text above.	.	.	C	C
SEC01.09	Access control system: creation of zone concepts The access authorization profiles of the access control system enable a distinction to be made between various security zones. Access permissions can be revoked or rendered ineffective at any time by the responsible authority. This can be done automatically or manually. B: Implementation is carried out as described in the text above. C: Anti-passback or at least a check when moving to another area is carried out. The access control system also enables the access time to be limited.	.	B	C	C

SEC: Security Systems & Organization

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
SEC01.10	Access control system: door open time monitoring	.	B	C	C

If a door leading to rooms which are important for the IT or strategically important (e.g. technical security center) is open for too long, a local alarm is triggered after one minute at the latest.

B: Implementation is carried out as described in the text above.

C: After the door has been open for two minutes, the alarm is also forwarded to a permanently manned office. Organizational measures are undertaken in response to the report.

SEC02.01	Intrusion detection system: use of an appropriate state-of-the-art intrusion detection system	B	C	C	C
----------	---	---	---	---	---

The intrusion detection system and all of the detectors connected to it have an increased protection against attempts to overcome them. The fundamental requirements of the EN 50131 are fulfilled, depending on the grade. These include, among others, tamper detection and protection, fault messages, arming, energy supply, message processing, display and forwarding, as well as the requirements placed on the data connection.

An installation company certificate is available.

Perimeter monitoring is carried out in the respective security areas.

B: A grade 2 system according to EN 50131 respectively VdS class B is used. Messages are signalled at least to an on-call standby service.

C: A grade 3 system according to EN 50131 respectively VdS class C is used. Messages are signalled to a permanently occupied station.

SEC02.03	Intrusion detection system: use of motion detectors in the IT areas	.	C	C	C
----------	---	---	---	---	---

In order to identify intruders, or if there are structural weaknesses in walls, motion detectors are installed as a trap surveillance system.

C: Implementation is carried out as described in the text above.

SEC02.04	Intrusion detection systems: monitoring of technical rooms	.	B	C	C
----------	--	---	---	---	---

At least the technical rooms with a central function (UPS, generator room, mechanical room) are monitored by intrusion detection systems.

B: When monitoring an area with several technical rooms, there is no need for individual monitoring of the room.

C: All plant rooms or the entire technical area are monitored.

SEC: Security Systems & Organization

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
SEC02.05	Intrusion detection system: monitoring of IT and telecommunication rooms	C	C	C	C
	Access to all IT and telecommunication rooms are incorporated into the intrusion detection system monitoring.				
	C: Implementation is carried out as described in the text above.				
SEC02.06A	Intrusion detection system: reliable remote data transmission	.	C	C	C
EN / ISO	Remote transmissions of the intrusion detection system are securely transmitted in accordance with EN 50136.				
	The alarm receiving center meets the basic structural, security-related and organizational requirements of the EN 50518.				
	C: Implementation is carried out as described in the text above.				
SEC03.01	Video surveillance system	.	.	B	C
	The corridors and accesses to the IT rooms are monitored with video cameras. Similarly, easily accessible external areas and external boundaries of the security area are included in the monitoring.				
	The images are transmitted to a permanently manned office and for the investigation of incidents stored for at least 30 days. Shorter retention periods must be justified and their integration and handling must be demonstrated in the internal organizational regulations.				
	B: Implementation is carried out as described in the text above.				
	C: The external areas and all of the facades are included in the video surveillance.				
SEC04.01	Monitoring of the perimeter and front area	.	.	B	C
	The security zone borders are monitored in such a way that unauthorized intrusion or crossing of the boundary can be detected.				
	B: Implementation is carried out as described in the text above.				
	C: The property also includes an additional monitoring border (protection zone 1) in the outdoor area which includes all of the objects on the site, e.g. along a perimeter fence.				

SEC: Security Systems & Organization

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
SEC05.01	Man trap	.	.	B	C
	<p>Access to the IT area (without telecommunication rooms) or to the entire secure area (protection zone 2) is provided by an effectively implemented single person separation system.</p> <p>Secondary access routes are secured accordingly, so that the system used to separate individuals cannot be bypassed.</p> <p>B: A combination of technical and organizational solutions, such as video surveillance and remote release of a lock door, can be used.</p> <p>C: The separation of individuals is performed technically and uses additional mechanisms in order to prevent misuse. Telecommunication rooms hosting mainly active components are integrated into single person separation concepts.</p>				
SEC06.01	ORG: Regular maintenance and inspection	.	C	C	C
	<p>With respect to the components of the electronic security systems, it is ensured by means of a maintenance agreement that they are regularly maintained (in accordance with the manufacturer's instructions, but at least once a year). The components of the access control system, especially the mechanical elements, are inspected regularly (at least once a year).</p> <p>C: Implementation is carried out as described in the text above.</p>				
SEC06.02	ORG: Securing the workplace for IDD administrators	.	B	C	C
	<p>The issue of the IDD is carried out in a formalized and transparent manner. Unused access cards are stored in a secure place and the administration of the IDDs, as well as the access control system itself, is carried out only after prior authentication. The computer workstation is also secured with a password when it is inactive.</p> <p>B: Implementation is carried out as described in the text above.</p> <p>C: IDD personalization and storage up to the time of the personal handover is performed in a room with access protection.</p>				
SEC06.03	ORG: Tracking of alarms	B	B	C	C
	<p>The monitoring of alarms from the security and building automation systems is regulated and is carried out 24/365 a year.</p> <p>B: Alarms are transmitted to the responsible data center employees (on-call service). Escalation procedures in case of unavailability are documented.</p> <p>C: A security service provider with a permanently manned control center (e.g. alarm receiving center/emergency call service control center) was contracted to track alarms, or security personnel is located on site in their own control center.</p>				

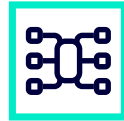
NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
SEC06.04	ORG: On-site security service provider	.	.	B	C

Trained security personnel familiar with the property are available and are able to carry out prompt investigations on site in the event of an alarm.

B: The security personnel are located in close proximity to the data center. The permissible reaction time until arrival on site is determined by the existing protective measures.

C: The security personnel are located on the data center premises. It is technically and organizationally guaranteed that there is a permanent readiness to receive alarms (with regard to security alarms as well as technical alarms) even during simultaneous investigations.

CAB: Cabling



NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
CAB01.01	Secured, separated and redundant WAN routes	.	B	C	C
	<p>The WAN routes run as far as to the facility transfer point (ENI – external network interface) on separate paths without any particular hazards due to fire and mechanical influences, or are sufficiently protected against them.</p> <p>B: Implementation is carried out as described in the text above.</p> <p>C: The external network interfaces are redundant and connected to each other by data links, and the routes run outside the IT rooms or telecommunications rooms and are separated from the MD (main distributor) for fire protection purposes.</p>				
CAB01.02E	Structure of the communication cabling	.	B	B	C
	<p>EN The communication cabling runs in a flexible and scalable manner across hierarchical, fixed installed structures (i.e. using main, intermediate and area distributors). The installation of additional components does not require any interruption to operations.</p> <p>B: Implementation is carried out as described in the text above.</p> <p>C: The distributors are redundant and form an A and B supply structure which are interconnected in such a way that the associated path remains functional in the event of failure of a component.</p>				
CAB01.03E	Redundant, separated telecommunication cable routing	.	.	C	C
	<p>EN Cabling layouts between the distributors are designed redundantly. Cable routing outside IT- and telecommunication-rooms is realized on physically separate ways and is protected against potential hazards.</p> <p>C: Implementation is carried out as described in the text above.</p>				
CAB01.04	Organized laying of cables	B	B	C	C
	<p>The cables are laid in an organized manner and on suitable cable trays. Mutual influencing of the cables by electromagnetic fields is minimized.</p> <p>B: Implementation is carried out as described in the text above.</p> <p>C: Data and electricity cables have their own cable routing systems. The necessary separation distance is calculated and implemented in accordance with EN 50174-2.</p>				

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
CAB01.05	Rack infeed via a connection which is secured against accidental loosening The connections are designed in such a way that accidental loosening is avoided and – where necessary – effective strain relief is provided. C: Implementation is carried out as described in the text above.	C	C	C	C
CAB01.06E	Implementation of crossing points EN Where different types of copper cable cross over one another (data cables, high power cables), an angle of 90 ° over the calculated separation distance is complied with. C: Implementation is carried out as described in the text.	.	C	C	C
CAB01.07E	Protection of the data cables against sources of interference EN Unprotected data cables maintain a minimum distance from sources of interference according to EN 50174-2 or harmlessness is shown by measuring techniques. Sources of interference are, for example, gas discharge lamps, arc welders, induction heaters, frequency converters, transformers, lightning conductors, high-voltage power lines and transmission devices. C: Implementation is carried out as described in the text above.	.	C	C	C
CAB02.01E	Implementation of cabinets and racks EN Cabinets and racks offer appropriate cable routing, considering permitted bending radii and cooling of the installed devices. Provider's equipment in meet-me rooms is installed in lockable cabinets. C: Implementation is carried out as described in the text above.	.	C	C	C
CAB03.01E	ORG: WAN supply through at least two providers EN The data services are provided by at least two different WAN providers. C: Implementation is carried out as described in the text above.	.	C	C	C
CAB03.02	ORG: Implementation of the WAN connection The WAN connection must be redundant. B: The provider can be a service provider or an access provider. In principle, the provisioning is carried out through different network exchanges and nodes. C: The network connection must be made via two different providers or there is a written confirmation from the provider that the paths of the different connections are running separately and are free of intersections.	.	.	B	C



POW: Power Supply

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
POW01.01	TN-S network configuration	B	C	C	C

The energy supply in the building is based on a 5-wire network. PE and N are routed separately. The neutral conductor is insulated and only bridged on the CEP (central earthing point) with PE. The N conductor is designed without any reduced cross-section. There is a grounding concept for central grounding, in which all types of operation are considered.

B: At least the IT area is included in the TN-S structure. Measures to avoid equalizing currents have been taken.

C: Implementation is carried out as described in the text above.

POW01.02	Electrical energy is supplied from various sources	.	B	C	C
----------	--	---	---	---	---

In addition to the primary power supply, a secondary (usually a second grid connection) or an additional supply (usually a standby power supply) is available. These are independent of the primary power supply.

B: Implementation is carried out as described in the text above.

C: The additional supply is based on a different technology of the primary and secondary supply and is usually provided by local generators.

POW01.02A	Electrical energy is supplied from various sources	.	.	B	C
-----------	--	---	---	---	---

EN

In addition to the primary power supply, a secondary (usually a second grid connection) or an additional supply (usually a standby power supply) is available. These are independent of the primary power supply.

B: The redundant connection to the mains can be either

- two supplies from separate and independent primary and secondary sources (e.g. two different substations), or
- two supplies from one primary source (e.g. ring connection to one substation, i.e. two primary supplies). In this case the additional supply is redundant as a combined system.

C: The redundant connection to the mains can be either

- two supplies from separate and independent primary and secondary sources (e.g. two different substations), or
- two supplies from one primary source, i.e. two primary supplies (e.g. via ring connection).

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
POW01.03	Route of primary and secondary supply lines	.	.	B	C
	<p>The feeds can be implemented through two branch lines or through ring lines.</p> <p>B: The lines are routed on separate paths with special protection against external influences up to the point of connection.</p> <p>C: The lines run separately as far as the connection point.</p>				
POW01.04	Secondary supply and additional supply	.	B	C	C
	<p>If the primary supply fails (and vice versa), the secondary of additional supply automatically takes over all critical load. After the primary supply is restored, there is an automatic (possibly manually initiated) return to normal operation. Secondary supplies must be available without time restrictions.</p> <p>B: Implementation is carried out as described in the text above.</p> <p>C: Additional supplies (usually emergency power generators) are also available without time restrictions.</p>				
POW01.05	Connection of the additional supply: redundancy and cable routing	.	.	B	C
	<p>The additional supply is available for all supply paths.</p> <p>B: The additional supply feeds directly into each power distribution system as a combined system. Looping from one system to another is not permitted.</p> <p>If the cables of different supply lines run together, they are protected against external influences until they are connected.</p> <p>C: Each supply path has an independent additional supply in a separate fire compartment. The cables of the individual additional supplies run separately from each other until they are connected.</p>				

POW: Power Supply

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
POW01.06	Redundant power supply for the IT devices	.	.	B	C
	<p>The low voltage supply and distribution is carried out through separate fire protection related systems and rooms. If one distribution system fails, the other systems can continue to supply the entire critical load. The load is distributed as symmetrically as possible over all distribution systems.</p> <p>B: Singular cable routes, switchgear or rooms on the medium-voltage side can be compensated for by additional measures in the additional supply (e.g. redundancy n+1 or preparation for the connection of a mobile additional supply).</p> <p>C: The medium-voltage switchgear is also redundant and separated for fire protection. Supplies and distributions for all IT consumers are implemented in 2N.</p>				
POW01.07A	Implementation of mains couplings	.	.	C	C
	<p>EN If couplings between redundant low-voltage distributions are used, these are protected against erroneous switching operations. They are protected on both sides by a circuit breaker. Both breakers are open during normal operation and are only switched manually.</p> <p>C: Implementation is carried out as described in the text above.</p>				
POW01.08A	Design of transformers and switchgear	.	C	C	C
	<p>EN The transformers have sufficient power reserves. Dry-type transformers comply with EN 60076-11 or IEC 60076-11. Low voltage switchgear combinations comply with EN 61439 or IEC 61439. Low voltage switchgear complies with EN 60947 or IEC 60497. High and medium voltage switchgear complies with EN 62271-200 or IEC 62271-200.</p> <p>In multi-stage expansion concepts, the selection of components allows for a scalable or modular solution.</p> <p>C: Implementation is carried out as described in the text above.</p>				
POW02.02	Supply lines with protection against external influences	.	B	C	C
	<p>The supply lines are protected in semi-public and the operator's own areas against external influences, such as mechanical damage, fire and water, to the extent that hazards are identified.</p> <p>B: Implementation is carried out as described in the text above.</p> <p>C: In addition, the routes are protected against tampering.</p>				

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
POW02.03	IT power distribution units have their own supply line without branches The IT area is supplied with its own power line from the LVMD/UPS. B: One branch is tolerated, provided that it is under the control of the data processing center operator. C: Implementation is carried out as described in the text above.	.	B	C	C
POW02.04	UPS distribution boards without external consumers Distribution boards downstream of the UPS only supply systems relevant to data center operations and that are under control of the data center operator. C: Implementation is carried out as described in the text above.	C	C	C	C
POW05.01	Overvoltage protection for the electricity supply For the energy supply there is staggered overvoltage protection. Owing to the risk of coupling, long supply routes require additional medium protection – cascaded if necessary – in the sub-distributions. C: Implementation is carried out as described in the text above.	C	C	C	C
POW05.02	Overvoltage protection for communication and signal lines All electrical lines (e.g. telecommunications, intrusion detection system, access control system and video surveillance equipment) are equipped with appropriate staggered overvoltage protection devices. C: Implementation is carried out as described in the text above.	C	C	C	C
POW06.01	Incorporated with POW10.08				
POW07.01	Earthing and equipotential bonding In the IT rooms there are independent busbars and/or mesh networks installed for low-impedance potential equalization in order to reduce the impacts of leakage and compensating currents. All metallic objects (e.g. racks, cable trays, piping and double floor supports) are connected to these. The potential equalization rails or mesh networks are grounded through the foundation. The network is grounded according to EN 50310 or ISO/IEC 30129. Floor coverings are selected in such a way that they reduce the risk of electrostatic charges. C: Implementation is carried out as described in the text above.	C	C	C	C

POW: Power Supply

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
POW08.01	Monitoring of leakage currents	.	B	B	C
	<p>The leakage currents in the low-voltage network are monitored for impermissibly high values. Monitoring takes place in the CEP bridge</p> <p>B: Implementation is carried out as described in the text above.</p> <p>C: In addition, the network on the UPS output side is monitored for leakage currents using residual current monitors (RCM).</p>				
POW08.02	Avoidance of central fault current protection devices and emergency power off switches	C	C	C	C
	<p>No central residual current circuit breaker for IT distributors or central control systems are used. Necessary emergency power off switches are protected against unauthorized and unintentional operation, if required.</p> <p>C: Implementation is carried out as described in the text above.</p>				
POW08.03	Network monitoring	.	B	B	C
	<p>Important measured values of the IT supply network (e.g. voltages, currents, apparent and effective power) are recorded centrally down to the sub-distributor level. All external conductors and the neutral conductor are included in the measurement. In the case of distribution networks which are completely redundant, the load distribution is monitored for symmetry and power reserves.</p> <p>B: Regular manual recording and control of the measured values is tolerated.</p> <p>C: The measured values are recorded automatically (continuously and centrally). In addition, the voltage quality at the infeed points is monitored (e.g. for harmonic distortion). Meaningful measured values are automatically monitored for limiting values. If these are exceeded/underrun, an alarm is given.</p>				
POW08.04A	Monitoring of voltage quality and design of measuring devices	.	C	C	C
EN	<p>The voltage quality is monitored at the feed-in points in accordance with EN 50160 or IEC/TS 62749. The measured quantities in the primary distribution are recorded with an accuracy of $\pm 0.5\%$ (accuracy class 0.5 or 0.5 S). The measured quantities in the secondary distribution are recorded with an accuracy of $\pm 1.0\%$ (accuracy class 1 or 1 S). The measuring devices are arranged with granularity level 2 according to EN 50600-2-2 or ISO/IEC 22237-3.</p> <p>C: Implementation is carried out as described in the text above.</p>				

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
POW09.01	UPS: Central UPS The energy supply to the IT consumers is secured by a central UPS. The voltage quality in the case of static systems is in line with EN 62040 or IEC 62040, and for dynamic systems with EN 88528-11 or IEC 88528-11. The power reserves of UPS systems are sufficient. C: Implementation is carried out as described in the text above.	C	C	C	C
POW09.02	UPS: Manual maintenance bypass The USP systems can be decoupled via a manual maintenance bypass (e.g. for maintenance purposes). B: Implementation is carried out as described in the text above. C: The manual maintenance bypass runs outside the UPS room (e.g. to control a room emergency).	B	C	B	B
POW09.03	UPS: Redundancies The complete failure of a UPS system does not lead to supply bottlenecks. B: There is a component redundancy of n+1 or a second active supply system available. C: An UPS system is installed on every supply path.	.	B	C	C
POW09.04	UPS: Installation of UPS and batteries in separate rooms with fire protection In order to prevent mutual influences (e.g. temperature, gassing, fire hazard), there is spatial and fire protection rated separation between the UPS and batteries. C: Implementation is carried out as described in the text above.	.	C	.	C
POW09.07	UPS: Batteries If maintenance-free batteries are used, the risk of individual block failures is minimized (e.g. through additional individual block monitoring, more frequent maintenance intervals or the early replacement of the batteries). C: Implementation is carried out as described in the text above.	.	.	C	C
POW09.08	Incorporated into POW09.01				

POW: Power Supply

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
POW09.09	UPS: Dimensioning of the energy store for complete shutdown of the IT The stored energy of the UPS is dimensioned in such a way that there can be an orderly shut down of all IT equipment. C: Implementation is carried out as described in the text above.	C	.	.	.
POW10.03	Additional supply: Preparation and contractual protection for a mobile additional supply In the case of a power failure, an back-up generator is available within a sufficiently short time. The connection is prepared and was tested beforehand. Contractual agreements for provision of the generator are available. C: Implementation is carried out as described in the text above.	C	.	.	.
POW10.04	Additional supply: Layout with power reserves The additional supplies have sufficient power reserves to be able to react to load jumps. C: Implementation is carried out as described in the text above.	C	C	C	C
POW10.05	Additional supply: Maintaining a sufficient fuel reserve The fuel storage system is dimensioned in such a way that full load operation of the entire load required for further operation of the data processing center is guaranteed. In addition, a supply contract has been concluded which regulates the further supply of fuel. B: The fuel storage is ensured for at least 24 h. C: The fuel storage is ensured for at least 48 h.	.	B	C	C
POW10.06	Additional supply: Tank system The tank system and the fuel pipes to the back-up generators are protected against sabotage and mechanical damage. Extreme outside temperatures are controlled e.g. by insulation, pipe trace heating or fuel additives. The system and the fuel pipes are monitored for leakage. B: Implementation is carried out as described in the text above. C: Each supply path has its own fuel tank system and supply pipe or, in the case of distributed redundancy, there are at least two independent tank systems to which each supply path has a supply pipe per tank system. Each system must be capable of holding the entire required fuel supply.	.	B	B	C

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
POW10.07	Additional supply: Regular function check The operational readiness of the additional supply is tested by regular load test runs. C: Implementation is carried out as described in the text above.	.	C	C	C
POW10.07A	EN Additional supply: Regular function check The operational readiness of the additional supply is tested by regular load test runs. If it is not possible to run the system in parallel with the mains for a function check when the data center load is insufficient, a load bank is available on site. C: Implementation is carried out as described in the text above.	.	C	C	C
POW10.08	Additional Supply: Secure installation of the mains switching control The mains switching control is protected against unauthorized access and independent of the mains supply. B: If there is only one singular switching control for multiple additional supplies, it is designed highly available (e.g. with redundant CPU). C: Each supply path has its own independent switching control.	.	B	B	C
POW11.01	ORG: Selectivity calculation/short circuit coordination study The selectivity of the switching elements has been checked for all relevant operating modes. Non- and partially selective elements have been assessed with respect to their network availability. B: At least one argumentatively guided selectivity evaluation has been carried out with respect to the design and gradation of the security elements/current limiters. C: A complete calculation of the load flow and short circuit currents has been carried out.	B	B	C	C
POW11.02	ORG: Monitoring of the operating states Important operating states of the electric power supply (e.g. UPS, back-up generator, SPD and RCM), as well as the availability of the supply voltage, are monitored. B: Checks and documentation of the components and their parameters are carried out on every working day if there is no automatic recording. C: The components are monitored automatically. Important parameters and critical deviations are reported to a permanently manned office.	.	B	C	C

POW: Power Supply

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
POW11.03	ORG: Transmission of technical fault messages Technical fault messages are transmitted for fault assessment and troubleshooting. The events and elimination of the faults are logged. Any changes carried out are recorded. B: Messages are directly transmitted to a standby service. C: The messages are reliably transmitted to a permanently manned location.	B	B	C	C
POW11.04	ORG: Regular maintenance of the electrical systems Electrical systems are maintained at least once a year on the basis of a maintenance agreement which is customized to the respective component. The maintenance performed is logged. C: Implementation is carried out as described in the text above.	C	C	C	C
POW11.05	ORG: Tests during initial commissioning and exchange During initial commissioning, function and integration tests were performed and documented. Upon the exchange of systems (e.g. UPS, back-up generators, transformer), test certificates from the manufacturer are available and limited function and integration tests have been carried out. B: Implementation is carried out as described in the text above. C: Tests under full and partial load upon initial commissioning have been carried out.	B	B	C	C



ACV: Air Conditioning & Ventilation

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
ACV01.01	Compliance with secure operational conditions in data center areas	B	C	C	C
	<p>The climatic room conditions (temperature, humidity and particle content) are adapted to the operation of the IT equipment used. Temperature control and monitoring are available.</p> <p>B: Implementation is carried out as described in the text above.</p> <p>C: There is also humidity control and monitoring.</p>				
ACV01.02	Sufficient ventilation of technical components and data center areas	.	C	C	C
	<p>Sufficient ventilation in an appropriate temperature range for the safe and design-compliant operation of data center areas and technical components, such as back-up generators, transformer, batteries, is ensured.</p> <p>If a mechanical ventilation of battery rooms is provided it is designed resiliently, provided that the number and type of batteries used poses a risk of hydrogen accumulation.</p> <p>C: Implementation is carried out as described in the text above.</p>				
ACV02.01	Hazard-free and airflow-optimized device installation	C	C	C	C
	<p>The rows of racks and CRAC units are set up and arranged in such a way that the air can circulate without any unnecessary obstacles in the room and raised floor or suspended ceiling, hotspots are prevented and the units are readily accessible for maintenance.</p> <p>C: Implementation is carried out as described in the text above.</p>				
ACV03.01	Leakage protection and monitoring	B	C	C	C
	<p>Leakages are reliably detected and impacts prevented or limited locally. The relevant quantity of liquid is always limited.</p> <p>In IT rooms, both measures for leakage monitoring and the active limitation of the quantity of leaking fluid are implemented. All IT rooms with liquid-carrying pipes are being considered.</p> <p>B: Implementation is carried out as described in the text above.</p> <p>C: In addition, the requirement applies to mission critical electrical installations with liquid-carrying pipes.</p>				

ACV: Air Conditioning & Ventilation

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
ACV04.01	Redundant design of active mechanical components (on the producer, distributor side)	.	B	B	C

A redundant design is created depending on the mechanical concept and component. This relates to active parts such as cooling towers, chillers and pumps or ventilation systems if they are the only system used for cooling.

B: The redundancy of the active components is (n+1).

C: The redundancy of the active components is 2n. In addition, recooling circuits are designed with 2n redundancy. The piping is implemented in such a way that local leakage does not result in an impairment of operations.

ACV04.02	Implementation of the piping and passive components	.	.	C	.
----------	---	---	---	---	---

Singular cooling distribution systems or sections have been implemented in high quality and have been checked for this with extensive quality assurance measures (e.g. radiographic inspection and pressure testing). The piping is segmented in such a way that the extent of damage in the event of a leak can be limited.

C: Implementation is carried out as described in the text above.

ACV04.02E	Implementation of the piping and passive components	.	.	B	C
-----------	---	---	---	---	---

EN

The cooling distribution is designed in such a way that a failure of passive components does not result in a failure of the IT. In addition, any planned maintenance is possible during operation.

B: Individual failures in passive components can be bypassed by switching to a secondary supply path (e.g. a loop circuit). A brief interruption of the cooling supply is permissible in this case.

The secondary supply path is passive in normal operation and provides the same cooling capacity as the primary supply path. All critical cooling consumers are connected to both the active and the passive path.

C: Supply paths are system redundant and installed independently in different areas of the data center. Both paths provide the same cooling capacity. The systems normally operate in parallel mode or in alternating mode if switching can take place without delay.

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
ACV04.02	Implementation of the piping and passive components	.	.	B	.
ISO	<p>The cooling distribution is designed in such a way that a failure of passive components does not result in a failure of the IT. In addition, any planned maintenance is possible during operation.</p> <p>C: Individual failures in passive components can be bypassed by switching to a secondary supply path (e.g. a loop circuit). A brief interruption of the cooling supply is permissible.</p> <p>The secondary supply path is passive in normal operation and provides the same cooling capacity as the primary supply path. All critical CRAHs are connected to both the active and the passive path.</p>				
ACV04.03	Design for maintenance without interruptions to operations	.	C	C	C
	<p>The plant is designed in such a way that maintenance can be carried out to active components at any time without interruptions to operations.</p> <p>C: Implementation is carried out as described in the text above.</p>				
ACV04.04	Protected routes against third-party influence and fire	.	C	C	C
	<p>The routes are protected in semi-public areas and the operator's own areas against mechanical damage and against fire, to the extent that hazards are identified.</p> <p>C: Implementation is carried out as described in the text above.</p>				
ACV04.05	Implementation and redundancy of the air conditioning (consumer side)	.	B	B	C
	<p>Circulating air cooling units or comparable technology are/is provided for IT rooms and singular telecommunication rooms with predominantly active technology with (n+1) redundancy.</p> <p>B: Implementation is carried out as described in the text above.</p> <p>C: Circulating air cooling units or comparable technology are/is also provided for the UPS rooms with (n+1) redundancy.</p>				
ACV04.05E	Implementation and redundancy of the air conditioning (consumer side)	.	B	B	C
EN	<p>Circulating air cooling units or comparable technology are redundant for IT and telecommunication rooms as well as singular UPS rooms.</p> <p>B: The redundancy is (n+1).</p> <p>C: The circulating air cooling units in IT and telecommunication rooms are designed with a system redundancy of 2n.</p> <p>N units are assigned to each of the two supply systems, operate independently of the other system and are located in different areas.</p>				

ACV: Air Conditioning & Ventilation

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
ACV04.05I	Implementation and redundancy of the air conditioning (consumer side)	.	B	B	C

ISO

Circulating air cooling units or comparable technology are redundant for IT and telecommunication rooms as well as singular UPS rooms.

B: The redundancy is (n+1).

C: The circulating air cooling units in IT and telecommunication rooms are designed with a minimum system redundancy of (n+1) and are connected to both cooling supply systems. Switchovers take place automatically.

ACV05.01	Room air filtering	B	C	C	C
----------	--------------------	---	---	---	---

The filtering of the room air, e.g. in the circulating air cooling units, is sufficiently dimensioned for the IT rooms to protect the electronics and the heat exchangers.

B: The filters used correspond at least to the class $ISO_{coarse} \geq 60\%$ according to ISO 16890.

C: The filters used correspond at least to class $ISO\ ePM_{10} \geq 50\%$ according to ISO 16890 or it has been proven that the air quality corresponds to class 8 according to ISO 14644.

ACV05.02	Extended protection against smoke and dust in IT rooms	.	.	.	C
----------	--	---	---	---	---

The IT rooms are subjected to an overpressure.

C: Implementation is carried out as described in the text above.

ACV05.03	Protection of the external air supply	.	B	B	C
----------	---------------------------------------	---	---	---	---

The external air is monitored with respect to temperature, humidity, dust and smoke. Any existing hazards from gaseous air contamination are countered with supplementary measures or forms of proof.

The closure of the external air intake is automatically ensured in the case of external contamination, with regionally specific risks being taken into account.

B: The air supplied from outside is filtered at least once in the central unit (at least class $ISO\ ePM_1 \geq 50\%$ or $ePM_{2,5} \geq 65\%$ according to ISO 16890). If the central unit has a belt drive, the filtering takes place in two stages.

C: The air supplied from outside is filtered in the central unit in two stages (minimum class $ISO\ ePM_{10} \geq 50\%$ AND class $ISO\ ePM_1 \geq 50\%$ or $ePM_{2,5} \geq 65\%$ according to ISO 16890).

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
ACV06.01	Local separation of the components in the central mechanical room	.	B	B	C
<p>Through the locally separated installation of switching units, power units and control systems, the risk of local fires being transferred directly to other parts of the plant is reduced.</p> <p>B: Implementation is carried out as described in the text above.</p> <p>C: Two central mechanical rooms are constructed.</p>					
ACV07.01	Prevention of tampering with the cooling towers	B	C	C	C
<p>Free access to the cooling towers and other external air conditioning systems is prevented.</p> <p>B: In the case of ground-level installation and access protection by a fence, it is ensured that electrical lines and switching elements (e.g. inspection switches) are protected against tampering.</p> <p>C: The access protection is equipped with a monitoring system and designed in such a way that manipulation from outside is prevented.</p>					
ACV07.02	Sufficient dimensioning and operationally reliable installation of the cooling towers	.	C	C	C
<p>The cooling towers are designed for the regional extreme temperatures (dry-bulb or wet-bulb temperature depending on the type of cooling towers) and their installation is airflow-optimized so that no performance reductions can occur. For installation at higher altitudes, the air pressure has been taken into account in the design.</p> <p>C: Implementation is carried out as described in the text above.</p>					
ACV08.01	Plan-compliant design and maintenance-friendly installation of the cooling systems	B	B	C	C
<p>The useful cooling capacity achieved corresponds to the calculated requirements. The systems are installed in such a way that they can be maintained and replaced unhindered and the impacts of vibrations of the systems on the technical and IT infrastructure are limited to an acceptable level.</p> <p>B: Implementation is carried out as described in the text above.</p> <p>C: The supplementary surfaces required for the planned maximum expansion stage of the data center are already available.</p>					

ACV: Air Conditioning & Ventilation

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
ACV09.01	Secure electrical supply to the components of the air-conditioning system	.	.	B	C

The failure of the energy supply system on one supply path does not result in a restriction on the air-conditioning to below the minimum supply.

B: Manual interventions (e.g. switching over from the A to the B supply) are accepted, provided that they can be performed at such short notice that there is no restriction to operations on the IT level.

C: An A/B supply to all relevant electrical components of the cooling system is present, including the outdoor facilities, or the redundant cooling supply systems are supplied independently from each other from the associated power supply paths.

ACV09.01	Secure electrical supply to the components of the air-conditioning system	.	.	B	C
----------	---	---	---	---	---

ISO

The failure of the energy supply system on one supply path does not result in a restriction on the air-conditioning below the minimum supply.

B: Manual interventions (e.g. switching over from the A to the B supply) are accepted, provided that they can be performed at such short notice that there is no restriction to operations on the IT level.

C: Each of the redundant, independent cooling supply systems is supplied by one of the redundant power distribution systems. Each shared component on the distributor and consumer side is supplied via its own automatic switching device from both redundant power distribution systems.

ACV09.02	Reliable water supply to the cooling towers with water spraying	.	.	B	C
----------	---	---	---	---	---

The water supply is ensured at all times by a redundant connection or storage for an operating time of at least 8 hours.

B: Implementation is carried out as described in the text above.

C: Pumps, pipe systems and water treatment systems are provided with a redundancy of (n+1).

ACV09.02A	Reliable water supply to the cooling towers with water spraying	.	C	C	C
-----------	---	---	---	---	---

EN

Necessary water supply systems have been implemented in the same availability as the air conditioning systems whose supply they have to ensure. This concerns sources, active as well as passive components and the electrical supply.

C: Implementation is carried out as described in the text above.

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
ACV09.03	Reliable control and regulation	.	B	C	C
	<p>After power failures, critical controls restart automatically after power recovery. They are either UPS-supplied or battery-buffered. If necessary, supplementary measures are taken for emergency cooling or to bridge the gap in case of long restart times.</p> <p>B: Implementation is carried out as described in the text above.</p> <p>C: When high-level controllers are used, the critical subordinate units are equipped with self-sufficient controllers, or redundant systems each operate with their own high-level controllers.</p>				
ACV09.03A	Reliable control and regulation	.	C	C	C
EN	<p>After power failures, critical controls restart automatically after power recovery. If necessary, supplementary measures are taken for emergency cooling or to bridge the gap in case of long restart times.</p> <p>When high-level controls are used, the critical subordinate units are equipped with autonomous controls or redundant systems operate with their own high-level controls.</p> <p>C: Implementation is carried out as described in the text above.</p>				
ACV10.01	Monitoring of the operating conditions	.	B	C	C
	<p>Importance operating states of the main components, as well as the pumped fluids, are monitored and documented. The monitoring generally relates to the temperature, humidity, load conditions, system pressures, mass flows, power consumption, heat metering (or calculated if necessary).</p> <p>B: Implementation is carried out as described in the text above.</p> <p>C: The monitoring and recording are carried out automatically.</p>				
ACV10.02	Independent monitoring of temperature and humidity	.	B	C	C
	<p>Risks associated with undetected malfunctions of the air-conditioning control system are minimized with additional, independent monitoring of the room temperature in the IT rooms.</p> <p>B: Implementation is carried out as described in the text above.</p> <p>C: The humidity in the IT room is also monitored independently.</p>				

ACV: Air Conditioning & Ventilation

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
ACV10.03E	Energy efficiency capability	.	C	C	C

EN50600 The outside air temperature and humidity are measured. In the IT rooms, the supply air temperature is measured with at least one sensor per cold aisle, the air humidity is measured at least at two representative points within the room, the exhaust air temperature at one point in front of each air-conditioning unit (granularity level 2 according to EN 50600-2-3). Humidity is measured at least at two representative points in the room.

C: Implementation is carried out as described in the text above.

ACV10.03I	Energy efficiency capability	.	C	C	C
-----------	------------------------------	---	---	---	---

ISO The outside air temperature and humidity are measured. In IT rooms, the supply air temperature is measured using at least one sensor every 5 racks, and the exhaust air temperature is measured at a point in front of each air conditioning unit (granularity level 2 according to ISO 22237-4).

For liquid-cooled racks or IT components, the liquid temperature is measured locally. Humidity is measured at least at two representative points in the room.

C: Implementation is carried out as described in the text above.

ACV11.01	ORG: Evidence of tests for tightness, corrosion protection and insulation	.	C	C	C
----------	---	---	---	---	---

All acceptance documents have been submitted, especially the verifications of the pressure/leakage test and the check of the execution of corrosion protection and insulation

C: Implementation is carried out as described in the text above.

ACV11.02	ORG: Regular maintenance of the components of the air-conditioning system	C	C	C	C
----------	---	---	---	---	---

All plant components, such as the CRAC units, cooling towers, chillers, valves, etc. are maintained at least once a year and regularly inspected.

C: Implementation is carried out as described in the text above.

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
ACV11.03	ORG: Transmission of technical fault messages	B	B	C	C
	<p>Technical fault messages are transmitted for fault assessment and troubleshooting. The events and elimination of the faults are logged. Any changes carried out are recorded.</p> <p>B: Messages are directly transmitted to a standby service.</p> <p>C: Technical fault messages are transmitted securely to a permanently manned office and specialized personnel are immediately called in to assess and rectify the fault.</p>				
ACV11.04	ORG: Tests during initial commissioning and exchange	B	B	C	C
	<p>During initial commissioning, function and integration tests were performed and documented. Upon the exchange of systems (chiller, CRAC etc.), test certificates from the manufacturer are available and limited function tests have been carried out.</p> <p>B: Implementation is carried out as described in the text above.</p> <p>C: Full load tests were carried out upon initial commissioning.</p>				



ORG: Organization

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
ORG01.01	Separation of IT production and archiving/backup	B	B	C	C
	<p>The data of the backup (mirroring) is transferred to a different fire compartment.</p> <p>B: Implementation is carried out as described in the text above.</p> <p>C: The data is transferred at least once a week to a different building if they are not mirrored directly in a different data center.</p>				
ORG02.01	Smoking ban signs	C	C	C	C
	<p>Regardless of a general ban on smoking throughout the entire area of operations, the secure area is also equipped throughout with smoking ban signs.</p> <p>C: Implementation is carried out as described in the text above.</p>				
ORG03.01	Regular facility inspections	B	B	C	C
	<p>The IT rooms, all relevant technical rooms, routes and external installations undergo a visual inspection at least once a week and the performance of the inspection recorded.</p> <p>B: Implementation is carried out as described in the text above.</p> <p>C: The inspections are carried out on the basis of a checklist.</p>				
ORG04.01	Proper operations	C	C	C	C
	<p>There is compliance in terms of adherence to the rules, tidiness, cleanliness, accessibility, inscriptions, signs, disposal, etc.</p> <p>C: Implementation is carried out as described in the text above.</p>				
ORG05.01	Realization of security management for physical matters	.	C	C	C
	<p>There are responsibilities for the implementation of physical security measures, the specifications of access and entry regulations and the handling of alarms.</p> <p>In addition, responsibilities for the provision of information to all employees and the recording and reporting of incidents are defined.</p> <p>The number of access authorizations is regularly checked for plausibility.</p> <p>Persons authorized to enter protection class 4 require additional authorization to take people with them.</p> <p>C: Implementation is carried out as described in the text above.</p>				

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
ORG05.02E	Realization of life cycle management	.	C	C	C
EN	<p>There are responsibilities for the optimized use of the technical components, taking into account the investment, operating and maintenance costs. For this, the relevant parameters (such as power losses, reliability, etc.) during operation are recorded and regularly evaluated.</p> <p>The evaluation is used to identify the technical components which have to be taken out of service/replaced.</p> <p>C: Implementation is carried out as described in the text above.</p>				
ORG05.03E	Realization of a customer management system	.	C	C	C
EN	<p>With respect to the letting of data center areas there are – with reference to the customer – rules concerning physical security, energy efficiency, capacity planning, business organization and the exchange of information.</p> <p>Customers are obliged to comply with the regulations, which is verified accordingly. The individuals with responsibility for customer management are informed in good time about important changes and fault incidents.</p> <p>C: Implementation is carried out as described in the text above.</p>				
ORG05.04E	Recording of important key indicators (KPI, Key Performance Indicators)	.	C	C	C
EN	<p>Important indicators, such as the mean duration for restoring a component fault (MTTR), security incidents, PUE and pPUE, deviations from expected product properties and the up-to-dateness of the data center strategy, are recorded, evaluated and used for process improvement.</p> <p>C: Implementation is carried out as described in the text above.</p>				
ORG06.01	Coordinating processes between IT operation, lifecycle management and facility management	.	B	C	C
	<p>IT system expansions are coordinated between IT operations and facility management. Similarly, there is coordination within facility management (e.g. with those responsible for lifecycle management) in the case of expansions or replacements in the field of building service equipment.</p> <p>B: Coordination is carried out informally.</p> <p>C: Coordination is carried out according to a formal process with corresponding recordings and release notes.</p>				
ORG07.01	Customized maintenance contracts for the individual trades	B	B	C	C
	<p>Maintenance contracts have been concluded for all trades which are relevant to operations.</p> <p>B: Implementation is carried out as described in the text above.</p> <p>C: The maintenance contracts are designed in such a way that the start of repair work is ensured not later than on the next working day.</p>				

ORG: Organization

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
ORG08.01	Arrangements for maintenance and repair works	.	C	C	C
	<p>The method of dealing with third-party personnel, the coordination process for maintenance windows, precautions for specific activities or switching operations, as well as special aspects of maintenance and repair work, are described in operating instructions.</p> <p>C: Implementation is carried out as described in the text above.</p>				
ORG09.01	Safety briefing for the personnel	C	C	C	C
	<p>The personnel are provided with safety instruction every year – and new employees at the beginning of their employment contract (e.g. regarding working below raised floors, fire protection, extinguishing, electric service rooms, etc). Proof of the scope and participation in the instruction is archived.</p> <p>C: Implementation is carried out as described in the text above.</p>				
ORG09.02	Employees and service providers who are trustworthy and subject to a confidentiality obligation	.	.	C	C
	<p>The personnel operating the data center, as well as service providers deployed for this purpose, are checked with respect to their trustworthiness and precautions such as their continuous accompaniment are taken. Furthermore, they are placed under a written obligation to maintain confidentiality.</p> <p>C: Implementation is carried out as described in the text above.</p>				
ORG10.01	Deputization rules	B	C	C	C
	<p>The technical infrastructure is looked after by correspondingly qualified personnel.</p> <p>B: Implementation is carried out as described in the text above.</p> <p>C: It is ensured that replacement personnel and arrangements for their deployment are provided.</p>				
ORG11.01	moved to CAB03.02
ORG12.01	Avoidance of publication of security-relevant data center information	C	C	C	C
	<p>Security-relevant data center information include signs in the outdoor area, room signs, floor overviews at entrances or elevators, as well as security-relevant references in brochures and on Internet sites.</p> <p>C: Implementation is carried out as described in the text above.</p>				

DOC: Documentation



NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
DOC01.01	Data center operating manual with security concept	B	C	C	C

A manual for the data center was created. The infrastructures and trades of the data center including their operation are documented and the document is available for the authorized employees.

B: The implementation of the relevant points in the catalogue of criteria is described in brief (a work template is provided by TÜV NORD).

C: The manual for the data center is detailed and comprehensive and addresses the security concept as well as the operation of the systems. It contains a description of the data center strategy, a hazard analysis (e.g. hazards due to technical failure or criminal actions) and the descriptions of the trades building construction incl. fire and water protection, technical fire protection, security systems, wiring, power and cold supply.

The organization of the technical building systems operation (operation with safety management, energy management, lifecycle management, maintenance regulations and responsibilities) is described.

The manual contains load balances for power supply and cooling.

Changes made are regularly updated, marked in the text and recorded in the history.

In the case of an EN 50600 / ISO 22237 certification, a plausible derivation of the security requirements from the business risk analysis with determination of the target level is provided.

DOC01.02	Environment risk analysis	.	B	C	C
----------	---------------------------	---	---	---	---

A risk analysis for the environment of the data center location has been prepared. Within a radius of 2,000 m, all those properties are designated – together with distance information – which can fundamentally be assumed to represent a hazard.

B: Implementation is carried out as described in the text above.

C: Within a radius of 500 m, all properties are identified – together with distance information – and assessed with respect to the degree of risk, with the counter-measures taken being delineated.

DOC: Documentation

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
DOC01.02A	Environment risk analysis	.	B	C	C
EN / ISO	<p>A risk analysis for the environment of the data center location has been prepared. Within a radius of 2,000 m, all those properties are designated – together with distance information – which can fundamentally be assumed to represent a hazard. In addition to all aspects discussed in the ENV chapter, risks such as air contamination, high wind speeds, hurricanes, lightning, precipitation, proximity to coastlines, location below sea level and explosive ordnance are analyzed.</p> <p>B: Implementation is carried out as described in the text above.</p> <p>C: Within a radius of 500 m, all properties are identified – together with distance information – and assessed with respect to the degree of risk, with the counter-measures taken being delineated.</p>				
DOC01.03	Alarm plan/emergency concept	B	B	B	C
	<p>An alarm plan with a list of the events/malfunction messages, initial measures and information chain is provided. Alternatively, there is direct implementation in a building management or alarm tracking system.</p> <p>B: Implementation is carried out as described in the text above.</p> <p>C: An emergency concept is also provided.</p>				
DOC01.04	Fire protection concept	B	B	C	C
	<p>A fire protection concept with the structural, technical and organizational specifications, as well as the conditions which specifically apply to the data center, is provided.</p> <p>B: A signed inspection report of the fire department is provided.</p> <p>C: Implementation is carried out as described in the text above.</p>				
DOC01.05E	Site survey in the case of new construction projects	.	C	C	C
EN	<p>A survey which assesses the geological, electrical and soil aspects of the site, as well as requirements from regulations and land-use plans, is provided.</p> <p>C: Implementation is carried out as described in the text above.</p>				

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
DOC02.01	Site and building plans There are meaningful building plans available in the form of floor plans. B: Implementation is carried out as described in the text above. C: Area and site plans are also provided (at least 2 km radius).	B	C	C	C
DOC02.02	Floor plans for the IT and technical areas Detailed room floor plans are available for the floor (areas) which accommodate the IT and technical areas, supply routes and traffic areas, as well as the direct vicinity of it (also above and below). The technical areas also include outdoor facilities, e.g. back-up generators and roof installations (cooling, lightning protection). C: Implementation is carried out as described in the text above.	C	C	C	C
DOC03.01	Route plans of the main supply paths There are trunk or cable routing route plans available for the main supply paths of electrical/network/cooling/extinguishing, as well as water and gas if applicable. B: Implementation is carried out as described in the text above C: Conflict points (e.g. intersections) are specially marked and compensation measures described. Risks with respect to supply routes on the supplier side have been assessed.	B	B	C	C
DOC03.02E	Documentation of the telecommunication cabling EN The telecommunication cabling with its distributor structures is documented in accordance with EN 50174-1. C: Implementation is carried out as described in the text above.	.	C	C	C
DOC04.01	Single-line diagram of the electrical supply A single-line diagram (SLD) for the electrical supply is available. The line diagram should take into account spatial references, designate outgoing circuits, cable types, circuit breakers and main fuses. C: Implementation is carried out as described in the text above.	C	C	C	C

DOC: Documentation

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
DOC04.02	Cooling and ventilation schematics Piping and instrumentation schematics and installation plans of the cooling systems are available along with floor plans and diagrams of the ventilation systems. C: Implementation is carried out as described in the text above.	C	C	C	C
DOC04.03	Overviews of fire alarm lines and detectors There are installation plans and schematics of the fire alarm lines and detectors available. C: Implementation is carried out as described in the text above.	C	C	C	C
DOC04.04	Overview of extinguishing and fire prevention equipment There are installation plans and schematics of extinguishing and/or fire prevention equipment available. C: Implementation is carried out as described in the text above.	C	C	C	C
DOC04.05	Plans of security systems, intrusion detection system/access control system/video Installation plans and diagrams of the safety equipment are provided. B: The diagrams of the safety equipment can be dispensed with if the system structure is sufficiently described in the documentation. C: Implementation is carried out as described in the text above.	B	C	C	C
DOC04.06A	Power requirement calculation and design specifications EN/ISO For the maximum power of the electricity supply system, all electrical components are taken into account, as well as their load behavior. The selected components are suitable for use in data center environments. C: Implementation is carried out as described in the text above.	.	.	C	C
DOC04.07A	Air-conditioning concept EN/ISO There is an air conditioning concept which specifies the energy efficiency class and describes the type of separation of hot and cold air and also the quantity of heat to be removed from the IT rooms. The balance between close control air-conditioning and energy efficiency is described. The explanations can also be integrated into the security concept. C: Implementation is carried out as described in the text above.	.	C	C	C

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
DOC04.08A	Supplementary risk assessment for the design of technical systems and constructions	.	C	C	C

EN/ISO

The necessity of special layouts of installations and constructional elements shall be assessed and documented e.g. in the security concept, this includes among others

- Generator: Fuel tank system and fuel lines
- Generator: Redundant controls and starter systems
- Generator: Refilling device for lubricants during operation
- Generator: Synchronization with mains supply(s)
- Generator and cooling units: Location of the data center above sea level
- Generator: Limitations for load testing
- Telecommunication provider: Two providers or 1 provider with guaranteed node- and edge-disjunct cable routing
- Design of intrusion resistance for the protected zones
- Needs analysis for fire extinguishing systems (Level 2 and 3)
- Manual or automated switching procedures
- Underground or above ground routing
- Air exchange and air pressure in data center areas
- Ambient conditions in technical areas
- Quality of outside air
- Effects of power failures on the BAS regarding air conditioning of the IT areas
- Load-bearing capacity of floors and ceilings
- Foundations
- Extinguishing agents in portable fire extinguishers
- Earthing & lightning protection system
- Need for locking and monitoring of racks, frames and cabinets
- Need to check materials/goods before transporting them to spaces of protection class 3 or 4
- The way in which the video images from different cameras can be displayed and the need for intelligent video analysis (including the aspect of false alarm prevention)

C: Implementation is carried out as described in the text above.

DOC05.01	Maintenance schedule	B	B	C	C
----------	----------------------	---	---	---	---

An annual maintenance schedule, as well as a list of the trades to be maintained with details of the contractual partner, maintenance cycle and maintenance scope, is provided.

B: Implementation is carried out as described in the text above.

C: Details of the response/repair agreements are provided.

DOC: Documentation

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
DOC06.01	Operating instructions	B	B	C	C
	Operating instructions for special cases and exceptional situations are provided, such as unusual switching operations, emergency infeeds, etc.				
	B: Information signs with brief explanations on the operating components are sufficient.				
	C: Implementation is carried out as described in the text above.				
DOC06.02E	Arrangements for data center customers in the case of third-party renting	C	C	C	C
EN	The arrangements relate to the following topics: general security precautions, access regulations, information on how the customer can contribute to energy efficiency, specifications for capacity planning, information on the organization of operations and the exchange of information.				
	C: Implementation is carried out as described in the text above.				
DOC07.01	List of rooms	C	C	C	C
	A list of all rooms and locations which are relevant to the operation of the data center is provided, stating the room designation, use, location, size and the possible properties of intrusion detection, access-controlled by means of an access control system, fire-monitored, extinguished (a working template is available upon request).				
	C: Implementation is carried out as described in the text above.				
DOC07.02	Data sheets	B	B	C	C
	The data sheets of the important technical components (transformer, UPS, back-up generators, switching device, chillers, CRAC unit, heat exchangers, pumps, intrusion detection system panel, access control system panel, video system, leakage system, measuring devices, fiber-optic cables) are provided.				
	B: Data sheets can be dispensed with if, for the above components, the properties, performance data and technical standard conformity are documented, e.g. in the security concept.				
	C: Implementation is carried out as described in the text above.				
DOC08.01	Verification of the execution of performance and function tests upon commissioning	B	B	C	C
	The verifications for the performance and function tests relate to the electrical and cooling supply, as well as the security systems in conjunction with commissioning.				
	B: Verifications of the function tests.				
	C: Verifications of performance and function tests.				



DDC: Dual Site Data Center

NO.	CRITERION/SUBCRITERION	L2	L3	L4
DDC01.01	The size of the data center IT areas differ by a maximum of 1/3. Data center operation largely occurs within a data center cluster. It is assumed that the systems and applications can run at both data centers without restriction. C: Implementation is carried out as described in the text above.	C	C	C
DDC02.01	The data centers are located in separate buildings and are supplied separately with a WAN connection, electricity and cooling Each of the data centers has its own energy and cooling supply with its own external connection. C: Implementation is carried out as described in the text above.	C	C	C
DDC02.02	Sufficient, risk-based distance between DC1 and DC2. The direct distance (straight line) between the data centers is several kilometers. C: Implementation is carried out as described in the text above.	.	.	C
DDC02.03	ENV: Dependencies on location risks An environmental analysis for both locations shows that the risks mentioned from the relevant individual ENV requirements cannot affect both data centers simultaneously. For DDC level 2, these are the ENV level 2 requirements. C: Implementation is carried out as described in the text above.	C	C	C
DDC02.04	ENV: Level of location risks at the individual locations Each data center must fulfill all other criteria in a minimum level with the exception of a maximum of one criterion. B: The minimum level per location is level 2. C: The minimum level per location is level 3.	.	B	C
DDC03.01	DC1 and DC2 are interconnected via a redundant data connection. Between the two data centers there are at least two data connections on separate paths. B: Implementation is carried out as described in the text above. C: The data connections are physically realized and have no intersection points in their path.	B	B	C

DDC: Dual Site Data Center

NO.	CRITERION/SUBCRITERION	L2	L3	L4
DDC04.01	<p>CON: Target level attainment of the individual data centers</p> <p>Each data center fulfills a minimum level in the CON area depending on the dual site target level.</p> <p>A: Each data center fulfills at least level 1.</p> <p>B: Each data center fulfills at least level 2.</p> <p>C: Each data center fulfills at least level 3.</p>	A	B	C
DDC04.02	<p>CON: Protective construction method using suitable building materials</p> <p>Reference: CON04.01. Both data centers fulfill at least level 3.</p> <p>C: Implementation is carried out as described in the text above.</p>	.	C	.
DDC04.03	<p>CON: Intruder-resistant security border for the IT zone</p> <p>Reference: CON04.02. Both data centers fulfill at least level 3.</p> <p>C: Implementation is carried out as described in the text above.</p>	.	C	.
DDC04.04	<p>CON: Avoidance of windows in the security area</p> <p>Reference: CON04.04. Each data center meets the dual site target level requirement.</p> <p>B: Each data center fulfills at least level 2.</p> <p>C: Each data center fulfills level 2.</p>	B	.	C
DDC04.05	<p>CON: Sabotage and access protection for ducts, manholes and external openings</p> <p>Reference: CON04.05. Each data center meets the dual site target level requirement.</p> <p>B: Each data center fulfills at least level 2.</p> <p>C: Each data center fulfills level 3.</p>	B	C	.
DDC05.01	<p>FIR: Target level attainment of the individual data centers</p> <p>Each data center fulfills a minimum level in the FIR area depending on the dual site target level.</p> <p>A: Each data center fulfills at least level 1.</p> <p>B: Each data center fulfills at least level 2.</p> <p>C: Each data center fulfills at least level 3.</p>	A	B	C

NO.	CRITERION/SUBCRITERION	L2	L3	L4
DDC06.01	SEC: Target level attainment of the individual data centers	B	C	C
	<p>Each data center fulfills a minimum level in the SEC area depending on the dual site target level.</p> <p>B: Each data center fulfills at least level 2.</p> <p>C: Each data center fulfills at least level 3.</p>			
DDC06.02	SEC: Security service provider on site	.	.	C
	<p>Reference: SEC06.04. One of the two data centers fulfills level 4. The security service also receives all technical alarms and the alarms of the security system of the other data center and is always staffed by 2 people.</p> <p>C: Implementation is carried out as described in the text above.</p>			
DDC07.01	CAB: Target level attainment of the individual data centers	A	B	C
	<p>Each data center fulfills a minimum level in the CAB area depending on the dual site target level.</p> <p>A: Each data center fulfills at least level 1.</p> <p>B: Each data center fulfills at least level 2.</p> <p>C: Each data center fulfills at least level 3.</p>			
DDC08.01	POW: Target level attainment of the individual data centers	A	B	C
	<p>Each data center fulfills a minimum level in the POW area depending on the dual site target level.</p> <p>A: Each data center fulfills at least level 1. The supply of the data centers is independent of each other.</p> <p>B: Each data center fulfills at least level 2.</p> <p>C: Each data center fulfills at least level 3.</p>			
DDC08.02	POW: Secondary supply	.	C	.
	<p>Reference: POW01.04. At least one of the two data centers meets level 3 and thus has a stationary back-up generator.</p> <p>C: Implementation is carried out as described in the text above.</p>			
DDC08.03	POW: Generator power supply	.	C	.
	<p>Reference: POW10.xx. At least one of the two data centers fulfills the generator requirements in level 3 with the stationary back-up generator.</p> <p>C: Implementation is carried out as described in the text above.</p>			

DDC: Dual Site Data Center

NO.	CRITERION/SUBCRITERION	L2	L3	L4
DDC09.01	ACV: Target level attainment of the individual data centers Each data center fulfills a minimum level in the ACV area depending on the dual site target level. A: Each data center fulfills at least level 1. B: Each data center fulfills at least level 2. C: Each data center fulfills at least level 3.	A	B	C
DDC10.01	ORG: Target level attainment of the individual data centers Each data center fulfills a minimum level in the ORG area depending on the dual site target level. A: Each data center fulfills at least level 1. B: Each data center fulfills at least level 2. C: Each data center fulfills at least level 3.	A	B	C
DDC10.02	ORG: Implementation of a security management system for physical issues Reference: ORG05.01. Each data center meets at least level 2. C: Implementation is carried out as described in the text above.	C	.	.
DDC11.01	DOC: Target level attainment of the individual data centers Each data center fulfills a minimum level in the DOC area depending on the dual site target level. B: Each data center fulfills at least level 2. C: Each data center fulfills at least level 3.	B	C	C
DDC11.02	DOC: Alarm plan/emergency concept Reference: DOC01.03. Each data center fulfills level 4. C: Implementation is carried out as described in the text above.	.	.	C
DDC12.01	Award: DDC Level 4 extended Each data center meets level 4 individually as an overall result. C: Implementation is carried out as described in the text above.	.	.	C



EFF: Energy Efficiency

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
EFF01.01	Calculation of the PUE-value The Power Usage Effectiveness (PUE) value is calculated as the quotient of the total annual energy demand of the data center and the annual energy demand of the IT. The PUE value is below 1.50.	.	C	C	C
EFF01.02	Measuring period The measured values are recorded continuously for 12 consecutive months as a floating average that is updated at least every hour. The measured values and the monthly interim results are recorded. The presentation of the measurement results is on a monthly basis.	.	C	C	C
EFF01.03	Recording of energy forms and energy sources The energy requirements for electricity, heating/cooling and all fuels required for data center operation are recorded. All forms and sources of energy are measured in kWh.	.	C	C	C
EFF01.04	Measuring devices The measuring devices are suitable for recording the respective measured variable. For measurement of the electrical current, the actual energy demand (effective values) must be measured.	.	C	C	C
EFF01.05	Measuring points Measurements are taken at the designated points for PUE category 2 (PUE2) according to EN 50600-4-2:2019. The IT power demand is measured at the sub-distribution boards in such a way that non-IT consumers can be delimited. The data center energy demand is determined as the sum of all forms and sources of energy supplied to the data center from outside via the system boundary and, if applicable, the data center's own energy supply (e.g. generator operation).	.	C	C	C

EFF: Energy Efficiency

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
EFF02.01	Data centers in mixed use buildings	.	C	C	C
	<p>For the calculation of the PUE value, only the energy demand for the data center is taken into account. If data center-relevant and non data center-relevant areas/ consumers are supplied by a jointly used infrastructure (e.g. a jointly used cooling system for the air conditioning of IT areas and office areas), the energy requirements of the non data center-relevant consumers are recorded and documented separately and are not taken into account when calculating the PUE value.</p>				
EFF03.01	Description of the measurement concept regarding energy efficiency	.	C	C	C
	<p>A description for the measurement concept for the PUE value with the measurement points and the individual energy forms is available. The measuring points are shown completely and distinctly – e.g. in the single-line diagram and in the cooling schematic. For the determination of the PUE value of data centers in buildings with mixed use, the non-DC-relevant consumers are documented and explained with their designation, function and their power values (e.g., electrical connected load of the consumer in kW). The energy requirements of the non-DC-relevant consumers and the method for recording and allocating the non-DC-relevant consumers are explained in a plausible manner (e.g. cooling distribution key).</p>				
EFF03.02	Presentation of the PUE value and the measurement results	.	C	C	C
	<p>The display for the PUE value is unambiguous and always contains the name of the data center, the identification for the PUE category according to EN 50600-4-2, the end date of the measurement period and two decimal figures (e.g. data center X, $PUE_2(2020-12-08) = 1.45$). The measurement results and measurement periods are complete, unambiguous and clearly presented.</p>				



PoC: Proof of Concept

The TSI.PoC is a certification process, in which it is determined if a data center concept in form of a description, drawings and schematics and their implementation (prototype) will fulfill at least 60 % of the TSI criteria. The subject to be examined consists of the required documentation and an implementation as a prototype. Compliance with the requirements is awarded with a TSI.PoC certificate.

Different from inspections of existing data centers the inspection of the prototype will be made according to the following basic principles:

1. An assessment of the criteria sections Environment (ENV) and Organization (ORG) will not be done within the PoC examination.
2. At least 60 % of all relevant TSI criteria have to reach the target level in the criteria sections CON, FIR, SEC, POW and ACV will be covered by the prototype and complied with. Faulty or insufficient implementations are rated as non-conformities and will result in conditions.
3. Within the 2-year validity of the certificate there will be an inspection of a second prototype for conformity with the original prototype.
4. For the criteria not covered by the prototype the manufacturer will provide operating instructions for the end user in form of a TSI compliance operational manual. The interfaces to the customer installation will be marked accordingly. The used technical components will be listed in a bill of materials.
5. Within the criteria section DOC, partially deviating from standard requirements, the criteria should be complied with as listed on page 63.

PoC: Proof of Concept

NO.	CRITERION/SUBCRITERION	L1	L2	L3	L4
DOC01.01	General model and concept description (CD)	C	C	C	C
DOC01.03	Alarm plan/emergency concept	B	B	B	C
DOC01.06	TSI compliance operational manual (TCOM)	C	C	C	C
DOC01.07	Bill of Materials (BOM)	C	C	C	C
DOC02.02	Floor plans of the IT- and technical area	C	C	C	C
DOC04.01	Single line diagram of the electrical supply	C	C	C	C
DOC04.02	Chilled water pipe and instrumentation plan	C	C	C	C
DOC04.03	Overviews of fire alarm lines and detectors	C	C	C	C
DOC04.04	Overview of extinguishing and fire prevention system equipment	C	C	C	C
DOC04.05	Plans of security systems, i.e. intrusion detection/access control/video surveillance	B	B	C	C
DOC07.02	Data Sheets	C	C	C	C
DOC08.01	Verification of the execution of performance and function tests upon commissioning	B	B	C	C

Glossary

ABBREVIATION	EXPLANATION
ACV	Evaluation Aspect Air conditioning and Ventilation (mechanical)
Additional Supply	An additional supply is an optional functional element that provides electrical power to the data center, such as a diesel generator. The additional supply provides electrical power when primary and secondary supplies are unavailable. Machines and electro-technology working party from government and communal administrations
CAB	Evaluation Aspect Cabling Aspiration smoke detection: A special fire detection system which continually sucks in air of a locally-limited area through holes in a piping system and feeds it to a highly sensitive (normally optical) smoke detector)
CON	Evaluation Aspect Construction
DC	Data Center
DDC	Dual-Site Data Center
DIM	Documentation of Infrastructural Measures
DOC	Evaluation Aspect Documentation Commission on the rules for the approval of the Electric Equipment (IEC 60309). Cable plug connector with noses for tension relief Blue = 200-250 V, Red = 380-480 V.
EFF	Energy Effectiveness
EMI	Electromagnetical interference
ENI	External Network Interface
ENV	Evaluation Aspect Environment
FAS	Fire alarm system

Glossary

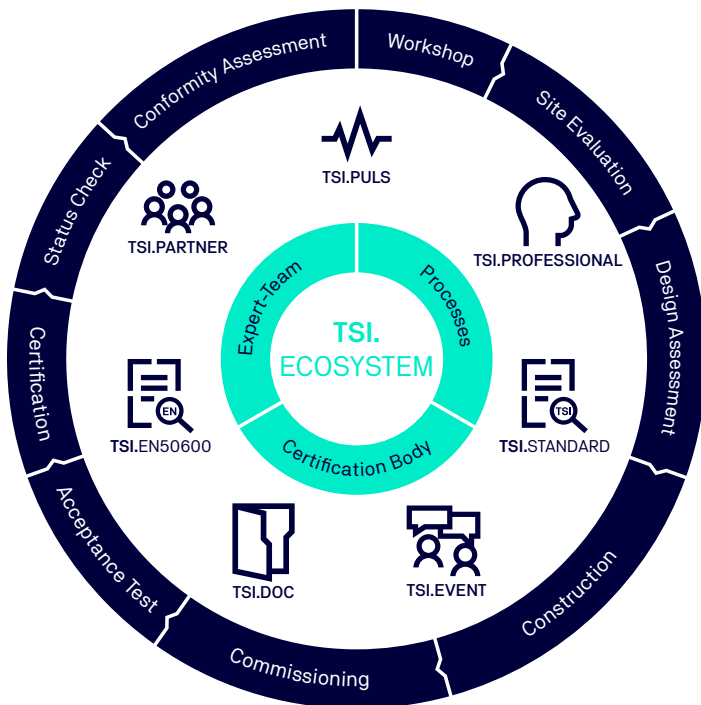
ABBREVIATION	EXPLANATION
FEE	Fire extinguishing equipment
FIR	Evaluation Aspect Fire Protection, Alarm and Extinguishing Systems
FOC	Fiber-optic cable
Generator	Back-up power system (e.g. diesel generator)
HDS	Hazard Detection System
IDS	Intrusion Detection System
IDD	Identification Device
Infrastructure components	Infrastructure components include all technical building systems such as generators, intrusion alarm systems, fire extinguishing systems, fire alarm systems, UPS, access control systems, etc.
IT rooms/areas	IT rooms are rooms in which predominantly IT and/or network equipment is installed. In this sense, TSI understands a telecommunications room with mainly active equipment also to be an IT room
LVMD	Low Voltage Main Distribution
MD	Main Distribution
MV	Medium Voltage
ORG	Evaluation Aspect Organization
P&ID	Piping and instrumentation diagram or mechanical schematic
POW	Evaluation Aspect Power Supply
Primary source	Electrical source for the primary supply, e.g. public utility power grid
Primary supply	Main power supply which under normal operating conditions provides electricity for the data center.
Protection class	Term based on EN 50600. A protection class area designates the quality of the intrusion protection of a room or area.
Protection zone	Normally consists of several adjacent rooms with the same protection level requirements.
PUE	Power Usage Effectiveness

ABBREVIATION	EXPLANATION
RCM	Residual-Current Monitoring Device: Measuring instrument which monitors the vector sum of all conduct occurrence (i.e. the conductor currents dependent on their phase length). In ideal cases, the sum of all currents in feed cables is the same as the sum of all currents in return cables, which is zero. However, insulation faults, faulty devices or inductive coupling with leakage currents and outside currents mean that the sum is no longer zero. This means that an RCM can be used to monitor the cables and consumers.
SA	Secure Area: Comprises of all rooms and external areas of a data center which supply the IT equipment and maintain operations
SEC	Evaluation Aspect Security Systems
SeCo	Security Concept
Secondary source	Electricity source for the secondary supply, e.g. public utility power grid
Secondary supply	Main power supply, which is independent of the primary supply and always available. Provides electricity for the data center in case of a primary supply interruption, Standby power supply which provides electricity for the data center if the primary supply fails. This is carried out via facilities which are used to manage, control and distribute electrical power to the electrical components
Semi-public	Areas are designated semi-public if they are not readily accessible to the public because there is a protection or control system
SP	Smoke protection (smoke tightness)
TBS	Technical Building Systems
TN-C network	(French: Terre Neutre-Combiné) is a network form of low-voltage networks in electrical engineering.
TN-S network	(French: Terre Neutre-Separé) is a network form in electrical engineering. For the protective function a conductor is provided for in the TN-Snetwork which is separated from the neutral conductor or the grounded outer conductor
UPS	Uninterruptable Power Supply

The TSI.ECOSYSTEM

With our evolved TSI.ECOSYSTEM we create added value for our customers and the market. Our competencies, methods and services ensure transparency, comparability and security throughout the entire life cycle of your data center.

In doing so, we always keep in mind the goal of identifying weak points as early as possible, which would otherwise lead to high correction costs, availability restrictions or even the downtime of a data center later on.



About TÜV NORD CERT

Our know-how for your success

TÜV NORD CERT is a well-established and reliable partner for inspection and certification services throughout the world. Our experts and auditors have extensive knowledge based on experience and are in general permanently employed by TÜV NORD. This guarantees independence and neutrality and also means that we can offer continuity in supporting our clients. The benefit to you is clear: our auditors accompany and support the development of your company and provide you with objective feedback.

TSI – Trusted Site Infrastructure

We have been carrying out evaluations and certifications of data centers within the TÜV NORD GROUP since 2001. With our unique TSI methodology, we offer companies an established tool for evaluating the physical security, availability and reliability of technical infrastructures. Our TSI.STANDARD has long since become the benchmark in the data center industry in Germany and is also increasingly in demand on the international market. The underlying criteria catalog is consistently analyzed and further developed by our experts in order to always represent to the current state of technology and standardization. Since its market launch, over 2,000 customer projects have already been successfully completed based on this TÜV NORD owned standard.

Inspired by
Knowledge

TÜV NORD CERT GmbH

Am TÜV 1

45307 Essen

T 0800 245-7457

F 0511 9986 69-1900

tuev-nord-cert.com

