TÜVNORD

Inspired by Knowledge

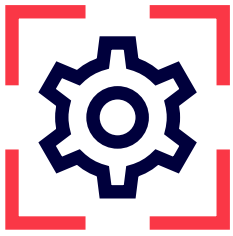
ISO/IEC 22237 Data Center Standard

What you need to know

TÜV®

TÜVNORDGROUP

Table of contents

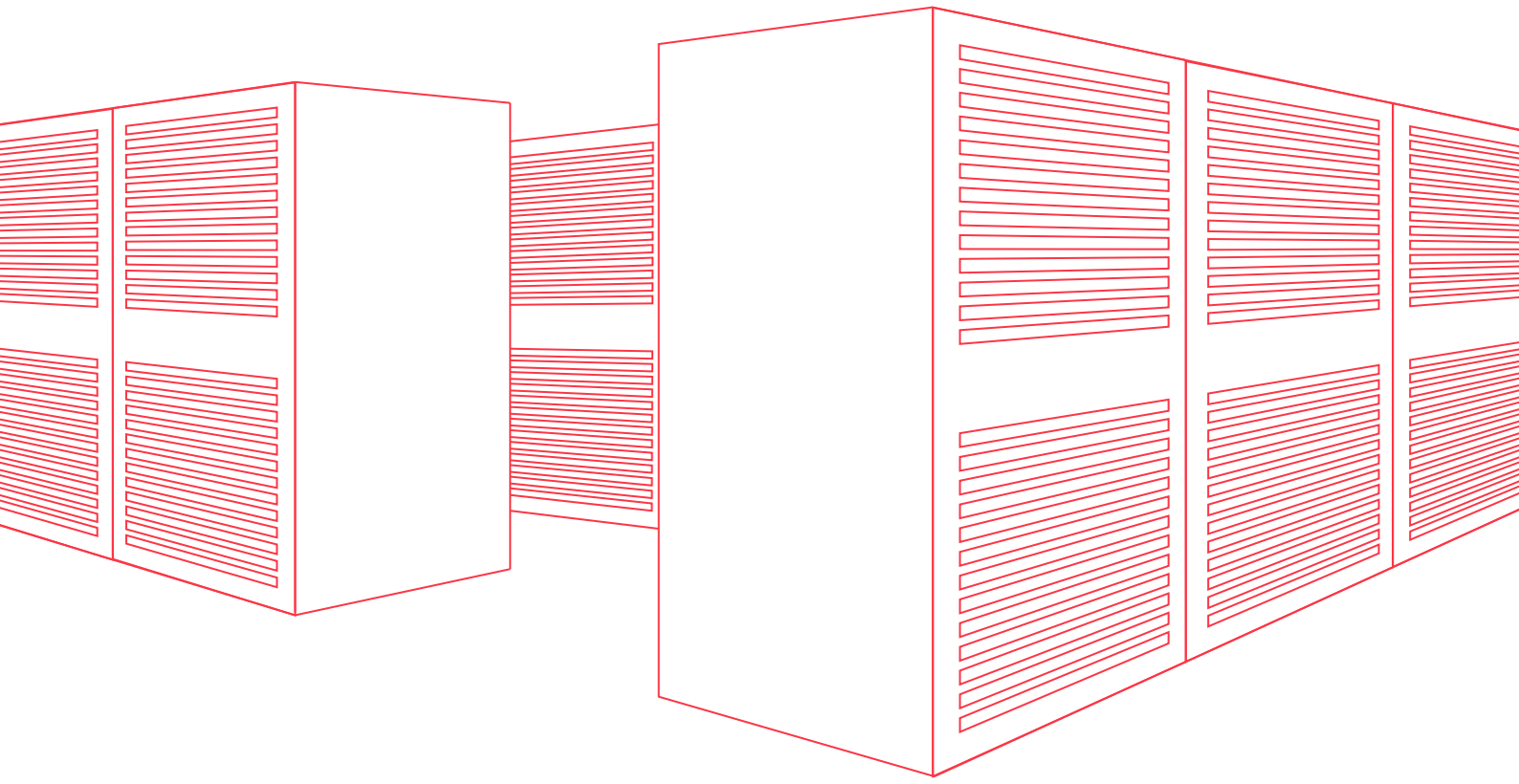


1. Introduction

The data center industry has been historically lacking a universal standard approach for physical security and availability. The EN 50600, on which the ISO/IEC 22237 is based, aimed at closing the gap on a European level. While successful in Europe with many operators aligning with the EN 50600, regions outside of Europe have seen little to no implementation of the standard.

The ISO/IEC 22237 provides a globally accepted approach for data center operators wishing to share comparable information about the physical security and availability of their data centers. Data centers are expected to provide uninterrupted availability to their customers and their data services. The international standard for data centers ISO/IEC 22237 provides an industry standard for all aspects of data centers such as construction, mission critical infrastructure and operation, ultimately ensuring the reliability of the IT infrastructure.

This whitepaper is focused on providing an overview of the present status of the international standard for data centers ISO/IEC 22237 and how a data center operator can reach a conformity to the standard.



2. ISO/IEC 22237 – The new standard with global impact

In 2018 the ISO committee ISO/IEC JTC 1/SC 39 “Sustainability for and by Information Technology” has decided to take up the EN 50600 series to the international level. Based on the EN 50600 documents, seven Technical Specifications (TS) have been decided, to be developed further into International Standards to include North American and Asian input. The committee defines its scope in standardization design practices, operation and management aspects to support resource efficiency, resilience and environmental sustainability for and by information technology, data centers and other facilities and infrastructure necessary for service provisioning.

Figure 1 shows the initial structure of the ISO/IEC 22237. The first part of the data center standard was an introductory part for general concepts (ISO/IEC 22237-1) and 6 sections for technical content (see Figure 2 on the next page).

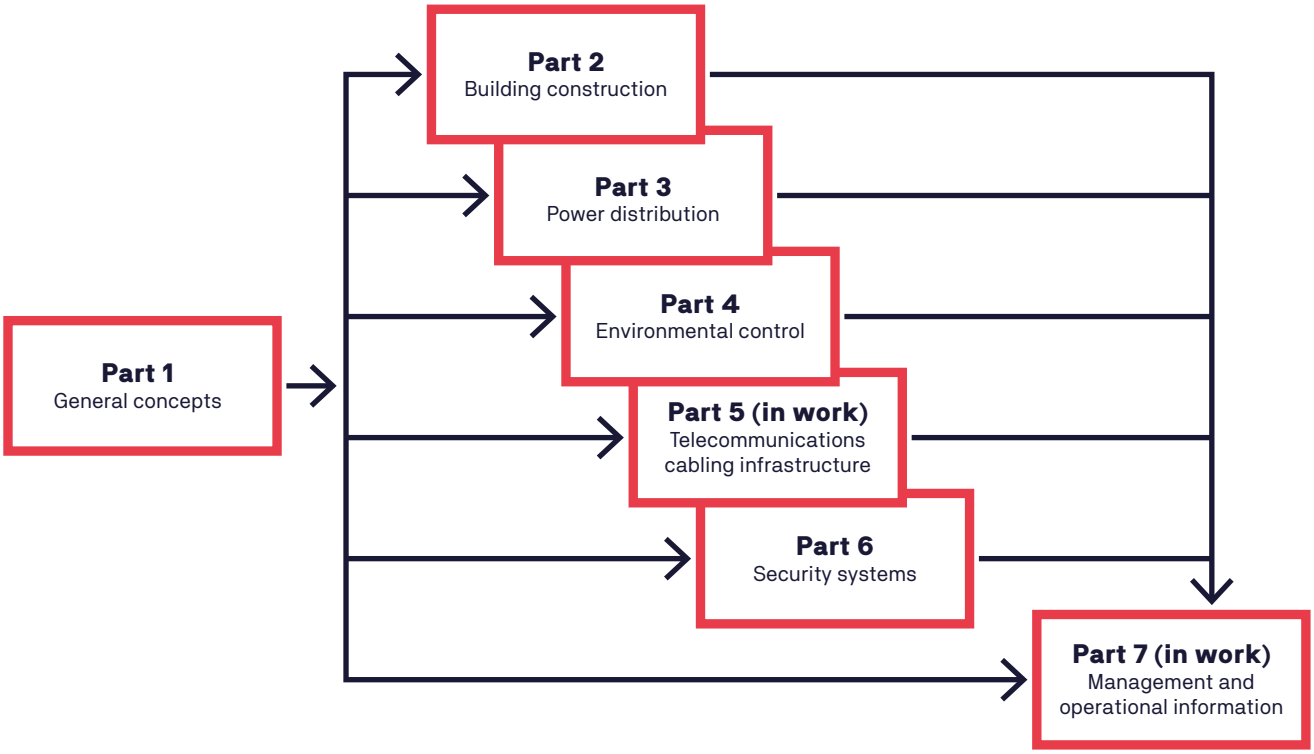


Figure 1: Excerpt from ISO/IEC 22237-1, First edition 2021-10

3. The ISO/IEC 22237 – ongoing development

ISO/IEC 22237	
ISO/IEC **22237-1** Information technology – Data centre facilities and infrastructures – **Part 1: General concepts**	
ISO/IEC **22237-2** Information technology – Data centre facilities and infrastructures – **Part 2: Building construction**	
ISO/IEC **22237-3** Information technology – Data centre facilities and infrastructures – **Part 3: Power distribution**	
ISO/IEC **22237-4** Information technology – Data centre facilities and infrastructures – **Part 4: Environmental control**	
ISO/IEC **TS 22237-5** Information technology – Data centre facilities and infrastructures – **Part 5: Telecommunications cabling infrastructure**	
ISO/IEC **22237-6** Information technology – Data centre facilities and infrastructures – **Part 6: Security Systems**	
ISO/IEC **TS 22237-7** Information technology – Data centre facilities and infrastructures – **Part 7: Management and operational information**	

 = ongoing development

Figure 2: The scope of ISO/IEC 22237 today

There is a continuous update and development on the ISO/IEC 22237. This results in an expanded scope. The standard specifies general requirements for all kinds of data centers irrespective of their size and physical construction:

- it describes general aspects of the facilities and infrastructures required to support effective operation of telecommunications within data centers,
- it specifies a classification system, based upon the key criteria of “availability”, “security” and “energy efficiency enablement” over the planned lifetime of the data center, for the provision of effective facilities and infrastructure, and
- it describes the general design principles for data centers upon which the requirements of the ISO/IEC 22237 series are based.

Currently published parts of the ISO/IEC 22237

ISO/IEC 22237-1:
General concepts

- Business risk analysis
- Data centre design: spaces and facilities
- Availability
- Physical security
- Energy efficiency enablement
- Design of data centers

ISO/IEC 22237-2:
Building Construction

- Site selection and location criteria
- Protection from environmental hazards
- Building and site configuration
- Physical intrusion and fire protection

ISO/IEC 22237-3:
Power distribution

- Power supply and distribution within data centers
- Availability
- Physical security
- Energy efficiency enablement and power distribution

ISO/IEC 22237-4:
Environmental control

- Environmental control within data centers
- Availability
- Physical security
- Energy efficiency enablement

ISO/IEC TS 22237-5:
Telecommunication cabling infrastructure

- Structured cabling systems
- Performance and connectivity requirements
- Physical infrastructure integration
- Compliance and interoperability

ISO/IEC 22237-6:
Security Systems

- Physical security measures
- Monitoring and alarm systems
- Interface with management tools
- Compliance with global standards

ISO/IEC TS 22237-7:
Management and operational information

- Operational information and parameter monitoring
- Acceptance test procedures
- Operational process governance
- Management process framework

4. Who is addressed?

The ISO/IEC 22237 adresses various parties that are involved in the design, planning, procurement, integration, installation, operation and maintenance of facilities and infrastructures within data centers.

In Part 1: "General Concepts" of the ISO/IEC 22237, these parties include:

MANAGEMENT	DESIGN & CONSTRUCTION	EQUIPMENT
▪ Owner ▪ Operator ▪ Facility Management ▪ ICT Management ▪ Project manager ▪ Main contractor	▪ Consultants ▪ Architects ▪ Building designers ▪ Construction companies ▪ System and installation designers ▪ Test and commissioning agents	▪ Suppliers of equipment ▪ Maintenance and installation companies

Figure 3: Parties addressed by the ISO/IEC 22237

It should be pointed out that one party in this listing is not included, which are the evaluators/auditors. The reason is that the ISO/IEC 22237 is designed as a guideline. Therefore, it does not include an evaluation scheme which is necessary for neutral, comparable and consistent third-party assessments.

A lack of an official defined evaluation scheme causes data center evaluators to come up with their own interpretations which result in assessments offered in the market to be different and therefore are not fully comparable.

5. Compliance to the ISO/IEC 22237

The ISO/IEC 22237 has a general setup of how a typical standard is structured. Important to note about the setup is that it includes a conformance clause, which defines what a data center operator needs to fulfill to reach a conformity.
The ISO/IEC 22237 generally differentiates between:

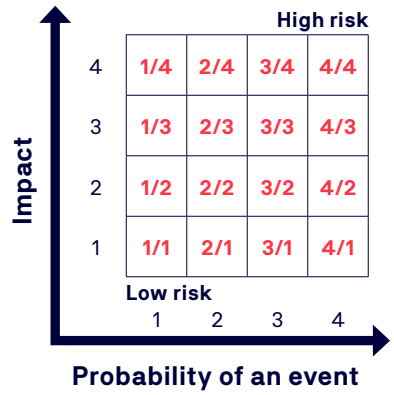
- **Recommendations:** are not mandatory for a conformity. They address special aspects which should be taken into account from a best practice perspective. They are usually classified by the words “should” or “should not”.
- **Requirements:** have to be fulfilled for a conformity. They are usually classified by the words “shall” or “shall not”.
- **Conditional Requirements:** are based on the risk assessment, which needs to be performed when intending to comply with the standard. Requirements have to be fulfilled if risks are identified.

5.1 Business Risk Analysis

Any data center that claims to be compliant with the standard must first complete a business risk analysis according to clause 5 of the ISO/IEC 22237-1.

As mentioned before some requirements are placed in the context of this risk analysis. This allows the topics to be applied more universally to a wide variety of circumstances. However, this comes at the price that ultimately the user of the standard must first determine the risk in detail in order to then draw the correct conclusions – the ISO/IEC 22237 greatly increases the challenge for data center designers and consultants.

The requirements of the availability of the mission critical infrastructure (electrical and mechanical systems), cabling infrastructures and the overall availability of the data center are derived from the conclusions of the business risk analysis. If the conclusions are misinterpreted, the availability will not match the business requirements.



Impact

1 = low: Loss of non-critical services
2 = medium: Failure of critical system functional elements but no loss of redundancy
3 = high: Loss of critical system redundancy but no loss of service
4 = critical: Loss of critical service or loss of life (which may be extended to address personal injury)

Probability of an event

1 = very low
2 = low
3 = medium
4 = high

Figure 4: Source: Example of a risk map according to ISO/IEC 22237-1, clause 5.

5. Compliance to the ISO/IEC 22237

5.2 Classification System

The ISO/IEC 22237 provides three classifications of Availability Class, Protection Class and Energy Efficiency Enablement Level for data centers.

These three classifications play a role in conformance clause of Part 1 of the ISO/IEC 22237.

The conformance clause demands that first of all, a business risk analysis has to be conducted and accordingly an appropriate availability class shall be selected, depending on how critical the data center is for the organization. Different protection classes are applied and an appropriate energy efficiency enablement level has to be selected.

AVAILABILITY CLASSES (AVAILABILITY)	PROTECTION CLASSES (SECURITY)	GRANULARITY LEVELS (ENERGY EFFICIENCY)
■ 4 different availability classes ■ Availability classes deal with technical redundancies in single to multiple paths	Protection classes against 5 different aspects: ■ unauthorized access (classes 1-4) ■ intrusion (classes 1-4) ■ internal fire events (classes 1-4) ■ internal environmental events (classes 1-4) ■ external environmental events (classes 1-3)	■ 3 different granularity levels for the monitoring and measurement of energy efficiency

Figure 5: The three classifications of the ISO/IEC 22237

5.2.1 Availability Classes

Four different grades of availability classes are defined for

- ISO/IEC 22237-3 (power distribution)
- ISO/IEC 22237-4 (environmental control)
- ISO/IEC TS 22237-5 (telecommunications cabling infrastructure)

The higher the availability class (AC), the more component and path redundancy is provided. AC 1–2 are built upon a single path layout, AC 2 with critical component redundancy, while AC 3–4 have at least a dual path, sometimes a multi path design, with component and path redundancies.

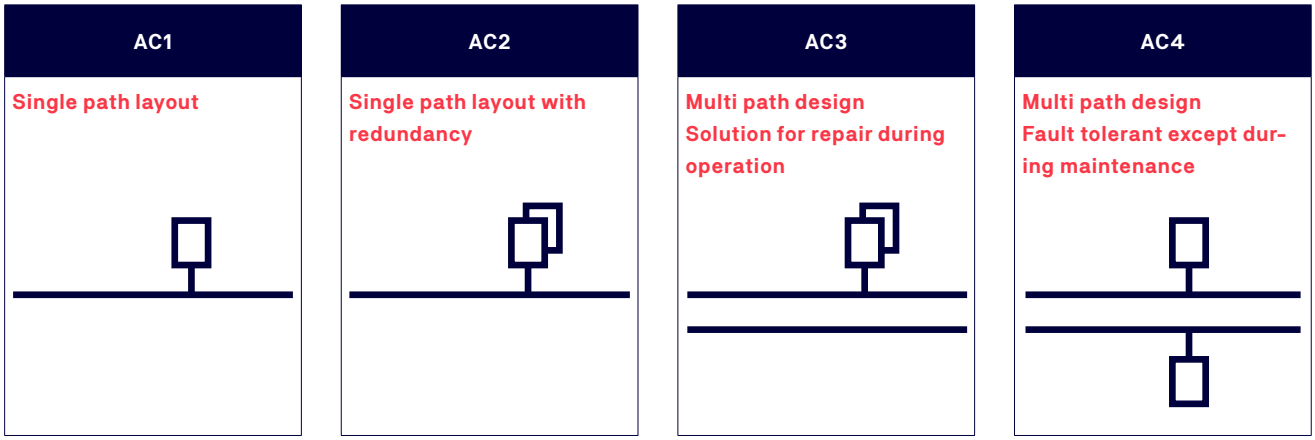


Figure 6: The path layouts of the different availability classes

5. Compliance to the ISO/IEC 22237

5.2.2 Protection Classes

The ISO/IEC 22237 defines five different areas of protection for data center spaces against the following events, also shown in Figure 7 below.

Protection against unauthorized access applies to all areas of the data center. The protection classes for the electrical and mechanical rooms are defined in parts 3 and 4 of the ISO/IEC 22237, which specify the rooms to be assigned to protection class 3. The assignment of all other areas are subject to the risk analysis.

For protection against intrusion, all areas of the data center are considered together with the intrusion delay and reaction times, based on the risk analysis.

Protection against internal and external environmental events has to comply with the desired availability class and is also dependent on the risk analysis.

PROTECTION CLASSES UNAUTHORIZED ACCESS

- At least three protection classes must be implemented
- ISO/IEC 22237-3 and ISO/IEC 22237-4 define the requirements regarding electrical and mechanical spaces

PROTECTION AGAINST INTRUSION

- Intrusion protection measures dependent on the purpose of the data center
- Intrusion delay time > time to stop intruder, multiple barriers increase intrusion delay time
- Construction in ISO/IEC 22237-2
- Security systems in ISO/IEC 22237-6

PROTECTION AGAINST ENVIRONMENTAL EVENTS

- Overheating, external fire
- Water, flood
- EMI, lightning
- Earthquake, explosion
- Other natural disasters

PROTECTION AGAINST INTERNAL ENVIRONMENTAL EVENTS

- Climate Control
- Humidity Control
- Temperature Stability

PROTECTION AGAINST FIRE EVENTS

- Fire Supression
- Thermal Barriers
- Heat Detection

Figure 7: Protection classes of the ISO/IEC 22237

5.2.3 Granularity Levels

The granularity levels (GL) define to which extent the technical infrastructure is monitored and how the measurement of the energy consumption is performed. Higher levels require increased levels of measurement and monitoring of the infrastructure. The three levels are listed below in Figure 8, for the illustration of the granularity level for the electrical system see Figure 9.

GL 1	GL 2	GL 3
A measuring concept that provides simple, general information for the entire data center.	A measuring concept that provides detailed information for specific facilities and infrastructure within the data center.	A measuring concept that provides granular data for the systems within the areas and supply paths of the data center.

Figure 8: Granularity levels of the ISO/IEC 22237

- In GL 1, the operator can distinguish on how much energy is consumed by the facility and how much energy is used for the IT.
- In GL 2, the operator needs a more detailed measurement energy concept with an in-depth overview of his distribution systems.
- In GL 3, the operator has to provide measurement for the energy consumption down to the individual electrical outlet level.

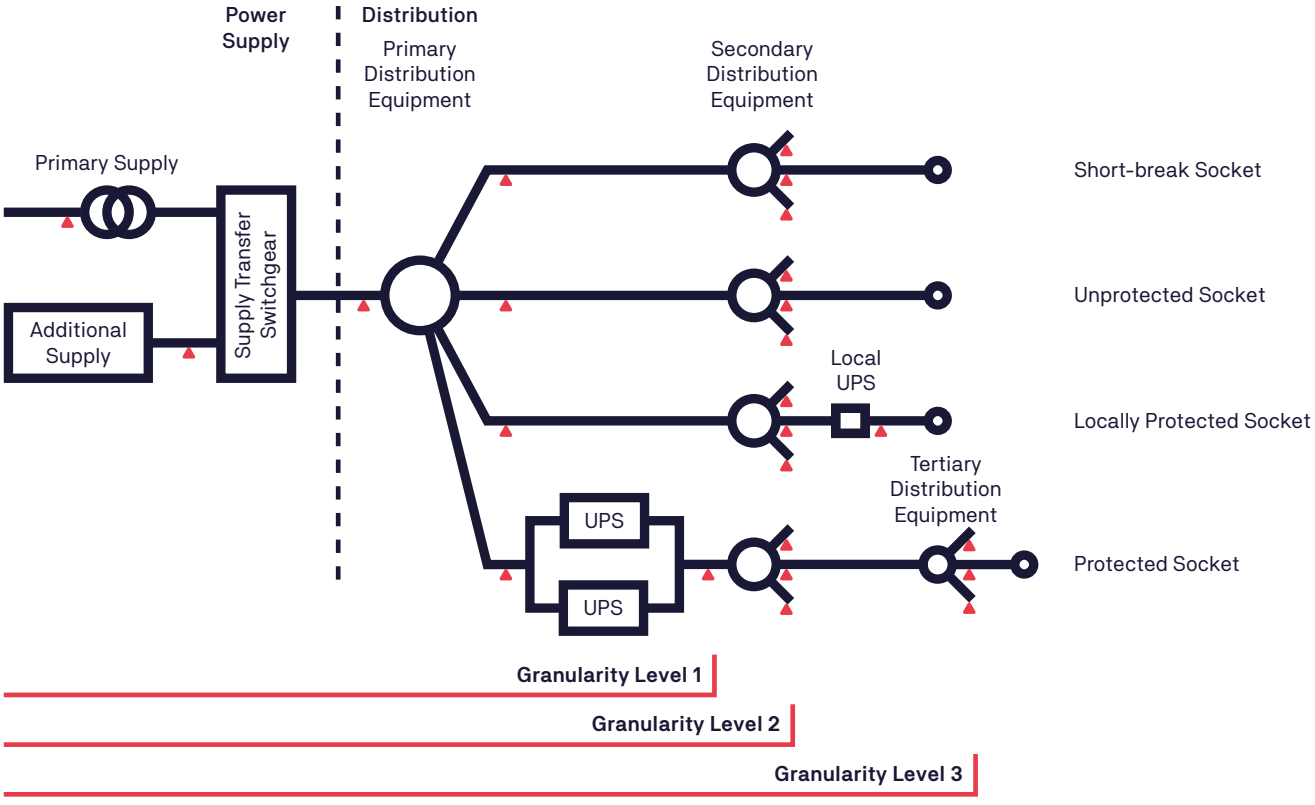


Figure 9: Source: ISO/IEC 22237-3:2021-10

6. Evaluation and Certification

The ISO/IEC 22237 has been developed as a technical guideline. It is intended to provide assistance to all parties directly or indirectly involved in the design, development and operation of data centers. For this purpose, a holistic approach is chosen, which explains all relevant trades and organizational necessities and provides requirements as well as recommendations.

Furthermore, the requirements are partly placed in the context of a risk analysis. This means that the topics can be applied more universally to a wide range of circumstances. However, this comes at the price that ultimately the user of the standard must first determine the specific risks in detail in order to then draw the correct conclusions. The assistance essentially consists of the fact that ISO/IEC 22237 outlines many considerations and names potential risks, but it does not provide any guidance as to which specific measures are required under which risks and which requirements are to be fulfilled in the case.

The standard requires the user to perform a business risk analysis (see 5.1) not only to derive security measures with basic requirements, but also to causally explain the design of individual measures.

This methodology raises the question of how conformity confirmations can be made, because there are no evaluation instructions – after all, the ISO/IEC 22237 primarily wants to be a guideline. This is also the reason why the market requires additional measures for the ISO/IEC 22237 to serve as a suitable basis for evaluation and certification.

The problems for a neutral, independent evaluation are:

- Risk assessment of the operator with regards to the necessity of an implementation of a measure
- No clear requirements depending on the degree of risk
- No evaluation instructions and specifications for the scope of an assessment
- No coordination body for the auditors

These problems are accompanied by the fact that the certificates issued are difficult to compare. The evaluation market is not regulated here. The disadvantages can be minimized by deriving a well founded evaluation criteria catalog. This approach is followed by TÜV NORD with its well established criteria catalogs "TSI.STANDARD" and "TSI.EN50600" which define the requirements extracted from the standard in detail and the scope of inspections. For the operator and for the evaluation body the scope of the required inspections is therefore clearly defined.

As not all parts of the ISO/IEC 22237 have been published, assessments solely based on the ISO/IEC 22237 are not recommended. Hence the requirements of the ISO/IEC 22237 have been adapted into our catalogs and allow an additional compliance to the standard.

7. ISO/IEC 22237 vs. EN 50600

The new ISO/IEC 22237 standard is the international data center standard consisting of seven parts. The parts 1,2,3,4 and 6 have been published until now. The structure is based on the EN 50600 as shown below.

The other parts (here marked by ⚙) are only available as Technical Specifications, while technical committees in the background are working on the adaptation, mainly the integration of data center concepts from North America and Asia.

ISO/IEC 22237	EN 50600
ISO/IEC 22237-1: General concepts	EN 50600-1: General concepts
ISO/IEC 22237-2: Building construction	EN 50600-2-1: Building construction
ISO/IEC 22237-3: Power distribution	EN 50600-2-2: Power distribution
ISO/IEC 22237-4: Environmental control	EN 50600-2-3: Environmental control
ISO/IEC TS 22237-5: Telecommunication cabling ⚙	EN 50600-2-4: Telecommunication cabling
ISO/IEC 22237-6: Security systems	EN 50600-2-5: Security systems
ISO/IEC TS 22237-7: Management and operational information ⚙	EN 50600-2-6: Management and operational information

Within the published parts of the ISO/IEC 22237 the following specific differences to the EN 50600 can be noted: EN 50600 is, for now, the more mature and more widely used data center standard in Europe. It provides a practical framework for how data centers are designed, built, and operated, with the main focus on the physical infrastructure and the availability that infrastructure can deliver. It also covers physical security and energy efficiency in a fairly specific way, so operators and suppliers can show that they meet defined and measurable requirements. In day-to-day work, EN 50600 has become the reference point in Europe and is routinely used in procurement, planning, and evaluation.

ISO/IEC 22237 covers essentially the same ground and is likewise centered on the physical data center environment and the availability it provides. It has been developed on the basis of EN 50600 and clearly takes its structure and many of its concepts from the European standard. In practice, the IEC 22237 can be seen as the internationalization of the EN 50600 approach, with adjustments to fit the ISO/IEC framework and a global audience. It sets requirements for site location, building construction, power, cooling, cabling, physical security, and related infrastructure systems. The idea is to achieve repeatable, clearly defined availability classes based on real design and installation choices. Operational and lifecycle requirements are included where they are needed to keep the infrastructure performing as intended, but they stay close to the physical systems rather than trying to define a separate management or policy framework.

Taken together, EN 50600 and ISO/IEC 22237 describe a largely aligned, infrastructure-centric view of data centers. EN 50600 is the established reference standard in Europe. The international ISO/IEC 22237 closely mirrors it, sharing the same fundamental structure and concepts while being derived to a significant extent from the European standard itself.

8. Criteria Catalogs TSI.STANDARD & TSI.EN50600

The TSI-Method (Trusted Site Infrastructure) has been available to the market since 2001. The goal of the TSI is to cover all relevant regulations and international standards, such as the EN 50600 and the ISO/IEC 22237, but also best practices adapted by sophisticated data centers. As it is becoming increasingly difficult to keep up to date with the latest developments in the data center industry for DC operators, the TSI.STANDARD/ TSI.EN50600 are great tools operators may use to represent current state of art by fulfilling the requirements, as the TSI.STANDARD is regularly updated. With over 2.000 data center projects since 2001, the TSI method has a well-established position in the market.

To make the standard ISO/IEC 22237 assessable, a much needed evaluation scheme has been adapted by TÜV NORD. The result of this is defined in the criteria catalogs.

The relevant and published parts of the ISO/IEC 22237 that have been integrated (to date) are:

- ISO/IEC 22237-1
- ISO/IEC 22237-2
- ISO/IEC 22237-3
- ISO/IEC 22237-4
- ISO/IEC 22237-6

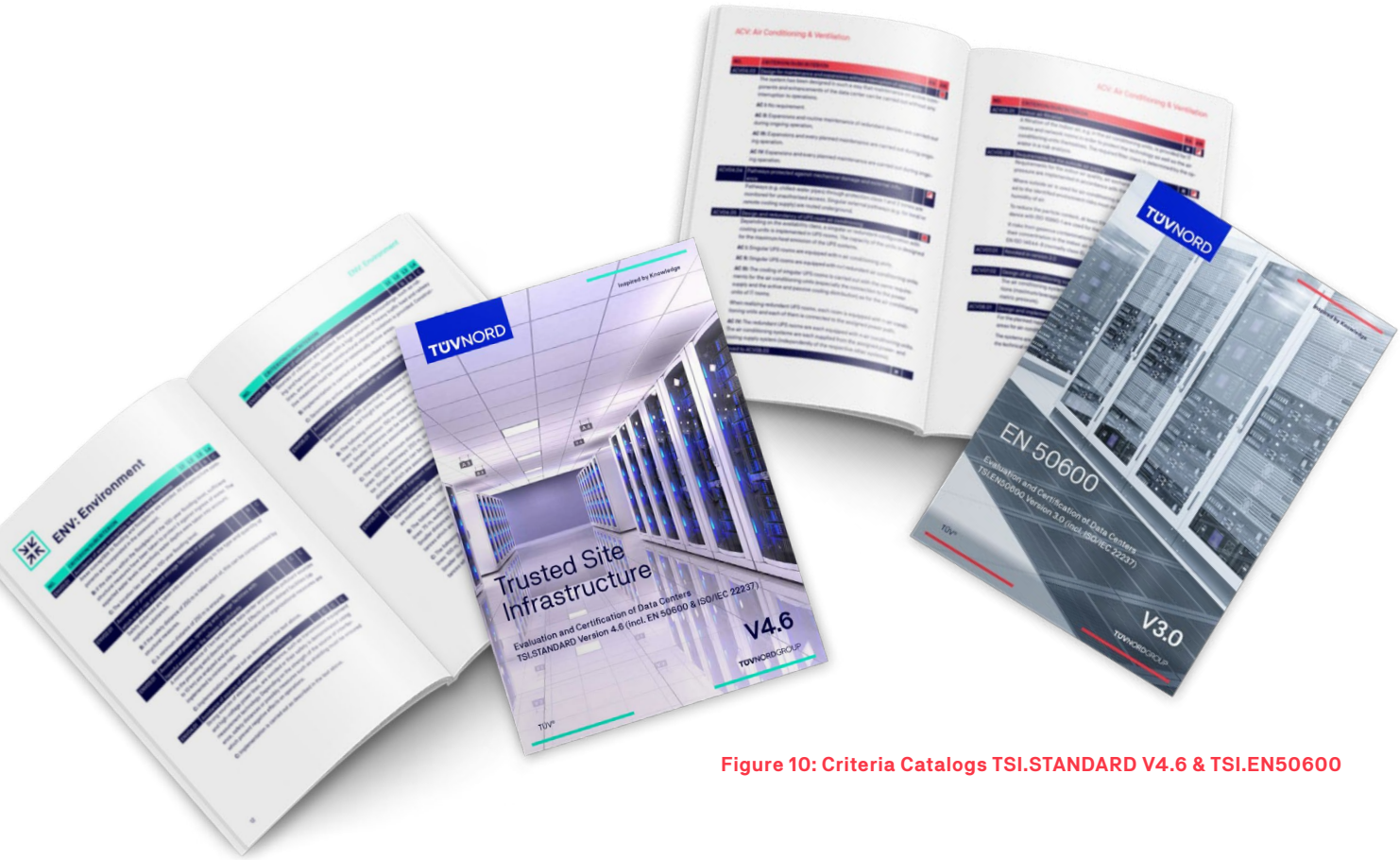


Figure 10: Criteria Catalogs TSI.STANDARD V4.6 & TSI.EN50600

9. TSI.STANDARD/TSI.EN50600 with ISO/IEC 22237 extension

With our catalogs including the ISO/IEC 22237 extension a proper understanding of how the requirements are intended on being implemented is provided.
With the criteria catalogs, all relevant requirements are identified and summarized. They have to be fulfilled by a DC operator in order to gain a conformity confirmation in the form of a certificate.

TÜV NORD provides its evaluations and certifications of the ISO/IEC 22237 based on the criteria catalogs. Based on the comparative analysis of the ISO/IEC 22237 published parts vs. EN 50600 the changes applied to the catalog are very few and operators which hold an EN 50600 certificate can achieve an additional ISO/IEC 22237 based on the currently published parts with only minimal efforts under specific conditions.

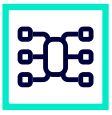
The criteria catalogs adress 9 major criteria aspects:

ENV: Environment
Umfeld

CON: Construction
Baukonstruktion

FIR: Fire Protection & Extinguishing Systems
Brandmelde- und Löschtechnik

SEC: Security Systems & Organization
Sicherheitssysteme und -organisation



CAB: Cabling
Verkabelung

POW: Power Supply
Energieversorgung

ACV: Air Condition & Ventilation
Raumlufttechnische Anlagen

ORG: Organization
Organisation

DOC: Documentation
Dokumentation

Figure 11: Illustration of the criteria aspects covered in the TSI.STANDARD/TSI.EN50600

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 respresent 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.

TÜVNORD

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

TÜV® 24-0583-06/24

TÜVNORDGROUP