TÜRK STANDARDI

TS EN 50600-3-1

Temmuz 2016

ICS 35.020; 35.160; 35.110

Bilgi Teknolojileri - Veri merkezi tesisleri ve altyapıları - Bölüm 3-1: Yönetim ve işletimsel bilişim

Information technology - Data centre facilities and infrastructures - Part 3-1: Management and operational information

Technologie de l'information - Installation et infrastructures de centres de traitement de données - Partie 3-1: Informations de gestion et de fonctionnement

Informationstechnik - Einrichtungen und Infrastrukturen von Rechenzentren - Teil 3-1: Informationen für das Management und den Betrieb

TÜRK STANDARDLARI ENSTİTÜSÜ
Necatibey Caddesi No.112 Bakanlıklar/ANKARA

Milli Önsöz

Bu standard, CLC/TC 215 “Electrotechnical aspects of telecommunication equipment” Teknik Komitesi tarafından hazırlanmış, CENELEC tarafından 26.01.2016 tarihinde onaylanmış ve Türk Standardları Enstitüsü Teknik Kurulu'nun 11.07.2016 tarihli toplantısında Türk Standardı olarak kabul edilerek yayımına karar verilmiştir.

Bu standardda kullanılan bazı kelimeler ve/veya ifadeler patent haklarına konu olabilir. Böyle bir patent hakkının belirlenmesi durumunda TSE sorumlu tutulamaz.

CENELEC üyeleri sırasıyla,Almanya, Avusturya, Belçika, Birleşik Krallık, Bulgaristan, Çek Cumhuriyeti, Danimarka, Estonya, Finlandiya, Fransa, Hırvatistan, Hollanda, İrlanda,İspanya, İsveç, İsviçre, İtalya, İzlanda, Kıbrıs, Letonya, Litvanya, Lüksemburg, Macaristan, Makedonya, Malta, Norveç, Polonya, Portekiz, Romanya, Slovakya, Slovenya, Türkiye ve Yunanistan'ın millî standard kuruluşlarıdır.

TS EN 50600-3-1 : 2016 standardı, EN 50600-3-1:2016 standardı ile birebir aynı olup, Avrupa Standardizasyon Komitesi'nin (Avenue Marnix 17, B-1000 Brussels) izniyle basılmıştır.

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 50600-3-1

March 2016

ICS 35.020; 35.110; 35.160

English Version

Information technology - Data centre facilities and infrastructures - Part 3-1: Management and operational information

Technologie de l'information - Installation et infrastructures de centres de traitement de données - Partie 3-1: Informations de gestion et de fonctionnement

Informationstechnik - Einrichtungen und Infrastrukturen von Rechenzentren - Teil 3-1: Informationen für das Management und den Betrieb

This European Standard was approved by CENELEC on 2016-01-26. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN 50600-3-1:2016 E

Contents

Page

Figures

Tables

European foreword

This document (EN 50600-3-1:2016) has been prepared by CLC/TC 215 “Electrotechnical aspects of telecommunication equipment”.

The following dates are fixed:

• latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2017–01–26
• latest date by which the national standards conflicting with this document have to be withdrawn	(dow)	2019–01–26

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

This document has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association.

Introduction

The unrestricted access to internet-based information demanded by the information society has led to an exponential growth of both internet traffic and the volume of stored/retrieved data. Data centres are housing and supporting the information technology and network telecommunications equipment for data processing, data storage and data transport. They are required both by network operators (delivering those services to customer premises) and by enterprises within those customer premises.

Data centres need to provide modular, scalable and flexible facilities and infrastructures to easily accommodate the rapidly changing requirements of the market. In addition, energy consumption of data centres has become critical both from an environmental point of view (reduction of carbon footprint) and with respect to economic considerations (cost of energy) for the data centre operator.

The implementation of data centres varies in terms of:

a) purpose (enterprise, co-location, co-hosting, or network operator facilities);

b) security level;

c) physical size;

d) accommodation (mobile, temporary and permanent constructions).

The needs of data centres also vary in terms of availability of service, the provision of security and the objectives for energy efficiency. These needs and objectives influence the design of data centres in terms of building construction, power distribution, environmental control and physical security. Effective management and operational information is required to monitor achievement of the defined needs and objectives.

This series of European Standards specifies requirements and recommendations to support the various parties involved in the design, planning, procurement, integration, installation, operation and maintenance of facilities and infrastructures within data centres. These parties include:

1) owners, facility managers, ICT managers, project managers, main contractors;

2) architects, consultants, building designers and builders, system and installation designers;

3) facility and infrastructure integrators, suppliers of equipment;

4) installers, maintainers.

At the time of publication of this European Standard, the EN 50600 series currently comprises the following standards:

— EN 50600-1, *Information technology — Data centre facilities and infrastructures — Part 1: General concepts*;

— EN 50600-2-1, *Information technology — Data centre facilities and infrastructures — Part 2-1: Building construction*;

— EN 50600-2-2, *Information technology — Data centre facilities and infrastructures — Part 2-2: Power distribution*;

— EN 50600-2-3, *Information technology — Data centre facilities and infrastructures — Part 2-3: Environmental control*;

- — EN 50600-2-4, *Information technology — Data centre facilities and infrastructures — Part 2-4: Telecommunications cabling infrastructure*;
- — EN 50600-2-5, *Information technology — Data centre facilities and infrastructures — Part 2-5: Security systems*;
- — EN 50600-3-1, *Information technology — Data centre facilities and infrastructures — Part 3-1: Management and operational information*;
- — FprEN 50600-4-1, *Information technology — Data centre facilities and infrastructures — Part 4-1: Overview of and general requirements for key performance indicators*;
- — FprEN 50600-4-2, *Information technology — Data centre facilities and infrastructures — Part 4-2: Power Usage Effectiveness*;
- — FprEN 50600-4-3, *Information technology — Data centre facilities and infrastructures — Part 4-3: Renewable Energy Factor*;
- — CLC/TR 50600-99-1, *Information technology — Data centre facilities and infrastructures — Part 99-1: Recommended practices for energy management*.

The inter-relationship of the standards within the EN 50600 series is shown in Figure 1.

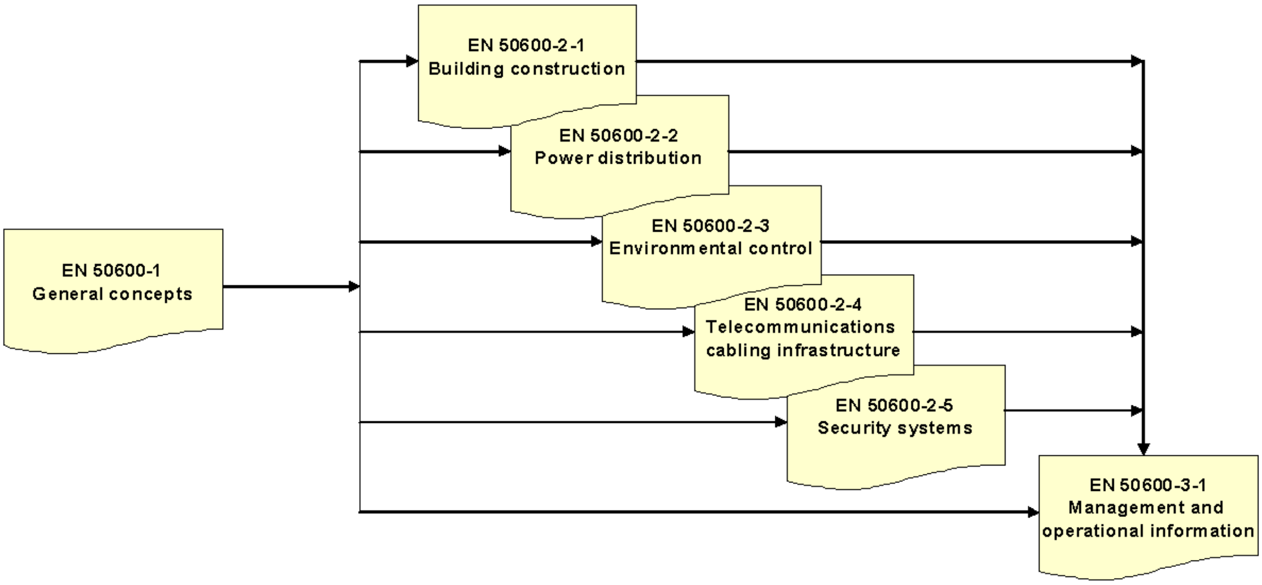

Figure 1 — Schematic relationship between the EN 50600 standards

EN 50600-2-X standards specify requirements and recommendations for particular facilities and infrastructures to support the relevant classification for “availability”, “physical security” and “energy efficiency enablement” selected from EN 50600-1.

EN 50600-3-X documents specify requirements and recommendations for data centre operations, processes and management.

This European Standard addresses the operational and management information (in accordance with the requirements of EN 50600-1). A data centre’s primary function typically is to house large quantities of computer and telecommunications hardware which affects the construction, operation, and physical security. Most of the data centres may impose special security requirements. Therefore, the planning of a data centre by the designer and the various engineering disciplines that will assist in the planning and implementation of the design of the data centre i.e. electrical, mechanical, security, etc. shall be carried out in cooperation with the IT and telecommunications personnel, network professionals, the facilities manager, the IT end users, and any other personnel involved.

This European Standard is intended for use by and collaboration between facility managers, ICT managers, and main contractors.

This series of European Standards does not address the selection of information technology and network telecommunications equipment, software and associated configuration issues.

1 Scope

This European Standard specifies processes for the management and operation of data centres. The primary focus of this standard is the operational processes necessary to deliver the expected level of resilience, availability, risk management, risk mitigation, capacity planning, security and energy efficiency.

The secondary focus is on management processes to align the actual and future demands of users. Figure 2 shows an overview of related processes.

The transition from planning and building to operation of a data centre is considered as part of the acceptance test process in Clause 6.

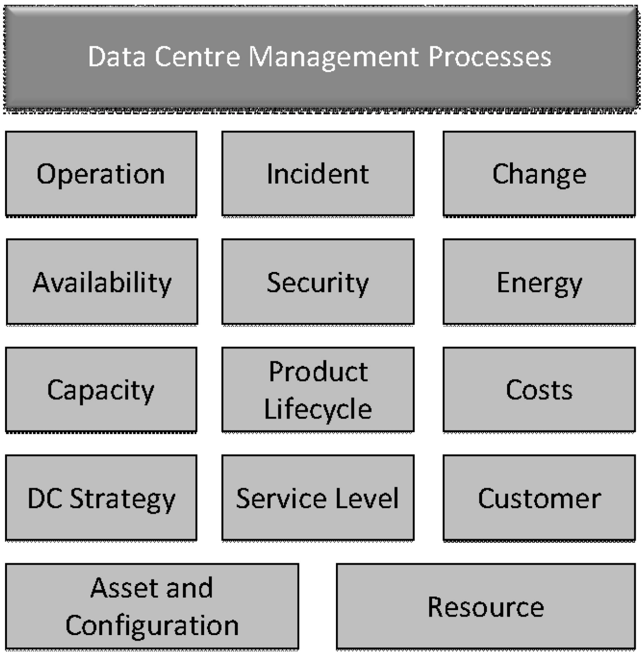

Figure 2 — Data centre management processes overview

NOTE 1 Only processes specific for data centres are in the scope of this document. Business processes like people management, financial management, etc. are out of scope.

NOTE 2 Specific skill sets are required of those working in and operating a data centre.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN 50600-1:2012, *Information technology — Data centre facilities and infrastructures — Part 1: General concepts*

EN 50600-2 (all parts), *Information technology — Data centre facilities and infrastructures*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in EN 50600-1, EN 50600-2-X and the following apply.

3.1.1
availability management
process for monitoring, analysis, reporting and improvement of availability

3.1.2
capacity Management
process for monitoring, analysis, reporting and improvement of capacity

3.1.3
change management
process for recording, coordination, approval and monitoring of all changes

3.1.4
configuration item
entity managed by configuration management

3.1.5
configuration management
process for logging and monitoring of configuration items

3.1.6
cost distribution model
model to distribute costs that cannot be directly related to an infrastructure item

3.1.7
cost management
process for monitoring, analysis and reporting of all infrastructure related costs

3.1.8
customer management
process for management of customers responsibilities

3.1.9
data centre strategy
process for alignment of actual data centre's capabilities and future demands of data centre's users and owners

3.1.10
energy management
process for monitoring, analysis, reporting and improvement of energy efficiency

3.1.11
incident management
process for responding to unplanned events and recovery of normal operation state

3.1.12
incident severity
incident category according to the four impact categories described EN 50600-1:2012, 4.3

3.1.13
key performance indicator
parameter used to evaluate performance

3.1.14
operations management
process for infrastructure maintenance, monitoring and event management

3.1.15
product lifecycle management
process for managing the timely renewal of infrastructure components and review of product lifecycle costs

3.1.16
provisioned capacity
capacity of the data centre’s actual installed infrastructure

3.1.17
security incident
unplanned event resulting in an actual or potential breach of security

3.1.18
security management
process for design and monitoring of security policies, analysis, reporting and improvement of security

3.1.19
service level management
process for monitoring, analysis and reporting of service level compliance

3.1.20
service level agreement
agreement defining the content and quality of the service to be delivered and the timescale in which it is to be delivered

3.1.21
total capacity
maximum capacity the data centre was designed for at full use in terms of e.g. space, power and cooling

3.1.22
used capacity
data centre’s actual capacity used by the IT and facility in terms of e.g. space, power and cooling

3.2 Abbreviations

For the purposes of this document, the abbreviations given in EN 50600-1 and the following apply:

CRAC	Computer Room Air Conditioning
CUE	Carbon Usage Effectiveness
EER	Energy Efficiency Ratio
ERE	Energy Re-use Efficiency
HVAC	Heating, Ventilation and Air Conditioning
IST	Integrated Systems Test
KPI	Key Performance Indicator

PUE	Power Usage Effectiveness[1]
pPUE	Partial Power Usage Effectiveness[1]
REF	Renewable Energy Factor
SLA	Service Level Agreement
TCO	Total Cost of Ownership
WRE	Water Re-use Effectiveness
WUE	Water Usage Effectiveness

4 Conformance

For a data centre to conform to this European Standard it shall have:

a) an implemented data centre strategy defined by stated business requirements;

b) an implemented set of service management policies and procedures covering the following:

   1) operations management;

   2) incident management;

   3) security management;

   4) customer management;

c) a monitored PUE KPI;

d) an asset management policy;

e) an environmental control policy;

f) a lifecycle management policy;

g) an energy management policy.

5 Operational information and parameters

5.1 General

In general, operators should understand the designed capacity and optimum operating parameters of the data centre. This is extremely important to maintain efficient operations and reliable service.

It is particularly important for the operators to understand the “N” design capacity to ensure that this is not exceeded. If the “N” design capacity is exceeded then some of the design redundancy will be lost which may effectively reduce the reliability class of the data centre.

At handover to operations instructions shall be delivered by designers and constructors on how to handle operational parameters of the infrastructure at different loads.

[1] It is recognized that the term “efficiency” should be employed for PUE but “effectiveness” provides continuity with earlier market recognition of the term.

At the beginning of data centre lifecycle IT loads will be low; therefore instructions for efficient part load operation are very important.

The following subclauses describe the information that operation retrieves from the various data centre subsystems of EN 50600-2-1 to EN 50600-2-5 together with operational parameters that shall be configured during the lifecycle of the data centre to achieve the goal to run at the optimal point for the given IT load.

5.2 Building construction as per EN 50600-2-1

All information delivered by the building management systems relating to any of the other subsystems in the building will be described in the relevant Subclauses 5.3 to 5.6.

The following information shall be handed over to operations:

a) maximum bearable load by construction;

b) escape routes;

c) technical: transmission heat/cooling;

d) documentation about installation for flood control;

e) regulatory requirements;

f) acoustic protection;

g) use of water-polluting substances (effluent water);

h) environmental regulations.

5.3 Power distribution as per EN 50600-2-2

5.3.1 General

To operate a data centre in a safe and efficient mode the following information is required at all metering points defined by the level of granularity:

a) active power load;

b) apparent power load;

c) power factor;

d) voltage;

e) current on each phase;

f) energy usage (consumption in kWh).

The following information shall be handed over to operations:

1) main power capacity;

2) back-up power source (e.g. generator);

3) power distribution capacities;

4) UPS capacity, battery capacity, modularity and efficiency at various IT loads;

5) resilience plan;

6) plan for protection from electrostatic discharge;

7) granularity level of energy efficiency enablement.

5.3.2 Generator parameters

The generator takes over after failure of the mains power supply. When the mains power supply returns a smooth power transition from the generator should be made. The procedure provides two parameters that need to be defined:

a) T1 – the time between the failure of the main supply and the start of the generator;

b) T2 – the time the generator shall run before switch off.

T1 should be large enough to prevent the generator from starting when it is not really needed. The UPS will keep the IT up and running for at least some minutes, but a safety period is needed in case the generator will fail to start and IT needs to be shut down. Also environmental conditions shall be kept under control to prevent overheating.

T2 should be large enough to ensure that the loading of the UPS batteries is on a level that enables a second failure of the mains power supply to be tolerated. In the worst case the second failure of mains power supply will happen immediately after the generator has switched off.

The ideal values of T1 and T2 will vary dependent on the capacity of the data centre and its current load. T1 and T2 shall be determined from the following:

1) IT load;

2) UPS capacity;

3) UPS battery re-charge/discharge times;

4) Expected rise of temperature after failure of the cooling;

5) Generator type and capacity.

Optimization of T1 an d T2 aims to protect the generator from bad working conditions, i.e. starting too early when not needed, not running long enough to securely handle consecutive failings of the mains power supply or running too long thus increasing fuel costs.

5.4 Environmental control as per EN 50600-2-3

5.4.1 General

For environmental control the basic measured parameters are temperature and humidity which need to be reported based on the level of granularity available. Some of the spaces can have additional environmental requirements such as control of the level of contaminants.

The following information shall be handed over to operations:

a) the cooling efficiency at various load conditions;

b) a document in which moisture control is detailed under various external environmental conditions (i.e. dry cold winters and hot humid summers);

c) example scenarios detailing the observable parameters which determine overall cooling efficiency and the interplay between those parameters, e.g. ventilator speeds, chilled water temperature, free cooling capabilities, IT heat load and IT airflow requirements. Metering should be in place to facilitate this process;

d) cooling capacity of each cooling component;

e) maximum cooling capacity of the computer room space;

f) maximum cooling capacity per cabinet.

5.4.2 Air handling parameters

With increasing IT load, computer rooms with access floor cooling require management of tiles with openings, pressure and cold water temperature at CRACs.

At low part load, openings are required at racks loaded with IT only. Low pressure will be sufficient to provide the necessary air flow and the cold water temperature can be higher as there is only little cooling capacity needed.

Operations shall be provided with an instruction set on how to adjust the cooling systems to match the heat load.

Where access floors are used for cooling this may include changing the open space in vented tiles, adding vented tiles to new equipment locations and removing them where equipment is removed.

Where CRAC units with variable speed fans are implemented this may include adjusting the fan speed to increase or reduce the volume of air provided for cooling.

Where chilled water cooling systems are implemented this may include varying the temperature of the cold water supply to match the cooling requirement.

The instructions should indicate whether redundant equipment such as CRAC units should be in service continuously or left in standby. The decision will normally depend on the relative efficiency of each operating mode.

5.4.3 Cooling parameters

In the situation where the cooling system utilizes a chilled water circuit, the chilled water feed temperature should be just low enough to provide sufficient cooling capacity, but otherwise as high as possible to minimize condensation on the heat exchanger resulting in a need for humidification. The higher feed temperature also expands the time in which the chilled water can be generated using a form of “free cooling”.

Operations will need an instruction set on how to handle cold water temperature at different conditions of heat load and outside air temperature. In addition, instructions may be needed to adjust power of pumps to the cooling demand.

5.4.4 Humidity parameters

Moisture control in the data centre should preferably be based on either dew point or absolute moisture content (g/m^3) measurements. Care should be taken that condensation will not occur anywhere near the IT equipment.

Operations will need an instruction set on how to set upper and lower limit of moisture to avoid unnecessary humidification and de-humidification.

5.5 Telecommunications cabling infrastructure as per EN 50600-2-4

There is no information expected from cabling infrastructure itself.

Automated infrastructure management systems offering real time documentation and efficient management of the physical layer should be considered for availability and operational purposes.

It is recommended to integrate the functionality of these systems into data centre management tools offering an overall infrastructure management.

5.6 Security systems as per EN 50600-2-5

For access control the necessary information should be delivery, visitor and employee records, access control systems, video records, and unauthorized entry and exit alarms. For additional information on access procedures see B.1.

For fire, the necessary information should be fire compartment penetration data (i.e. location and status of fire barriers) and all types of warning information being generated by the various detection systems, inspection records. A cause and effect algorithm shall be available which describes what happens at each stage of a fire or security event. For additional information on fire suppression procedures and maintenance of fire barriers see B.1.4 and B.2.

For other internal environmental events, the necessary information should be inspection records for leaks etc. For additional information on EMC directive procedures see B.3.

6 Acceptance test

6.1 General

Handover to operations are described as phase 11 of the design process in EN 50600-1. A critical aspect of this handover is acceptance testing to ensure that the constructed facility matches the original design intent.

There is a unique opportunity for extensive acceptance testing of the infrastructure prior to the first implementation of IT and the connected starting point of productive operation of a data centre. Cross domain tests can be carried out only during pre-production phase. All test results shall be documented.

It is strongly recommended to involve operational personnel in acceptance tests.

Documentation shall be provided by vendors and suppliers of infrastructure prior to start of tests.

No responsibility for “completed” construction areas should be undertaken by the site Operations Management without the formal acceptance of the area according to defined criteria. These should include the following:

a) a full commissioning programme has been successfully completed up to and including Integrated Systems Testing (IST) with all commissioning records fully updated;

b) all required training has been completed;

c) Operations Management should not undertake any management responsibility until they have satisfied themselves that the systems are working through acceptance testing and are able to be properly maintained;

d) Operations Management should have the opportunity to recruit and train staff well before live operations commence. Ideally the core staff should be present during commissioning;

e) the following documentation should be made available prior to handover into live operations:

1) up to date and accurate “As-Built” records and drawings including engineering single line diagrams;

2) a full set of Operations and Maintenance manuals, including Standard Operating Procedures, Maintenance Operating Procedures, Emergency Operating Procedures, escalation procedures etc.;

3) comprehensive commissioning records;

4) an up to date and accurate Asset Register;

5) a documented Planned Maintenance Schedule and a full set of maintenance records;

6) all documentation required for compliance with statutory regulation;

7) all documentation required for compliance with voluntary standards and certificates.

6.2 Building construction (EN 50600-2-1) tests

Escape routes should be checked to ensure that they are free of blockages.

The technological support of the escape routes e.g. emergency lights, escape routes pictograms, etc. shall be tested.

6.3 Power distribution (EN 50600-2-2) tests

Resilience tests require switching off parts of the infrastructure to prove fail safe operation as planned.

Testing of generators requires a significant time of operation of the generators to ensure bridging of failure of mains power supply for multiple hours.

UPS systems shall be on load when testing the generator as power factor at UPS input may have an impact on generator start-up conditions.

A procedure to return to mains power supply shall be described and tested.

An integrated test of the power system should be performed to ensure that the critical IT load remains functional throughout a simulated power outage. It is important that this test is performed in all permutations of the redundant system configurations and with a simulated IT load which matches the maximum design capacity. All tests shall be documented.

6.4 Environmental control (EN 50600-2-3) tests

An integrated test of the cooling system should be performed to ensure that the temperature and humidity in the computer room spaces remains within the design limits. It is important that this test is performed in all permutations of the redundant system configurations and with a simulated IT load which matches the maximum design capacity.

Part load operation tests shall be carried out to approve the operational instructions for HVAC and cooling configuration.

Testing humidity control will require adding and removing moisture from the air in the computer room, either by testing equipment or by using the CRACs, if more than one CRAC is available for this purpose.

In case of controlling contaminants testing is only possible if the contaminants can be removed without impact on the operational conditions.

6.5 Telecommunications cabling infrastructure (EN 50600-2-4) tests

Link and/or channel tests shall be carried out and documented to provide evidence that cabling is implemented as designed.

6.6 Security systems (EN 50600-2-5) tests

Security systems shall be tested according to the security concept. Make sure that multiple alarms are presented to security personnel in a way that:

a) enables them to easily identify the most important alarm;

b) workflow is presented to the personnel in clear instructions;

c) actions to be taken are acknowledged and documentation is enforced by the workflow.

There may be interaction between safety and security systems, such as in case of a fire, detection escape routes are released that are blocked in normal operation. Interactions like this are part of the safety concept and shall be tested and approved.

Tests shall be carried out and documented to ensure that each and every fire detector functions correctly and elicits the appropriate response from the fire alarm system, sounders, strobe lights, voice alarm systems and links to other systems. This shall be done by reference to the design specification and the cause and effect algorithm.

6.7 Energy efficiency enablement tests

For detailed and granular energy efficiency enablement, monitoring infrastructure shall be tested. All test results shall be documented.

6.8 Energy efficiency strategy tests

To achieve energy efficiency at any desired level, part load operation of all infrastructure subsystems shall be tested and approved. All test results shall be documented.

When testing environmental control systems (see 6.4) with simulated IT load, this load shall be subsequently reduced simulating part load operation. Check that operation of the systems according to the instructions leads to the desired energy efficiency.

6.9 Monitoring tests

During all tests of 6.2 to 6.8 accompanying monitoring tests shall be carried out to ensure event generation due to threshold and failure detection. All test results shall be documented.

7 Operational processes

7.1 General

The following processes are considered as operational processes:

a) Operations Management – infrastructure maintenance, monitoring and event management;

b) Incident Management – responding to unplanned events, recovery of normal operation state;

c) Change management – logging, coordination, approval and monitoring of all changes;

d) Configuration management – logging and monitoring of configuration items;

e) Capacity management – monitoring, analysis, reporting and improvement of capacity.

7.2 Operations management

7.2.1 Purpose

The aim of operations management is to keep the data centre at the status of normal operation. Maintenance of infrastructure is carried out according to the supplier’s maintenance plan. Monitoring is implemented for detection of actual status and failures, as well as to support management processes, e.g. energy management, lifecycle management, capacity management and availability management. Operational parameters are adjusted according to the instructions provided in the handover documentation referred to in Clause 6.

7.2.2 Activities

7.2.2.1 Maintenance

Operations management shall manage an overall maintenance plan for all infrastructure elements compliant to the instructions of the vendor. Consolidation shall be carried out to minimize downtimes of structures of resilience.

Information about scheduled and on-going maintenance shall be provided to incident management by operations management.

When necessary, information to the customer is provided by customer management.

7.2.2.2 Monitoring

Operations management has to implement a monitoring infrastructure to provide information about the status and failures of all data centre infrastructure elements. Additional data for use in management processes such as energy management, lifecycle management, capacity management and availability management is acquired by monitoring.

For larger data centres it is recommended to set-up a separate logical network for technical purposes for monitoring and controlling of infrastructure.

7.2.2.3 Event management

The exceptional status of an infrastructure element or the total infrastructure is handled as an event. Event management aims to define threshold values and maintain these after changes. During periods of maintenance events should be managed in a way that unnecessary alarms are suppressed.

Event management also aims to provide confirmation, consolidation and forwarding of events to other processes like Incident Management or energy management.

7.2.3 Base KPI

7.2.3.1 Mean time between failure (MTBF)

The aim of operations management is to maximize the time between failures.

EN 50600-1:2012, 4.3, describes four impact categories:

a) low: Loss of non-critical services;

b) medium: Failure of critical system components but no loss of redundancy;

c) high: Loss of critical system redundancy but no loss of service to clients;

d) critical: Loss of critical service to one or more clients or loss of life (which may be extended to address personal injury).

The KPI shall be reported for every impact category.

MTBF is a well-known KPI, but it requires a set of failures to be calculated. Before the second failure, it is not possible to determine a “time between failures”. Before the third failure, there is no concept of “mean”. Therefore it can be useful to report the actual time between failures, especially for the higher impact categories.

7.2.3.2 Number of incidents

Prevention of failures leads to less incidents. Therefore, the number of incidents is a KPI for operations management.

7.2.4 Advanced KPI

7.2.4.1 Availability

A failure can impact the availability of the data centre. The focus of operations management is to maintain availability. Therefore availability is an advanced KPI for operations management.

7.2.4.2 Unplanned replacement of infrastructure components

Maintenance as an activity in operations management aims to replace components under controlled conditions, i.e. scheduled, budgeted and approved. The need for unplanned replacement of infrastructure is a deviation from good maintenance. Therefore, unplanned replacement of infrastructure components is an advanced KPI for operations management.

7.3 Incident management

7.3.1 Purpose

The aim of Incident Management is removal of failures and recovery to normal operation state. Accidents should be handled as an incident category.

7.3.2 Activities

7.3.2.1 Removal of failures

Incident Management receives messages about failures from Event Management. Incidents are registered, monitored, solved and closed.

In addition, every incident is categorized with respect to the incident severity according to the four impact categories described EN 50600-1:2012, 4.3:

a) low: Loss of non-critical services;

b) medium: Failure of critical system components but no loss of redundancy;

c) high: Loss of critical system redundancy but no loss of service to clients;

d) critical: Loss of critical service to one or more clients or loss of life (which may be extended to address personal injury).

Incident logging registers the beginning and the end of every failure for the purpose of analysis in availability management.

Customer management provides information to the customer if necessary.

7.3.2.2 Recovery of normal operation

Incident Management ensures that all adverse effects of an incident are removed.

In case a change is needed to go back to normal operations the change will be registered for change management.

It is recommended to review each incident and the response to it and where possible changes made to prevent the incident from re-occurring and to improve the response should the incident be repeated

7.3.3 Base KPI: Mean time to repair (MTTR)

The aim of Incident Management is to minimize the time of outages.

The KPI MTTR shall be reported for every impact severity.

MTTR is a well-known KPI but it requires – as well as MTBF (see 7.2.3.1) – a set of failures to be calculated. Before the first failure, it is not possible to determine a “time to repair”. Before the second failure there is no concept of “mean”. Therefore it can be useful to report the actual time to repair, especially for the higher impact severities.

7.3.4 Advanced KPI: SLA compliance

Where a Service Level Agreement (SLA) is in place then compliance to the SLA is an advanced KPI for incident management.

7.4 Change management

7.4.1 Purpose

The aim of change management is recording, coordination, approval and monitoring of all changes.

7.4.2 Activities

7.4.2.1 Recording of changes

Processes like Incident Management, capacity management, energy management or availability management can register changes for the change management process. The creator of a change shall give a description of the change and the desired outcome.

7.4.2.2 Coordination

Changes shall be planned in order to enable proper coordination. Downtimes should be minimized by coordinating changes relating to the same system. Resources shall be made available to ensure that the change can be completed successfully.

Change management shall provide information about planned changes to operations management.

Customer management provides information to the customer whenever necessary.

7.4.2.3 Approval

An impact/risk analysis is required for every change to evaluate any associated risks and mitigate against them. A fall-back plan is necessary for changes that cannot be implemented successfully.

Changes shall be approved by a change manager or a change advisory board. Emergency changes are approved by the respective emergency board.

A change that is not approved can be re-worked to reduce the risk of failure or to improve fall-back capabilities.

7.4.2.4 Monitoring

All changes shall be monitored and the creator shall be informed about the status, especially when the change is implemented successfully.

The change shall be reviewed by the creator to analyze the desired effect. Change management supports other management processes with information about unwanted side-effects.

7.4.3 Base KPI: Complete change logging

The logging of changes shall be complete in order to avoid unapproved changes. Therefore, the completeness of change logging is a KPI for change management.

7.4.4 Advanced KPI

7.4.4.1 Unapproved changes

Changes shall be approved in order to ensure quality of changes and fall-backs. Therefore, the percentage of unapproved changes is an advanced KPI for change management.

7.4.4.2 Unsuccessful changes

The percentage of unsuccessful changes is an advanced KPI for change management.

7.5 Asset and configuration management

7.5.1 Purpose

The aim of asset and configuration management is recording and monitoring of all assets and their configurations (configuration items). It comprises identifying, recording, setting parameters and status monitoring of all relevant configuration Items including:

a) elements of infrastructure;

b) documentation;

c) software and applications for data centre management;

d) service level agreements.

7.5.2 Activities

7.5.2.1 Logging of configuration items

All configuration Items shall be discovered, recorded and maintained in a configuration management database.

NOTE Data Centre Infrastructure Management (DCIM) is a term used to describe a tool (or suite of tools) which record the configuration of items contained within the data centre. These tools are usually in the form of a configuration management database. Also other tools providing this functionality are available.

7.5.2.2 Provide configuration item information

All other processes rely on the information in the configuration management database. The information shall be presented to the processes in a way to support them best.

7.5.2.3 Status monitoring

Configuration management is responsible for keeping information in the configuration management database up-to-date. The actual status of a configuration Item is determined and compared to the database information. In case of deviations, the database is updated.

7.5.3 Base KPI

7.5.3.1 Completeness of configuration management database

Gaps in the configuration management database affect the effectiveness of all other data centre management processes. Therefore, the completeness of the configuration management database is a KPI for configuration management.

7.5.3.2 Timeliness and accuracy of configuration item status

Inaccurate configuration Item status data can lead to wrong decisions in the other data centre management processes. Therefore, the timeliness and accuracy of the configuration management database is a KPI for configuration management.

7.6 Capacity management

7.6.1 Purpose

7.6.1.1 General

Capacity management aims to optimize the usage of the data centre’s provisioned capacity. Therefore, it has to monitor, analyze, manage and report the capacity of the data centre’s infrastructure.

7.6.1.2 Categories of capacity

In data centre capacity management three categories of capacity shall be distinguished:

a) Total capacity: the maximum capacity that the infrastructure was designed for at full use;

b) Provisioned capacity: the capacity of the actual installed infrastructure;

c) Used capacity: the actual capacity used by the IT and facility.

There is a strong relation between the level of redundancy, the provisioned and the used capacity. Overloading the provisioned capacity leads to a loss of redundancy, but not necessarily to a failure. Loss of redundancy leads to an increase of risk of failure and affects the availability management process. This might be accepted as a part of the data centre’s strategy, but usually is an unwanted state of operation.

7.6.1.3 Time frames of capacity management

Due to very different lead times of different infrastructure elements analysis shall be conducted at three time frames:

a) short-term;

b) mid-term;

c) long-term.

On short-term all infrastructure components shall be managed that can be purchased and implemented within weeks, e.g. racks, open tiles for raised floors, cabling.

On mid-term all infrastructure components shall be managed that can be implemented within the concept of the actual design of the data centre, e.g. UPS modules, additional CRACs or other modular infrastructure elements.

To reduce energy consumption, especially under part load conditions, only enough infrastructure should be installed to provide sufficient capacity for the next 18 months. Additional infrastructure to bring the data centre to full capacity should be installed in time to meet the forecasted requirements. CLC/TR 50600-99-1 (currently being voted)[2] provides recommendations for improving the energy management (i.e. reduction of energy consumption and/or increases in energy efficiency) of data centres.

7.6.1.4 Levels of granularity

There are also different levels of granularity for data centre capacity management:

1) total data centre;

2) computer room;

3) infrastructure component;

4) rack/cabinet;

5) IT component.

For the process to be effective, a minimum monitoring level comprising data centre, computer rooms and infrastructure has to be chosen. This is comparable to energy efficiency enablement granularity level 2 (detailed – as defined in EN 50600-1).

For a granular capacity management the complexity can be extended to the rack/cabinet level and the IT component level.

7.6.2 Activities

7.6.2.1 Monitoring

The total capacity of the data centre is determined by its design. At handover of the data centre full details of the capacity limitations shall be provided to operations management.

Monitoring strategy shall be implemented to ensure that increased IT load does not cause the design capacity to be exceeded.

The capacity management process shall define which values should be compared with the design capacity e.g. actual or worst case peak power, peak current and minimum coefficient of performance (COP) of the cooling are important parameters.

[2] This Technical Report introduces the recommendations of the “EU Code of Conduct Best Practices for data centres” into the EN 50600 framework.

7.6.2.2 Analysis

For a short-term analysis (see 7.6.1.3) a forecast of expected rack/cabinet space needed versus the actual rack space in use is carried out for the next three months. New racks/cabinets can be provided within weeks as long as floor space is available.

For a mid-term analysis UPS usage and cooling usage are forecasted against the provisioned capacity for the next 18 months. It can require several months to acquire and install extensions for these infrastructure elements and short-term acquisition can lead to higher investment due to tight schedule.

A long-term analysis should be carried out for the next three years analyzing the limits of the following four dimensions of capacity that cannot be extended without a major redesign of the data centre:

a) Total rack/cabinet space;

b) Total electrical capacity;

c) Total cooling capacity;

d) Expected total weight load of an access floor (if applicable).

Hitting one of these limits may end the lifetime of the data centre requiring an early approach for a new data centre strategy.

7.6.2.3 Management

If the provisioned capacity falls below the expected capacity needs of the next 18 months, capacity management works out a plan for extending the capacity taking into account energy efficiency and operational safety requirements. Capacity management triggers product Lifecycle management (see 8.6) to buy new infrastructure when needed.

Capacity management registers changes to implement new infrastructure items when purchased by product lifecycle management. As there can be implications to energy efficiency, energy management has to be informed about those changes, too.

7.6.2.4 Reporting

Capacity management reports to data centre management the capacity in the three categories and the actual usage.

7.6.3 Base KPI: Balance of actual usage and capacity reserve

As capacity management aims to maximize the actual usage by keeping an acceptable capacity reserve for unexpected load, the percentage of capacity used divided by capacity available for each of the four dimensions (rack/cabinet space in use, electrical usage, cooling usage and weight load usage of the access floor) is a KPI for capacity management.

8 Management processes

8.1 General

The following processes are considered as management processes:

a) availability management – monitoring, analysis, reporting and improvement of availability;

b) security management – monitoring, analysis, reporting and improvement of security;

c) energy management – monitoring, analysis, reporting and improvement of energy efficiency;

d) product lifecycle management – management of the timely renewal of infrastructure and review of product lifecycle costs;

e) cost management – monitoring, analysis and reporting of all infrastructure related costs;

f) data centre strategy – alignment of actual capabilities and future demands of data centre users and owners;

g) service level management – monitoring, analysis and reporting of service level compliance;

h) customer management – management of customers and data centres responsibilities.

8.2 Availability management

8.2.1 Purpose

The aim of availability management is to ensure that the actual availability meets the desired availability. Infrastructure resilience pre-requisites are described in the four availability classes of EN 50600-1:2012, 6.2 and Table 1. Availability management is responsible for monitoring, analysis, reporting and improvement of the data centre’s availability.

8.2.2 Activities

8.2.2.1 Monitoring and analysis

Incidents leading to a failure of one or more IT components affect the availability of the data centre. Availability management records and analyzes incidents which lead to a reduction of the availability to determine the root cause, the responsible party and what, if anything can be done to prevent a re-occurrence. Any failures which are deemed to be caused due to the actions of a customer are reported to customer management. e.g. the failure of the customer to connect IT equipment to two redundant power feeds where they are available.

During maintenance and incident resolution the resilience of the data centre may be reduced. EN 50600-2-2 states that it can be assumed that during system maintenance or repair, unless specified by the client, a degraded level of resilience is permitted (see EN 50600-2-2:2014, 6.2.6.1). Availability management monitors these events and records the time needed to return to the desired availability. Availability management minimizes the risk of failures by minimizing the duration of operation at a degraded level of resilience.

8.2.2.2 Reporting of availability

Availability management is responsible to determine KPI associated to data centre’s availability.

a) mean time between failure;

b) mean time to repair;

c) availability;

d) loss of availability for which the data centre is responsible;

e) loss of availability for which the customer is responsible;

f) periods of reduced resilience per availability class.

8.2.2.3 Improvement

Availability management records the changes made to improve the availability. The effect of those changes is measured by improvements to the KPIs.

8.2.3 Base KPI: Availability accounted to data centre’s responsibility

Availability management aims to optimize the availability. Therefore, availability is a KPI for availability management.

To supplement this KPI information on whether loss of availability was the responsibility of the data centre or the customer may be recorded.

Availability values shall always be reported with the period of measurement.

8.2.4 Advanced KPI: Periods of reduced resilience

In periods of reduced resilience the risk of failure is higher than in normal operation. Availability management aims to minimize these times of reduced resilience. Therefore, “periods of reduced resilience” is an advanced KPI for availability management.

8.3 Security management

8.3.1 Purpose

The aim of security management is to ensure that security is not breached. Security systems are described in EN 50600-2-5. Security Management is responsible for creating, updating and issuing policies and procedures for monitoring, analysis, reporting and improvement of the data centres security. This includes threat and vulnerability analysis and access control policies and procedures.

8.3.2 Activities

8.3.2.1 Design and monitoring of security policies

Security management agrees with data centre management about the desired protection class. Security management is responsible to design security policies aligned to this protection class, to inform all staff about the policies and to monitor compliance.

8.3.2.2 Access control

All service personnel and visitors to the facility shall be registered and processed according to operational procedures, see B.1 for further information. Security management is responsible to organize registration and tracking of service personnel.

8.3.2.3 Assessment of threats and vulnerability

Security management is responsible for assessment of threats and vulnerability to enhance protection of the data centre and the data it contains. A risk assessment shall be done at regular intervals. It is recommended that this is carried out once a year as a minimum, or immediately as a result of the following events:

a) change in Threat to the data centre, or change in the National Threat level, where the data centre is located;

b) where major structural changes have occurred in the data centre;

c) where major technology changes have been implemented to systems supporting the data centre.

8.3.2.4 Reporting

Every security incident shall be recorded and reported to management. In addition perceived threats and vulnerabilities shall be assessed on a regular basis and reported to the data centre management.

8.3.2.5 Improvement

Security management records changes made to improve the protection. The effect of these changes is reported in the KPIs.

8.3.3 Base KPI: number of security incidents

Security management aims to protect the data centre and data against unauthorized access. Every breach of the protection and every breach of a security policy shall be registered as a security incident.

Security incident values shall always be reported with the period of registration.

8.4 Resource management

8.4.1 Purpose

Resource management aims to monitor, analyze, report and improve usage and re-use of resources of a data centre and to minimize environmental impact of data centre operation. Data centre management shall approve a policy for resource management to define which of the following resources are managed under the process:

a) electrical energy usage;

b) re-use of heat;

c) renewable energy;

d) carbon usage;

e) water usage and re-use;

f) IT equipment usage.

Management of electrical energy usage is a major task within resource management and is delegated to a separate energy management process (see 8.5).

8.4.2 Activities

8.4.2.1 Resource monitoring

Meter and sensor readings shall be collected for all resource monitors on a regular basis.

8.4.2.2 Resource accounting

All meter and sensor readings are validated and errors reported. Meter readings are transformed into resource usage. Aggregation of data are carried out and accounted to data centre sub-systems, if applicable.

8.4.2.3 Resource controlling

Resource usage is related to parameters like IT energy use or external temperature. KPI are calculated from conclusive data, unexpected deviations are reported.

8.4.2.4 Resource management

Resource controlling results are analyzed for improvement potential. Measures are derived and changes are registered to improve the resource efficiency. Effectiveness of measures is verified by KPI.

8.4.3 Base KPIs

8.4.3.1 Overview

KPI for resource management should be selected based on the resource management policy, for example:

a) ERE – Energy Re-use Efficiency;

b) REF – Renewable Energy Factor;

c) CUE – Carbon Usage Effectiveness;

d) WUE – Water Usage Effectiveness.

KPI for energy management are defined in 8.5.3.

8.4.3.2 Energy Re-use Efficiency (ERE)

Energy Re-use Efficiency is defined as:

$$ERE = \frac{E_{\text{DC}} - E_{\text{reuse}}}{E_{\text{IT}}} \tag{1}$$

where:

E_{DC} = total energy consumption of the data centre in kWh

E_{reuse} = re-used energy of the data centre in kWh

E_{IT} = energy consumption of IT equipment in kWh

There is a relationship between ERE and PUE (see 8.5.3.2.1). ERE accounts for energy re-use which is not included in a PUE calculation, i.e. where there is no energy re-use then ERE = PUE. The minimum value for ERE is 0 which corresponds to a total re-use of energy.

8.4.3.3 Renewable Energy Factor (REF)

Renewable Energy Factor is defined as:

$$REF = \frac{E_{\text{ren}}}{E_{\text{DC}}} \times 100\% \tag{2}$$

where:

E_{ren} = renewable energy owned and controlled by the data centre in kWh

E_{DC} = total energy consumption of the data centre in kWh

REF gives the percentage of renewable energy used by the data centre. The minimum is 0 % for no usage of renewable energy; the maximum is 100 % for a data centre using renewable energy only.

FprEN 50600-4-3 (currently submitted to voting) provides detailed requirements for the determination and reporting of REF.

8.4.3.4 Carbon Usage Effectiveness (CUE)

Carbon Usage Effectiveness is defined as:

$$CUE = PUE \times G_c \text{ in g/kWh} \tag{3}$$

where:

PUE = Power Usage Effectiveness (see 8.5.3.2.1)

G_{C} = carbon emission in g/kWh

Carbon emission per kWh can be read from the supplier’s bill and can vary due to the fraction of renewable energy and nuclear energy. Nuclear energy is defined as non-renewable, but free of carbon (and other greenhouse gases).

8.4.3.5 Water Usage Effectiveness (WUE)

Data centres using water for cooling processes should consider putting water under the policy of resource management, especially when cooling systems can use either water or electrical energy.

Water Usage Effectiveness is defined as:

$$WUE = \frac{W_{\mathrm{DC}}}{E_{\mathrm{IT}}} \text{ in m}^3\text{/kWh or l/kWh} \tag{4}$$

where:

W_{DC} = amount of water used in the data centre in m^3 or l

E_{IT} = energy consumption of IT equipment in kWh

Data centres returning the used water partially or totally in an unaltered state (except its temperature) to its origin should also use Water Re-Use Effectiveness, which is defined as:

$$WRE = \frac{W_{\mathrm{DC}} - W_{\mathrm{reuse}}}{E_{\mathrm{IT}}} \text{ in m}^3\text{/kWh or l/kWh} \tag{5}$$

where

W_{DC} = amount of water used in the data centre in m^3 or l

W_{reuse} = amount of water re-used in the data centre in m^3 or l

E_{IT} = energy consumption of IT equipment in kWh

Comparable to ERE, the minimum of WRE is 0 for total re-use; the maximum is WUE for non re-use.

8.5 Energy management

8.5.1 Purpose

Energy management aims to monitor, analyze, report and improve the energy efficiency of the data centre. For the process to be effective, at minimum energy efficiency enablement granularity level 2 (see EN 50600-1) shall be chosen in all areas.

NOTE An accompanying process energy management in IT does not exist in IT service management. Introduction of such a process would be very important, as the energy use of IT – as all other aspects concerning IT, too - is out of scope in this standard. A process energy management for IT is necessary to support the energy management process for data centres in a way to minimize the total energy use of a data centre. In addition, there are many relations between the features of IT components and the energy use of the facility to operate it. Without an energy management process for IT there is no process interface to address these issues.

At minimum, all data centres shall determine the KPI PUE (see 8.5.3.2.1 to comply with this standard.

8.5.2 Activities

8.5.2.1 Energy monitoring

Meter and sensor readings shall be collected for all monitors described in EN 50600-2-2 and EN 50600-2-3 on a regular basis.

8.5.2.2 Energy accounting

All meter and sensor readings are validated and errors reported. Energy meter readings are transformed into energy use. Aggregation of data are carried out and accounted to data centre sub-systems.

8.5.2.3 Energy controlling

Energy use is related to parameters like IT energy use or external temperature. KPI are calculated from conclusive data, unexpected deviations are reported.

8.5.2.4 Energy management

Energy controlling results are analyzed for improvement potential. Measures are derived and changes are registered to improve the energy efficiency. Effectiveness of measures is verified by KPI.

8.5.3 Base KPI

8.5.3.1 General

KPI for energy management are divided in two groups: general energy management KPI and specific KPI for data centres with access floor based environmental control.

8.5.3.2 General energy management KPI

8.5.3.2.1 Power Usage Efficiency (PUE)

Power Usage Efficiency is a widely accepted KPI and defined as:

$$PUE = \frac{E_{\mathrm{DC}}}{E_{\mathrm{IT}}} \qquad (6)$$

on an annual basis,

where:

E_{DC} = total energy consumption of the data centre in kWh

E_{IT} = energy consumption of IT equipment in kWh

NOTE 1 PUE is often named (technically incorrect) as Power Usage Effectiveness.

NOTE 2 FprEN 50600–4-2 (currently submitted to voting) provides detailed requirements for the determination and reporting of PUE and its derivatives.

8.5.3.2.2 Partial Power Usage Efficiency (pPUE)

Partial Power Usage Efficiency addresses the specific energy use of every data centre sub-system and is defined as:

$$pPUE_{\text{sub}} = \frac{E_{\text{sub}} + E_{\text{IT}}}{E_{\text{IT}}} \tag{7}$$

where:

E_{sub} = energy consumption of the sub-system in kWh

E_{IT} = energy consumption of IT equipment in kWh

Calculation of pPUEs allows analyzing the efficiency improvement potential of every sub-system. Therefore it is an important set of KPI for energy management.

8.5.3.3 Specific KPI: Partial Power Usage Efficiency for environmental control

Management of energy efficiency of access floor based environmental control is a complex activity. The pPUE for the environmental control sub-system is the relevant KPI:

a) to analyze the actual energy efficiency of this type of computer rooms;

b) to measure the effect of changes in air flow management.

A substantial improvement will decrease the pPUE value.

8.5.4 Advanced KPI

8.5.4.1 General

KPI for energy management are divided in two groups: general energy management KPI and specific KPI for a detailed analysis of computer rooms in data centres with access floor based environmental control.

8.5.4.2 General energy management KPI - Energy Efficiency Ratio (EER)

Energy Efficiency Ratio is a KPI specific for the energy use of cooling which is a major contributor to total energy use in most data centres. It is defined as:

$$EER = \frac{Q_{\text{removed}}}{E_{\text{cooling}}} \tag{8}$$

on an annual basis;

where:

Q_{removed} = total heat removed from data centre in kWh

E_{cooling} = total energy use of the cooling system in kWh

NOTE Additional KPI can be useful, e.g. for data centres with direct water cooling.

8.5.4.3 Specific KPI for data centres with access floor based environmental control

8.5.4.3.1 Bypass

Bypass is cold air not going through IT components and returning unused to the CRAC. Bypass is directly lowering the energy efficiency of the air flow, because too much air is moved and return air temperature is lowered. On the other hand, without enclosures bypass cannot be avoided. The calculation of the KPI is defined in the OpenDCME model (www.opendcme.org):

$$BP = \frac{T_{\text{ro}} - T_{\text{CRACi}}}{T_{\text{ro}} - T_{\text{CRACo}}} \tag{9}$$

where:

BP = bypass

T_{ro} = temperature at rack/cabinet outlet in °C

T_{CRACi} = temperature at CRAC inlet in °C

T_{CRACo} = temperature at CRAC outlet in °C

8.5.4.3.2 Recirculation

Recirculation is hot air returning to the IT component air inlet being used twice before returning to the CRAC. Recirculation is lowering the energy efficiency of the air flow indirectly by requiring a lower supply air temperature. The calculation of the KPI is defined in the OpenDCME model (www.opendcme.org):

$$RC = \frac{T_{\text{ri}} - T_{\text{CRACo}}}{T_{\text{ro}} - T_{\text{CRACo}}} \tag{10}$$

where

RC = re-circulation

T_{ri} = temperature at rack/cabinet inlet in °C

T_{ro} = temperature at rack/cabinet outlet in °C

T_{CRACo} = temperature at CRAC outlet in °C

8.5.4.3.3 Temperature spreading between hot and cold aisle

The energy efficiency of heat exchangers depends on the temperature difference between hot and cold air: the higher the difference, the higher the energy efficiency. Good air flow management will result in a high temperature difference, e.g. 16 K.

8.5.4.3.4 Supply air temperature

The energy efficiency of the cooling system depends on the temperature of supply and return water (or coolant fluid): the higher the temperatures, the higher the energy efficiency; especially for free cooling systems. Therefore, supply air temperature shall be as high as possible.

However, IT equipment with variable speed fans will increase the fan speed at higher temperatures resulting in higher energy consumption. The CRACs will use less energy, but the total energy use will rise. Therefore, the supply air temperature shall be set to the optimum point to minimize energy consumption.

8.5.4.3.5 Supply air humidity

Modern IT equipment allows operation in a wide range of humidity for supply air. A broad range is required for energy efficiency, because the energy intensive humidification and de-humidification process is avoided most of the year.

8.5.4.3.6 Pressure difference between hot and cold aisle

In computer rooms without enclosures a pressure difference between the access floor and the rack level is required to control the air volume of CRACs with frequency controlled fans. Building the pressure under the access floor requires energy from the CRAC. The lower this pressure difference is set, the higher the energy efficiency of the air flow will be.

For computer rooms with enclosures only a small pressure difference is required. It will build-up between hot and cold aisle where the racks and the IT components are located. The IT will drive the air flow through the rack and the CRACs only need to return the air to the cold aisle. A minimum over-pressure in the cold aisle is sufficient for operational safety to avoid recirculation through openings.

8.6 Product lifecycle management

8.6.1 Purpose

Product lifecycle management aims to purchase optimal infrastructure components and review product lifecycle costs. A Total Cost of Ownership (TCO) approach shall include energy costs as well as investment and maintenance costs. Requirements of operations concerning reliability, maintainability and integration into monitoring and event management shall also be considered. Decommissioning of infrastructure elements shall be based on actual TCO and according to disposal obligations.

8.6.2 Activities

8.6.2.1 Tender and purchase procedure

When new equipment is needed or existing equipment needs to be replaced product lifecycle management aims to select the best products for the data centre.

Besides costs for investment and maintenance which is typically a decision parameter, product lifecycle management shall estimate the expected costs for energy use of the new product. This requires an assumption about the expected load which will be delivered by capacity management. Several products, e.g. UPS´s can be operated in different modes with different energy efficiency. Product lifecycle management needs to make sure that the mode selected for TCO estimation is appropriate for later operation in the data centre.

Another important decision parameter is serving the operational needs. Reliability and maintainability are important to achieve the desired availability. Integration in monitoring and event management is important to avoid unnecessary complexity for these processes.

Product lifecycle management informs capacity management and operations management about the supply of new equipment or just operations management in case of supply for replacement.

8.6.2.2 Monitoring during lifetime

At time of tendering and purchase of an equipment item, product lifecycle management shall rely on the vendors´ specifications. Nevertheless, these specifications are based on laboratory measurements and there can be a significant deviation from the specification at operation in a real data centre. Therefore, product lifecycle management monitors the actual costs and operational properties of every equipment item during lifetime. Costs per item will be delivered by cost management (see 8.7).

Product lifecycle management without support of a cost management process is less effective, as it is missing the capability to review real costs against the estimations tenders were based on. In addition, deviation from the vendors´ specification will not be detected, thereby affecting energy efficiency.

8.6.2.3 Decommissioning

Product lifecycle management shall select those equipment items for decommissioning that are affecting optimal operations, either by its behaviour in monitoring and event management, or by its non-optimal maintenance or energy costs. Age of the equipment can be a parameter, too, as maintenance costs can rise at the end of the lifecycle, but it should not be the primary decision parameter.

8.6.3 Base KPI: Deviation from expected product properties

Every equipment item should have the expected properties. Product lifecycle management aims to select the best items based on these expectations, therefore it shall make sure that the expectations are met. Thus, deviation from expectation is a KPI for product lifecycle management.

For TCO there will be always a deviation due to uncertainty in operational load. This deviation should be within an acceptable range.

8.7 Cost management

8.7.1 Purpose

Cost management aims to monitor, analyze and account all infrastructure related costs to equipment items. Costs that are not directly related to an item shall be distributed by cost models. Cost management is responsible to develop and maintain comprehensible cost models.

8.7.2 Activities

8.7.2.1 Monitor and analyze costs

Typically book-keeping is responsible for monitoring all costs at an enterprise level. Data centre cost management receives from book-keeping that part of the total that is concerned with data centre infrastructure items. It validates all bookings and separates costs that can be directly related to items from those that cannot.

8.7.2.2 Develop and maintain cost distribution models

It is possible that costs do not directly relate to an infrastructure item, but clearly belong to the infrastructure costs. Therefore, a cost model to distribute the costs is needed, e.g. a maintenance fee for a data centre sub-system can be paid in advance at the beginning of the year independently from the actual amount of maintenance needed for the items of the sub-system. Cost management shall decide how to distribute these costs:

a) related to the invest for every item;

b) related to the actual maintenance carried out throughout the year;

c) related to the actual operation hours of every item (which can be different for resilient components);

d) according to a mixture of multiple relations.

Whatever the model will be, it should be comprehensive to product lifecycle management and data centre management. In models with multiple relations operations management shall be consulted to optimize the weighting of relations. Cost management is responsible for maintaining the distribution model and ensuring an appropriate distribution, e.g. a cost-by-cost model.

8.7.2.3 Account costs

All costs are accounted to infrastructure items to support product lifecycle management in calculation of the TCO.

Various cost metrics can be derived from accounted costs to assist in monitoring the performance of the data centre. The appropriate measures will be determined by the Management and may include:

a) cost per square meter of computer room;

b) cost per rack/cabinet;

c) cost per total IT power connected;

d) cost per IT energy used;

e) cost per network data volume;

f) cost per data stored;

g) cost for unused capacities.

8.7.3 Base KPI

8.7.3.1 Completeness of cost accounting

The value of cost management rises with the completeness of the accounting. Incomplete accounting can lead to wrong decisions in product lifecycle management. The KPI is defined as ratio of unaccounted costs to total costs.

8.7.3.2 Cost metrics

The delivery of cost metrics to data centre management is important to make costs more transparent. Therefore, capability to deliver cost metrics is a KPI for cost management.

8.8 Data centre strategy

8.8.1 Purpose

At the beginning of the initial planning of a data centre there is a clear idea of the owner about the needs the data centre shall serve. During the long lifetime of a data centre, the needs will change and thus the strategy of operation. Power density, cooling strategy and even the desired level of resilience can change during a data centre’s lifetime due to new technologies in IT and facility. Also the level of desired operational maturity (see Table A.2) can change according to the needs of users and owners.

Data centre strategy aims to align the actual capabilities and future demands of data centre’s users and owners. Actual capabilities are reflected in data centre’s implemented processes and KPI. Future demands can be derived from a business and IT strategy of the owners or the users. In addition, expectations for the data centre service market can give input to a strategy alignment. It can be quite a complex process of customer questionnaire and market observation to create a strategy based on valid assumptions.

8.8.2 Activities

8.8.2.1 Assess current capabilities

For every process implemented a set of KPI should be used to assess the quality of the process execution. Processes with poor performance shall be inspected for lack of resources, insufficient interaction with other processes or organizational resistance. Processes with lower management attention will always deliver lower results, so operational excellence shall be developed by raising attention to new processes while keeping high process quality at the existing processes.

8.8.2.2 Implement processes and KPI

As operational excellence maturity and resources allow, new processes can be implemented as a part of the Data Centre Strategy. The organization shall be able to follow the Data Centre Strategy to accept the value of the new processes; otherwise organizational resistance will be more likely than process quality.

For existing processes it can be useful to step forward from base KPI to advanced KPI for quality assessment. Once the process is implemented and delivers an acceptable quality, continuous improvement should be applied to develop the organization’s capabilities.

The implementation of each new strategy shall define the parameters and information to be passed between the different management processes and the KPI to be used.

8.8.2.3 Design a new strategy

To align the current and future capabilities, design of a new strategy can be necessary. The following items should be addressed:

a) is the resilience level adequate for the business needs?

b) are sufficient capacities provided for the expected power densities?

c) are there new technologies on the market that can support the strategy?

d) should new or additional customer segments be addressed with the data centre’s services?

e) are the services offered at competitive market cost levels?

Changes in requirements concerning availability or power density and improvements in energy efficiency can significantly impact the total capacity (see 7.6). Therefore, an adjustment of a data centre strategy should always consider these implications.

8.8.2.4 Sourcing strategy

Besides technical resources, data centre strategy has to develop a sourcing strategy for external suppliers. Personnel needs to be trained on those activities kept in the data centre’s organization. Relying on suppliers may in return require skills in project management and supplier management.

8.8.2.5 Strategy agreement

Once a new strategy is developed it needs to be agreed on with the owner. Impact of changes on budgets and operational cost should be analyzed as a preparation. After the formal agreement the new strategy has to be transferred into the organization in order to ensure compliance.

8.8.3 Base KPI: Actuality of agreed strategy

Alignment of strategies requires regular communication between data centre management and customers or owners. The time a strategy remains valid depends on the purpose of a data centre, e.g. whether it is an internal or external service provider. Alignment in frequent small steps can lead to lower investment costs, but requires more resources for strategy development. A period of validity between one to three years is recommended.

8.9 Service level management

8.9.1 Purpose

Service level management aims to ensure that the delivered service quality matches the agreed Service Level Agreement (SLA). Therefore, it shall monitor, analyze and report service level compliance. It is important to understand that the SLA can be between the data centre and an external customer or a customer internal to the same organization. It is recommended that in both cases the SLA is documented to avoid misunderstandings.

8.9.2 Activities

8.9.2.1 Monitor service quality

The service quality of a data centre can be monitored by a selection of KPI of the implemented processes: incident management, availability management, security management, energy management and cost management. The monitored service quality reflects the data centre’s capabilities towards the user. To know about these capabilities is a pre-requisite for formal agreements.

8.9.2.2 Service level agreement

A SLA can be written based upon information from monitoring systems. After approval of the data centre management, the SLA can be offered to customers (external or internal). The SLA shall then be communicated to the organization in order to ensure compliance. Where variations to the standard data centre SLA are agreed with customers the monitoring and KPIs shall be adjusted accordingly.

8.9.2.3 Report SLA compliance

Compliance of all SLAs shall be reported for internal purposes and also to customers. It is recommended that annual service level reviews are carried out to assess compliance with SLAs and determine any improvements which are necessary.

8.9.2.4 Analysis and improvement

Service level management is responsible to support the organization in SLA compliance. If the service quality is not sufficient for the planned or agreed on SLA, improvements need to be developed. Service level management registers changes to improve service quality and connected KPI, when applicable.

8.9.3 Base KPI: Discrepancy between service quality and SLA

Service level management aims to deliver the right service quality. A significant discrepancy between service quality and SLA shall be avoided – in both directions: too low service quality and too high service quality. Higher service quality than required normally leads to higher cost for infrastructure or organizational resources. Therefore, the discrepancy between service quality and SLA is a KPI for Service Level Management.

8.10 Customer management

8.10.1 General

Dependent on the purpose of a data centre and its security policies, there is a wide variety policy defining how the data centre manages its customers. Some restrict physical access to a minimum and others allow relatively free access.

It is also important to define the customer’s responsibilities in relation to safety, energy efficiency, capacity, connectivity and housekeeping to ensure that the customer understands the operational parameters of the data centre and works within them. For instance customers need to be aware of the following:

a) the availability of redundant power feeds and the benefit of connecting IT equipment with dual power supplies to both feeds;

b) the need to unpack equipment in dedicated areas outside the computer room to reduce the risk of fire and contamination;

c) the benefit of managing the cabling within their cabinets;

d) energy efficiency measures such as a hot and cold aisle configuration and the benefit of installing blanking panels between equipment.

There are many other issues to be considered which should be documented and presented to the customer as part of the agreement for providing data centre services.

Regular audits should be undertaken to ensure that agreed policies are being complied with.

8.10.2 Purpose

Customer management aims to develop a strategy for interaction with the customer and to manage customer’s and data centre’s responsibilities. It commits customers to contribute to the housekeeping, security and energy efficiency of the data centre and makes formal agreements about all communication paths.

8.10.3 Activities

8.10.3.1 Develop a strategy

The customer management strategy needs to be in line with the strategies for availability, security and energy efficiency. Policies have to be defined to separate the customer’s responsibilities from the data centre’s responsibilities. The policies shall be approved by Data Centre management and shall be communicated to the organization to ensure compliance.

8.10.3.2 Commitments on security and energy efficiency

Customer management informs the customers about their obligations concerning compliance to security policies. It supports the customer to contribute to the overall data centre energy efficiency by consulting on energy efficient IT components and measures in the computer room. With every customer a formal agreement about the acceptance of the policies shall be documented and a customer management commitment to the agreement is recommended.

8.10.3.3 Communications and escalations

Customer management shall be informed about all escalations in other processes. It should synchronize with service level management on the summary about communication issues prior to a service meeting. Customer management and service level management should conduct the meetings together whenever possible.

8.10.4 Base KPI: Policy compliance

There are several KPI determining the compliance of the customer’s duties and responsibilities dependent on the policies, e.g.:

a) number of failures due to power supply connection errors;

b) number of issues due wrong sided IT components into racks (hot and cold aisle mix-up);

c) number of IT components with insufficient energy efficiency features;

d) number of issues concerning cable management;

e) number of issues concerning fire loads.

8.10.5 Advanced KPI: Complaints about communication

Customer management aims to establish a good communication between data centre and customer. Non-working communication paths will lead to complaints, either from the customer or from the data centre’s organization. Therefore, the number of these complaints is an advanced KPI for customer management.

Annex A
(informative)

Example for process implementation

A.1 Prioritization of processes

Implementation of processes and KPI in an existing organization cannot be done in a single step. It is a process in itself and the result is a continuous improvement of the organizations maturity. Therefore, data centre strategy needs to define the prioritization of processes to be implemented and the KPI to control the processes.

The prioritization of processes depends on the business model and business requirements of a data centre.

Table A.1 shows an example for a prioritization of processes.

Table A.1 — Prioritization of processes

Priority 1	Priority 2	Priority 3
Operations management	Change management	Energy management
Incident management	Service level management	Configuration management
Security management	Capacity management	Cost management
Customer management	Availability management	Product lifecycle management

A.2 Maturity

Data centre managers wishing to position their organization with respect to its maturity will find an example of a maturity matrix with four levels in Table A.2.

Table A.2 — Operational levels

Elements of operational maturity	Operational levels			
	Level 1	Level 2	Level 3	Level 4
Control facilities and Infrastructures	low	medium	high	Very high

Design and definition
(Q = Quality plan,
A = Availability, S = Security,
F = Functionality,
E = Efficiency,
C = Certification program)
	A, S,	Q, A, S, F	Q, A, S, F, E,	Q, A, S, F, E, C

Planning	check of activities which are defined in the quality plan (Q, A)	spot-check of activities which are defined in the quality plan (Q, A,S)	regular control of activities which are defined in the quality plan (Q, A,S,E)	permanent control of all activities which are defined in the quality plan (Q, A,S,F,E,C)
Establishing of building and DC infrastructure				
Handover, approvals, putting into operation	functionality shall be checked before putting into operation	data centre function shall be checked. DC service technicians and operators shall be instructed.	Entire data centre function shall be checked by experts. DC service technicians and operators shall be very-well instructed.	Entire data centre function shall be checked and certified by experts. DC service technicians and operators shall be very well instructed.
Processes, monitoring, reporting, KPI (see NOTE)	Priority 1 processes with base KPI and determination of PUE	Priority 1 processes with advanced KPI + priority 2 processes with base KPI	Priority 1 processes with advanced KPI + priority 2 processes with advanced KPI + continuous improvement process	Level 3 + priority 3 processes with base KPI + certified continuous improvement process
Qualification of technical planning engineers	qualification process for personnel	qualification process for personnel and systems	continuous qualification process for components, systems, personnel and management	Certified continuous qualification process for components, systems, personnel and management
Qualification of installation company				
Qualification of vendor				
Qualification of operating company/personal				
Operation, control and management	Operational, control and management rules shall be carried out	Level 1 + improvement process for operation, control and management	Level 2 + continuous improvement process for operation, control and management.	Level 3 + certified continuous improvement process for operation, control and management

NOTE These levels correspond to the prioritization defined in A.1.

Annex B
(normative)

Security systems

B.1 Access to the data centre premises

B.1.1 Manned guarding

Manned guarding provides a visible deterrent on site, and provides expertise in physical protection processes, such as the management and handling of site visitors, and on-site security incidents. Manned guarding may be utilized in static positions, such as the security control room, or via the provision of random mobile patrols around site.

Guarding personnel should only have access to critical assets when subject to one or more of the following:

a) site operational procedures;

b) operational requirements;

c) ‘two man rule’ access.

Remote monitoring of alarm systems may also be used to control access to premises or rooms when the correct authentication is presented.

B.1.2 Employees and other authorized personnel

B.1.2.1 Requirements

A system of “due diligence” checks (see B.1.2.2) shall be considered for all employees in support of the mitigation of insider threats, i.e. authorized personnel performing unauthorized actions.

Guarding personnel shall be subject to more rigorous “due diligence” checks than those applied to other personnel.

In a situation where guarding personnel are managing access control systems, appropriate controls shall be in place to ensure that audit logs cannot be altered, tampered, or deleted, thus destroying evidential integrity. This integrity is generally required to support a potential criminal prosecution as a result of a security incident.

The access control system audit logs shall be inspected on a weekly/monthly basis by the internal security manager or site security manager.

B.1.2.2 Recommendations

In the absence of national or local regulations addressing “due diligence” check the following should be considered as a non-exhaustive list:

a) verification of identity which should include some form of nationally recognized identity card with photographic information (e.g. passport, driving licence);

b) verification of address (e.g. by the provision of utility bills);

c) a legal right to work;

d) verification of academic and professional qualifications;

e) verification of submitted Curriculum Vitae (positive checking of previous employment references and educational qualifications for a minimum period of five years);

f) relevant checks of criminal records;

g) additional checks, including financial history, where the employee or authorized person is expected to have access to sensitive or critical data assets.

The need for random searching of employees and other authorized personnel should be considered.

B.1.3 Visitors

B.1.3.1 Requirements

Suitable operational processes shall be in place to accommodate the management and ‘handling’ of visitors to the data centre.

Mechanisms shall be in place whereby requests for access are lodged with an appropriate entity, for example the security manager, or on-site guarding personnel where present.

Visitors shall be informed of the requirement to present suitable credentials to act as verification of identity, prior to gaining access. The credentials shall contain some form of photographic identification, for example:

a) national Identity card where applicable;

b) driving licence when supported by photographic identification;

c) passport.

Local procedures may identify other suitable photographic identity documents.

On verification of identity and visit authorization, visitors shall be issued with a pass, clearly identifying them (by means of colour or similar) as visitors. This pass shall be worn and be visible at all times.

Access to data centre spaces of a given Protection Class (in accordance with EN 50600-2-5) shall only be granted once visitors/personnel have completed the data centre site booking in and registration process. Where their security clearance status is unknown, access may be granted subject to the following:

d) authorized personnel or visitors escorted at all times by appropriate security personnel;

e) authorized personnel or visitors escorted by appropriate personnel with security clearance;

f) personnel or visitors who have previously obtained and retain their verified security clearance having unescorted access as directed by local policy.

Static or mobile patrol guarding services service shall comply with a recognized industry standard.

Initial security checks on visitors and validation of their visit shall be undertaken:

1) upon entrance to the building, at the boundary between Protection Class 1 and 2 for data centre premises without external barriers;

2) upon entrance to the area of Protection Class 1 for data centre premises with external barriers.

Access from an area of one Protection Class to another and to spaces within the same Protection Class shall be controlled, and access granted to authorized personnel only, based on the ‘need to know’ requirement.

B.1.3.2 Recommendations

Dependent upon the access mechanisms in place within the data centre, visitor badges may be clearly differentiated (by means of colour or similar) to permit limited access to approved communal areas, or the specific space associated with a particular customer the visitor is representing.

Dependent upon locally agreed protocols, visitor access may be escorted or unescorted. In situations requiring a high degree of security provenance, unescorted access would only be granted once appropriate checks had been made in relation to security clearance(s) and the principle of ‘need to know’.

To support and facilitate the movement of visitors through the facility, a ‘white list’ should be created. The “white list” will be managed by the security manager of the data centre, or by authorized guarding personnel as appropriate.

The need for random searching of visitors should be considered.

B.1.4 Deliveries

B.1.4.1 Requirements

The physical protection processes, procedures and building construction shall be appropriate to the assets that they are protecting. This would include the data assets requiring protection, as well as the infrastructure that supports the operation of the data centre.

To accommodate deliveries in data centres requiring high levels of security control, additional operational controls shall be employed to support the delivery process. This includes, but is not limited to:

a) searching of vehicles prior to access to the loading bay;

b) prior booking of delivery and issue of unique visitor reference;

c) supervision of the loading/unloading operations by appropriate personnel;

d) monitoring of the above by video surveillance systems (see EN 50600-2-5 for further details).

The nature and extent of these controls shall be determined by an appropriate risk assessment, or provision of operational requirements from the entity whose data are being hosted.

B.1.4.2 Recommendations

Appropriate supervision of the delivery process should be supported by security cleared personnel, or on-site guarding personnel.

A documented procedure should be created in relation to the management and handling of deliveries accounting for the operational security controls implemented in B.1.4.1.

Where regular deliveries are received from a supplier, consideration should be given to creating an appropriate ‘white list’ for delivery personnel to support timely unloading of the delivery. Pre-screening of delivery personnel will support the unloading operations.

The operational procedure should be distributed to personnel responsible for the management and handling of deliveries.

Dependent upon locally agreed procedures, an appropriate notice period may be required prior to the delivery detailing:

a) drivers details;

b) load contents;

c) any access requirements necessary for unloading.

Subject to agreed local protocols, an escalation process should be agreed to accommodate emergency deliveries that fall outside of standard protocols.

B.1.5 Physical protection of deliveries

B.1.5.1 Requirements

Not applicable.

B.1.5.2 Recommendations

Premises containing data centre spaces should have an external barrier which acts as the boundary of Protection Class 1 as described in EN 50600-2-5. The need for such a barrier increases as the required degree of security increases.

B.2 Fire suppression systems

Where a gaseous extinguishing system (see EN 50600-2-5) is used, a periodic review (at intervals of no greater than 12 months) shall be undertaken to determine whether boundary penetration or other changes to the protected space have occurred that affects leakage and extinguishant concentration/performance – and which would affect the fire performance of the space.

If such a review

a) cannot be achieved using visual inspection, it shall be established by undertaking seal integrity tests and comparing the result with the design/original performance assessment;

b) indicates a change to the type of hazard within the protected space, an increase in protected volume or any leakage that would result in an inability to retain the extinguishant for the required period, remedial action shall be carried out (which may require the system to be redesigned to provide the original degree of protection).

In order to facilitate functional testing, it shall be possible to activate the system without disruption of the operation of the data centre space within which it is installed.

It is recommended that the type of hazard within the space, and the volume it occupies, be regularly checked to ensure that the required concentration of extinguishant can be achieved and maintained.

Functional testing shall be possible anytime. If operating resource cannot be turned off during operation, the gas extinguishing system shall have an operating device (preferable a key switch) with which the automatic turn-off function of operating resource, e.g. IT accessories or ventilation, may be rendered inoperable. The operating status shall be clearly marked on a separate display and at a location that is continuously manned.

Personnel working in the electronic equipment area should be trained in the safe use of all available fire-fighting equipment.

Only authorized persons shall be able:

1) to shut down the operation of the data centre space;

2) re-start ventilation;

3) re-start any disabled equipment.

B.3 Management of electrical interference

Procedures shall be in place to control the use of devices that are not required to conform to the EMC Directive (e.g. mobile telephones).

Bibliography

FprEN 50600-4-1[3], *Information technology — Data centre facilities and infrastructures — Part 4-1: Overview of and general requirements for key performance indicators*

FprEN 50600-4-2[3], *Information technology — Data centre facilities and infrastructures — Part 4-2: Power Usage Effectiveness*

FprEN 50600-4-3[3], *Information technology — Data centre facilities and infrastructures — Part 4-3: Renewable Energy Factor*

CLC/TR 50600-99-1, *Information technology — Data centre facilities and infrastructures — Part 99-1: Recommended practices for energy management*

[3] Currently being voted.